A STUDY OF RANK FOUR PERMUTATION GROUPS

Thesis by

James Thomas Renfrow

In Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1969

(Submitted April 2, 1969)

ACKNOWLEDGMENTS

I want to thank Professor Marshall Hall Jr. for serving as my advisor prior to and during the preparation of this thesis.

I also want to thank Professor David Wales for many enlightening and fruitful discussions.

The National Science Foundation and the California Institute of Technology have given me the financial support needed for my graduate education, and for this I give them thanks.

Finally, and most importantly, I want to thank my wife, Diane. She has been a constant source of encouragement, and has been willing to understand all the anxiety involved in the preparation of this thesis.

ABSTRACT

In this thesis we study rank 4 permutation groups. A rank 4 group is a finite transitive permutation group acting on a set Ω such that the subgroup fixing a letter breaks up Ω into 4 orbits. The main tool employed in examining rank 4 groups is the use of intersection matrices, an idea introduced by Donald Higman. Intersection matrices are used to obtain relations between the lengths of the four orbits associated with a rank 4 representation and the degrees of the irreducible characters in the permutation character of the representation. It is shown that two orbits of the representation are paired if and only if two of the characters are complex conjugates of one another. All the maximal primitive rank 4 groups are determined.

Techniques are developed, using intersection matrices, to find all rank 4 representations of known finite groups. Group theoretic results about possible rank 4 groups are derived from the intersection matrices which would have to correspond to the rank 4 representation.

TABLE OF CONTENTS

LIST OF TABLES

INTRODUCTION

The idea of considering transitive permutation groups in terms of the number of orbits of the subgroup fixing a point has been given special consideration by Donald Higman. The rank of a transitive group is the number of orbits of the subgroup fixing a point. The rank 2 groups are simply the multiply transitive groups. The rank 3 groups have been investigated by Higman [9, 10,]. Higman has also considered the matter of rank for every finite value [8]. In this paper we specialize our attention to rank 4 groups.

In the first five chapters we consider numerical relationships which exist in rank 4 groups. In Chapter Two a bound on the order of rank 4 groups is found and the bound is shown to be sharp in the sense that the bound is actually attained. In Chapters Three, Four, and Five, the relationships between the lengths of the orbits of the subgroup fixing a point and the degrees of the irreducible characters contained in the permutation character are examined. Incidence and intersection matrices are used in deriving these and other relationships.

In the last three chapters we consider more of the applications of intersection matrices to the study of rank 4 groups. In Chapter 6 we find the maximal rank 4 groups. Chapter 7 deals with techniques which can be used to find the rank 4 representations of known finite groups. In the last chapter we include several results about the order of a rank 4 group and some of the conjugate classes of the group. These results are specialized to the case where one of the orbits has length p, where p is a prime.

CHAPTER I

NOTATION, DEFINITIONS, AND ELEMENTARY RESULTS

The notations and definitions used in this thesis are standard and can be found in Higman [8] and in Wielandt [13]. For the sake of completeness the more important ones will be given here.

All groups mentioned in this thesis will be finite. G will denote a transitive permutation group acting on the set, $\Omega = \{1,2,\ldots,n\}$, of n elements, where n is a positive integer. G_i will denote the subgroup of G consisting of all elements of G which fix the point i. H, N and K will also denote subgroups of G and will be defined as they are used.

We denote the rank of G by r. This means that for each $i \in \Omega$, Ω is decomposed by G_i into r G_i-orbits. We will label the orbits of G_i as $\Gamma_o(i)$, $\Gamma_1(i)$, $\Gamma_2(i)$, ..., and $\Gamma_{r-1}(i)$. The orbits will be chosen so that $\Gamma_j(i)^g = \Gamma_j(i^g)$ where g is an element of G. We define $\Gamma_{j'}(i) = \Gamma_j'(i)$ as $\{i^{g^{-1}} | i^g \in \Gamma_j(i), g \in G, i \in \Omega\}$. In section 16 of [13] it is shown that $\Gamma_j'(i)$ is also an orbit of Ω under G_i and that the pairing $\Gamma_j(i) \longleftrightarrow \Gamma_j'(i)$ is well defined. An orbit, $\Gamma_j(i)$, is said to be self-paired if $\Gamma_j(i) = \Gamma_j'(i)$, and paired if $\Gamma_j(i) \neq \Gamma_j'(i)$. Two paired orbits will have the same length as is shown in Theorem 16.3 of [13].

All representations of groups will be over the field of complex numbers. The permutation representation of G will be denoted by P and the character of this representation will be denoted by χ. The absolutely irreducible characters contained in χ will be denoted by χ_i. We can write $\chi = \Sigma e_i \chi_i$ where e_i denotes the multiplicity of χ_i in χ. According to Proposition 29.2 of [13], $\Sigma e_i^2 = r$.

The following lemma, while quite elementary, is also quite necessary to the study of groups of rank less than six.

Lemma 1.1: Let G be a transitive permutation group of rank $r \leq 5$. If $\chi = \Sigma e_i \chi_i$, then $e_i = 1$ for all i.

Proof: Since G is transitive, we see from Theorem 32.3 of [3] that the 1_G, the identity character on G, occurs with multiplicity 1.

If $r \leq 4$, then $\Sigma e_i^2 = 4$ implies that $e_i = 1$ for all i.

If $r = 5$, then either χ is the sum of five distinct irreducible characters, each with multiplicity 1, or χ is the sum of the identity character and another irreducible character, θ, which has multiplicity 2. In the first type all the multiplicities are 1 since the characters are distinct.

Let us examine the second type. If there is an element $g \in G$ which fixes no points of Ω then $\chi(g) = 0 = 1 + 2\theta(g)$. This means $\theta(g) = -\frac{1}{2}$ which is a contradiction since $\theta(g)$ must be an algebraic integer and $-\frac{1}{2}$ is not an algebraic integer. Thus no element in G moves every point of Ω. Let $|G_1| = h$ and $|\Omega| = n$. The total number of elements is at most $(|G_1|-1) + (|G_2|-1) + \ldots + (|G_n|-1) + 1$ or $n(h-1) + 1$. The order of the group is $|\Omega| \cdot |G_1| = nh$ since G is transitive. Thus $n(h-1) + 1 \geq nh$ or $1 \geq n$ which is a contradiction. Hence the first type is the only one possible.

The theory of induced characters plays an important role in the theory of permutation characters. We will briefly summarize some of the most important concepts about induced characters. A standard treatment of induced characters can be found in Chapter 6 of [3]. Let G be a group and let H be a subgroup of G. Let θ be a character of H. Define a function $\dot{\theta}$ on G as follows. $\dot{\theta}(g) = \theta(g)$ if $g \in H$ and $\dot{\theta}(g) = 0$ if $g \notin H$. We can now define a function $\theta|^G$ on G. We define $\theta|^G(g) = \Sigma\dot{\theta}(x^{-1}gx)$ where this sum is taken over all elements x of G, where g is also an element of G. $\theta|^G$ is a character of G and is the character of G induced from the character θ on H. If Ψ and φ are two characters of G we define an inner product of the characters by $(\Psi,\varphi)_G = (G:1)^{-1} \sum_{g \in G} \Psi(g)\, \varphi(g^{-1})$. We now consider another relation between the characters of G and the characters of H. If φ is a character of G, then we define $\varphi|_H$ as $\varphi|_H(h) = \varphi(h)$ where $h \in H$. This function, called the restriction of φ to H, is a character of H. The Reciprocity Theorem, due to Frobenius, states that if φ is a character of G and θ is a character of H then $(\varphi,\theta|^{G})_{G} = (\varphi|_{H},\theta)_{H}$. If a group G is represented as a transitive permutation group on the cosets of a subgroup H, then $1_{H}|^{G}$ is the permutation character for this representation.

CHAPTER II

A BOUND ON THE ORDER OF RANK 4 GROUPS

In this chapter we develop an inequality involving the order, g, of a rank 4 group G, the order, h, of the subgroup fixing a letter, G_a, and the index, k, of G_a in $N_G(G_a)$. Using this formula we find all the rank 4 representations associated with the PSL(2,p) groups and the Janko simple group, J, of order 175,560.

Before we derive the order inequality we prove an elementary lemma which we will use.

Lemma 2.1: Let G be a finite transitive permutation group. Let G_a be the subgroup fixing the letter a. Let $k = (N_G(G_a): G_a)$. Then there are k orbits of length 1 for the group G_a.

Proof: Let $G = G_a + G_a x_2 + \dots + G_a x_k + \dots + G_a x_{|\Omega|}$ be a coset decomposition of G where $N_G(G_a) = G_a + G_a x_2 + \dots + G_a x_k$. It is well known that there is a permutation isomorphism between G acting on the cosets of G_a and G acting on the points of Ω. We will show that every element of G_a fixes G_a, $G_a x_2, \dots$, and $G_a x_k$. $G_a x_i x = G_a(x_i x x_i^{-1})x_i = G_a x_i$ if $x \in G_a$ and $2 \leq i \leq k$ since $x_i x x_i^{-1} \in G_a$. If $j > k$, then $x_j \notin N_G(G_a)$ and so there exists a $y \in G_a$ such that $x_j\, y\, x_j^{-1} \notin G_a$ and hence $G_a\, x_j\, y = G_a\, x_j\, y\, x_j^{-1}\, x_j \neq G_a\, x_j$ for equality would imply $x_j\, y\, x_j^{-1} \in G_a$. Thus G_a, $G_a\, x_2, \dots$, and $G_a\, x_k$ are exactly the elements fixed by all elements of G_a.

If G_a is the subgroup fixing a letter, then $1_{G_a}|^G$ is the character of G. Using Proposition 29.2 of [13], we see that $(1_{G_a}|^G, 1_{G_a}|^G)$, the sum of the squares of the multiplicities of the irreducible representations contained in the permutation representation, is the rank of G. Using Frobenius' Law of Reciprocity, we have

$$(1_{G_a}|^G, 1_{G_a}|^G)_G = (1_{G_a}, 1_{G_a}|^G|_{G_a})_{G_a} =$$

$$= |G_a|^{-1}\sum_{y\in G_a}\Big(|G_a|^{-1}\sum_{x\in G\ \&\ x^{-1}yx\in G_a} 1\Big).$$

G will be a rank 4 group if and only if

$$(|G_a|)^{-2}\sum_{y\in G_a}\Big(\sum_{x\in G\ \&\ x^{-1}yx\in G_a} 1\Big) = 4.$$

Since

$$(|G_a|)^{-2}\sum_{y\in G_a}\Big(\sum_{x\in G\ \&\ x^{-1}yx\in G_a} 1\Big) \geq$$

$$\geq (|G_a|)^{-2}\Big(|G| + \sum_{y\in G_a^{\#}}\Big(\sum_{x\in N_G(G_a)} 1\Big)\Big) =$$

$$= (|G_a|)^{-2}(|G| + (|G_a| - 1)|N_G(G_a)|),$$

if G is to be a rank 4 group, we must have $4 \geq h^{-2}\ (g + (h-1)kh)$. From this we see that $h(k + (4-k)h) \geq g$. If G is a rank 4 group such that $k = 1$, then $h(3h + 1) \geq g$. If G is a rank 4 group such that $k = 2$, then $h(2h + 2) \geq g$. If G is a rank 4 group such that $k = 3$, then $h(h + 3) \geq g$. From lemma 2.1 we know that $k = 4$

implies all the orbits of G_a have length 1 and also from the lemma we see that k cannot be bigger than 4 for a rank 4 group.

If G is a rank 4 group and if equality holds in the inequality just derived then this gives additional information on the group. Equality holds if and only if the following occurs: If $x \in G$ and $y \neq 1 \in G_a$ and $x^{-1} y x \in G_a$ then $x \in N_g(G_a)$. This means the G_a, $a \in \Omega$, form a disjoint collection of sets. If a group G satisfies this condition then only the identity fixes more than one point and hence G must be a Frobenius group.

These formulae are sharp. If we consider the relative holomorph of an elementary abelian group of order 9 with an involution we obtain a group of order 18. If we represent this new group on the cosets of a subgroup of order 3, we have a rank 4 representation with k = 3, g = 18, and h = 3. If the simple group of order 60 is represented on the cosets of the subgroup of order 5, then k = 2, g = 60, and h = 5. If G is the group given by the defining relations, $G = \langle a,b,c \mid a^2=b^2=c^{13}=1,\ ab=ba,\ aca=c^{-1},\ bcb=c^{-1} \rangle$ and we represent G on the cosets of a Sylow 2 group then k = 1, h = 4, and g = 52.

We can summarize these results in the following theorem.

Theorem 2.2: Let G be a rank 4 group of order g, let G_a be the subgroup fixing a letter and let $|G_a| = h$, and let $k = [N_g(G_a):G_a]$. The inequality $g \leq h\ (k + (4-k)h)$ is then valid and equality holds if and only if $G_a \cap G_b = 1$ for all a and b in Ω with $a \neq b$. This inequality is sharp in the sense that for k = 1, 2, and 3, there are groups in which equality is attained.

