The Number Irreducible Constituents Permutation Representation of $G$

B. Razzaghmaneshi

Department of Mathematics and Computer science Islamic Azad University Talesh Branch, Talesh, Iran

Corresponding author: B Razzaghmaneshi

ABSTRACT: Let $D_i, \ldots, D_r$ be the different irreducible constituents of the permutation representation $G^*$ of $G$. In addition let $f_i$ be the degree of $D_i (i = 1, \ldots, r)$ and let $\chi_i = Tr(D_i)$ be the character of $D_i$. Let the numbering be chosen so that $D_1$ is the identity representation. Then number the irreducible constituents $D_i$ of $G^*$ such that $f = p$ and the representations $D_3, \ldots, D_r$ are conjugate. In particular $f_3 = \ldots = f_r = f$, and $f$ divides $p-1$.

Keywords: permutation representation, orbits, irreducible constituents.

INTRODUCTION

In 1943, R. Brauer studied about permutation groups and find the permutation groups of prime degree and related classes of Groups (See (4)). From years 1906 to 1936. W.A.Manning studied about primitive groups and finding the primitive groups of classes six, ten, twelve and fifteen. And in 1906, W.Burnside introduced and researched the about transitive groups, of prime degree (See (2)), and in 1921, he worked about the certain simply-transitive permutation group and obtained a beautiful consequence (See (3)). (See (11),(12),(13),(14),(15),(16),(17) and (18)). In 1937 J.S. Frame determined the degrees of the irreducible components of simply transitive permutation groups, and in 1941, he obtained the double cosets of a finite groups (See (5) and (6)). And also in 1952, he finding the irreducible representation extracted from two permutation groups (See (7)). G.A.Miller (1897 & 1915), (See (19) & (20)), E.T.Parker (1954), (See (21)), M. Suzuki (1962), (See (23)), J.G.Thompson (1959), (See (24)), M.J.Weiss (1928), (See (25) & (26)), H.Wielandt (1935 & 1956) (See (27) & (28)) and H.Zassenhaus (1935), (See (30)) are studied about transitive and primitive groups and their obtaind the beautiful and more consequence. Now in this paper we will prove number the irreducible constituents $D_i$ of $G^*$ such that $f = p$ and the representations $D_3, \ldots, D_r$ are conjugate. In particular $f_3 = \ldots = f_r = f$, and $f$ divides $p-1$.

2. Preliminares

In this chapter we study the notations, elementary properties, lemmas and theorems, whose we will used in chapter 3.

2.1. Elementary notions and definitions

Let $\Omega$ be a finite set of arbitrary elements which for natural numbers $1,2,\ldots,n$ as the points and $\Delta$ subset of $\Omega$. Then a permutation on $\Omega$ is a one-to-one mapping of $\Omega$ onto itself. We denote the image of the point $\alpha \in \Omega$ under the permutation $p$ by $\alpha^p$. We write $p = \begin{pmatrix} 1 & 2 & \ldots & n \\ p_1 & p_2 & \ldots & p_n \end{pmatrix}$. We define the product $pq$ of two permutations $p$ and $q$ on $\Omega$ by the formula $\alpha^{pq} = (\alpha^p)^q$. trivially $pq$ is again a permutation on $\Omega$.
With respect to the operation above, all the permutations on $\Omega$ form a group, the symmetric group $S^\Omega$. Let $G$ be a permutation group on $\Omega$, in short $G \leq S^\Omega$. We say that a set $A \subseteq \Omega$ is a fixed block of $G$ or is fixed by $G$ if $A = A^G$. Then each $g \in G$ induces a permutation on $\Delta$ which we denote by $g^\Delta$. We call the totality of $g^\Delta$'s formed for all $g \in G$ the constituent $G^\Delta$ of $G$ on $\Delta$ (for example $G = G^\Delta$). $G^\Delta$ is a permutation group on $\Delta$. Obviously the mapping $g \rightarrow g^\Delta$ is a homomorphism: $G \rightarrow G^\Delta$. If this mapping is an isomorphism, that is, $|G^\Delta| = |G|$, then the constituents $G^\Delta$ is called faithful. Every group $G$ on $\Omega$ is formed for all $n$ variables. We call the totality of $n$ variables the reducible representations appearing in $G^r$. In particular, the group of all matrices $g^*$ with $g \in G$ can be regarded in the following way as a linear substitution in $\vert \Omega \vert = n$ variables. The variables $X_1, \ldots, X_n$ are taken as points. We form column vectors corresponding to the linear transformation $x \rightarrow g^* x$, where $g^* = \delta_{\alpha \beta} \begin{pmatrix} 1 & \alpha = \beta \\ 0 & \alpha \neq \beta \end{pmatrix}$ is the well-known Kronecker symbol. We call $g^*$ the permutation matrix corresponding to $g$. Such a matrix contains exactly one 1 in each row and column and zeros everywhere else. In addition, every permutation matrix $g^*$ is orthogonal, i.e., the transpose $g^{*t}$ of $g^*$ is identical with its inverse: $g^* g^{*t} = \delta_{\alpha \beta} \begin{pmatrix} 1 & \alpha = \beta \\ 0 & \alpha \neq \beta \end{pmatrix}$, we obtain a faithful representation of $S^\Omega$ by $g \rightarrow g^*$. Now let $G \leq S^\Omega$. By $G^*$ we denote the group of all matrices $g^*$ with $g \in G$. Obviously $G^*$ is isomorphic to $G$. We call $G^*$ the permutation representation of $G$.

