A S T U D Y O F S O M E F I N I T E

P E R M U T A T I O N G R O U P S

by Peter M. Neumann

April, 1966

The Queen's College,

O x f o r d

ABSTRACT

This thesis records an attempt to prove the two conjectures:

Conjecture A Every finite non-regular primitive permutation group of degree n contains permutations fixing one point but fixing at most $n^{\frac{1}{2}}$ points.

Conjecture C Every finite irreducible linear group of degree $m > 1$ contains an element whose fixed-point space has dimension at most $\frac{1}{2}m$.

Variants of these conjectures are formulated, and C is reduced to a special case of A. The main results of the investigation are:

Theorem 2 Every finite non-regular primitive permutation group of degree n contains permutations which fix one point but fix fewer than $\frac{1}{4}(n + 3)$ points.

Theorem 3 Every finite non-regular primitive soluble permutation group of degree n contains permutations which fix one point but fix fewer than $n^{7/18}$ points.

Theorem 4 If H is a finite group, F is a field whose characteristic is 0 or does not divide the order of H, and M is a non-trivial irreducible H-module of dimension m over F, then there is an element h in H whose fixed-point space in M has dimension less than $\frac{1}{2}m$.

Theorem 5 If H is a finite soluble group, F is any field, and M is a non-trivial irreducible H-module of dimension m over F, then there is an element h in H whose fixed-point space in M has dimension less than $\frac{7}{18} m$.

Proofs of these assertions are to be found in Chapter II; examples which show the limitations on possible strengthenings of the conjectures and results are marshalled in Chapter III. A detailed formulation of the problems and results is contained in §1.

PREFACE

I owe my interest in the problems described in this thesis to a rich correspondence with Dr James Wiegold. It was the examples described here in §11, which we finally arrived at *via* some far less elegant examples of my own, which first pointed the way. Very little of §§ 3, 11 are my own results, and only part of the work in §7 is original.

I am very grateful to my supervisor, Professor G. Higman, F.R.S., for his kind encouragement and for many suggestions, and for a wide background of valuable instruction and supervision more generally; and to Dr Wiegold who, unwittingly at the time, set me off on this investigation, and whose friendly influence has helped in many, many ways.

The Queen's College,
Oxford.

Peter M. Neumann

April, 1966.

CONTENTS

CHAPTER I: PROLEGOMENA

1. Statement of the problems and results.

In a letter dated 7th October 1963 Dr James Wiegold asked the following question, which had arisen in joint work of his with Dr J.A.H. Shepperd. He wrote:

"Let G be primitive on n symbols and let $\mu(G)$ be the most symbols moved by an element of G which does not move everything; and let $g(n)$ be the minimum of all $\mu(G)$, G ranging over the primitive groups of degree n. What can be said about $g(n)$? We hope it will be near $n-1$, . . . "

I shall give examples in Chapter III to show that this hope is in vain: there are primitive permutation groups in which every element fixing one point fixes many. Nevertheless, 'many' cannot be interpreted too freely: I show, among other things, that a primitive, non-regular permutation group of degree n always contains permutations fixing one point, but fixing fewer than $(n+3)/4$ points. It seems very unlikely that this result is near to the whole truth, and most of this essay consists of an effort to do better, together with variations on the main theme which arose naturally in the investigation.

We will be primarily concerned with the following functions.

Let G be a permutation group of finite degree, and, for $g \in G$, let $\chi(g)$ denote the number of points fixed by g. Then define[1]:

$$\mu(G) = \min \{ \chi(g) \mid g \in G, \ \chi(g) \geq 1 \};$$

$$f(n) = \max \{ \mu(G) \mid G \text{ primitive and not regular, of degree } n \};$$

$$f_{trans}(n) = \max \{ \mu(G) \mid G \text{ transitive, not regular, of degree } n \};$$

$$f_{sol}(n) = \max \{ \mu(G) \mid G \text{ soluble, primitive, not regular, of degree } n \};$$

$$f_{rn}(n) = \max \{ \mu(G) \mid G \text{ primitive, containing a regular normal subgroup of degree } n \}.$$

In case the relevant set of permutation groups is empty, the integer on the left side of the equation is defined to be 1. To illustrate the information which these functions carry: for example, if $f(n) = m$, then

(i) every primitive, non-regular permutation group of degree n contains a permutation fixing one point but fixing at most m points; and

(ii) if there is a primitive, non-regular group of degree n (i.e., in this example, if $n > 2$) then there is such a group in which every permutation fixing one point fixes at least m points.

The functions f, f_{sol}, f_{rn} seem to depend more on the arithmetic structure of their argument n than on the size of n. For example, a primitive soluble group necessarily has prime-power degree

---

1) Warning: this is a change from the notation of page 1.

(Galois: see Lemma 3.8), so that $f_{sol}(n) = 1$ if n is not a power of a prime. Again, a well-known theorem of Burnside ([B] §251, pp 339-341) asserts that a non-soluble transitive group of prime degree - which is necessarily primitive, then - is 2-fold transitive. A non-trivial transitive group is well-known to contain permutations which have no fixed points, so that a 2-fold transitive group contains permutations fixing precisely one point, unless its degree is 2 . Thus if G is non-soluble and of prime degree then $\mu(G) = 1$; if G is soluble and of prime degree then it is easy to see (Lemmas 3.8 and 3.6) that either G is regular or again $\mu(G) = 1$. Therefore,

$$f_{trans}(n) = f(n) = f_{sol}(n) = f_{rn}(n) = 1$$

if n is prime.

To have some measure of how large these functions may be I define

$$\left.\begin{aligned} \delta_* &= \limsup \frac{f_*(n)}{n} \\ \gamma_* &= \limsup \frac{\log f_*(n)}{\log n} \end{aligned}\right\} \quad * \in \{\ , \text{trans}, \text{sol}, \text{rn}\}\ .$$

Thus for any positive ε there are numbers A_* , B_* such that, for all n ,

$$f_*(n) < (\delta_*+\varepsilon)n + A_*$$

$$f_*(n) < B_* n^{(\gamma_*+\varepsilon)} .$$

For transitive groups in general the picture is almost complete: it is easy to prove (§5)

Theorem 1 (i) For all $n \geq 2$, $f_{trans}(n) \leq \frac{1}{2}n$; in other words, every transitive, non-regular permutation group of degree $n \geq 2$ contains permutations fixing one point but fixing at most $\frac{1}{2}n$ points.
(ii) If n is even then $f_{trans}(n) = \frac{1}{2}n$.

Consequently, $\delta_{trans} = \frac{1}{2}$ and $\gamma_{trans} = 1$.

The best answer we can give to Dr Wiegold's question is

Theorem 2 (i) For all $n \geq 2$, $f(n) < \frac{1}{4}(n+3)$; that is, every primitive, non-regular group of degree $n \geq 2$ contains permutations fixing one point but fixing fewer than $\frac{1}{4}(n+3)$ points.
(ii) For infinitely many values of n, $f(n) \geq n^{1/3}$; that is, for suitable n there are primitive, non-regular groups of degree n in which every permutation fixing one point fixes at least $n^{1/3}$ points.

There is a huge gap between the upper bound given by (i) and the lower bound for $f(n)$ given by (ii). In fact, I would answer Dr Wiegold's question with

Conjecture A $\delta = 0$; $\gamma \leq \frac{1}{2}$; and, even more strongly, $f(n) \leq n^{\frac{1}{2}}$ for all n.

The last two clauses of this conjecture look reasonable on the evidence available and provide a useful target at which to aim - but I shall not be heartbroken if the last, or both of them, turn out to be false. I cannot believe, however, that δ is not zero.

For certain classes of primitive groups I can do better than Theorem 1. Namely,

Theorem 3 (i) For all $n \geq 1$, $f_{sol}(n) < n^{7/18}$;

(ii) for all $n \geq 2$, $f_{rn}(n) < n(\log n)^{-\frac{1}{2}}$.