To illustrate the use of this formula we will find all rank 4 representations of the PSL(2,p) groups and also show that there are no rank 4 representations of the Janko simple group of order 175,560.

If one represents PSL(2,p) as a permutation group on the cosets of a subgroup of order $\leq p-1$ then we must have $(p-1)(3(p-1)+1) \geq \frac{1}{2}p\ (p^2-1)$ which means p = 2 or p = 3. PSL(2,3) has a rank 4 representation on a subgroup of order 2. If we represent the group on the cosets of a subgroup of order p, then the order relation requires p = 2, 3, or 5. If one represents PSL(2,5) on the cosets of a Sylow 5 subgroup, one obtains a rank 4 group. In the case of a subgroup of order p + 1, p must be 2, 3, 5, or 7. The representation for p = 5 has rank 3 and the representation for p = 7 has rank 6. In Chapter 20 of [2], all the subgroups of PSL(2,p) are determined and it is shown that the orders of the subgroups either are less than p-1 or have order p, p +1, $\frac{1}{2}p(p-1)$, 12, 24, or 60. If one looks at the group of order $\frac{1}{2}p(p-1)$, this is precisely the subgroup fixing a letter in a doubly transitive representation. If PSL(2,p) is to have a rank 4 representation on a subgroup of order 12, p must be 2, 3, 5, or 7. The only possibility is for p = 7 and this gives a rank 3 representation. If PSL(2,p) is to have a rank 4 representation on a subgroup of order 24, p must be congruent to + 1 or - 1 mod 8 and $24(73) \geq \frac{1}{2}(p)(p-^{2}-1)$ so $p = 7$ is the only possibility. In this case we have a doubly transitive representation. When we consider a subgroup of order 60, we see that $p \equiv \pm 1 \ (5)$ and also $10{,}860 \geq \frac{1}{2}p(p^2-1)$ and hence $p = 11$ or 19. In the case of $p = 11$ we obtain a doubly transitive representation, and in the case of $p = 19$ we obtain a rank 5 representation. One can see from this that there are precisely two rank 4 representations of PSL(2,p), namely PSL(2,3), represented on the cosets of a subgroup of order 2 and PSL(2,5), represented on the cosets of a subgroup of order 5.

On page 48 of [11] all maximal subgroups of Janko's simple group are listed. The largest maximal subgroup has order 660 and is isomorphic to PSL(2,11). Representing the group on the cosets of this subgroup gives a rank 5 representation. The next largest subgroup, which incidentally is also a maximal subgroup, has order 168. Since $175{,}560 > 168(3 \cdot 168 + 1)$ there can be no other possible subgroups which we must consider. Thus we see that Janko's simple group has no rank 4 representations.

CHAPTER III

IMPRIMITIVE RANK 4 GROUPS

In this chapter we will consider the relationship which exists between the degrees of the irreducible representations of the permutation representation and the orbit lengths of the subgroup fixing a letter in an imprimitive rank 4 group.

An imprimitive group, let us recall, is a transitive group G which has at least one subgroup H which properly contains G_1 and is properly contained in G. The length of a chain of subgroups between G_1 and G cannot become arbitrarily large. In fact we have the following lemma.

Lemma 3.1: Let G be an imprimitive rank 4 group and let $G_1 \subsetneq H^1 \subsetneq H^2 \subsetneq \ldots \subsetneq H^k \subsetneq G$ be a chain of subgroups between G_1 and G. Then $k \leq 2$.

Proof: Consider the identity character 1_{G_1}. $1_{G_1}|^{H^1}$ is the sum of 1_{H^1} and at least one other irreducible character, θ_1, of H^1. Likewise $1_{H^1}|^{H^2}$ is the sum of 1_{H^2} and at least one other irreducible character, θ_2, of H^2. In the same way we see that $1_{H^i}|^{H^{i+1}}$ is the sum of $1_{H^{i+1}}$ and at least one other irreducible character, θ_{i+1}, of

H^{i+1}. Thus $1_{G_1}|^G \supseteq 1_G + \theta_1|^G + \theta_2|^G + \ldots + \theta_k|^G + \theta'$, where θ' is a nonidentity character contained in $1_{H^k}|^G$. Using Lemma 1.1 we see that all the irreducible characters contained in $1_{G_1}|^G$ ($= \chi$) occur with multiplicity 1 since G has rank 4. Hence $\theta_i|^G$ and $\theta_j|^G$, $i \neq j$, have no irreducible characters in common and hence $k \leq 2$.

We now turn to the two cases which arise in imprimitive rank 4 groups. The first case is the one where there are precisely four groups in a proper chain from G_1 to G. The second case is the one where there are precisely three groups in a proper chain from G_1 to G. We first prove a lemma which will be useful in both cases and also in later work.

Lemma 3.2: Let G be an imprimitive rank 4 permutation group. Let $\Gamma_0(1)$, $\Gamma_1(1)$, $\Gamma_2(1)$, and $\Gamma_3(1)$ denote the four orbits of G_1 and without loss of generality let $1 \leq i \leq j \leq k$ denote their lengths, respectively. Then the sets of imprimitivity have lengths $1 + i$ and/or $1 + i + j$.

Proof: Let H be a subgroup of G such that $G_1 \subsetneqq H \subsetneqq G$. Let us determine the set of imprimitivity of H that contains 1. Since $H \neq G_1$, this set contains more than one point. If a point from one of the orbits of G_1 is in this set then every element of the orbit is in this set. Those orbits of G_1 which are not in this set must contain complete sets of imprimitivity of H. If $\Gamma_1(1)$, the smallest nontrivial orbit of G_1, is not in this set we have a contradiction for this would imply either $1 + j$, $1+k$, or $1 + k + j$ divides i. Thus one of the possible lengths of a set of imprimitivity of H is $1 + i$. If a set of imprimitivity were to contain the point 1 and two other orbits then in a similar fashion one could see that it would have to be the point and the two smallest nontrivial orbits. Such a set would have length $1 + i + j$.

Let us now consider case 1. Let H and K be two subgroups of G such that $G_1 \subsetneq H \subsetneq K \subsetneq G$. The length of a set of imprimitivity of H must be $1 + i$ and the length of a set of imprimitivity of K must be $1 + i + j$. This means that $[H:G_1] = 1 + i$ and $[K:H] = (1 + i + j)/(1 + i)$ and $[G:K] = n/(1 + i + j)$ where $n = 1 + 1 + j + k$.

We will now determine the degrees of the irreducible characters of the permutation character. If we induce the identity representation, 1_{G_2}, to H, we can use an argument similar to the one in Lemma 3.1 to show that $1_{G_1}|^H$ is the sum of 1_H and precisely one other irreducible character, θ_1, of H. The degree of θ_1 will be i. Likewise $1_H|^K$ is the sum of 1_K and precisely one other irreducible character, θ_2, of K. The degree of θ_2 will be $[(1+i+j)/(1+i)] - 1$ or $j/(i+1)$. In a similar manner we see that $1_K|^G = 1_G + \theta_3$ where θ_3 is an irreducible character of G. Since $\chi = 1_{G_1}|^G$ is the sum of precisely 4 distinct irreducible characters, $\theta_1|^G$ and $\theta_2|^G$ must be irreducible. The degree of $\theta_1|^G$ is (deg θ_1) · [G:H] = i · n/(1 + i). The degree of $\theta_2|^G$ is (deg θ_2) · [G:K] = [j/(1+i)][n/(1+i+j)]. The degree of θ_3 is n/(1+i+j) - 1 or k/(1+i+j). These results are summarized in the following theorem.

Theorem 3.3: Let G be an imprimitive rank 4 permutation group. Let the lengths of the orbits of G_1 be denoted by 1, i, j, and k, where $1 \leq i \leq j \leq k$. If there are two subgroups H and K such that $G_1 \subsetneqq H \subsetneqq K \subsetneqq G$, then the degrees of the irreducible characters contained in the permutation character are 1, in/(1+i), jn/[(1+i)(1+i+j)], and k/(1+i+j).

We will now examine case 2. Suppose that in any chain between G_1 and G precisely one subgroup can be inserted. Let H be such a subgroup, that is, $G_1 \subsetneqq H \subsetneqq G$. The sets of imprimitivity of H may have length 1 + i or 1 + i + j.

Suppose the sets have length 1 + i. Then $[H:G_1]$= 1 + i and [G:H]= n/(i+1). $1_{G_1}|^H$ is a character of degree 1 + i. If $1_{G_1}|^H$ is the sum of 1_H and two other irreducible characters then $1_H|^G$ is the sum of 1_G and precisely one other irreducible character of degree n/(i+1) - 1 or (j+k)/(1+i). If $1_{G_1}|^H$ is the sum of 1_H and precisely one other irreducible character, θ, of H then the following cases can occur. $\theta|^G$ may be irreducible, in which case we have an irreducible character of G of degree ni/(i+1), or $1_H|^G$ is the sum of 1_G and one other irreducible character of G of degree $(j+k)/(1+i)$. In either case we must have an irreducible character of G of degree $ni/(1+i)$ or $(j+k)/(1+i)$.

We will now assume the sets of imprimitivity of H have length $1 + i + j$. In this case G is doubly transitive on the sets of imprimitivity of H and hence $1_H|^G$ is the sum of 1_G and precisely one other irreducible character of G of degree $k/(1+i+j)$ or $k/(n-k)$. These results can be summarized in the following theorem.

Theorem 3.4: Let G be an imprimitive rank 4 permutation group. Let the lengths of the four orbits of G_1 be denoted by 1, i, j, and k where $1 \leq i \leq j \leq k$. If the length of a maximal chain of subgroups from G_1 to G is 3, that is, $G_1 \subsetneqq H \subsetneqq G$, then (1) if $[H:G_1] = 1 + i$, the degree of one of the irreducible characters contained in the permutation character must be either $ni/(1+i)$ or $(j+k)/(1+i)$, or (2) if $[H:G_1] = 1 + i + j$ the degree of one of the irreducible characters contained in the permutation character must be $k/(n-k)$.

We will now give some examples of imprimitive groups. In Chapter 2 we listed several groups which actually have imprimitive rank 4 representations. The relative holomorph, G, of the elementary abelian subgroups of order 9 with an involution gives a rank 4 representation with orbit lengths 1, 1, 1, and 3. In this case all the irreducible characters of G are of degree 1 or 2 and this is what comes from Theorem 3.4. If we represent the alternating group on 5 letters, A_5, on the cosets of a Sylow 5 subgroup we obtain an imprimitive rank 4 representation in which the orbit lengths are 1, 1, 5, and 5. The degrees of the characters in this representation are 1, 3, 3, and 5, and 5 is the value which comes from Theorem 4.3.

An infinite set of examples results from the following groups. Let S_n be the symmetric group on n letters and let A_{n-1} be the alternating group on n-1 letters. The only proper subgroup of S_n which contains A_{n-1} as a proper subgroup is S_{n-1}. Representing S_n on the cosets of A_{n-1} we obtain a rank 4 representation of degree 2n with the orbit lengths being 1, 1, n-1, and n-1. Using Theorem 3.4 we see that we must have a character of degree n or n-1 associated with the permutation character of this representation. One can easily see from Chapter 8 of [12], that there is no character of degree n for S_n when n is greater than 5, and hence the character must have degree n-1.

CHAPTER IV

INCIDENCE AND INTERSECTION MATRICES

In this chapter we will develop the ideas which will be used in the remainder of this thesis. In the first part of this chapter we will give results found in [13] and in [8]. We will then refine and extend these results for rank 4 groups. We conclude the chapter by proving the following fundamental theorem: If G is a rank 4 group two of the orbits of G_1 are paired if and only if two of the irreducible characters contained in the permutation character are conjugate.

If Γ_i denotes an orbit of the subgroup of G fixing a letter, we can define an incidence matrix, $B_i = \left(\beta^i_{ab} \right)$, as

$$\beta^i_{ab} \quad \begin{aligned} &= 1 \text{ if } a \in \Gamma_i(b) \\ &= 0 \text{ otherwise} \end{aligned}$$

These matrices have the following properties:

B1. $B_o = I$ and $\sum_{i=o}^{r-1} B_i = F$ where F denotes the matrix with all entries equal to 1. See Proposition 28.2 of [13].

B2. $B_o, B_1, \ldots, B_{r-1}$ is a basis for the commuting algebra of the permutation representation of G. See Proposition 28.4 of [13].

B3. If Γ_i and Γ_j are paired orbits, then $B_i^T = B_j$. See Theorem 28.9 of [13].

If we again let Γ_k, of length ℓ_k, denote an orbit of the subgroup of G fixing a letter we can define an intersection matrix, M_k, associated with this orbit as follows: $M_k = \left(u^k_{ij} \right)$, where

$$u^k_{ij} = |\Gamma_k(b) \cap \Gamma_i(a)| \quad \text{if} \quad b \in \Gamma_j(a).$$

We call u^k_{ij} an intersection number.

We list here the important properties of intersection matrices and numbers found in Section 4 of [8].

M1. $\sum_i u^k_{ij} = \ell_k$, $\sum_k u^k_{ij} = \ell_i$, and $u^k_{ij} = u^i_{kj'}$, where j' denotes the number of the orbit paired with Γ_j.