2.2. Theorem

(See (22)). If a transitive permutation group $G$ is regarded as a matrix group $G^*$, then the matrices which commute with all the matrices of $G^*$ form a ring $V = V(G)$. We call $V$ “the centralizer ring corresponding to $G$”. $V$ is a vector space over the complex number field which has the matrices corresponding to the orbits $\Delta$ of $G_1$ as a linear basis. In particular, the dimension of $V$ coincides with the number $k$ of orbits of $G_1$.

Proof

See (29), Theorem 28.4)

Let $D_1, \ldots, D_r$ be the different irreducible representations appearing in $G^*$ where $D_1$ is the identity representation. In the following we always denote by $f_i$ the degree of $D_i$ ($i = 1, \ldots, r$), and by $e_i$ the multiplicity of $D_i$ in $G^*$. In particular, $\sum e_i f_i = n$ we have $e_1 = f_1 = 1$ and $e_2 \leq \ldots \leq e_r$, the reduction of $G^*$ gives for an appropriately chosen unitary $n \times n$ matrix $U$:

$$U^{-1} G^* U = \begin{bmatrix} D_1, D_2, \ldots, D_2, \ldots, D_n, \ldots, D_n \end{bmatrix}.$$ 

2.3. Proposition

Let $M$ be the $n \times n$ matrix whose elements are all 1. then $\sum B(\Delta) = M$. (Here the summation is over all orbits of $G_i$)

Proof

See (29), proposition 28.2).
2.4. Theorem
V is commutative if and only if all the $e_i=1$.

Proof
See ((29) , Theorem 29.3)

2.5. Theorem (29.8)
V is commutative if and only if the class matrices

$$E_i = \sum_{g \in C_i} g^*$$

(i = 1,...,n) whose $C_i$ be the ith class of conjugate elements of G, generate V, i.e., when each $B \in V$ has a (not necessarily unique ) representation $B = \sum_{i=1}^{r} z_i E_i$.

Proof
See ((29), Theorem 29.8)

2.6. Theorem
$$Tr(B(\Gamma) f(\Delta)) = \begin{cases} o & \text{if } \Gamma \neq \Delta \\ \Gamma | n & \text{if } \Gamma = \Delta \end{cases}$$

Let $\Gamma$ and $\Delta$ be two orbits of $G_1$, then

Proof
See ((29), Theorem 28.10)

2.7. Definition
By a Burnside-group (in short : B-group) we mean an abstract finite group $H$ with the property that every primitive group containing the regular representation of $H$ as a transitive subgroup is doubly transitive. (See (28), p.343).

2.8. Theorem
(See (27)). Every cyclic group of composite order is a B-group.

Proof
See ((29), Theorem 25.3)

2.9. Theorem
(See (10)): $G$ is doubly transitive. If in addition $G_{\Delta}$ is primitive on $\Gamma$, then $G$ is even doubly primitive (Jordan theorem).