(iii) For infinitely many values of n, $f_{rn}(n) \geq f_{sol}(n) \geq n^{1/3}$.

The situation is far more satisfactory, therefore, as far as soluble groups only are concerned: $\delta_{sol} = 0$ and $1/3 \leq \gamma_{sol} \leq 7/18$.

Actually I would expect, but have been unable to prove:

Conjecture B A primitive, non-regular, soluble permutation group of degree n always contains permutations fixing one point but fixing at most $n^{1/3}$ points. That is, $f_{sol}(n) \leq n^{1/3}$; and $\gamma_{sol} = 1/3$.

For primitive groups containing regular normal subgroups Theorem 3 does at least imply that $\delta_{rn} = 0$. And even if Conjecture A turns out to be false,

Conjecture A_{rn} $\qquad f_{rn}(n) \leq n^{\frac{1}{2}}$

must surely be true. Perhaps Theorem 3 and Conjecture A_{rn} are not really as special as they seem. All the examples I know of primitive groups G in which $\mu(G)$ is reasonably large either contain regular normal subgroups, or contain primitive subgroups containing regular normal subgroups. In fact, the only example with which I am familiar, of a primitive group G containing no regular subgroup and for which $\mu(G) > 1$, is Janko's simple group, of order 175,560, acting by conjugation on its Sylow 2-subgroups: every element which normalises one Sylow 2-subgroup normalises at least two. In this case $\mu(G) = 2$, for an element of order 7 normalises precisely two Sylow 2-subgroups, while the degree n is 1045 (see [5], especially §VI).

There is a natural analogue for linear groups of these problems and results on permutation groups. If H is a group, M is a finite-dimensional H-module over a field F, and $h \in H$, define $\phi(h)$, or, where necessary to avoid ambiguity, $\phi_M(h)$, to be the dimension of the fixed-point space of h in M; and put $m = \dim M$.

Conjecture C If M is a non-trivial irreducible FH-module then there exists $h \in H$ such that $\phi(h) \leq \frac{1}{2}m$.

The restriction to non-trivial modules is trivially necessary, but we could, without losing generality, restrict further to faithful modules M. For, if $C_H(M)$ is the centralizer of M in H, that is, the kernel of the representation of H on M, then M is naturally a faithful $H/C_H(M)$-module, trivial if and only if H acts trivially on M, irreducible if and only if H acts irreducibly on M, and furthermore, if $\bar{h}$ is the image of $h \in H$ under the canonic epimorphism of H onto $H/C_H(M)$, then $\bar{h}$ and h have the same fixed-point space in M. Where necessary or convenient (in §§ 7, 8) we shall assume therefore that M is a faithful FH-module. As one step towards verifying Conjecture C I prove:

Theorem 4 If the characteristic of the field F is 0 or does not divide the order of the group H, and if M is an FH-module of dimension $m > 0$, such that, for all $h \in H$, $\phi(h) \geq \frac{1}{2}m$, then M contains a non-zero trivial FH-submodule.

This theorem verifies the conjecture in a slightly strengthened form for the cases it covers: direct consequences (with the same hypotheses as the theorem) are

Corollary 4(i) If M is irreducible then there exists an element h in H such that $\phi(h) < \frac{1}{2}m$.

Corollary 4(ii) If for all h in H,

$$\phi(h) \geq \tfrac{1}{2}m + k \qquad (k \geq 0),$$

then M contains a trivial FH-submodule of dimension $2k + 1$.

This latter result comes from the fact that, under the hypotheses of Theorem 4, M is completely reducible, that is, every submodule of M is complemented in M. The proof of the theorem is at heart only very elementary character theory, and will be found in §7. That section also contains a proof that of F only the characteristic is relevant for Conjecture C.

Further evidence is supplied by Lemma 7.4 from which it follows that if H is a group which gives a counterexample to the conjecture, then H has a composition factor which cannot be generated by two of its elements. No such finite simple group is at present known to exist.

Conjecture C is certainly not true in the strong form given by Corollary 4(ii) in general. There are examples, described in §12, of faithful modules M of dimension m, such that, for all $h \neq 1$ in H, $\phi(h) = m - 1$, and yet the trivial submodule of M is only 1-dimensional. All the same, Theorem 4 may well be true without restriction on the field F.

For a soluble group H the conjecture is certainly correct, for (see above) the composition factors of H are all cyclic.

However we can improve on Theorem 4 without restriction on the field in this case:

Theorem 5 If H is a finite soluble group, M is a non-trivial irreducible FH-module of dimension m, then

(i) there exists $h \in H$ such that $\phi(h) < \frac{7}{18} m$;

(ii) if the characteristic of F is 2 then there exists $h \in H$ such that $\phi(h) < \frac{1}{3} m$.

I would expect, but have not been able to prove, that this bizarre '$< 7/18$' can be replaced by '$\leq 1/3$':

Conjecture D If H is soluble and M is a non-trivial irreducible FH-module of dimension m then there exists h in H such that

$$\phi(h) \leq \frac{1}{3} m .$$

Conjecture B is equivalent to this statement with a prime field $GF(p)$ for F (Lemmas 3.8 and 3.6), and therefore, by Lemma 7.1, to Conjecture D for any field whose characteristic is not 0. However, Lemma 7.2 shows that D is true if and only if it is true for fields of non-zero characteristic. Thus in fact, Conjectures B and D are equivalent.

These representation-theoretic questions arise partly as analogues of the questions on permutation groups, partly as tools for studying primitive permutation groups which contain regular abelian normal subgroups. They have their analogues for operator groups in general, and these are needed for primitive permutation groups having regular (not necessarily abelian) normal subgroups.

In this generality I can prove very little - just enough to give Theorem 3(ii). Conjecture A_{rn} is equivalent (by Lemmas 3.7 and 3.6) to

Conjecture E If H is a non-trivial group of automorphisms of the finite group A, and if A is H-simple (that is, the only H-invariant subgroups are the trivial group and A itself), then there is an element h in H such that $|\mathrm{fix}_A(h)| \leq |A|^{\frac{1}{2}}$.

Here $\mathrm{fix}_A(h)$ denotes the subgroup of A consisting of all elements which h leaves invariant. Again, since Conjecture C is true for fields of characteristic 0, and since its truth for an arbitrary field of characteristic $p > 0$ follows from its truth for the field with p elements (Lemma 7.1), C is, in fact, just a special case of E. Another special case, which arose originally in quite a different context, is obtained by taking A to be simple and H its group of inner automorphisms:

Conjecture W (J. Wiegold) If A is a non-abelian finite simple group, and c is the size of the largest conjugacy class in A, then $|A| \leq c^2$.

In other words, any finite simple group A contains an element, the order of whose centralizer is at most $|A|^{\frac{1}{2}}$. Again, a counterexample could not be generated by two elements, for, if all the centralizers in A have index less than $|A|^{\frac{1}{2}}$, then any two centralizers have non-trivial intersection, and so the centralizer of any two-generator subgroup of A is not trivial.

To summarise: Conjecture A_{rn} is equivalent to Conjecture E, and therefore a proof of A_{rn}, and *a fortiori* a proof of Conjecture A, would give proofs of E and of its special cases, C and W. Similarly, Conjecture B is equivalent to Conjecture D.

For infinite permutation groups the situation really is very simple indeed. The group G containing all permutations of finite support of an infinite set is even k-fold transitive for any finite k, but, by definition, every permutation in G fixes all but finitely many of the available points.

2. Further notation and definitions.

For describing permutation groups the notation I will use is basically that of H. Wielandt's book [W]. In particular, I will reserve the symbols

G for a finite group;

Ω for a t r a n s i t i v e G-space;

n for the degree of G;

α for a given point of Ω: $\alpha \in \Omega$.