M2. $u^k_{io} = \delta_{ik}\ell_k$ and $u^k_{oi} = \delta_{ik'}$

M3. $\ell_j u^k_{ij} = \ell_i u^{k'}_{ji}$ and $\ell_i u^j_{k'i} = \ell_j u^k_{i'j} = \ell_k u^i_{j'k}$

M4. M_k has column sum ℓ_k.

M5. $M_o, M_1, \ldots, M_{r-1}$ are linearly independent and $\sum_k M_k = \hat{F}$, where $\hat{F}$ denotes the matrix whose ith row is $(\ell_i, \ell_i, \ldots, \ell_i)$, $i = 0, 1, \ldots, r-1$.

M6. The algebra generated by $M_o, M_1, \ldots, M_{r-1}$ is isomorphic as an algebra to the algebra generated by $B_o, B_1, \ldots, B_{r-1}$.

M7. M_i and B_i satisfy the same minimal polynomial.

M8. $M_k L = \ell_k L$ where $L = (\ell_o, \ell_1, \ldots, \ell_{r-1})^T$.

We will now specialize our discussion to the case where the rank of the group is four. In this case we know from Theorem 29.5 of [13] that the commuting algebra of the permutation representation is commutative.

We will now consider the situation in which two of the orbits, Γ_1 and Γ_2, are paired. Let us first examine M_1, the intersection matrix for one of the paired orbits. To simplify notation and to facilitate reading of this work we will substitute unsubscripted letters for the intersection numbers whenever possible. The transition from one notation to the other is rather straightforward. Thus we can give M_1 by

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ \ell_1 & a & b & c \\ 0 & d & e & f \\ 0 & g & h & i \end{pmatrix},$$

where the first row and column have been determined from M2.

We will now try to construct M_2. Using M2 we can determine that the first row is (0, 1, 0, 0) and the first column is $(0, 0, \ell_1, 0)^T$, for $\ell_1 = \ell_2$ because Γ_1 and Γ_2 are paired. Using the fact that $\ell_1 = \ell_2$ and M3, we see that $u_{11}^2 = u_{11}^1$, $u_{22}^2 = u_{22}^1$, $u_{33}^2 = u_{33}^1$, $u_{21}^2 = u_{12}^1$, and $u_{12}^2 = u_{21}^1$. Using M1 we see that $u_{23}^1 = u_{13}^2$ and $u_{13}^1 + u_{23}^1 + u_{33}^1 = \ell_1 = \ell_2 = u_{13}^2 + u_{23}^2 + u_{33}^2$ and so $u_{13}^1 = u_{23}^2$. From this we know that M_2 is

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & a & d & f \\ \ell_1 & b & e & c \\ 0 & x & y & i \end{pmatrix},$$

where x and y must still be determined. Since M_1 and M_2 commute, $M_1M_2 = M_2M_1$. The (3,0) entry in M_1M_2 is $\ell_1 h$. The (3,0) entry in M_2M_1 is $\ell_1 x$. Thus $h = x$. Using M8 we see that $h\ell_1+y\ell_1+i\ell_3 = \ell_1\ell_3$ from $M_2L = \ell_1 L$ and $h\ell_1+g\ell_1+i\ell_3 = \ell_1\ell_3$ from $M_1L = \ell_1 L$ so $y = g$

and M_2 is completely determined from M_1. M_3 is also completely determined since $M_3 = \hat{F} - M_2 - M_1 - I$.

We will now reduce the number of variables appearing in the matrices by using other properties of the matrices. The first column in M_1M_2 is $(\ell_1,\ell_1 b,\ell_1 e,\ell_1 h)^T$. The first column of M_2M_1 is $(\ell_1,\ell_1 a,\ell_1 b,\ell_1 h)^T$. From this we see that $a = b = e$. We know that the column sums of M_1 must be ℓ_1 (by M4). Thus

(1) $d + g = \ell_1 - a$

(2) $f + c + i = \ell_1$

(3) $h = \ell_1 - 2a - 1$.

Using M8 we obtain three more relations

(4) $\ell_1 d + \ell_3 f = \ell_1^2 - \ell_1 a$

(5) $\ell_3 c = \ell_1^2 - 2a\ell_1 - \ell_1$

(6) $\ell_1 g + \ell_1 h + \ell_3 i = \ell_3 \ell_1$.

We may solve these six equations and obtain b, c, e, f, g, h, and i in terms of a and d.

$b = a$

$c = \ell_1(\ell_1 - 2a - 1)/\ell_3$

$e = a$

$f = \ell_1(\ell_1 - a - d)/\ell_3$

$g = \ell_1 - a - d$

$h = \ell_1 - 2a - 1$

$i = \ell_1(\ell_3 - 2\ell_1 + 3a + d + 1)/\ell_3$

In the case where all the orbits are self-paired we can carry out a similar reduction. For the sake of convenience we will again use unsubscripted letters to denote the intersection numbers. From M2 it is immediate that the first row of M_1 is (0, 1, 0, 0) and the first column is $(0, \ell_1, 0, 0)^T$. Thus we have M_1 as

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ \ell_1 & a & b & c \\ 0 & d & e & f \\ 0 & g & h & i \end{pmatrix},$$

We should note that the case in which two of the orbits are paired is separate from this case and the letters a, b, c, . . . , i are not related to the ones in the previous case.

We will now express M_1 in terms of a, d, and e. Using M3 we see that $b = \ell_1 d/\ell_2$. Applying M1 to the columns of M_1 we see that $g = \ell_1 - a - d - 1$ and $h = \ell_1 - e - \ell_1 d/\ell_2$. Again using M3 we see that $c = \ell_1(\ell_1 - a - d - 1)/\ell_3$ and that $f=\ell_2(\ell_1-e-\ell_1 d/\ell_2)/\ell_3$. The number i can be determined by using M1 on the last column sum of M_1. We obtain $i = (\ell_1\ell_3 - \ell_1^2 + a\ell_1 + 2d\ell_1 + \ell_1 - \ell_1\ell_2 + e\ell_2)/\ell_3$.

Using M2 it is immediate that the first row of M_2 is (0, 0, 1, 0) and that the first column of M_2 is $(0, 0, \ell_2, 0)^T$. We denote M_2 by

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & p & q & r \\ \ell_2 & s & t & w \\ 0 & x & y & z \end{pmatrix},$$

The first row of M_1M_2 is (0, p, q, r). The first row of M_2M_1 is $(0, d, e, \ell_2(\ell_1 - e - \ell_1 d/\ell_2)/\ell_3)$. Thus p = d, q = e, and r = $= \ell_2(\ell_1 - e - \ell_1 d/\ell_2)/\ell_3$. Using M3 we see that $s = \ell_2 e/\ell_1$ and

$x = \ell_2 - e - \ell_2 e/\ell_1$. Using M1 on the fourth column of M_2 we find that $z = (\ell_2\ell_3 - \ell_2\ell_1 + 2e\ell_2 + d\ell_1 - \ell_2^2 + t\ell_2 + \ell_2)/\ell_3$.

The matrix M_3 can be determined from the relation $M_3 = \hat{F} - M_1 - M_2 - I$ given in M5.

We have thus shown the following theorem.

Theorem 4.1: Let G be a rank 4 group. If two of the orbits, Γ_1 and Γ_2, of the subgroup fixing a letter are paired then the intersection matrices are completely determined from ℓ_1, ℓ_2, ℓ_3, and the intersection numbers u^1_{11} and u^1_{21}. If all the orbits of the subgroup fixing a letter are self-paired then the intersection matrices are completely determined from ℓ_1, ℓ_2, ℓ_3, and the intersection numbers u^1_{11}, u^1_{21}, u^1_{22}, and u^2_{22}.

We will now study the relationship between the eigenvalues of the incidence matrices and the values of the irreducible characters of the permutation character. Since the incidence matrix B_i and the intersection matrix M_i satisfy the same minimal polynomial they have the same eigenvalues, and only the multiplicities of the eigenvalues are different. The relevant facts which we will use in the remainder of this thesis with regard to this matter are contained in the following theorem.

Theorem 4.2: Let G be a rank 4 group. Let χ_1, χ_2, and χ_3 denote the nonidentity characters contained in the permutation character. Then

(1) χ_1, χ_2, and χ_3 are rational characters if and only if the eigenvalues of the incidence matrices are rational,

(2) χ_1, χ_2, and χ_3 are real characters if and only if the eigenvalues of the incidence matrices are real, and

(3) at least one of the characters χ_1, χ_2 and/or χ_3 is complex if and only if some of the eigenvalues of some of the incidence matrices are complex.

Proof: Let g_1, g_2, . . . , and g_i be the elements of G in a conjugate class, C_j, of G. Let α_j denote the element in the group ring of G given by $g_1 + g_2 + . . . + g_i$. In the usual way we define $P(\alpha_j)$ to be $P(g_1) + P(g_2) + . . . + P(g_i)$. The class matrices $P(\alpha_1)$, $P(\alpha_2)$, . . . , and $P(\alpha_k)$ are in the commuting algebra of the permutation representation, by Theorem 29.7 of [13]. Since the commuting algebra is commutative, $P(\alpha_1)$, $P(\alpha_2)$, . . . , and $P(\alpha_k)$ generate the commuting algebra and without loss of generality we may assume $P(\alpha_1)$, $P(\alpha_2)$, $P(\alpha_3)$, and $P(\alpha_4)$ are a basis for the algebra. B_o, B_1, B_2, and B_3 are also a basis. Since $P(\alpha_i)$ has only integer entries and since $\Sigma B_i = F$, $P(\alpha_i) = \sum_{j=0}^{3} a_{ij} B_j$ where the a_{ij} are integers. If we let $A = (a_{ij})$, then A is nonsingular for it carries a basis to a basis, and its inverse $C = (c_{ij})$ will consist of rational entries. Thus every B_i is a rational linear combination of the $P(\alpha_j)$.

Since the multiplicities of χ_1, χ_2, and χ_3 are 1, all the elements of the commuting algebra, when transformed by a unitary matrix, U, which completely reduces the permutation representation of G, must be in diagonal form as is shown on page 85 of [13], and the diagonal entries are the eigenvalues. Each eigenvalue of a class matrix is a rational multiple of the value of χ_1, χ_2, χ_3, or 1_G on that class, as can be seen on page 235 of [3].

Let us show (1). If χ_1, χ_2, and χ_3 are rational then the eigenvalues of $P(\alpha_1)$, $P(\alpha_2)$, $P(\alpha_3)$, and $P(\alpha_4)$ are all rational. Since the B_i's are a rational linear combination of the $P(\alpha_j)$ all their eigenvalues must be rational. Since their eigenvalues are also algebraic integers their eigenvalues must be integers. If, on the other hand, all the eigenvalues of the B_i's are integers, then the eigenvalues of the $P(\alpha_j)$ must be rational numbers because each $P(\alpha_j)$ is a rational linear combination of the B_i's. Thus also χ_1, χ_2, and χ_3 must be rational.

Let us now prove (2). This result is proved in just the same way as (1) except that we realize that the eigenvalues of the B_i's are real if and only if the eigenvalues of the $P(\alpha_j)$ are real.

The proof of (3) follows from (2). For if some of the incidence matrices have complex eigenvalues and all the characters, χ_1, χ_2, and χ_3 are real then this contradicts (2). On the other hand if all the eigenvalues of the incidence matrices are real then all the characters, χ_1, χ_2, and χ_3, must be real.

We are now able to prove the following fundamental theorem.

Theorem 4.3: Let G be a rank 4 group. Two of the orbits of the group fixing a letter are paired if and only if two of the characters are complex characters and are conjugate.

Proof: Suppose two of the orbits are paired, say Γ_1 and Γ_2. Using B3 we see that $B_1^T = B_2$. Let U be a unitary matrix which transforms the permutation representation to the four irreducible representations. Then $U^{-1}B_1 U = \bar{U}^T B_1 U$ is a diagonal matrix. If all the eigenvalues of B_1 were real, then

$$\bar{U}^T B_1 U = \overline{\bar{U}^T B_1 U}^T = \bar{U}^T B_1^T U = U^{-1} B_2 U$$

which implies that $B_1 = B_2$, which is a contradiction since B_1 and B_2 are linearly independent by property B2. Hence B_1 and therefore B_2 have complex eigenvalues, and those in B_2 are the complex conjugates of those in B_1. Because the characteristic equation of B_1 has real coefficients and one of the eigenvalues of B_1 is ℓ_1, by M8, the other distinct eigenvalues must be one other real eigenvalue and two complex values which are conjugate. Since the trace of B_i, $i \neq 0$, is zero the multiplicities of the complex eigenvalues are the same. Since $B_3^T = B_3$ all its eigenvalues must be real. From Theorem 4.2 we know that there must be complex characters contained in the permutation character, χ. Since $\chi = \bar{\chi}$ the complex characters must be conjugates of one another.

Suppose that two of the characters are complex conjugates. This means that some of the eigenvalues of some of the incidence matrices must be complex. Suppose B_1 has complex eigenvalues. If Γ_1 is self-paired then $B_1^T = B_1$, and by a process similar to the one used in the first part of the proof we can see that all the eigenvalues of B_1 would be real which is a contradiction. Hence Γ_1 is paired with another orbit.