Proof
See ((29), Theorem 13.1)

2.10. Definition
A permutation group $G$ on $\Omega$ is called semiregular if, for each $\alpha \in \Omega$, $G_{\alpha} = \{1\}$; and $G$ is called regular if it is semiregular and transitive. Accordingly, every regular group is also semiregular and subgroups as well as constituents of semiregular groups are semiregular. In the case of semiregular groups, the degree and minimal degree coincide.

2.11. Proposition
The order of a semiregular group is a divisor of its degree. A transitive group is regular if and only if its order and degree are equal.

Proof
See ((29), Proposition 4.2)
2.12. Theorem
Every normal subgroup \( \neq 1 \) of a primitive group is transitive.

Proof
See ((29), Theorem 8.8)

2.13. Theorem
The representation module associated with \( G^* \) contains a one-dimensional invariant subspace corresponding to

\[
\begin{bmatrix}
1 \\
\vdots \\
1
\end{bmatrix}
\]

the identity representation, namely, the one generated by \( e_j \), and because of the transitivity of \( G \) it contains no others. The identical representation therefore appears in \( G^* \) with multiplicity exactly 1.

Proof
See ((29)), theorem 29.1

2.14. Theorem
\( G \) is doubly transitive if and only if \( \dim V(G) = 2 \). In this case \( G^* \) has exactly two irreducible constituents. In particular, we have \( r = k \) and \( V(G) \) commutative.

Proof
See((29), Theorem 29.9)

2.15. Theorem
(See (1), p.341). Every nonsolvable transitive group of prime degree is doubly transitive.

Proof
See ((29), Theorem 11.7 and (1), p. 341)

2.16. Proposition
Every abelian group \( G \) transitive on \( \Omega \) is regular. \( G \) is its own centralizer in \( S^\Omega \).

Proof
See ((29), Proposition 4.4)

2.17. Proposition
If \( G \) is primitive on \( \Omega \) and \( \alpha \) and \( \beta \) are different points of \( \Omega \), Then either \( G_{\alpha} \neq G_{\beta} \) or \( G \) is a regular group of prime degree.

Proof
See ( (29), Proposition 8.6)

2.18. Theorem
Let \( G \) be transitive on \( \Omega \), \( |G| \) not a prime number, \( \alpha \in \Omega, \beta \in \Omega, \alpha \neq \beta \). Let \( G \) have a subgroup \( H \) intransitive on \( \Omega \) with the properties \( \beta^G_\alpha \subseteq \beta^H \) and \( |\beta^H| \leq |\alpha^H| \). Then \( G \) is imprimitive and \( |\beta^H| = |\alpha^H| \).

Proof
See ((29), Theorem 27.5).

2.19. Theorem
Paired orbits have the same length.
2.20. Definition

Let $G$ be transitive and consider the orbits of $G$. With each of these orbits $\Delta$ (including the trivial $\Delta = \{ 1 \}$) we associate in the following way a matrix $B(\Delta) = (v_{\alpha,\beta})$, $\alpha, \beta = 1, \ldots, n$, with elements:

$$v_{\alpha,\beta} = \begin{cases} 1, & \text{if there exists } g \in G \text{ and } \delta \in \Delta \text{ with } 1^g = \beta \text{ and } \delta^g = \alpha. \\ 0, & \text{otherwise} \end{cases}$$

Thus, in the first column of $B(\Delta)$ we have exactly those $v_{\alpha,\beta} = 1$ for which $\alpha \in \Delta$ holds. If $\Gamma \neq \Delta$, the ones of $B(\Gamma)$ and $B(\Delta)$ do not occur in the same place. On the other hand, for each place $(\alpha, \beta)$ there is an orbit $\Delta$ of $G$, (namely, the one in which the $\alpha$-th element of $\Delta$ lies) such that $B(\Delta)$ has 1 in this position.

2.21. Theorem

The matrices corresponding by definition 2.18 to paired orbits of $G$ are transposes: $B(\Delta') = (B(\Delta))^t$.