That is, the elements of G act as unary operators on Ω so that $\omega(g_1g_2) = (\omega g_1)g_2$ and $\omega 1 = \omega$ for all $\omega \in \Omega$, $g_1, g_2 \in G$. If Ω_1 and Ω_2 are G-spaces, then $\phi: \Omega_1 \to \Omega_2$ is a G-morphism if $(\omega g)\phi = (\omega\phi)g$ for all $\omega \in \Omega_1$, $g \in G$, and I will embellish 'morphism' with appropriate prefixes in the usual way, to describe properties which ϕ may enjoy as a mapping of sets. Thus G is primitive on Ω if the only G-epimorphisms of Ω are isomorphisms and the mappings of Ω onto the trivial, one-point, G-spaces. If H is a subgroup of G then $\Omega(H)$ will denote the coset space

$$\Omega(H) = \{Hx \mid x \in G\},$$

on which G acts by right translation: $(Hx)g = H(xg)$ for all

Hx $\varepsilon \Omega(H)$, $g \varepsilon G$. In $\Omega(H)$ we always take α to be H itself. As in [W], if $\omega \varepsilon \Omega$ then the stabilizer of ω is

$$G_\omega = \{ g \varepsilon G \mid \omega g = \omega \} \leq G ,$$

and, if $\Gamma = \{\omega_1, \omega_2, \ldots, \omega_r\} \subseteq \Omega$, then

$$G_\Gamma = G_{\omega_1, \omega_2, \ldots, \omega_r} = \bigcap_{i=1}^{r} G_{\omega_i} .$$

I shall also use

$$S(G) = S_\Omega(G) = \bigcup_{\omega \varepsilon \Omega} G_\omega \subseteq G .$$

That is, $S(G)$ is the subset consisting of all elements of G which have at least one fixed point on Ω. If $g \varepsilon G$, put

$$\mathrm{fix}(g) = \{ \omega \varepsilon \Omega \mid \omega g = \omega \} = \{ \omega \varepsilon \Omega \mid g \varepsilon G_\omega \} \subseteq \Omega .$$

If A is a subgroup of G then Ω becomes an A-space by restriction. An A-orbit is a transitive A-subspace of Ω ; and, if $g \varepsilon G$, then a g-cycle is a $gp(g)$-orbit.

If X is any set or group, then, as we have already used, $|X|$ denotes the number of elements in X : thus $n = |\Omega|$; and if $g \varepsilon G$, then $\chi(g) = |\mathrm{fix}(g)|$. If A is a subgroup of G , put

$$t(A) = t_\Omega(A) = \text{number of } A\text{-orbits on } \Omega ;$$

$$a(A) = a_\Omega(A) = n/t(A) .$$

and similarly, if $g \varepsilon G$, put

$$t(g) = t_\Omega(g) = \text{number of } g\text{-cycles on } \Omega ;$$

$$a(g) = a_\Omega(g) = n/t(g) ;$$

and, $\lambda(G) = \lambda_\Omega(G) = \max \{ a(g) \mid g \varepsilon G \}$.

Thus $a(A)$ is the average orbit length of A on Ω; $a(g)$ is the average cycle length of g on Ω, and this average cycle length is, for all $g \in G$, at most $\lambda(G)$.

The kernel of the representation of G on Ω is denoted by $C_G(\Omega)$; it is the unique largest normal subgroup of G contained in G_α. Ω is a faithful G-space if $C_G(\Omega)$ is trivial, and quite generally, Ω can be identified with a faithful $G/C_G(\Omega)$-space in the natural way. If G_α is normal in G, so that $G_\alpha = C_G(\Omega)$, then I shall say that G is a regular group, or that G acts regularly on Ω. Thus G is regular in this sense if and only if $G/C_G(\Omega)$ is regular in the usual sense.

In §§ 7, 8, 12, H will denote a finite group, F a field, and M a non-zero FH-module. That is, M is a finite-dimensional vector space over F on which H acts as a group of non-singular linear transformations. I will reserve m to denote $\dim M$ throughout. If $u \in M$, then $C_H(u) = \{h \in H \mid uh = u\}$, and $C_H(M)$ is the kernel of the representation of H on M. If $h \in H$ I will use $\mathrm{fix}(h)$ to denote also the space of fixed points of h on M, or - if confusion threatens - I will use subscripts, $\mathrm{fix}_M(h)$, for safety, just as in the notation for permutation groups. I have already defined

$$\phi(h) = \phi_M(h) = \dim_F(\mathrm{fix}_M(h)) :$$

define also

$$\psi(h) = \psi_M(h) = \phi(h)/m .$$

If X is a group then $Y \subseteq X$, $Y \leq X$, $Y \lhd X$ mean respectively that Y is a subset of X, Y is a subgroup of X, Y is a normal subgroup of X; Y is subnormal in X if there is a chain

$$Y = Y_0 \lhd Y_1 \lhd \ldots \lhd Y_r = X .$$

The group T is a factor of X if $T \cong Y/Z$ where $Y \leq X$ and $Z \lhd Y$; it is a proper factor unless $Y = X$ and $Z = 1$; it is a subnormal factor if Y is subnormal in X; and a composition factor if it is a simple subnormal factor, that is, if Y is subnormal in X and Z is a maximal normal subgroup of Y. If $Y_1, Y_2 \subseteq X$, then

$$Y_1Y_2 = \{y_1y_2 \mid y_1 \in Y_1, \ y_2 \in Y_2\} \subseteq X ,$$

and we recall here that, if Y_1, Y_2 are subgroups of X, then Y_1Y_2 is a subgroup if and only if $Y_1Y_2 = Y_2Y_1$, and in any case,

$$|Y_1Y_2| = |Y_1| \cdot |Y_2| / |Y_1 \cap Y_2| .$$

If $A \leq X$ and $Y \subseteq X$, then

$$C_A(Y) = \{a \in A \mid a^{-1}ya = y \text{ for all } y \in Y\}$$

$$N_A(Y) = \{a \in A \mid a^{-1}Ya = Y\} .$$

If $x \in X$, $Y \leq X$, then $Y^x = x^{-1}Yx$, and

$$\text{core}(Y) = \bigcap_{x \in X} Y^x = \text{the largest normal subgroup of } X \text{ contained in } Y .$$

In fact, $\text{core}(Y)$ is the kernel of the permutation representation of X on the coset space $\Omega(Y)$; similarly, $|X:Y|$, the index of Y in X, is the degree of the coset space, $|\Omega(Y)|$.

If $x, y \in X$ then $[x,y]$ denotes the commutator $x^{-1}y^{-1}xy$. The Frattini subgroup of X, $\Phi(X)$ is the intersection of all maximal proper subgroups of X: if X is a p-group (p is a prime number) then $\Phi(X)$ is the unique smallest normal subgroup of X whose

factor group is elementary abelian of exponent p - that is, $\Phi(X)$ is then generated by all p^{th} powers and commutators of elements of X. The centre of X is denoted by $\zeta(X)$, and the upper central series by $1 = \zeta_0(X) \leq \zeta_1(X) \leq \zeta_2(X) \leq \ldots$. Of this, all we will require is that $\zeta_1(X) = \zeta(X)$, and that $\zeta_2(X)/\zeta_1(X) = \zeta(X/\zeta_1(X))$, so that

$$\zeta_2(X) = \{x \in X \mid [x,y] \in \zeta(X) \text{ for all } y \in X\}.$$

Finally, C_k denotes a cyclic group of order k; S_k denotes the symmetric group of degree k, the group of all permutations of a set of k points; and, as has already appeared many times, 1 denotes at the same time the unit element of any group or field, the trivial group, and the natural number for which it usually stands.

3. A list of prerequisites.

The basic facts about transitive permutation groups are all conveniently listed in the first few pages of [W]. Only the following useful lemma, from which follows the well-known facts that G is primitive (on Ω) if and only if G_α is maximal in G, and that Ω is G-isomorphic to the coset space $\Omega(G_\alpha)$, does not appear there explicitly.

Lemma 3.1 If Ω_1, Ω_2 are transitive G-spaces, $\alpha_1 \in \Omega_1$, $\alpha_2 \in \Omega_2$, then there is a G-morphism $\phi: \Omega_1 \to \Omega_2$ such that $\alpha_1\phi = \alpha_2$ if and only if $G_{\alpha_1} \leq G_{\alpha_2}$.