CHAPTER V

DEGREES OF IRREDUCIBLE REPRESENTATIONS

In this chapter we will study the relationship between the orbit lengths of the stabilizer of a point in a primitive rank 4 group and the degrees of the irreducible representations contained in the permutation representation. The case for imprimitive groups was considered in Chapter 3.

Throughout this chapter we will let U denote a unitary matrix which completely reduces the permutation representation of G. If C is any matrix in the commuting algebra of the permutation representation of G, then $U^{-1}C\,U$ will be a diagonal matrix, and will have the form

$$\begin{pmatrix} \alpha_0 & & & & & & & & & & \\ & \alpha_1 & & & & & & & & & \\ & & \ddots & & & & & & 0 & & \\ & & & \alpha_1 & & & & & & & \\ & & & & \alpha_2 & & & & & & \\ & 0 & & & & \ddots & & & & & \\ & & & & & & \alpha_2 & & & & \\ & & & & & & & \alpha_3 & & & \\ & & & & & & & & \ddots & & \\ & & & & & & & & & \alpha_3 \end{pmatrix},$$

where α_i occurs d_i times, where d_i represents the degree of χ_i. This can be seen from page 85 of [13]. Note that the α_i are not necessarily distinct one from the other. If all the α_i were distinct then we would know the value of d_1, d_2, and d_3 if we knew the multiplicities of α_1, α_2, and α_3. If all the α_i are not distinct we simply know the sum of two or three of the degrees.

The matrices in the commuting algebra which we will consider are the three incidence matrices B_1, B_2, and B_3. Corresponding to each of them are the intersection matrices M_1, M_2, and M_3 respectively. In Chapter 4 it was noted in M6 and M7 that the algebra generated by the M_i's is isomorphic to the algebra generated by the B_i's, and that M_i and B_i both satisfy the same minimum polynomial. The connection between M_i and B_i will now be made clearer. The isomorphism mentioned above comes from the usual linear extension of the map $B_i \to M_i$. On pages 30 and 31 of [8] a way of obtaining M_i from B_i is described. We will briefly describe this procedure. First an element $a \in \Omega$ is picked and all the points of Ω are arranged in the orbits of the subgroup fixing a. The arrangement results in 16 blocks in each B_i. Each of these blocks has constant column sum and if these column sums are inserted in the appropriate places in a four by four matrix the matrix M_i is the result.

The first case we will consider is when all the orbits are self-paired. We are able to obtain three equations, involving d_1, d_2, and d_3, from which we can solve for d_1, d_2, and d_3. The first equation comes from the fact that the sum of the degrees of the irreducible representations is the degree of the permutation representation.

(1) $1 + d_1 + d_2 + d_3 = n.$

The second equation comes from the fact that the trace of B_i is zero if $i = 1, 2,$ or 3. The eigenvalue with multiplicity 1 in B_i is ℓ_i, as is shown on page 31 of [8]. If we denote the other three eigenvalues of B_i by α_{i1}, α_{i2}, and α_{i3} then we have

(2) $\ell_i + \alpha_{i1}d_1 + \alpha_{i2}d_2 + \alpha_{i3}d_3 = 0.$

The third equation comes from Theorem 28.10 of [13] and is that the trace of B_i^2 is $\ell_i n$ if $i = 1, 2,$ or 3. Thus we have

(3) $\ell_i^2 + \alpha_{i1}^2 d_1 + \alpha_{i2}^2 d_2 + \alpha_{i3}^2 d_3 = \ell_i n.$

Solving these equations for d_1, d_2, and d_3 we obtain

$$d_1 = \frac{(n-1)\alpha_{i2}\alpha_{i3} + n\ell_i - \ell_i^2 + \ell_i(\alpha_{i2} + \alpha_{i3})}{(\alpha_{i1} - \alpha_{i2})(\alpha_{i1} - \alpha_{i3})},$$

$$d_2 = \frac{(n-1)\alpha_{i1}\alpha_{i3} + n\ell_i - \ell_i^2 + \ell_i(\alpha_{i1} + \alpha_{i3})}{(\alpha_{i2} - \alpha_{i1})(\alpha_{i2} - \alpha_{i3})}, \text{ and}$$

$$d_3 = \frac{(n-1)\alpha_{i1}\alpha_{i2} + n\ell_i - \ell_i^2 + \ell_i(\alpha_{i1} + \alpha_{i2})}{(\alpha_{i3} - \alpha_{i1})(\alpha_{i3} - \alpha_{i2})}.$$

These equations will be valid, that is, the denominators of the fractions will be nonzero, if for some value of i, α_{i1}, α_{i2}, and α_{i3} are all distinct. This will occur exactly when at least one of the three intersection matrices M_1, M_2, or M_3 has four distinct eigenvalues. If this is the case then we have determined the degrees of the irreducible characters in the permutation character in terms of the eigenvalues of the intersection matrices and the orbit lengths of the subgroup fixing a point.

In Theorem 4.8 of [8] it is shown that a rank 4 group is primitive if and only if M_1, M_2, and M_3 are irreducible. On page 53 of [7] it is shown in this case that the value ℓ_i is a simple root of the characteristic equation of M_i. Combining these two facts we see that if there are only two or three distinct eigenvalues of M_i, ℓ_i still occurs with multiplicity 1.

If none of the three matrices M_1, M_2, or M_3 has four distinct eigenvalues there will be several cases to consider.

Case I. All three matrices have three distinct eigenvalues.

Case II. Two have three distinct eigenvalues and one has only two distinct eigenvalues.

Case III. One has three distinct eigenvalues and two have only two distinct eigenvalues.

Case IV. All three have only two distinct eigenvalues.

None can have simply one distinct eigenvalue, for as we noted before ℓ_i is a simple eigenvalue of M_i. To simplify notation we will denote a four by four diagonal matrix by (a, b, c, d), where a, b, c, and d represent the elements on the diagonal. Let N_i denote the diagonal matrix equivalent to M_i.

In case III a representative case would be $N_o = (1, 1, 1, 1)$, $N_1 = (\ell_1, \alpha, \alpha, \beta)$, $N_2 = (\ell_2, \gamma, \gamma, \gamma)$, and $N_3 = (\ell_3, \delta, \delta, \delta)$ and one can see that the dimension of the algebra generated by these four matrices would be 3 which is a contradiction.

In case IV we can easily see that $\langle N_o, N_1, N_2, N_3\rangle$ would be an algebra of dimension 2 which would also be a contradiction.

In case I there are several possibilities. If we have $N_o = (1, 1, 1, 1)$, $N_1 = (\ell_1, \alpha, \alpha, \beta)$, $N_2 = (\ell_2, \gamma, \gamma, \delta)$, and $N_3 = (\ell_3, \zeta, \zeta, \eta)$, the algebra $\langle N_o, N_1, N_2, N_3\rangle$ would have dimension 3 which would be a contradiction. Without loss of generality we may suppose we have either $N_o = (1, 1, 1, 1)$, $N_1 = (\ell_1, \theta_1, \theta_1, \theta_2)$, $N_2 = (\ell_2, \lambda_1, \lambda_1, \lambda_2)$, and $N_3 =$ $= (\ell_3, \mu_1, \mu_2, \mu_1)$ or $N_o = (1, 1, 1, 1)$, $N_1 = (\ell_1, \theta_1, \theta_1, \theta_2)$, $N_2 = (\ell_2, \lambda_1, \lambda_2, \lambda_1)$, and $N_3 = (\ell_3, \mu_1, \mu_2, \mu_2)$. Using equations (1) and (2) as before we can find the degree of one of the nonidentity representations for N_1, N_2, and N_3. Suppose these three degrees, one from each of the three nontrivial matrices, are denoted by f_1, f_2, and f_3 respectively. If they are all different then they represent the degrees of the three separate irreducible representations. If two are equal, as in $f_1 = f_2$ and $f_1 \neq f_3$, then the degrees of the irreducible representations must be 1, f_1, f_3, and $n - f_1 - f_3 - 1$. If all three are equal then the degrees of the irreducible representations must be 1, f_1, f_1, and $n - 2f_1 - 1$.

In case II if $N_o = (1, 1, 1, 1)$, $N_1 = (\ell_1, \theta_1, \theta_1, \theta_1)$, $N_2 = (\ell_2, \lambda_1, \lambda_1, \lambda_2)$, and $N_3 = (\ell_3, \mu_1, \mu_1, \mu_2)$, then $\langle N_o, N_1, N_2, N_3\rangle$ would be an algebra of dimension 3 which is a contradiction. We may thus assume that $N_o = (1, 1, 1, 1)$, $N_1 = (\ell_1, \theta_1, \theta_1, \theta_1)$, $N_2 = (\ell_2, \lambda_1, \lambda_1, \lambda_2)$, and $N_3 = (\ell_3, \mu_1, \mu_2, \mu_1)$. Using equations (1) and (2) in connection with N_2 and N_3 we may determine the degrees of two of the irreducible representations,

d_1 and d_2. The degree of the remaining one will be $n - d_1 - d_2 - 1$. In the case where all the orbits are self-paired we have determined the degrees of the irreducible representations.

Let us now consider the case where two of the matrices, B_1 and B_2, are paired with each other. From the work done in Chapter 4 and from the material given in this chapter on primitive groups we know that there must be four distinct eigenvalues of M_1, denoted by ℓ_1, λ, $\bar{\lambda}$, and θ, where λ is complex. Since the degree of two of the irreducible representations are equal, we suppose $d_1 = d_2$. The two equations

$$\ell_1 + d_3\theta + d_1(\lambda + \bar{\lambda}) = 0 \quad \text{and}$$

$$1 + d_3 + 2d_1 = n$$

can be solved for d_1 and d_3. We obtain

$$d_1 = \frac{\ell_1 + \theta(n - 1)}{2\theta - (\lambda + \bar{\lambda})} \quad \text{and}$$

$$d_3 = \frac{(n - 1)(\lambda + \bar{\lambda}) + 2\ell_1}{(\lambda + \bar{\lambda}) - 2\theta}.$$

If $\lambda + \bar{\lambda} - 2\theta$ is zero, that is, the determinant of the matrix of coefficients is zero, then we can form two more equations, $1 + d_3 + 2d_1 = n$ and $\ell_1^2 + d_3\theta^2 + 2\lambda\bar{\lambda}d_1 = n\ell_1$, using Theorem 28.10 of [13] and solve for d_1 and d_3. If the determinant of the matrix of coefficients is zero in this case also, then this implies that $\theta^2 = \lambda\bar{\lambda}$. If $\lambda + \bar{\lambda} = 2\theta$ then $\lambda^2 + 2\lambda\bar{\lambda} + \bar{\lambda}^2 = 4\theta^2$ and hence $\lambda^2 + 2\lambda\bar{\lambda} + \bar{\lambda}^2 = 4\lambda\bar{\lambda}$ or $(\lambda - \bar{\lambda})^2 = 0$. This is a contradiction of the fact that the number λ must be complex. Hence one of the two sets of equations yields a solution of the problem.

CHAPTER VI

MAXIMAL RANK 4 GROUPS

If G is a rank 4 group it is said to be a maximal rank 4 group if n is maximal with respect to the length, ℓ, of the smallest orbit of G_a, other than the orbit containing a. In this chapter we will prove a result for rank 4 groups similar to one Higman proved for rank 3 groups. We will however be able to obtain much more precise results.

The theorem that Higman was able to prove is Theorem 1 of [9], and is: If G is a transitive group of rank 3 and degree $n = \ell^2 + 1$, where ℓ is the length of a G_a- orbit, then $n = 5, 10, 50,$ or 3250.

The result we will obtain is: If G is a primitive rank 4 group and ℓ is the length of the smallest nontrivial orbit of G_a then the lengths of the other two orbits are at most $\ell(\ell - 1)$ and $\ell \cdot (\ell - 1) \cdot (\ell - 1)$ and if equality is attained then the group must be the dihedral group on seven letters.

If the group G is imprimitive then we can't obtain any bounds on the size of Ω. If we consider as G, the symmetric group on n letters, S_n, and as the group fixing a letter, the alternating group on n-1 letters, A_{n-1}, then this gives an imprimitive representation and the orbit lengths are 1, 1, n-1, and n-1.

A result which is very necessary in proving this theorem is Theorem 4.8 of [8] and it states that G is primitive if and only if M_i, the intersection matrices associated with Γ_i, i = 1, 2, and 3, are irreducible.

We prove the theorem by first considering three possible cases. The first is the one in which two orbits are paired and the shortest orbit is the self-paired one. The second is the one in which two orbits are paired and they each have the shorter length. The third is the one in which all orbits are self-paired.