Proof

See ([29], Theorem 16.3).

2.22. Theorem

If $G_\alpha$ has an orbit $\Gamma$ with $|\Gamma| = 2$, then $G$ contains a regular normal subgroup $R$ of index 2. $G$ is a Frobenius group.

Proof

See ([29], Theorem 18.7)

2.23. Theorem

(A) If the irreducible constituents of $G^*$ are all different, i.e., if all the multiplicities $e_i = 1$, then the rational number

$$q = n^{-2} \prod_{i=1}^{k} \frac{n_i}{f_i}$$

is an integer.

(B) If in addition the $k$ numbers $n_i$ are all different, then $q$ is a square.

(C) If the irreducible constituents of $G^*$ all have rational characters, then $q$ is a square. The hypothesis is always fulfilled if the degrees $f_i$ are all different.

Proof of 2.23. (A)

It suffices to show that $q$ is an algebraic integer. The notation of the preceding section is continued. Let $U$ again be the unitary transformation matrix introduced in §2. From the hypothesis $e_i = 1$ it follows that every matrix $M = U^{-1}B(U)$ with $B \in V$ has diagonal form. Because $B_i = B(\Delta_i) \in V(G)$, we have in particular

$$M_i = U^{-1}B(U) = [w_{1i}, w_{2i}, \ldots, w_{ki}]$$

which $\frac{1}{f_i} I$ is the $f_i$ by $f_i$ identity matrix.

Let $w_i$ be the diagonal elements of the matrix $M = U^{-1}B(U)$ for arbitrary $B \in V$. We put

$$B = \sum_{i} z_i B_i, \quad z = \begin{pmatrix} z_1 \\ \vdots \\ z_k \end{pmatrix}, \quad w = \begin{pmatrix} w_1 \\ \vdots \\ w_k \end{pmatrix}$$
\(N = \{1, n_2, \ldots, n_k\}, \quad F = \{f_1, f_2, \ldots, f_k\}\), and \(I = (w_{ij})\); \(i, j = 1, \ldots, k\). From \(M = U^{-1}BU\) it follows that \( \overline{MM} = U^{-1}B'BU\), since \(U\) was assumed unitary. With the aid of 2.4 we now obtain
\[
z'Nn = \sum_{i=1}^{k} z_i z_j n_{ij} = \sum_{i, j} z_i z_j \text{Tr}(B_i B_j') = \text{Tr}(B'B) = \text{Tr}(\overline{MM}) = \sum_{i} \overline{w}_i w_j f_i = \overline{w}' f w.
\]

Because of this, we have \(Nn = \overline{I}I\). By taking the determinant
\[
n^k \prod_{i} n_i = |Nn| = |F| |\overline{I}I| = \prod_{i} f_i |\overline{I}I| = |I|.
\]
we get
\[
\text{The } w_{ij}, \text{ as eigenvalues of the matrix } B_i \text{ which has integer coefficients, are algebraic integers, and therefore } |I| \text{ and } |\overline{I}I| \text{ are also algebraic integers.}
\]

We wish to show that \(|I|\) is divisible by \(n\). By 2.3, \(\sum_j B_j = M\) where \(M\) is the \(n \times n\) matrix consisting of \(n\) ones. \(M\) has the eigenvalue \(n\) occurring with multiplicity 1 belonging to the eigenvector \(\begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}\). Its remaining eigenvalues are 0. In the diagonal matrix \(\sum_j M_j, n\) therefore appears exactly once, the remaining elements being 0. Therefore \(\sum_j w_{ij} = n\) for \(i=1\) and \(=0\) for the remaining. This implies
\[
|I| = \begin{vmatrix} n & w_{j2} & \cdots & w_{jk} \\ 0 & w_{22} & \cdots & w_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & w_{k2} & \cdots & w_{kk} \end{vmatrix} = 0 \pmod{n}.
\]

Hence \(q = n^2 |\overline{I}I| |I|\) is an algebraic integer, hence also a rational integer.