Recall also the useful fact that $A \leq G$ is transitive on Ω if and only if $G_\alpha A = G$. Along similar lines:

Lemma 3.2 If $G_\alpha \leq A \leq G$ and $G = N_G(G_\alpha).A$, then Ω is the union of $|G:A|$ A-orbits which are all A-isomorphic.

Proof. Let Δ_1 be the A-orbit of Ω containing α, let Δ_2 be any A-orbit, and let α_2 be a point in Δ_2. Since G is transitive on Ω, there exists $g \in G$ such that $\alpha g = \alpha_2$. By assumption, $g = xa$ with $x \in N_G(G_\alpha)$, $a \in A$. Therefore

$$G_{\alpha_2} = (xa)^{-1} G_\alpha xa = a^{-1} G_\alpha a \leq A ,$$

and, since

$$a^{-1} G_\alpha a = G_{\alpha a} \leq A ,$$

we have

$$A_{\alpha a} = G_{\alpha a} = G_{\alpha_2} = A_{\alpha_2} .$$

By Lemma 3.1 there is an A-isomorphism of Δ_1 to Δ_2 mapping αa to α_2 (if we had $G = C_G(A).A$, then this A-isomorphism would be produced by operating on Δ_1 with x, where now $x \in C_G(A)$ and $g = xa$). Thus the A-orbit containing α is A-isomorphic to any other A-orbit of Ω, and, since A-isomorphism is an equivalence relation, therefore all A-orbits of Ω are isomorphic. That there are just $|G:A|$ distinct A-orbits in Ω is then trivial.

Next a very familiar numerical result (see [B], §145, pp 189-191).

Lemma 3.3 (i) If Δ is a transitive G-space then $\sum_{g \in G} \chi(g) = |G|$;

(ii) If Δ consists of t G-orbits then $\sum_{g \in G} \chi(g) = t|G|$.

Proof. Clause (ii) follows directly from (i). To prove (i), put

$$X = \{(\delta, g) \mid \delta g = \delta\} \subseteq \Delta \times G ,$$

and calculate $|X|$. On the one hand,

$$|X| = \sum_{g \in G} |\mathrm{fix}(g)| = \sum_{g \in G} \chi(g) ,$$

and on the other hand, if G is transitive on Δ, then

$$|X| = \sum_{\delta \in \Delta} |G_\delta| = |\Delta| . |G_\delta| = |G| .$$

A very similar argument proves the little key result:

Lemma 3.4 If A is any group, $A_1, A_2, \ldots, A_r$ are (not necessarily distinct) subgroups of A of index at least $k > 1$, then there is an element of A contained in fewer than r/k of the A_i.

Proof. For $a \in A$ put

$$\theta(a) = |\{ i \mid 1 \leq i \leq r , \ a \in A_i \}| ,$$

and let

$$\mu = \min \{ \theta(a) \mid a \in A \} .$$

Then put

$$X = \{ (i,a) \mid a \in A_i \} \subseteq \{1, \ldots, r\} \times A .$$

On the one hand,

$$|X| = \sum_{a \in A} \theta(a) > |A| . \mu ,$$

with strict inequality because $\theta(1) > \mu$ (since $k > 1$). But also,

$$|X| = \sum_{1}^{r} |A_i| \leq r . |A|/k .$$

Thus $\mu < r/k$, and this gives the result. The case where A is G and the A_i are the stabilizers in G, so that $r = k = n$, gives the well-known fact (which Wielandt attributes to Jordan)

Corollary: Since G is transitive it contains permutations with no fixed points on Ω.

The next lemma is a useful consequence of primitivity.

Lemma 3.5 (Jordan[2]) If G is primitive and faithful on Ω and $\Delta \neq \{\alpha\}$ is a G_α-orbit in Ω, then every composition factor of G_α appears as a factor of $G_\alpha^\Delta = G_\alpha / G_{\alpha,\Delta}$.

Proof (Higman). Suppose that

$$X = G_\alpha \cap G_{\alpha_2} \cap \dots \cap G_{\alpha_r}$$

is subnormal in G_α. We will prove by induction on $n-r$ that every composition factor of G_α is isomorphic to a factor of a composition factor appearing between G_α and X. Certainly, if $n-r$ is 0 (or 1) then $X = 1$ and the statement is correct. If $n-r > 0$, then since G is primitive on Ω, there is a permutation $g \in G$ such that $\alpha g \in \{\alpha_2, \dots, \alpha_r\}$, but

$$\{\alpha_2 g, \dots, \alpha_r g\} \neq \{\alpha_2, \dots, \alpha_r\}.$$

Then, of course,

$$g^{-1}Xg = G_{\alpha g} \cap G_{\alpha_2 g} \cap \dots \cap G_{\alpha_r g}$$

is subnormal in $g^{-1}G_\alpha g = G_{\alpha g}$; so that

$$Y = X \cap g^{-1}Xg = G_\alpha \cap G_{\alpha_2} \cap \dots \cap G_{\alpha_r} \cap G_{\alpha_2 g} \cap \dots \cap G_{\alpha_r g}$$

is subnormal in

$$X \cap g^{-1}G_{\alpha g}g = X \cap G_{\alpha g} = X,$$

and subnormal factors appearing between X and Y are isomorphic to factors of subnormal factors appearing between $g^{-1}G_\alpha g$ and $g^{-1}Xg$, that is, between G_α and X. Hence Y is subnormal in G_α, and composition factors between G_α and Y appear as factors of composition

---

2) See § 14.

factors between G_α and X. However, Y is, by construction, an intersection of more stabilizers than X, and so we may assume (inductive hypothesis) that every composition factor of G_α is isomorphic to a factor of a composition factor appearing between G_α and Y. Therefore every composition factor of G_α is isomorphic to a factor of a composition factor between G_α and X, as we wished to show. In particular, if $X = G_{\alpha,\Delta}$ and Δ is a G_α-subspace of Ω, then X is normal in G_α, and the lemma follows.

Lemma 3.6 If G is faithful and contains a normal subgroup A which is regular on Ω, then Ω, as G_α-space, is G_α-isomorphic to A, on which G_α acts by conjugation. Consequently, if $g \in S(G)$, then

$$\chi(g) = |C_A(g)| .$$

This is Theorem 11.2 in [W]. The isomorphism is the obvious one: if $\omega \in \Omega$ we map ω to the unique element $\omega\phi \in A$ such that $\alpha(\omega\phi) = \omega$.

Lemma 3.7 If G is primitive and faithful on Ω and contains a regular normal subgroup A, then $G_\alpha = H$ operates faithfully on A by conjugation (in G), and A is H-simple. In particular, A is a minimal normal subgroup of G. (See [W], Proposition 11.4). Conversely of course, if the group A is H-simple where H is a group of automorphisms of A, then the split extension $G = HA$ of A by H acts faithfully and primitively on the coset space $\Omega(H)$, and contains A as a regular normal subgroup.

The proof is straightforward: by 3.6 the centralizer of A in H is the kernel of the representation of G_α on Ω and is

therefore trivial; that is, H operates faithfully on A by conjugation. And, if $B \leq A$ is H-invariant, then HB is a subgroup and it contains H. Primitivity of G translates into maximality of H in G, and so HB is either H or G, therefore B is either 1 or A. That is, A is H-simple, and a minimal normal subgroup of G.

Notes 1. It follows that A is characteristically simple, and is therefore a direct power of some simple group. If it is abelian then it is elementary abelian of prime exponent p, and may therefore be identified in the usual way with an H-module over $GF(p)$. In this case H-simplicity is just irreducibility of A qua $GF(p)H$-module.

2. Again if A is abelian, then $A = C_G(A)$, and A is the unique minimal normal subgroup of G; that is, G is then monolithic. For, certainly then $A \leq C_G(A)$, so that $C_G(A) = A.(C_G(A) \cap H)$. But we have shown that $C_G(A) \cap H = C_H(A)$ is trivial. Therefore $A = C_G(A)$. Any minimal normal subgroup of G either is contained in A or intersects A trivially; in either case it centralizes A and so must be contained in A. Thus A is, indeed, the only minimal normal subgroup of G.