In case 1 the intersection matrix for the smallest orbit, Γ_3, the one which is self-paired, will be:

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & \alpha & \beta & \ell_1(\ell_3 - \beta - \alpha)/\ell_3 \\ 0 & \beta & \alpha & \ell_1(\ell_3 - \beta - \alpha)/\ell_3 \\ \ell_3 & \ell_3 - \beta - \alpha & \ell_3 - \beta - \alpha & * \end{pmatrix},$$

where * represents the quantity $(\ell_3^2 - \ell_3 - 2\ell_1 (\ell_3 - \beta - \alpha))/\ell_3$. If $\ell_3 - \beta - \alpha$ is zero then one can see by interchanging rows and columns 2 and 4 that the matrix is reducible and hence the group is imprimitive. If $\ell_3 - \beta - \alpha$ is non zero then $\ell_1 (\ell_3 - \beta - \alpha)/\ell_3$ must be an integer less than or equal to $(\ell_3 - 1)/2$ if ℓ_3 is odd and $(\ell_3 - 2)/2$ if ℓ_3 is even. This implies that ℓ_1 is less than or equal to $\ell_3(\ell_3 - 1)/2$ or $\ell_3(\ell_3 - 2)/2$ and n is less than or equal to $\ell_3^2 + 1$ or $\ell_3^2 - \ell_3 + 1$ respectively.

In case 2 the intersection matrix for one of the paired orbits, Γ_1, is

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ \ell_1 & \alpha & \alpha & \ell_1(\ell_1 - 2\alpha - 1)/\ell_3 \\ 0 & \beta & \alpha & \ell_1(\ell_3 - \alpha - \beta)/\ell_3 \\ 0 & \ell_1 - \alpha - \beta & \ell_1 - 2\alpha - 1 & * \end{pmatrix},$$

where * represents $\ell_1\ (\ell_3 - 2\ell_1 + 3\alpha\ell_1 + \beta + 1)/\ell_3$. If G is to be primitive then $\ell_1\ (\ell_1 - 2\alpha - 1)/\ell_3$ and/or $\ell_1\ (\ell_1 - \alpha - \beta)/\ell_3$ must be nonzero. If both $\ell_1 - \alpha - \beta$ and $\ell_1 - 2\alpha - 1$ are nonzero, then ℓ_3 can be maximal when $\ell_1 - 2\alpha - 1 = \ell_1 - 1$ and $\ell_1 - \alpha - \beta = \ell_1 - 1$ which is the case when $\alpha = 0$ and $\beta = 1$. In this case $\ell_3 = \ell_1\ (\ell_1 - 1)$. If $\ell_1 - 2\alpha - 1$ is zero, then $\alpha = (\ell_1 - 1)/2$ and hence $\ell_3 \leq \ell_1\ (\ell_1 + 1)/2$. If $\ell_1 - \alpha - \beta$ is zero, then $\ell_3 \leq \ell_1\ (\ell_1 - 2\alpha - 1)$ and is maximal when $\alpha = 0$. In this case $\beta = \ell_1$ and $\ell_3 \leq \ell_1\ (\ell_1 - 1)$. Hence $n \leq 1 + \ell_1 + \ell_1^2$ or $n \leq (2 + 5\ell_1 + \ell_1^2)/2$.

In case 3 the intersection matrix for the orbit, Γ_1, of shortest length is:

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ \ell_1 & a & \ell_1 d/\ell_2 & \ell_1(\ell_1-a-d-1)/\ell_3 \\ 0 & d & e & \ell_2(\ell_1-e-\ell_1 d/\ell_2)/\ell_3 \\ 0 & \ell_1-a-d-1 & \ell_1-e-\ell_1 d/\ell_2 & * \end{pmatrix},$$

where * represents the quantity $(e\,\ell_2 + \ell_1\ell_3 - \ell_1^{\,2} + a\ell_1 + 2d\ell_1 + {}$ $+ \ell_1 - \ell_1\ell_2)/\ell_3$. If d and $\ell_1 - a - d - 1$ are both nonzero, then ℓ_2 and ℓ_3 are both less than or equal to $\ell_1\ (\ell_1 - 2)$. If d is zero, then $\ell_1 - a - d - 1$ may not be zero. Thus ℓ_3 must be $\leq \ell_1\ (\ell_1 - 1)$. If $\ell_1 - e - \ell_1 d/\ell_2$ were now zero then the matrix would be reducible. Since $\ell_2\ (\ell_1 - e - \ell_1 d/\ell_2)/\ell_3$ must be a positive integer less than or equal to $\ell_1 - 1$, ℓ_2 will have its largest value when $\ell_1 - e - \ell_1 d/\ell_2 = 1$ and $\ell_2 = \ell_3\ (\ell_1 - 1)$ or $\ell_2 = \ell_1\ (\ell_1 - 1)^2$. If $d \neq 0$ and $\ell_1 - a - d - 1 = 0$ an argument using the interchange of orbits Γ_2 and Γ_3 leads to the same answer, with $\ell_2 = \ell_1\ (\ell_1 - 1)$ and $\ell_3 = \ell_1\ (\ell_1 - 1)^2$. The total length, n, is therefore at most $\ell_1^{\,3} - \ell_1^{\,2} + \ell_1 + 1$.

The maximal case to consider is therefore case 3. We should note that in case the smallest orbit has length 2 we need to consider several possibilities. When the smallest orbit has length ≥ 3, clearly case 3 is the desired one.

The intersection matrix associated with the smallest orbit Γ_1 when the other two orbits have length $\ell_1 (\ell_1 -1)$ and $\ell_1 (\ell_1 - 1)^2$ is

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ \ell_1 & 0 & 0 & 1 \\ 0 & 0 & \ell_1-1 & \ell_1-1 \\ 0 & \ell_1-1 & 1 & 0 \end{pmatrix}.$$

Its characteristic polynomial is $(x - \ell_1)(x^3 + x^2 - 2(\ell_1 - 1)x - (\ell_1 - 1))$. The discriminant of $x^3 + x^2 - 2(\ell_1 - 1)x - (\ell_1 - 1)$ is $36 (\ell_1 -1)^2 + 4(\ell_1 -1) + 4(\ell_1 -1)^2 + 32 (\ell_1 - 1)^3 - 27 (\ell_1 - 1)^2$ and is always positive where $\ell_1 \geq 2$. From this fact and the fact that G is primitive we know that the characteristic equation has four distinct real roots.

Suppose $x^3 + x^2 - 2(\ell_1 - 1) x - (\ell_1 - 1) = 0$ has an integer solution, y. Thus $y^2 (y + 1) = (\ell_1 - 1)(2y + 1)$ or $y^2 (y + 1)/(2y + 1) = \ell_1 - 1$ unless $y = -\frac{1}{2}$ which is not possible since y must be an algebraic integer. Hence $y^2 (y + 1)/(2y + 1)$ must be an integer. y^2 and $2y + 1$ have no factors in common for if p is a prime and $p \mid y^2$ then $p \mid y$ and $p \mid 2y$ and hence $p \nmid 2y+1$. $y + 1$ and $2y + 1$ do not have any factors in common for if p is a prime and $p \mid y+1$ then $p \mid 2y + 2$ and $p \nmid 2y+2-1$. If

$2y + 1$ is 1 then $y = 0$ and $\ell_1 - 1 = 0$ or $\ell_1 = 1$ which is impossible. Hence for any integer $\ell_1 \geq 2$, $x^3 + x^2 - 2(\ell_1 - 1)x - (\ell_1 - 1) = 0$ has no integral solutions.

We now need a lemma to show that the characters and hence the irreducible representations which occur in the permutation representation, in addition to the identity representation, must be of the same degree.

Lemma 6.1: Let G be a rank 4 group and M be an intersection matrix for one of the nontrivial orbits. If the eigenvalues of the matrix are four distinct real numbers, exactly one of which is rational, then the irreducible characters in the permutation character consist of the identity character of G and three algebraically conjugate characters, each with the same degree.

Proof: From Theorem 4.2 we see that all the nonidentity characters in the permutation character must be real but not rational. There is a finite extension field of the rational numbers which is a splitting field for G. Consider all automorphisms of this field over the rational field. If σ is any such automorphism then σ fixes the permutation character for it is rational. Since the nonidentity characters assume values not in the rational field there must be automorphisms which permute these characters among themselves. Hence the characters are algebraically conjugate and hence the degrees of these characters must be the same.

Since the degrees of the three characters we are considering must be the same, each must have the value $(\ell_1 + \ell_1 (\ell_1 - 1) + \ell_1 (\ell_1 - 1)^2)/3$. When simplified, this value becomes $(\ell_1^3 - \ell_1^2 + \ell_1)/3$.

We now need a general theorem due to Frame. Theorem of Frame [4]: Let G be a transitive group of degree n. Let ℓ_i denote the lengths of the orbits of G_a. Let d_i denote the degrees of the absolutely irreducible representations of G contained in the permutation representation. Let r denote the rank of G. If the irreducible representations contained in the permutation representation are all distinct then the rational number

$$q = n^{r-2} \prod_{i=1}^{r} \frac{\ell_i}{d_i}$$

is an integer. If the irreducible representations all have rational characters, then the integer q is a square.

Using Frame's Theorem we find that: $(\ell_1^3-\ell_1^2+\ell_1+1)^2\cdot\ell_1\cdot\ell_1(\ell_1-1)\cdot\ell_1(\ell_1-1)^2/((\ell_1^3-\ell_1^2+\ell_1)/3)^3$ must be an integer. Since $\ell_1^3 - \ell_1^2 + \ell_1 + 1$ and $\ell_1^3 - \ell_1^2 + \ell_1$ have no factors in common, this is equivalent to showing that $\ell_1^3 (\ell_1 - 1)^3 \cdot 3^3 /(\ell_1^3 \cdot (\ell_1^2 - \ell_1 + 1)^3)$ is an integer which is equivalent to showing $3(\ell_1 - 1) /(\ell_1^2 - \ell_1 + 1)$ is an integer. This means $\ell_1^2 - \ell_1 + 1 \leq 3\ell_1 - 3$ or $(\ell_1 - 2)^2 \leq 0$.

This is true only for $\ell_1 = 2$. In this case the lengths of the orbits are 1, 2, 2, and 2. The dihedral group on seven letters is an example of such a group.

We will now show that this is the only case. If G is a primitive rank 4 group on seven letters then the orbits of G_a must have length 1, 2, 2, and 2, for otherwise another orbit would have length 1 and the group would be imprimitive. From Theorem 18.7 of [13] it is immediate that the order of the group must be 14. There are precisely two groups of order 14 and the only one which is a rank 4 group is the dihedral group on seven letters.

We note that in any of the three cases we considered if the length of the smallest orbit of G_a is 2 then the value of n must be less than or equal to 7. Hence we have indeed found all the maximal primitive rank 4 groups.

CHAPTER VII

RANK 4 REPRESENTATIONS OF KNOWN FINITE GROUPS

In this chapter we will discuss a procedure which can be used in finding the rank 4 representations of a finite group. The procedure is not an algorithm whose output is all the rank 4 representations of a known finite group. It is quite useful however in showing that a group has no rank 4 representations. We will illustrate the technique by finding the rank 4 representations of the Hall Janko simple group.

We begin with a finite group G. If G is to have a rank 4 representation then there must be three absolutely irreducible characters of G such that the sum of these three irreducible characters and the identity character form a character all of whose values are non-negative integers, for this would be the permutation character associated with a possible representation. If no such combination of characters exists then there can be no rank 4 representations of the group G.

All these combinations of three irreducible characters and the identity character need not be permutation characters. At present there are no necessary and sufficient conditions which guarantee that such a combination of characters would be a permutation character. There are several necessary conditions which can be used to eliminate several possibilities. Let us denote by χ' the character under consideration, that is, one which possibly may be a permutation character. The first requirement is that the degree of the character must divide the order of the group, since the group must be transitive on precisely that number of points. Another necessary requirement concerns the number of points fixed by a permutation. It is easy to see that if x is an element and a is an integer then the number of points fixed by x is not greater than the number of points fixed by x^a. The value of a permutation character is simply the number of points an element fixes. Thus another criterion for χ' to be a permutation character is that $\chi'(x) \leq \chi'(x^a)$ for all integers a and all elements x.

From the character χ' one can usually determine what size the orbits must be. For example, if $\chi'(x) = 1$, where x is an element of order 11, then each of the three nontrivial orbits associated with G_a must be a multiple of 11. By making use of several of these values of χ' one can usually show that the actual nontrivial orbit lengths, (ℓ_1, ℓ_2, ℓ_3), must be among a rather small set of triples of positive integers. Using the Theorem of Frame one can eliminate even more of these triples.

If one knows three numbers which may be the nontrivial orbit lengths of G_a corresponding to a rank 4 representation then one can try to construct intersection matrices corresponding to those orbit lengths. This process is best carried out on a digital computer. If two of the characters are complex conjugates then one has a two parameter system and if all the characters are real then one has a four parameter system, as was shown in Theorem 4.1. The first step is to pick parameters for one intersection matrix, usually the one corresponding to the nontrivial orbit of smallest length. Only those parameters which give an intersection matrix with all non-negative integer entries need to be considered. One can then calculate the characteristic equation of the matrix. Since one of the eigenvalues of the matrix must be the orbit length, ℓ , one has a cubic factor and $(x - \ell)$ as the other factor. If all the characters are rational then all the eigenvalues of the cubic equation must be rational by Theorem 4.2. Since they are also algebraic integers they must be rational integers. If two of the characters are complex conjugates and the intersection matrix is associated with a paired orbit then the roots of the cubic equation must be two complex values and one integer. If two of the characters are real and algebraically conjugate, then either one of the roots of the cubic equation has multiplicity greater than one, or else one of the roots is an integer and the other two are distinct irrational numbers. If all three characters are algebraically conjugate then either one of the roots of the cubic has multiplicity greater than one or else all three roots are irrational.