**Proof of 2.23(C). (a)**

Because of the hypothesis \(e_1 = \cdots = e_k = 1\), the commutativity of \(V\) follows by 2.4. Theorem 2.5 yields the existence of \(k\) class matrices \(C_1, \ldots, C_k\) and of complex numbers \(x_{ij}\) such that
\[
B_i = \sum_{j=1}^{k} x_{ij} C_j, \quad (i = 1, \ldots, k).
\]

Conversely by 2.2 there are also \(x_{ij}'\) with \(C_i = \sum_{j=1}^{k} x_{ij}' B_j\). The \(x_{ij}\) are, by well-known theorems of linear algebra, uniquely determined and rational, since the matrices \(B_i\) and \(C_i\) are rational.

(b) By hypothesis all the irreducible characters appearing in \(G^*\) are rational. Thus the matrices \(U^{-1}C_i U\) appearing in the proof of 2.5 are also rational. By (a) the matrices \(M_i = U^{-1}B_i U = \sum_{j} x_{ij} U^{-1} C_j U\) are then rational. The \(w_{ij}\) are therefore rational. Since the \(w_{ij}\) were already in the proof of 2.23 (A) shown to be algebraic integers, they are rational integers. \(|I| = |\overline{w}_{ij}|\) is therefore a rational integer. Since \(n\) divides \(|I|\), \(n^2 |I|\) is also a rational integer, and \(q\) is therefore a square as was asserted.
(c) The hypothesis that all the irreducible characters appearing in $G^*$ are rational is fulfilled if the degrees $f_i$ of the irreducible constituents of $G^*$ are all different. For since $G^*$ is rational, with each irreducible representation $D_i$ all representations conjugate to it appear in $G^*$. Because all of the $f_i$ are different, these coincide with $D_i$, and $X_i$ is therefore rational.

3. Main Result

In this chapter we prepare the proof number the irreducible constituents $D_i$ of $G^*$ such that $f_2 = p$ and the representations $D_3, \ldots, D_r$ are conjugate. In particular $f_3 = \ldots = f_r = f$ and $f$ divides $p-1$.

Proof

For proof of main result of this paper we prove the following steps.

(Step 1) We can assume without loss of generality that $p \neq 2$. For if $p = 2$, then $G$ is easily seen to be $S^4$ or $A^4$; hence $G$ is doubly transitive.

(Step 2) Every element different from 1 of a Sylow $p$-subgroup of $G$ is a product of two $p$-cycles. Every Sylow $p$-subgroup of $G$ is semiregular and has order $p$.

Proof

Let $P$ be a Sylow $p$-subgroup of $G$ and $I \neq x \in P$. Since the order of $P$ is a power of $p$, $x$ consists of $p$-cycles and cycles of length 1. By 2.6 (theorem of Jordan) $G$ has no $p$-cycles and $x$ is therefore a product of two $p$-cycles. In particular, $x$ moves every point, hence $P$ is semiregular. By 2.11, $|P|$ is a divisor of $2p$, thus $|P| = p$ because $p \neq 2$ by (Step 1).

(Step 3) If $g \in G$ and $a$ is the order of $g$, then either $a = p$ or $(a, p) = 1$.

Proof

We assume that $p$ divides $a$ and $p \neq a$. Then $h = g^{a/p} \neq 1$, thus $h$ has order $p$. By (Step 2), $h$ is a product of two $p$-cycles. Therefore in $g$ no cycle can appear whose length is prime to $p$, since $h$ has only cycles of length $p$. If $g$ were a $2p$-cycle, $G$ would contain the regular group $<g>$, which is cyclic and of composite order $2p$. By 2.8 (theorem of Schur) $G$ would be doubly transitive, which is not the case. $g$ therefore has only $p$-cycles, hence has order $p$, which contradicts our assumption.

We again denote by $D_1, \ldots, D_r$ the different irreducible constituents of the permutation representation $G^*$ of $G$. In addition let $f_i$ be the degree of $D_i(i=1, \ldots, r)$ and let $X_i = \text{Tr}(D_i)$ be the character of $D_i$. Let the numbering be chosen so that $D_1$ is the identity representation. We now prove:

Theorem

We can number the irreducible constituents $D_i$ of $G^*$ such that $f_2 = p$ and the representations $D_3, \ldots, D_r$ are conjugate. In particular $f_3 = \ldots = f_r = f$ and $f$ divides $p-1$.