3. On the other hand, if A is non-abelian then G may very well (§ 11) contain two distinct minimal normal subgroups. In this case, however, there can never be more than two minimal normal subgroups, they are isomorphic, they are each other's centralizers in G, and they are both regular. For, if B is also a non-trivial minimal

normal subgroup of G, and if $B \neq A$, then of course $B \cap A = 1$, and $B \leq C_G(A)$. Therefore $B \cap H = 1$, and BH, which is a subgroup properly containing H, must be G; that is, B is another normal complement for H in G, and so B is regular on Ω. Now $C_G(A) \geq B$, and so $C_G(A) = B.(C_G(A) \cap H) = B$; similarly, $C_G(B) = A$; and therefore there can be no other minimal normal subgroups in G. If $C = gp(A, B) = A \times B$, and $D = H \cap C$, then, since $C \geq A$, we have $C = AD$, and since $C \geq B$ also $C = BD$. Therefore

$$A \cong C/B = BD/B \cong D/(D \cap B) = D$$

$$B \cong C/A = AD/A \cong D/(D \cap A) = D .$$

Thus $A \cong B$, and in fact, we can choose this isomorphism as an H-isomorphism in such a way that H intersects the direct square $A \times B$ in its 'diagonal'.

4. In fact, I know of no example of a primitive group G containing one and only one regular non-abelian normal subgroup. If G is such a group, and $A = A_1 \times A_2 \times \ldots \times A_r$ where $A_i \cong S$ for all relevant i, and S is a simple group, then the set of direct factors $\{A_1, A_2, \ldots, A_r\}$ is a characteristic set of subgroups of A (see, for example, [H], pp 127-131, or [S], 4.6.3, p.84). Consequently H permutes the factors A_i, and, since A is H-simple it permutes them transitively. Put $H_1 = N_H(A_1)$, so that H_1 acts as a group of automorphisms of A_1, that is, of S, and let B_1 be an H_1-invariant subgroup of A_1. If $h_1, h_2, \ldots, h_r \in H$ are elements for which $A_1^{h_i} = A_i$, and if we put $B_1^{h_i} = B_i \leq A_i$,

then $B = B_1 \times B_2 \times \ldots \times B_r \leq A$ is H-invariant. Therefore B is 1 or A, and so B_1 is 1 or A_1: that is, A_1 (i.e. S) is H_1-simple. Furthermore (this is where our assumption that A is the only minimal normal subgroup of G enters) H contains no non-trivial inner automorphisms of A, and it follows that H_1 contains no non-trivial inner automorphisms of S.

We have shown now that there is a primitive permutation group containing precisely one regular non-abelian normal subgroup only if, and clearly if, there is a finite simple group S which is H_1-simple for some group H_1 of automorphisms containing no non-trivial inner automorphisms. There is no finite simple group with this property known: if the "known" finite simple group S is H_1-simple then H_1 contains all the inner automorphisms of S.

These last two notes are a digression: they will not be needed elsewhere in this thesis. However, they seem significant enough to be worth noting, and yet I have not found them recorded anywhere else. Moreover, they do suggest that Conjecture W (page 9) is perhaps not as special a case of Conjecture E as it seems.

In general a normal subgroup of a primitive group need not be regular. However:

Lemma 3.8 If G is primitive and faithful on Ω, and if A is a non-trivial nilpotent normal subgroup of G, then A is regular. [Most of this and the preceding lemma were known already to Galois].

Proof. If $X = A \cap G_\alpha$ then X is normal in G_α and is a proper subgroup of A. Since A is nilpotent, $N_A(X)$ contains X properly ([H], Corollary 10.3.1, p.154), therefore $N_G(X)$ contains G_α properly, and must be all of G. Since G_α contains no non-trivial normal subgroup of G, $X = 1$, and so A is regular.

In particular, if G is soluble, then its Fitting subgroup, A, the maximal nilpotent normal subgroup of G, is non-trivial, therefore regular, hence by 3.7 is the unique minimal normal subgroup in G, and can be treated as a faithful irreducible H-module over $GF(p)$, where $H \cong G_\alpha \cong G/A$. Incidentally, since $|A| = n = |\Omega|$ is a power of p, this gives the well-known fact [Galois] that a primitive soluble group has prime-power degree.

Last in this list, Clifford's Theorem:

Theorem 3.9 Let M be a faithful irreducible H-module over a field F, where H is a finite group containing a non-trivial normal subgroup N. Let $M_1^*, \ldots, M_r^*$ be the non-isomorphic irreducible N-submodules of M, and let $M_1, \ldots, M_r$ be the corresponding characteristic N-submodules of M - that is, for $i = 1, \ldots, r$, M_i is the sum of all N-submodules of M isomorphic to M_i^*. Then

(i) $M_1^*, \ldots, M_r^*$ are conjugate N-modules: the N-modules U, V are conjugate if there is an automorphism α of N, and an F-isomorphism $\phi: U \to V$, such that, for all $u \in U$, $x \in N$,

$$(ux)\phi = (u\phi)(x\alpha) .$$

(ii) $$M = M_1 \oplus M_2 \oplus \dots \oplus M_r ,$$

and, more generally, if U is an N-submodule of M, then

$$U = U_1 \oplus U_2 \oplus \dots \oplus U_r$$

where $U_i = U \cap M_i$, $i = 1, \dots, r$.

(iii) H acts as a transitive permutation group on the set $M_1, \dots, M_r$, and N is in the kernel of this permutation representation.

There is a proof in [CR], p.343. Two familiar facts are straightforward consequences of Clifford's Theorem: if the finite group H has a faithful irreducible representation over some field, then its centre must be cyclic; and if it has a faithful irreducible representation over a field of characteristic $p > 0$, then H contains no non-trivial normal p-subgroup. Both can of course be proved more directly.

4. Elementary inequalities.

The following relations come directly from the definitions:

(4.1) $$0 \le \delta_* \le 1 ; \qquad 0 \le \gamma_* \le 1 ;$$

(4.2) if $\delta_* > 0$ then $\gamma_* = 1$; if $\gamma_* < 1$ then $\delta_* = 0$;

(4.3) for all n,

$$f_{trans}(n) \ge f(n) \ge f_{rn}(n) \ge f_{sol}(n) .$$

The last inequality in this sequence is a consequence of 3.8: every primitive soluble permutation group contains a regular normal subgroup.

Consequently,

$$\delta_{trans} \geq \delta \geq \delta_{rn} \geq \delta_{sol}$$

$$\gamma_{trans} \geq \gamma \geq \gamma_{rn} \geq \gamma_{sol} \ .$$

Lemma 4.4 (i) $\mu(G)/n \leq |G_\alpha|/|S_\Omega(G)|$;

(ii) $\mu(G)/n \leq 1/a_\Omega(G_\alpha)$.

Proof (i) Since G is transitive on Ω, by Burnside's Theorem (3.3),

$$|G| = \sum_{g \in G} \chi(g) = \sum_{g \in S(G)} \chi(g) \geq |S(G)|\mu(G) \ .$$

Therefore

$$\mu(G)/n \leq \frac{|G|}{n} \cdot 1/|S(G)| = |G_\alpha|/|S(G)| \ .$$

(ii) Again by Lemma 3.3,

$$t(G_\alpha)\,|G_\alpha| = \sum_{g \in G_\alpha} \chi(g) \geq |G_\alpha|\mu(G) \ ,$$

so that

$$\mu(G)/n \leq t(G_\alpha)/n = 1/a(G_\alpha) \ .$$

In both cases strict inequality holds when G is not regular, because then $\chi(1) > \mu(G)$.