From the eigenvalues one can determine the multiplicities of the eigenvalues in the corresponding incidence matrices and thus in some cases the degrees of the irreducible rpesentations contained in the permutation representation. If these degrees do not agree with those which were known beforehand then this intersection matrix is not the one associated with the representation under consideration. If all the eigenvalues are integers then one can use the formulae developed in Chapter 5 to find the degrees of the characters. If two of the eigenvalues are complex then the formulae in Chapter 5 will also yield the degrees of the characters. If precisely two of the eigenvalues are irrational but all are real, then the multiplicity of the two irrational eigenvalues must be the same and hence one can solve for the degrees without finding out explicitly what the two irrational eigenvalues are. If all three of the eigenvalues are irrational but real then all the degrees must be equal and one can easily check to see if this is true.

If one has obtained one of the nontrivial intersection matrices it is usually the case that the other two nontrivial intersection matrices are uniquely determined by it. In any case there are only a relatively small number of possibilities which one must consider. The intersection matrices thus obtained can be used either to find the subgroup of G corresponding to G_a or else to show that no such subgroup exists. One procedure will be examined in the next chapter.

We now apply this method to the Hall Janko simple group, J, of order 604,800. If one represents J on the cosets of a particular subgroup of order 2160 then one obtains a rank 4 representation, as is stated on page 449 of [7]. The combination of the four irreducible characters of J associated with this representation is the only combination of characters which could give a rank 4 representation of any degree for J. This was verified using a computer. The degrees of the characters are 1, 90, 63, and 126. The permutation character, χ, is given by:

Order of an element, x:	1	7	2	4	8	6	12	10	10	2	6
$\chi(x)$:	280	0	40	4	2	1	1	0	0	12	0

Order of an element, x:	10	10	3	3	5	5	5	5	15	15
$\chi(x)$:	2	2	1	4	10	10	0	0	1	1

where this listing of elements corresponds to the one given on page 435 of [7].

Let us consider an element, a, of order 12. It fixes exactly one letter. The element, a^2, fixes all points fixed by a and those in the 2-cycles of a. Since $\chi(a^2) = 1$, a has no 2-cycles. a^3 has order 4 and fixes 4 points so there is precisely one 3-cycle in a. a^4 has order 3 and must fix either 1 or 4 points. The fixed points of a^4 consist of the original fixed point and all those contained in 2-cycles or 4-cycles. Since there are no 2-cycles and since fixing a 4-cycle would result in at least 5 fixed points we must conclude that a contains no 4-cycles. The cycles of a must consist of one of length 1, one of length 3, and then the rest must have lengths which are multiples of 6. Thus the orbits of the subgroup fixing a point must consist of one of length 1, two of lengths which are multiples of 6, and one whose length is congruent to 3 mod 6.

Let us consider another element, b, of order 15. It fixes exactly one letter. b^3 fixes 10 letters and so there are three 3-cycles in b. b^5 has order 3 and the number of fixed points of b^5 must be congruent to 1 mod 5. This means b^5 has exactly one fixed point and hence b has no 5-cycles. The nontrivial orbit lengths of the subgroup fixing a point must have one of the three arrangements,

(1) 15K, 15L, 15M+9,

(2) 15K, 15L + 3, 15M + 6, or

(3) 15K + 3, 15L + 3, 15M + 3,

where K, L, and M denote positive integers.

Since the subgroup fixing a letter must be transitive on each of its three nontrivial orbits, the length of each orbit must divide the order of the subgroup, which is 2160. We shall call this property D in the discussion which follows.

In case (1), using property D, one can show that M can assume only the values 1, 3, or 9. In each of these cases 15M + 9 has the form 6N. Thus we may suppose 15L = 6R + 3. Using property D this implies that L = 1, 3, or 9. Using property D again we see that 15K = 6S only when K = 2, 4, 6, 8, 12, and 16. Notice that K + L + M = 18 since 279 = 18·15+9. The following triples, (K,L,M,), are possible: (16,1,1), (12,3,3), (8,9,1), (8,1,9), (6,3,9), and (6,9,3).

In case (2), using property D, one can see that L can assume only the values 1, 3, or 7 and M can assume only the values

2 or 14. For each of these values of L and M, the numbers are of the form 6T. Thus 15K = 6U + 3. Hence K = 1, 3, or 9. The following triples, (K,L,M), are possible: (1,3,14), (3,1,14), and (9, 7, 2).

In case (3) K, L, and M can each assume only the values 1, 3, or 7. Each of the orbits would then have a length which would be a multiple of 6, which is not possible.

Using the Theorem of Frame it is possible to eliminate all but one of the above possibilities. Since all the characters are rational, the integer, q, mentioned in the theorem must be a square. In all the possibilities for case 1, 5^3 exactly divides q and thus these are eliminated. In the first two possibilities in case 2, an odd power of 3 exactly divides q and hence the orbit lengths of the representation must be 1, 135, 108, and 36, and indeed for these values q is a square.

Since the characters are rational all the eigenvalues of the intersection matrices must be integers. Using a computer all possible intersection matrices for the orbit of length 36 were examined and it was found that there was only one such that the multiplicities of the eigenvalues in the corresponding incidence matrix agreed with the known degrees of the characters. The other two intersection matrices could then be determined uniquely.

If we let ℓ_1 be the orbit of length 36, ℓ_2 be the orbit of length 108, and ℓ_3 be the orbit of length 135, then the intersection matrices are:

$$M_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 36 & 5 & 5 & 4 \\ 0 & 15 & 11 & 16 \\ 0 & 15 & 20 & 16 \end{pmatrix},$$

$$M_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 15 & 11 & 16 \\ 108 & 33 & 41 & 44 \\ 0 & 60 & 55 & 48 \end{pmatrix}, \text{ and}$$

$$M_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 15 & 20 & 16 \\ 0 & 60 & 55 & 48 \\ 135 & 60 & 60 & 70 \end{pmatrix}.$$

The characteristic equations of the three matrices M_1, M_2, and M_3 are, respectively, $(x - 36)(x - 6)(x + 6)(x + 4)$, $(x - 108)(x - 10)(x + 2)(x + 12)$, and $(x - 135)(x-15)(x+5)(x+5)$.

Relative to a suitable unitary transformation the incidence matrices are:

$$B_1 = \begin{pmatrix} 36 & & & & & & & & & \\ & -6 & & & & & & & \bigcirc & \\ & & \ddots & & & & & & & \\ & & & -6 & & & & & & \\ & & & & -4 & & & & & \\ & & & & & \ddots & & & & \\ & \bigcirc & & & & & -4 & & & \\ & & & & & & & 6 & & \\ & & & & & & & & \ddots & \\ & & & & & & & & & 6 \end{pmatrix},$$

$$B_2 = \begin{pmatrix} 108 & & & & & & & & & \\ & 10 & & & & & & & \bigcirc & \\ & & \ddots & & & & & & & \\ & & & 10 & & & & & & \\ & & & & -12 & & & & & \\ & & & & & \ddots & & & & \\ & \bigcirc & & & & & -12 & & & \\ & & & & & & & -2 & & \\ & & & & & & & & \ddots & \\ & & & & & & & & & -2 \end{pmatrix}, \text{ and}$$

$$B_3 = \begin{pmatrix} 135 & & & & & & & & & & \\ & -5 & & & & & & & & & \\ & & \ddots & & & & & \bigcirc & & & \\ & & & -5 & & & & & & & \\ & & & & 15 & & & & & & \\ & & & & & \ddots & & & & & \\ & & \bigcirc & & & & 15 & & & & \\ & & & & & & & -5 & & & \\ & & & & & & & & \ddots & & \\ & & & & & & & & & -5 \end{pmatrix},$$

where the multiplicities of the eigenvalues, in order, are 1, 90, 63, and 126.

CHAPTER VIII

APPLICATIONS OF INTERSECTION MATRICES

In this chapter we will give some more results about rank 4 groups which are obtained using intersection matrices. Information is obtained about the order of a primitive rank 4 group and also about the cardinality of some of the conjugate classes of elements of the group. The results are closely examined in the case in which one of the orbits associated with the rank 4 representation has length p, where p is a prime.

If a rank 4 group, G, is primitive then each intersection matrix must be irreducible, using Theorem 4.8 of [8]. From the Perron- Frobenius theory on page 53 of [6] this implies that the length of the orbit associated with an intersection matrix must be a simple root of the characteristic equation of the intersection matrix. If all the irreducible characters contained in the permutation character are rational then all the eigenvalues must be rational integers. In addition these eigenvalues must be such that when they are substituted in the appropriate formulae in Chapter 5 the values that they yield for the degrees of the irreducible characters must be positive integers.

Using a computer it is an easy, but somewhat long, procedure to find all possible intersection matrices, corresponding to a given set of orbit lengths, which are the intersection matrices for primitive rank 4 groups which have only rational irreducible characters in the permutation character.

If the length of the smallest nontrivial orbit of the subgroup fixing a point has length ℓ, then the other two orbits must have lengths less than or equal to $\ell(\ell-1)$ and $\ell(\ell-1)^2$. Given the length, ℓ, of such an orbit, there are only a finite number of possible orbit lengths corresponding to possible rank 4 groups. Using the computer one can then determine all possible intersection matrices corresponding to these orbit lengths. This procedure was carried out for the cases in which the smallest nontrivial orbit had length between 4 and 15 inclusive. If the eigenvalues of the intersection matrix corresponding to the orbit of smallest length are all simple roots of the characteristic equation, then the degrees of all three of the nontrivial irreducible characters can be determined from the formulae developed in Chapter 5. If one of the eigenvalues has multiplicity two then only one of the degrees can be obtained. The case in which one eigenvalue occurred with multiplicity three did not occur in the cases examined. In Table 1 are listed the possible orbit lengths and corresponding degrees of characters associated with the intersection matrix having only simple eigenvalues in its characteristic equation. In Table 2 are listed the possible orbit lengths and one degree for these are the cases in which one of the eigenvalues has multiplicity two. The lists in these two tables correspond to all possible primitive rank 4 groups all of whose irreducible characters in the

TABLE I

POSSIBLE ORBIT LENGTHS AND CHARACTER DEGREES

FOR RANK 4 REPRESENTATIONS

ORBIT LENGTHS				DEGREES OF CHARACTERS				$\|\Omega\|$
1	4	12	18	1	6	14	14	35
1	5	10	20	1	9	10	16	36
1	6	8	12	1	6	8	12	27
1	6	12	16	1	4	10	20	35
1	6	24	32	1	14	21	27	63
1	7	14	14	1	6	8	21	36
1	7	28	84	1	24	32	63	120
1	7	21	35	1	7	21	35	64
1	7	42	126	1	32	66	77	176
1	8	16	20	1	9	10	25	45
1	8	32	64	1	20	20	64	105
1	8	56	70	1	30	50	54	135
1	9	27	27	1	9	27	27	64
1	9	12	18	1	3	12	24	40
1	10	24	30	1	13	25	26	65
1	10	12	40	1	7	27	28	63
1	10	20	50	1	10	20	50	81
1	10	15	30	1	7	28	20	56
1	10	80	140	1	55	77	98	231
1	11	88	110	1	55	77	77	210
1	11	66	132	1	44	55	110	210
1	12	15	40	1	16	17	34	68
1	12	15	60	1	22	32	33	88
1	12	75	120	1	64	65	78	208
1	12	16	48	1	7	21	48	77
1	12	72	90	1	21	28	125	175
1	12	48	64	1	12	48	64	125
1	12	108	243	1	91	104	168	364
1	13	65	65	1	26	39	78	144
1	13	52	130	1	16	49	130	196
1	14	63	126	1	51	68	84	204
1	14	49	56	1	35	35	49	120
1	14	112	128	1	51	84	119	255
1	14	140	385	1	135	140	264	540

TABLE I (CONTINUED)

POSSIBLE ORBIT LENGTHS AND CHARACTER DEGREES

FOR RANK 4 REPRESENTATIONS

ORBIT LENGTHS				DEGREES OF CHARACTERS				$\|\Omega\|$
1	14	56	64	1	15	35	84	135
1	14	168	672	1	189	266	399	855
1	15	35	45	1	12	20	63	96
1	15	18	30	1	8	10	45	64
1	15	20	60	1	18	32	45	96
1	15	105	135	1	54	96	105	256
1	15	27	45	1	10	22	55	88
1	15	54	90	1	36	48	75	160
1	15	20	24	1	16	18	25	60
1	15	20	30	1	10	11	44	66
1	15	105	455	1	84	140	351	576
1	15	45	135	1	18	30	147	196
1	15	75	125	1	15	75	125	216
1	15	75	165	1	40	50	165	256
1	15	195	429	1	156	208	275	640
1	15	210	280	1	22	230	253	506

TABLE II

POSSIBLE ORBIT LENGTHS AND ONE CHARACTER

DEGREE FOR RANK 4 REPRESENTATIONS

ORBIT LENGTHS				DEGREE OF A CHARACTER	$\|\Omega\|$
1	5	5	5	5	16
1	5	5	5	10	16
1	7	14	28	28	50
1	7	21	21	21	50
1	8	8	8	8	25
1	9	9	9	6	28
1	9	9	9	21	28
1	10	10	15	10	36
1	10	15	30	20	56
1	10	15	30	35	56
1	12	12	24	12	49
1	12	18	18	12	49
1	12	16	16	24	45
1	12	16	16	20	45
1	14	14	35	14	64
1	14	14	56	34	85
1	14	21	28	14	64
1	14	21	63	54	99
1	14	28	42	34	85
1	14	28	56	44	99
1	14	14	28	38	57
1	14	35	35	50	85
1	14	21	21	18	57
1	14	42	42	54	99

permutation character are rational and whose smallest nontrivial orbit for the subgroup fixing a letter has length greater than or equal to 4 and also less than or equal to 15.