Proof. 4(a)

By (Step 2) there is an $x \in G$ which is the product of two $p$-cycles. Without loss of generality we may put $x = (12 \ldots p)(p+1 \ldots 2p)$. The characteristic polynomial of the permutation matrix $x$ associated with $x$ is $(z^{p-1})^2$. Hence $x$ has the eigenvalues $1, u, \ldots, u^{p-1}$, all with multiplicity 2, where $u$ is a primitive $p$th root of unity. We wish to investigate how these eigenvalues are distributed among the $D_i(x)$. $D_1(x)$ has the eigenvalue 1 with multiplicity 1 and no others, since $D_1$ is the identity representation.
4(b) We now show that \( f_1 > 1 \) holds for \( i \geq 2 \). We assume \( f_1 = 1 \). Since \( G \) is not Abelian, but \( D_i(G) \) is Abelian, \( D_i \) is not faithful. The normal subgroup \( N \) of all \( n \in G \) with \( D_i(n) = 1 \) is therefore different from 1 and hence (by 2.10) is transitive. Thus \( D_i(N) = 1 \) and also \( D_i(N) = 1 \), which by 2.11 cannot be the case. (Note: This argument is valid for all primitive non-Abelian groups.)

4(c) Let the numbering of the irreducible constituents \( D_1, D_2, \ldots, D_i \) be chosen so that \( D_2(x) \) has 1 as an eigenvalue. Because \( f_2 > 1 \) and since the eigenvalue 1 occurs for \( x \) only twice, \( D_2(x) \) has an eigenvalue different from 1 which without loss of generality may be assumed to be \( u \).

4(d) All representations conjugate to a \( D_i \) are constituents of \( G^* \) since \( G^* \) is rational. \( D_2 \) is conjugate to itself, for otherwise a \( D_i(x) \) with \( i \geq 2 \) would have the eigenvalue 1, which is impossible since \( x \) has the eigenvalue 1 altogether only twice. Therefore \( D_2(x) \) has the eigenvalues \( 1, u, \ldots, u^{p-1} \), all with multiplicity 1, for if an eigenvalue, say \( u \), appeared in \( D_2(x) \) with multiplicity 2, then because of the rationality of \( x^2 \) so would \( u^2, \ldots, u^{p-1} \). Then, however, \( D_1 \) and \( D_2 \) would be the only irreducible constituents of \( G^* \), and by 2.14 \( G \) would be doubly transitive. Hence we obtain \( f_2 = p \).

4(e) The remaining eigenvalues \( u, \ldots, u^{p-1} \) (all with multiplicity 1) of \( x \) are divided among the remaining representations \( D_3, \ldots, D_i \). We now prove that these representations are conjugate to each other and therefore have the same degree \( f \). For \( i = 3 \) there is nothing more to show. We assume \( r \geq 4 \). It suffices (without loss of generality) to prove that \( D_3 \) is conjugate to \( D_4 \). Let \( u \) be an eigenvalue of \( D_3(x) \), \( u^s \) one of \( D_4(x) \) \((1 < s \leq p - 1) \). Because \( p, |G / p| = 1 \) \((\text{by (Step2)})\) there is an \( m \) which is a solution of the two congruences \( m \equiv s(p) \) and \( m \equiv l (p) \). This yields \( m, |G| = 1 \), and therefore an irreducible constituent \( D_i \) of \( G^* \) conjugate to \( D_3 \) is defined by \( D_i(x) \). It is also an eigenvalue of \( D_4(x) \). Since \( u^s \) occurs altogether only once in \( D_3, \ldots, D_i \) we have \( D_4 = D_4 \), hence \( D_4 \) conjugate to \( D_3 \).

4(f) In particular we obtain \( p - 1 \equiv 0 \). In addition, 4(d) and 4(e) show that all the \( D_i \) occur only with multiplicity 1: \( e_1 = \ldots = e_i = 1 \).

REFERENCES


Manning WA. 1933. The degree and class of multiply transitive groups. Trans. Amer. Math. Soc. 35, 585-599.