Of these two inequalities, (i) looks the more promising since it seems extremely likely that for primitive, non-regular groups G, $|S(G)|/|G_\alpha|$ tends to infinity with the degree n (this is not true for merely transitive non-regular groups, as the examples in § 10 show). This, by (i), would then be enough to prove that δ is zero. On the other hand, I prove Theorem 2 by examining (ii) in greater detail: it is a strong restriction on a primitive group G that the average orbit length of a stabilizer, $a(G_\alpha)$ is at most 4. It is tempting to conjecture that for primitive groups $|G_\alpha|$ is bounded in terms of $a(G_\alpha)$. If this were true it, too, would be sufficient to prove (though less directly) that $\delta = 0$.

Lemma 4.5 If Ω_1, Ω_2 are transitive G-spaces, $\phi: \Omega_1 \to \Omega_2$ is a G-morphism, then for all $g \in G$, $a_{\Omega_2}(g) \leq a_{\Omega_1}(g)$. Therefore $\lambda_{\Omega_2}(G) \leq \lambda_{\Omega_1}(G)$.

Proof. If $\alpha_1 \in \Omega_1$, $\alpha_2 \in \Omega_2$ and $\alpha_1\phi = \alpha_2$, then, by Lemma 3.1, $G_{\alpha_1} \leq G_{\alpha_2}$. If $|G_{\alpha_2} : G_{\alpha_1}| = k$, then for all $\omega \in \Omega_2$, $|\omega\phi^{-1}| = k$. Consequently

(i) $$n_1 = |\Omega_1| = k|\Omega_2| = n_2 ;$$

and (ii) if $g \in G$ and Γ is a g-cycle in Ω_2, then $\Gamma\phi^{-1}$ is the union of at most k g-cycles in Ω_1: hence

$$t_{\Omega_1}(g) \leq kt_{\Omega_2}(g) .$$

Therefore

$$a_{\Omega_1}(g) = n_1/t_{\Omega_1}(g) \geq kn_2/kt_{\Omega_2}(g) = a_{\Omega_2}(g) ,$$

which is what the lemma states.

If Ω_1, Ω_2 are isomorphic A-spaces, for some group A, then of course $\lambda_{\Omega_1}(A) = \lambda_{\Omega_2}(A)$, and, if Ω is the union of A-subspaces all isomorphic to, say, Ω_1, then it is likewise trivial that $\lambda_{\Omega}(A) = \lambda_{\Omega_1}(A)$. Therefore a corollary of Lemma 3.2 is

Lemma 4.6 If $G_\alpha \leq A \leq G$, if $G = N_G(G_\alpha).A$, and if Ω_1 is an A-orbit in Ω, then

$$\lambda_{\Omega_1}(A) = \lambda_{\Omega}(A) \leq \lambda_{\Omega}(G) .$$

CHAPTER II: UPPER BOUNDS

5. Transitive groups.

Here is the proof of Theorem 1 (i). We suppose that $\mu(G) > \frac{1}{2}n$ and prove that G is then regular on Ω. Our supposition means that, if $g_1, g_2 \in S(G)$ then both g_1 and g_2 fix more than $\frac{1}{2}n$ points, and so we have - by definition of $\frac{1}{2}$ - that $\mathrm{fix}(g_1) \cap \mathrm{fix}(g_2)$ is not empty. Consequently $g_1 g_2^{-1} \in S(G)$, and so $S(G)$ is a subgroup of G. By Lemma 3.3,

$$|G| = \sum_{g \in G} \chi(g) = \sum_{g \in S(G)} \chi(g)$$

$$> |S(G)| . \tfrac{1}{2}n = \tfrac{1}{2} |S(G) : G_\alpha| . |G_\alpha| n = \tfrac{1}{2} |S(G) : G_\alpha| . |G| .$$

Comparing the first and last items here gives $|S(G):G_\alpha| < 2$, and since this index must be a positive integer, we have $|S(G):G_\alpha| = 1$; that is, $S(G) = G_\alpha$. However, $S(G)$ is normal in G, hence G_α is normal, and G is regular. Therefore if G is a non-regular transitive group then G contains a permutation g with $1 \leq \chi(g) \leq \frac{1}{2}n$. This proves the theorem.

6. Primitive groups.

The proof of Theorem 2 (i) basically is a search for those primitive groups G in which $a(G_\alpha) \leq 4$, as suggested by Lemma 4.4(ii). Let G be faithful and primitive on Ω, and not regular (that is, not a cyclic group of prime order). Since G_α is maximal and not

normal, $N_G(G_\alpha) = G_\alpha$, so that $G_\alpha = G_\beta$ if and only if $\alpha = \beta$. Thus $\{\alpha\}$ is the only G_α-orbit of length 1 in Ω. We distinguish three cases:

1. all G_α-orbits of Ω other than $\{\alpha\}$ have length at least 4;
2. Ω contains a G_α-orbit of length 2;
3. Ω contains a G_α-orbit of length 3.

Case 1. If all non-trivial G_α-orbits have length 4 or more, then

$$n \geq 1 + 4(t(G_\alpha) - 1) = 4t(G_\alpha) - 3,$$

so that, by Lemma 4.4, in this case

$$\mu(G) < n/a(G_\alpha) = t(G_\alpha) \leq \tfrac{1}{4}(n+3).$$

Case 2. If there is a G_α-orbit of length 2 then G is dihedral of order $2n$, where the degree n is prime. For, if $\beta \in \Omega$ and the G_α-orbit containing β has length 2, then $G_{\alpha,\beta} = G_\alpha \cap G_\beta$ has index 2 in G_α. It then has index 2 also in G_β, is normalized by both G_α and G_β, and, since these are maximal and distinct, it is normal in G. Consequently, $G_{\alpha,\beta}$, a normal subgroup of G contained in G_α, is trivial, G_α is cyclic of order 2, and G, being generated by two subgroups of order 2, is dihedral. Moreover, n is then an odd prime since G_α is maximal in G. And now, $\mu(G) = 1 < \frac{1}{4}(n+3)$, which settles this case.

Case 3. Suppose that Ω contains a G_α-orbit Δ of length 3, say $\Delta = \{\beta_1, \beta_2, \beta_3\}$. First, if G_α contains just one cyclic subgroup X of order 3, then X is normal in any stabilizer in

which it is contained, and since X is certainly not normal in G, X is contained in one and only one stabilizer. If x is a generator of X then $\chi(x) = 1$, and so $\mu(G) = 1 < \frac{1}{4}(n+3)$.

We may suppose therefore that G_α does not contain just one cyclic subgroup of order 3. In particular, G_α cannot act regularly on Δ, for if it did, by Lemma 3.5, G_α would be a 3-group, $G_\alpha \cap G_{\beta_1}$, of index 3 in both G_α and G_{β_1}, would be normal in G, therefore trivial, and G_α itself would be cyclic of order 3. So G_α acts then as the full symmetric group on Δ: $G_\alpha / G_{\alpha,\Delta} \cong S_3$. And again, $G_{\alpha,\Delta}$ cannot be trivial, otherwise G_α would be isomorphic to S_3 which has just one cyclic subgroup of order 3.

The next step is to show that Ω contains at least as many G_α-orbits of length 6 as G_α-orbits of length 3. To do this, write G_i for G_{β_i}, $i = 1, 2, 3$, and put

$$X = G_{\alpha,\Delta} = G_\alpha \cap G_2 \cap G_3 = G_\alpha \cap G_1 \cap G_3 = G_\alpha \cap G_1 \cap G_2 .$$

These equalities follow from the same statement in S_3. Then, since $X \neq 1$ and $X \lhd G_\alpha$ we must have $N_G(X) = G_\alpha$. Since $G_{1,2} = G_1 \cap G_2$ contains X, which has index 6 in G_1 and G_2, it follows that $G_{1,2}$ has index 1, 2, 3 or 6 in G_1 and in G_2. Of these, 1 is trivially impossible; 2 is also impossible as Case 2 above has shown; and if this index were 3, then X would have index 2 and would be normal in $G_{1,2}$, this would imply

$$G_{1,2} \leq N_G(X) = G_\alpha ,$$

and $X = G_\alpha \cap G_{1,2} = G_{1,2}$, which would not be so. Therefore $G_{1,2}$

has index 6 in G_1 and in G_2, and so $G_{1,2} = X$; similarly, $G_{2,3} = G_{1,3} = X$.