We will now examine the case in which the length of the smallest nontrivial orbit is 5.

In Table 2 there are two cases we must examine. In the first case the orbit lengths are 1, 5, 5, and 5 and one of the characters has degree 5. The intersection matrix for one of the orbits is

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 5 & 0 & 2 & 2 \\ 0 & 2 & 2 & 1 \\ 0 & 2 & 1 & 2 \end{pmatrix}.$$

Without loss of generality we may assume that the subgroup fixing a point, 16, breaks up into the following orbits:
{16},{1,2,3,4,5},{6,7,8,9,10}, and {11,12,13,14,15}. From the intersection matrix we see that we can assume that the subgroup fixing 1 has the orbit structure:
{1}, {16,6,7,11,12}, and two other orbits. Suppose an element, x, of order 5 fixes 16 and 1. It must then fix 2, 3, 4, 5, and also 6, 7, 11, and 12, and this in turn implies that it must fix all 16 points, that is, it is the identity. If p is a prime greater than 5 then $p \not\equiv 0$ (16) and thus if there were an element of order p it would necessarily fix a point. Since it would have to move

the points in orbits of length 1, p, p^2, etc. and since $p > 5$, such an element would necessarily fix all the points.

Suppose 25 divides the order of a rank 4 group associated with this intersection matrix. Since none of the orbits is a multiple of 25, a subgroup of order 25 must be elementary abelian. Let a and b, both of order 5, generate the subgroup. We may also suppose that a has the form (16) (1,2,3,4,5)$\cdots$. Since b centralizes a, and the only elements of order 5 centralizing (1,2,3,4,5) are powers of it, this constituent of b must be a power of (1,2,3,4,5). Thus ab^i, for some integer i, must fix 16, 1,2,3,4, and 5. Thus $ab^i = 1$ and hence b is simply a power of a which is a contradiction. Hence 5 exactly divides the order of the group. The order of the group must be of the form $2^j \cdot 3^k \cdot 5$. Brauer [1] has shown that if this group is simple, then it is either A_5, A_6, or the orthogonal group O(5,3). None of these groups has a rank 4 representation corresponding to the orbit lengths and degrees given above.

In the second case from Table 2 the orbit lengths are 1, 5, 5 and 5 and one of the degrees is 10. The other two non-trivial degrees must sum up to 5 and each degree must be able to be determined from at least one of the intersection matrices, as was seen in Chapter 5. Since this is not the case, this possibility cannot occur.

The only possibility listed in Table 1 is the case in which the orbit lengths are 1, 5, 10 and 20 and the degrees are

1, 9, 10, and 16. The intersection matrices for the orbits of lengths 5, 10, and 20, respectively, are

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 5 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 4 & 4 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 \\ 10 & 2 & 4 & 2 \\ 0 & 8 & 4 & 6 \end{pmatrix}, \text{ and}$$

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 4 & 4 & 2 \\ 0 & 8 & 4 & 6 \\ 20 & 8 & 12 & 11 \end{pmatrix}.$$

In this case let $\Omega = \{1, 2, . . ., 35, 36\}$ and let $\Gamma_0(36)$, $\Gamma_1(36)$, $\Gamma_2(36)$, and $\Gamma_3(36)$ be respectively $\{36\}$, $\{1,2,3,4,5\}$, $\{6, . . ., 15\}$, and $\{16, . . ., 35\}$. We will again show that 5 exactly divides the order of any primitive rank 4 group corresponding to these intersection matrices. Suppose 25 divides the order of the group. Then again we will have two elements a and b, each of order 5, which generate an elementary abelian subgroup of order 25. As was shown previously, we can find an element, $x = ab^i$, for some integer i, such that x fixes 36, 1, 2, 3, 4, and 5. Let us look at $\Gamma_1(1)$, $\Gamma_1(2)$, $\Gamma_1(3)$, $\Gamma_1(4)$, and $\Gamma_1(5)$. From the intersection matrices we see that each of these orbits must contain 36 and 4 points of $\Gamma_3(36)$. These orbits have the point 36 in common and hence cannot have any other points in common. Thus the 20 points of $\Gamma_3(36)$ must each occur once among these 5 orbits. This implies that x fixes all 20 points of $\Gamma_3(36)$ for it must take $\Gamma_1(i)$ into itself and since x fixes 36 it must fix the other 4 points, for i = 1, 2, 3, 4, and 5. Let us examine $\Gamma_1(6)$. This contains one point from $\Gamma_2(36)$ and four points from $\Gamma_3(36)$. If x does not fix 6, then $\Gamma_1(6)^x$ contains at least four points in common with $\Gamma_1(6)$ and this is a contradiction. Hence x fixes 6, and, as one can easily see, every other point in $\Gamma_2(36)$. Thus x is the identity and b is a power of a which is a contradiction. Thus 5 exactly divides the order of the groups.

We will now show that the order of any group associated with these intersection matrices must have an order of the form $2^j \cdot 3^k \cdot 5$. If p, a prime greater than 5, divides the order of the group then any element of order p in the group must fix at least one letter for $p \not\equiv 0$ (36). Suppose y is an element of order p which fixes 36. It must also fix 1, 2, 3, 4, and 5 since $p > 5$. Continuing in a manner similar to the one stated above one can show that y fixes all the elements of Ω. Thus the order of the groups must be of the form $2^j \cdot 3^k \cdot 5$. The three simple groups which have an order of this form do not have a rank 4 representation corresponding to these matrices. We have thus proved the following theorem:

Theorem 8.1: There are no simple groups which have a primitive rank 4 representation such that all the irreducible characters in the permutation character are rational and such that the smallest nontrivial orbit has length 5.

We will now actually give some examples of groups which have rank 4 representations corresponding to these intersection matrices given above. In order to make the calculations somewhat easier we include some results of general interest.

Let G be a group and let H be a subgroup of G. Let σ be an involutory automorphism of G which takes H into itself. Let G* denote the semi-direct product of G and σ and let H* denote the semi-direct product of H and σ. Suppose ρ is an irreducible character of G. We want to investigate $\rho|^{G^*}$. For ease of writing we will denote the element, $g*\sigma$, of G* by g*, and $\rho|^{G^*}$ by ρ^*. The element x will denote any element of G*.

We will first investigate ρ^* (g*). The formula for ρ^* (g*) is $\rho^*(g^*) = (|G|)^{-1} \sum_{x \in G^*} \mathring{\rho}\ (x^{-1}g^*x)$ where the value of $\mathring{\rho}$ is ρ if the argument $x^{-1}g^*x$ is in G and is zero if $x^{-1}g^*x$ is not in G. Since all elements $x^{-1}g^*x$ are not in G for any $x \in G^*$, we conclude that $\rho^*(g^*) = 0$.

We will now examine $\rho^*(g)$. Again we have $\rho^*(g) = (|G|)^{-1} \sum_{x \in G^*} \mathring{\rho}(x^{-1}gx)$. We note that for every element

$g \in G$ we have $\rho(g_1^{-1} g\, g_1) = \rho(g_1^{-1} g\, g_1)$ and for $g_1{*}$ we have $\dot{\rho}((g_1{*})^{-1} g g_1{*}) = \rho(g_1^{-1} g^{\sigma} g_1)$. Thus $\rho{*}(g) = \rho(g) + \rho(g^{\sigma})$. If we denote $\rho(g^{\sigma})$ by $\rho^{\sigma}(g)$ we have $\rho{*}(g) = \rho(g) + \rho^{\sigma}(g)$.

We can now compute the number of irreducible characters of $G{*}$ which are contained in $\rho{*}$. If we consider the inner product $(\rho{*}, \rho{*})_{G*}$ we find that

$$(\rho{*}, \rho{*}) = (2|G|)^{-1}\Big(\sum_{g\in G} \Big(\rho(g) + \rho^{\sigma}(g)\Big)\Big(\overline{\rho(g) + \rho^{\sigma}(g)}\Big)\Big) =$$

$$= (2|G|)^{-1} \sum_{g\in G} \Big(\rho(g)\overline{\rho(g)} + \rho^{\sigma}(g)\, \overline{\rho^{\sigma}(g)} + \rho(g)\, \overline{\rho^{\sigma}(g)} + $$

$$+ \rho^{\sigma}(g)\, \overline{\rho(g)}\Big).$$

If ρ does not equal ρ^{σ} then the usual orthogonality relations for irreducible characters give us

$$(\rho{*}, \rho{*}) = (2|G|)^{-1} \sum_{g\in G} \Big(\rho(g)\overline{\rho(g)} + \rho^{\sigma}(g)\, \overline{\rho^{\sigma}(g)}\Big) = \frac{2|G|}{2|G|} = 1$$

and in this case $\rho{*}$ is an irreducible character of $G{*}$. If ρ does equal ρ^{σ} then we have

$(\rho{*}, \rho{*}) = (2|G|)^{-1}(|G| + |G| + |G| + |G|) = 2$ and thus $\rho{*}$ is the sum of two distinct irreducible characters of $G{*}$. If we denote the two irreducible characters by θ_1 and θ_2 then $(\rho{*},\theta_1)_{G*} = (\rho{*}, \theta_2)_{G*} = 1$. Using the Law of Reciprocity we have $(\rho,\theta_1|_{G*})_{G*} = (\rho,\theta_2|_{G*})_{G*} = 1$ and hence the degrees of θ_1 and θ_2

are each not less than the degree of ρ. Since the degree of $\theta_1 + \theta_2$ is twice the degree of ρ, we know that the degrees of ρ, θ_1 and θ_2 are the same.

We now come back to the task of finding some examples of groups which correspond to the intersection matrices we have given previously. It is well known that the degrees of the irreducible characters of a group divide the order of the group. The least common multiple of 16, 9, and 10 is 720 and thus 720 must divide the orders of the groups we are seeking.

The symmetric group on 6 letters, S_6, has order 720. A subgroup of order 20 is the normalizer of an S(5), a Sylow 5 subgroup of S_6, and has index 36 in S_6. Let us denote S_6 by G and $N_G(S(5))$ by N. The character $1_N|^G$ is the sum of five irreducible characters of G and hence G represented on the cosets of N has rank 5. We list the five characters.

	1^6	$1^4 2$	$1^3 3$	$1^2 4$	$1^2 2^2$	123	15	6	24	2^3	3^2
1_G	1	1	1	1	1	1	1	1	1	1	1
χ_1	5	3	2	1	1	0	0	-1	-1	-1	-1
χ_2	5	-1	-1	1	1	-1	0	0	-1	3	2
χ_3	9	-3	0	1	1	0	-1	0	1	-3	0
χ_4	16	0	-2	0	0	0	1	0	0	0	-2

The complete character table of S_6 can be found on page 266 of [12]. The heading for each column of this table describes the cycle structure of the various permutations of S_6.

In Section 162 of [2] it is shown that the outer automorphism group of S_6 has order 2. We can choose the automorphism, σ, in such a way that $N^{\sigma} = N$. The automorphism interchanges elements of the form $1^3 3$ with those of the form 3^2. Thus $\chi_1^{\sigma} \neq \chi_1$ and $\chi_2^{\sigma} \neq \chi_2$. There are two other irreducible characters of S_6 of degree 5 but each of them assumes a value of -3 for at least one element of G. Hence we must have $\chi_1^{\sigma} = \chi_2$ and $\chi_2^{\sigma} = \chi_1$. The character, χ_3, is fixed by σ for the only other character of degree 9 assumes the value 3 on an element of G. Since χ_4 is the only character of degree 16 in S_6 we have $\chi_4^{\sigma} = \chi_4$.