For any G_α-orbit Γ of length 3, choose $\gamma \in \Gamma$, choose $\delta \neq \alpha$ in the G_γ-orbit containing α, and let Γ^* be the G_α-orbit containing δ. This means that $G_\delta = x^{-1}G_\alpha x$ for some element $x \in G_\gamma - G_\alpha$, and, by the preceding paragraph, that $G_\delta \cap G_\alpha$ has index 6 in G_α and is normalized by G_γ. Thus Γ^* certainly is a G_α-orbit of length 6. Suppose that $\Gamma_1^* = \Gamma_2^*$, where Γ_1 and Γ_2 are G_α-orbits of length 3. Then, if γ_i, δ_i, x_i are the ingredients going into the making of Γ_i^*, $i = 1, 2$, then there is an element $g \in G_\alpha$ such that $\delta_1 g = \delta_2$. Hence

$$G_{\delta_2} = g^{-1}G_{\delta_1}g,$$

so that $$G_{\delta_2} \cap G_\alpha = g^{-1}G_{\delta_1}g \cap G_\alpha = g^{-1}(G_{\delta_1} \cap G_\alpha)g,$$

and

$$G_{\gamma_2} = N_G(G_{\delta_2} \cap G_\alpha) = g^{-1}N_G(G_{\delta_1} \cap G_\alpha)g = g^{-1}G_{\gamma_1}g = G_{\gamma_1 g}.$$

Therefore $\gamma_2 = \gamma_1 g$ and so $\Gamma_1 = \Gamma_2$. The other way round, then: if $\Gamma_1 \neq \Gamma_2$ then $\Gamma_1^* \neq \Gamma_2^*$ and so Ω contains at least as many G_α-orbits of length 6 as G_α-orbits of length 3.[3)]

If there are $t_1 \geq 1$ G_α-orbits of length 3, therefore t_1 G_α-orbits of length 6 obtained as above, and then

$$t_2 = t(G_\alpha) - 1 - 2t_1$$

---

3) Dr. Donald Livingstone has kindly pointed out that part of this argument is just a very special case of a result of W.A. Manning (see [W], Theorem 17.7).

further G_α - orbits each of length at least 4 , then

$$\begin{aligned} n &\geq 1 + 3t_1 + 6t_1 + 4t_2 \\ &= 1 + 9t_1 + 4t(G_\alpha) - 4 - 8t_1 \\ &= 4t(G_\alpha) - 3 + t_1 \\ &> 4t(G_\alpha) - 3 . \end{aligned}$$

Therefore, as before,

$$\mu(G) < n/a(G_\alpha) = t(G_\alpha) < \tfrac{1}{4}(n+3) .$$

The three cases treated cover every possibility, and so, since in every case, $\mu(G) < \frac{1}{4}(n+3)$, it follows that $f(n) < \frac{1}{4}(n+3)$ and the proof of Theorem 2 (i) is complete.

In the course of the proof we have shown that if the average orbit length of non-trivial G_α - orbits is less than 4 then G_α is trivial, cyclic of order 2 , cyclic of order 3 , or S_3 . In all these cases the structure of G itself can be completely determined: if G_α is trivial then G is cyclic of prime order; if $G_\alpha \cong C_2$ then G is dihedral of order $2p$ (p prime); and if $G_\alpha \cong C_3$ or $G_\alpha \cong S_3$ then G contains a self-centralizing element of order 3 , and Feit and Thompson [2] have catalogued all groups which can occur.

7. Representation theory.

We turn now to Conjecture C and a linear analogue of these problems on permutation groups. Throughout this section H is a finite group, F is a field, and I shall say that the FH-module M ,

of dimension m over F, has property C if M gives a counter-example to Conjecture C, that is, if M is a non-trivial irreducible FH-module such that, for all $h \in H$, $\psi(h) = \phi(h)/m > \frac{1}{2}$. We begin with a necessary technicality:

Lemma 7.1 If K, L are fields of the same characteristic then there is a KH-module having property C if and only if there is an LH-module with property C.

This lemma follows directly from its special case in which $K \leq L$ and L is algebraically closed. For, in general, if $\overline{K}$, $\overline{L}$ are the algebraic closures of K and L respectively, and if P is the prime field of the same characteristic as K and L, then $K \leq \overline{K}$, $\overline{K} \geq P$, $P \leq \overline{L}$, and $\overline{L} \geq L$; then, from the special case applied in turn to each of these pairs of fields, we get the result for the fields K and L. For the rest of this proof we will suppose therefore that L is an algebraically closed field and that K is a subfield of L.

If U is an irreducible KH-module, V is an irreducible LH-module, define

$U^L = U \otimes_K L$ as LH-module;

V_K to be an irreducible KH-submodule of V.

We identify $u \in U$ with $u \otimes 1$ in U^L, and, as usual, write $u\lambda$ for $u \otimes \lambda$, $u \in U$, $\lambda \in L$. Notice that, if V is an irreducible LH-module, then by neglecting scalar multiplications of elements of V by elements of L not contained in K, we certainly can identify V

as a KH-module - infinite-dimensional unless the degree of L over K is finite. However, H is finite and so V certainly contains some non-zero irreducible KH-submodule V_K. Since $\sum_{\lambda \in L} V_K \lambda$ is an LH-module contained in V, it must be all of V, and, since for any $\lambda \in L$, $V_K \lambda$ is a KH-submodule of V isomorphic to V_K, it follows that V is isomorphic as KH-module to a direct sum of, perhaps infinitely many, irreducible KH-submodules all isomorphic to V_K. As a consequence, any irreducible KH-submodule of V is isomorphic to V_K, and thus V_K is determined unambiguously (up to isomorphism) by V. Notice that V_K is the trivial KH-module if and only if V is the trivial LH-module.

Moreover, if U is an irreducible KH-module, and Λ is a basis for L over K, then

$$U^L = U \otimes_K L = \sum_{\lambda \in \Lambda} U \otimes \lambda ,$$

and the sum on the right is direct. Consequently, every irreducible KH-submodule of U^L is isomorphic to U; and so, if W is a composition factor of U^L as LH-module, then $W_K \cong U$. Conversely, if V is an irreducible LH-module, then V is isomorphic to a composition factor (actually, an epimorphic image) of $(V_K)^L$. [Much of all this is implicit in [CR] § 29; all that is needed in addition is some form of the Axiom of Choice to get a direct sum from a sum of infinitely many irreducible modules.]

With this notation, suppose that U is a KH-module, V is an LH-module, and U, V are related as above. That is, $U \cong V_K$ and V is a composition factor of U^L. I shall show that then, for all $h \in H$,

$$\chi_U(h) = \chi_V(h) .$$

Now $K \leq \overline{K} \leq L$, and as $\overline{K}$ is algebraically closed it is a splitting field for H ([CR], § 29). That is ([CR], 29.15, p.203), there is a composition factor W of the $\overline{K}H$-module $U^{\overline{K}}$ such that

$$V = W^L , \quad \text{and so} \quad W = V_{\overline{K}} .$$

Now if $w_1, \ldots, w_r$ is a $\overline{K}$-basis for W, and if

$$w_i h = \sum_{j=1}^{r} w_j a_{ij}(h) \qquad h \in H ; \quad i = 1, \ldots, r ,$$

then all the coefficients $a_{ij}(h)$ are algebraic over K; therefore

$$K^* = K(a_{ij}(h) \mid h \in H ; \ i = 1, \ldots, r ; \ j = 1, \ldots, r) ,$$

the subfield of $\overline{K}$ generated over K by all these finitely many coefficients, is a finite extension of K; and, if $X = W_{K^*}$, then clearly $W = X^{\overline{K}}$. Now

(a) $\chi_X(h) = \chi_V(h)$ for all $h \in H$.