If we consider the semi-direct product of G with σ we have $G*\sigma$ which we denote by G*. From the general results we obtained earlier we know that $\chi_1|^{G*}$ and $\chi_2|^{G*}$ are the same irreducible character of G* and that $\chi_3|^{G*}$ and $\chi_4|^{G*}$ each are the sum of two distinct irreducible characters of G*. Let us denote $N*\sigma$ by N*. The inner product, $(1_{N*}|^{G*},\chi_i|^{G*})_{G*}$ has the same value as $(1_N|^G,\chi_i)_G$ because, as has been shown previously, any character of G induced to G* vanishes off of G. Thus $(1_{N*}|^{G*},\chi_i|^{G*})_{G*}$ has the value 1 for i = 1, 2, 3, and 4. This implies that $1_{N*}|^{G*}$ contains four irreducible characters. Their degrees are 1, 10, 9, and 16. Thus G* represented on the cosets of N* has a rank 4 representation.

We must now show that this representation we have corresponds to the three intersection matrices we have previously given. We know the degrees of this representation to be 1, 9, 10, and 16 and we know that $|\Omega| = 36$. Thus the length of the smallest nontrivial orbit of the subgroup fixing a point must be less than 12. Therefore the intersection matrices corresponding to this representation of S_6^* must be among the ones which are summarized on Tables 1 and 2. There is one other possibility besides the one we have given previously. It occurs in Table 2 and is the case in which the orbit lengths are 1, 10, 10, and 15. The subgroup fixing a letter, in this case N*, must be divisible by each of its orbit lengths since the subgroup is transitive on each of them. Since $15 \nmid 40$, we can rule out this possibility. We have thus shown that S_6^* represented on the cosets of N* does indeed correspond to the three intersection matrices mentioned earlier which occur in Table 1.

We consider now the alternating group on six letters, A_6. The character table of A_6 is

	1	(ab)(cd)	(abc)	(abcde)	(acebd)	(abcd)(ef)	(abc)(def)
χ_o	1	1	1	1	1	1	1
χ_1	5	1	2	0	0	-1	-1
χ_2	5	1	-1	0	0	-1	2
χ_3	9	1	0	-1	-1	1	0
χ_4	10	-2	1	0	0	0	1
χ_5	8	0	-1	$\frac{1}{2}(1+\sqrt{5})$	$\frac{1}{2}(1-\sqrt{5})$	0	-1
χ_6	8	0	-1	$\frac{1}{2}(1-\sqrt{5})$	$\frac{1}{2}(1+\sqrt{5})$	0	-1

and can also be found on page 337 of [5]. The elements on top denote the cycle structure of the various conjugate classes.

Let us denote A_6 by G and the normalizer in A_6 of a Sylow 5 subgroup by N. If we represent G on the cosets of N we obtain a rank 6 representation. If χ denotes the permutation character for this representation then $\chi = \chi_o + \chi_1 + \chi_2 + \chi_3 + \chi_5 + \chi_6$.

In the symmetric group on six letters, S_6, there is an element, τ, of order 4 and of the form (abcd)(e)(f), which normalizes the Sylow 5 subgroup, S(5), of N. If S(5) is generated by an element a, then $\tau^{-1}\, a\, \tau = a^2$. Thus $\chi_o^{\tau} = \chi_o$, $\chi_1^{\tau} = \chi_1$, $\chi_2^{\tau} = \chi_2$, and $\chi_3^{\tau} = \chi_3$. Since $\chi_5^{\tau}(a) = \chi_5(a^{\tau}) = \chi_5(a^2) = \chi_6(a)$ we have $\chi_5^{\tau} = \chi_6$ and $\chi_6^{\tau} = \chi_5$.

As we have seen before there is an outer automorphism of S_6 which also acts on A_6. It is of order 2, and let us choose it so that it also centralizes the S(5) under consideration. Let us denote this automorphism by σ. We see that $\chi_o^{\sigma} = \chi_o$, $\chi_3^{\sigma} = \chi_3$, and $\chi_5^{\sigma} = \chi_5$, and $\chi_6^{\sigma} = \chi_6$. The last two equalities hold because a^{σ} is either a or a^{-1}. Since σ interchanges elements of the form (abc) and (abc)(def) we see that $\chi_1^{\sigma} = \chi_2$ and $\chi_2^{\sigma} = \chi_1$.

We now consider the element $\nu = \sigma\, \tau$ which is contained in the semi-direct product of S_6 and σ. We see that $\nu^2 = (\sigma\tau)^2 = \sigma^2\, \tau^{\sigma}\, \tau$ which is either τ^2 or 1 depending on whether σ fixes τ or takes it to τ^{-1}. Thus ν^2 is in A_6. If we denote by G* the subgroup of $S_6 * \sigma$ generated by A_6 and ν we obtain a group which has A_6 as a subgroup of index 2. Since ν also normalizes N we can denote the subgroup generated by N and ν by N*. We note that $\chi_o^{\nu}=\chi_o$, $\chi_1^{\nu}=\chi_2$, $\chi_2^{\nu}=\chi_1$, $\chi_3^{\nu}=\chi_3$, $\chi_5^{\nu}=\chi_6$, and $\chi_6^{\nu}=\chi_5$. From calculations similar to the ones carried out in the previous example we can see that $1_{N*}|^{G*} = 1_{G*} + \chi_1|^{G*} + \theta + \chi_5|^{G*}$ where θ is one of the irreducible characters of G* contained in $\chi_3|^{G*}$. The degrees of the characters are 1, 9, 10, and 16. As we have seen before, this gives us a rank 4 representation which corresponds to the 3 intersection matrices given earlier in the chapter. This group G* has order 720.

Some of the material contained in the first part of this chapter can be generalized. We do this in the theorems that now follow.

Theorem 8.2: Let G be a group which has a primitive rank 4 representation. If the orbit lengths of the subgroup fixing a point are 1, p, ℓ_2, and ℓ_3, where ℓ_2 and ℓ_3 are not less than the prime p, and if $q > p$ is a prime which does not divide $|\Omega|$, then $q \nmid |G|$.

Proof: Suppose such a prime, q, does divide the order of the group. Since $|\Omega| \not\equiv 0 \ (q)$, any element, $x \in G$, of order q must fix a point. Suppose x fixes the point 1. Then x must also fix the points of $\Gamma_1(1)$, where Γ_1 has length p, for the nontrivial cycles of x will have length at least q. In a similar fashion one can see that the Γ_1 orbit of each of these p points will be fixed pointwise by x. If this process is continued we obtain a list of points that are fixed by x. In Theorem 1.12 of [8] it is shown that because G is primitive every point of Ω can be reached by such a chain of orbits. Hence x fixes all the points of Ω. This is a contradiction and the theorem is proved.

Theorem 8.3: Let G be a group which has a primitive rank 4 representation. Suppose that the orbit lengths of the subgroup fixing a point are 1, p, ℓ_2, and ℓ_3 where p is a prime and $p \leq \ell_2 < p^2$ and $p \leq \ell_3 < p^2$ and $|\Omega| \not\equiv 0$ (p). Let M_1 be the intersection matrix associated with the orbit of length p. If p occurs as an entry in the matrix precisely once, then p exactly divides the order of G.

Proof: Since G_{p+1} is transitive on $\Gamma_1(p+1)$, the orbit of length p, $p \mid |G_{p+1}|$ and hence $p \mid |G|$.

Suppose $p^2 \mid |G|$. Then $p^2 \mid |G_{p+1}|$ for $p \nmid [G:G_{p+1}]$. Suppose a and b are two elements of order 5 which generate an elementary abelian p group of order p^2. Such a subgroup exists because we cannot have an element which fixes a point and has a cycle of length p^2. We may assume that a, b $\in G_{p+1}$ and $a = (p+1)(1,2,\ldots,p)\cdots$. Since only powers of $(1,2,\ldots,p)$ centralize it, and since b centralizes a we must be able to find an integer i such that $x = ab^i$ fixes $p + 1, 2, \ldots,$ and p. Thus we have an element x of order p which fixes these p + 1 points. Let us examine $\Gamma_1(1)$, $\Gamma_1(2)$, ..., and $\Gamma_1(p)$. Because p occurs exactly once in the intersection matrix M_1, each of these orbits contains points from at least two different orbits associated with p + 1. x must map $\Gamma_1(1)$ to $\Gamma_1(1)$, ..., and $\Gamma_1(p)$ to $\Gamma_1(p)$ and it must also map the points of each orbit associated with p + 1 within each of these p orbits into themselves. These sets have cardinality less than p and hence x must fix all the points of $\Gamma_1(1)$, $\Gamma_1(2)$, ..., and $\Gamma_1(p)$. Continuing on we obtain a list of points fixed by x. Using the same result of Higman that is contained in Theorem 8.2 we see that this list includes all the points of Ω. Hence x is the identity and b is a power of a which is a contradiction. Hence $p^2 \nmid |G|$.

We now want to use the intersection matrices to tell us something about the size of conjugate classes of elements of a group G when G has a rank 4 representation. We then apply it to the case in which one of the orbits associated with the rank 4 representation has length p.

Theorem 8.4: Let G have a rank 4 representation. The number of elements in a conjugate class of G each of whose members fixes no letters in the representation must be an integer multiple of the greatest common divisor of the lengths of the three nontrivial orbits of the subgroup fixing a point.

Proof: Let C denote the element in the group ring of G consisting of the sum of all elements in one conjugate class of G. This conjugate class is chosen so that each element of G in it fixes no points in the rank 4 representation. Since C is in the center of the group ring, the matrix representation, P (C), is in the commuting algebra of P and hence is a linear combination of B_o, B_1, B_2, and B_3, the incidence matrices. Each of these matrices has $(1, 1, \ldots, 1)^T$ as an eigenvector and the corresponding eigenvalue in each case is the length of the orbit associated with the matrix, since each incidence matrix has exactly this many 1's in each of its rows. The matrix, P (C), has $(1, 1, \ldots, 1)^T$ as an eigenvector and this corresponds to the eigenvalue which is the cardinality of C.

P (C) can be represented by $\sum_{i=o}^{3} b_i B_i$ where the b_i are non-negative integers. Since each element in the conjugate class under consideration fixes no element of Ω, $b_o = 0$. B_1, B_2, B_3, and P (C) may all be simultaneously diagonalized by an appropriate unitary matrix, U, and the eigenvalues ℓ_1, ℓ_2, ℓ_3, and $|C|$ must correspond in relation to their position on the diagonal since each is the eigenvalue of greatest magnitude in each of the matrices. This comes from results on page 66 of [6]. Thus $|C| = b_1\ell_1 + b_2\ell_2 + b_3\ell_3$ and the result is proved.

We now specialize this to the case where one of the orbits of the subgroup fixing a point has length p, when p is a prime. We will also assume that the rank 4 representation is primitive. Using the result that if G is a primitive group and $1 \leq \ell_1 \leq \ell_2 \leq \dots \leq \ell_k$ are the lengths of the orbits of G_a then g.c.d.$(\ell_1, \ell_k) \neq 1$ for $1 \leq i \leq k$, one can see in the rank 3 case that if one of the orbits of the subgroup fixing a point has length p then the other nontrivial orbit must have a length a multiple of p. In the case of rank 5 groups the Janko simple group of order 175,560, when represented on the cosets of the subgroup of order 660, has orbit lengths 1, 11, 12, 110, and 132. Thus in the rank 5 case it is not necessarily true that if one of the orbits has length a prime, then all the other nontrivial orbits must have length a multiple of that prime. In the rank 4 case the validity of the result is an open question. We therefore state the following corollary to the above theorem in the following form.

Theorem 8.5: If G is a primitive rank 4 group and if each of the nontrivial orbits of the subgroup fixing a point has length a multiple of p, a prime, then the cardinalities of the conjugate class of G each of whose elements fixes no points of Ω must all be multiples of p.

REFERENCES

1. Brauer, R., "On simple groups of order $5 \cdot 3^a \cdot 2^b$," Bull. Amer. Math. Soc., 74 (1968), 900 - 903.

2. Burnside, W., Theory of Groups of Finite Order. Dover, New York, 1955.

3. Curtis, C. W. and I. Reiner, Representation Theory of Finite Groups and Associative Algebras. Interscience, New York, 1962.

4. Frame, J. S., "The double cosets of a finite group," Bull. Amer. Math. Soc., 47 (1941), 458 - 467.

5. Frobenius, G., "Über die Composition der Charaktere einer Gruppe," Sitzungsberichte der Königlich Preussichen Akademie der Wissenschaftern zu Berlin, (1899), 330 - 339.

6. Gantmacher, F. R., The Theory of Matrices. Vol. II. Chelsea, New York, 1960.

7. Hall, M. and D. Wales, "The simple group of order 604,800," J. Algebra, 9 (1960), 417 - 450.

8. Higman, D. G., "Intersection matrices for finite permutation groups," J. Algebra, 6 (1967), 22 - 42.

9. ____________, "Finite permutation groups of rank 3," Math. Zeitschrift, 86 (1964), 145 - 156.

10. ____________, "Primitive rank 3 groups with a prime subdegree," Math. Zeitschrift, 91 (1966), 70 - 86.

11. Janko, Z., "A new finite simple group with abelian Sylow 2 subgroups and its characterization," J. Algebra, 3 (1966), 147 - 186.

12. Littlewood, D. E., The Theory of Group Characters and Matrix Representations of Groups. Oxford, London, 1958.

13. Wielandt, H., Finite Permutation Groups. Academic, New York, 1964.