Proof. Since

$$V = W^L = (X^{\overline{K}})^L = X^L = X \otimes_{K^*} L ,$$

we have $\dim_{K^*}(X) = \dim_L(V)$, and thus it is only necessary to prove that if $h \in H$ then $\phi_X(h) = \phi_V(h)$. If $x_1, \ldots, x_r$ is a basis for X over K^*, therefore also for V over L, and if

$$x_i h = \sum_{j=1}^{r} x_j a_{ij} \qquad i = 1, \ldots, r ,$$

$a_{ij} \in K^*$, then $\underline{h} = \text{matrix}(a_{ij})$ is the matrix of h with respect

to $x_1, \ldots, x_r$ both on X and on V. Therefore

$$\begin{aligned} \dim_{K^*} \mathrm{fix}_X(h) &= \dim_{K^*}(X) - \mathrm{rank}(\underline{h} - \underline{1}) \\ &= \dim_L(V) - \mathrm{rank}(\underline{h} - \underline{1}) \\ &= \dim_L \mathrm{fix}_V(h) . \end{aligned}$$

(Here $\underline{1}$ denotes the appropriate unit matrix.) Thus $\phi_X(h) = \phi_V(h)$ and statement (a) follows. Further,

(b) $\psi_U(h) = \psi_X(h)$ for all $h \in H$.

Proof. If $\beta_1, \ldots, \beta_k$ is a basis for K^* over K, then if Y is any K^*-subspace of X and $y_1, \ldots, y_s$ is a K^*-basis for Y, then $\{ y_i \beta_j \mid i = 1, \ldots, s ; \ j = 1, \ldots, k \}$ is a K-basis for Y as K-subspace of X. In particular,

$$\dim_K(Y) = k \dim_{K^*}(Y) .$$

Now, since X is a K^*H-composition factor of U^{K^*} it is certainly, as KH-module, isomorphic to the direct sum of, say, t KH-modules isomorphic to U. If $h \in H$, then $\mathrm{fix}_X(h)$ is a K^*-subspace of X, and therefore

$$k \dim_{K^*} \mathrm{fix}_X(h) = \dim_K \mathrm{fix}_X(h) = t \dim_K \mathrm{fix}_U(h)$$

while

$$k \dim_{K^*}(X) = \dim_K(X) = t \dim_K(U) .$$

Hence

$$\psi_X(h) = \frac{\dim_{K^*} \mathrm{fix}_X(h)}{\dim_{K^*}(X)} = \frac{\dim_K \mathrm{fix}_U(h)}{\dim_K(U)} = \psi_U(h) ,$$

as we had predicted.

This completes the proof of Lemma 7.1 : we have in fact shown slightly more. Namely, in the general case, if P is the prime field contained in both K and L, and if U is an irreducible KH-module,

V is a composition factor of the LH-module $(U_P)^L$, then $\psi_U(h) = \psi_V(h)$ for all $h \in H$. Since moreover, if U is not trivial, then V is not trivial, we have that, if U has property C then V has property C. A corollary, more of the proof than of the lemma itself, which is better adapted for the proof of Theorem 4, is:

Corollary. If K, L are fields of the same characteristic, namely 0 or a prime which does not divide $|H|$, and if U is a non-zero KH-module, then there is a non-zero LH-module U^*, such that $\psi_{U^*}(h) = \psi_U(h)$ for all $h \in H$, and U^* contains a non-zero trivial LH-submodule if and only if U contains a non-zero trivial KH-submodule.

For the proof, let P be the prime field contained in both K and L. Our assumptions allow us to suppose (by Maschke's Theorem, [CR], Theorem 10.8, p.41) that

$$U = U_1 \oplus U_2 \oplus \dots \oplus U_r$$

where the U_i are irreducible KH-submodules of U, and, say, $\dim_K(U_i) = m_i$, $\dim_P((U_i)_P) = p_i$. Put

$$k_i = p_1 \cdot\cdot p_{i-1}{}^{m_i} p_{i+1} \cdot\cdot p_r$$

and

$$U_P = k_1(U_1)_P \oplus k_2(U_2)_P \oplus \dots \oplus k_r(U_r)_P,$$

where $k_i(U_i)_P$ denotes the direct sum of k_i PH-modules all isomorphic to $(U_i)_P$. Finally, put

$$U^* = (U_P)^L = U_P \otimes_P L$$

as LH-module. Then, exactly as in (a) and (b) above, $\psi_{U^*}(h) = \psi_U(h)$ for all $h \in H$, and clearly, U^* contains a non-zero trivial submodule if and only if U contains a non-zero trivial submodule.

Lemma 7.2 Let p be a prime number which does not divide $|H|$, let L be the algebraic closure of the prime field $GF(p)$, and let K be the field of all algebraic numbers (i.e., the algebraic closure of the rational field). Then there is a correspondence $M \dashrightarrow M^{\#}$ between KH-modules M and LH-modules $M^{\#}$, such that

(i) $M_1^{\#} \cong M_2^{\#}$ if and only if $M_1 \cong M_2$;

(ii) every (finite-dimensional) LH-module arises as $M^{\#}$ for a suitable KH-module M;

(iii) $\dim_K(M) = \dim_L(M^{\#})$;

(iv) $(M_1 \oplus M_2)^{\#} \cong M_1^{\#} \oplus M_2^{\#}$;

(v) If M is a trivial module then $M^{\#}$ is trivial;

(vi) If $h \in H$ then $\phi_M(h) = \phi_{M^{\#}}(h)$.

A proof can be found in [CR], Chapter XII. The correspondence can be described as follows: let R be the ring of algebraic integers in K, $\underline{p}$ the prime ideal in R containing p, so that $R/\underline{p} \cong L$. If M is a KH-module with K-basis $u_1, \ldots, u_m$, and X is the RH-submodule generated by $u_1, \ldots, u_m$ then we put

$$M^{\#} = X/\underline{p}X$$

and regard $M^{\#}$ as an LH-module. We may certainly do this, as $M^{\#}$ is an RH-module annihilated by $\underline{p}$. It turns out, since $p \nmid |H|$, that $M^{\#}$ depends only on M and not on the particular basis $u_1, \ldots, u_m$; that $M^{\#}$ is irreducible if and only if M is irreducible; and that $(M_1 \oplus M_2)^{\#} \cong M_1^{\#} \oplus M_2^{\#}$ (see, in particular, [CR], Remark 1 on p.600).

To prove part (vi), if $h \in H$ we may simply apply parts (i) - (v) to the module M as $gp(h)$-module. Alternatively, we can calculate directly in the following way. Since the order of h is finite and K is algebraically closed, we may pick a K-basis $x_1, \ldots, x_m$ for M consisting of eigenvectors of h : say

$$x_i h = x_i \lambda_i \qquad i = 1, \ldots, m .$$

Now each eigenvalue λ_i is an algebraic integer, in fact, a k^{th} root of unity, where k is the order of h. Therefore, using $x_1, \ldots, x_m$ in the construction of $M^{\#}$ from M (and embellishing symbols with $\#$ to denote images under the canonic epimorphism from X to $X/\underline{p}X$) we see that

$$x_i^{\#} h = x_i^{\#} \lambda_i^{\#} \qquad i = 1, \ldots, m .$$

Now precisely $t = \phi_{M^{\#}}(h)$ of these $\lambda_i^{\#}$ are 1 : say, $\lambda_i^{\#} = 1$ for $1 \leq i \leq t \leq m$. This means that

$$\lambda_i = 1 + \varepsilon_i \qquad 1 \leq i \leq t ,$$

where $\varepsilon_i \in \underline{p}$. Also, $\lambda_i^k = 1$ for all relevant i, and so, if $1 \leq i \leq t$, then

$$(1 + \varepsilon_i)^k = \sum_{j=0}^{k} \binom{k}{j} \varepsilon_i^j = 1 ,$$

therefore

$$\sum_{j=1}^{k} \binom{k}{j} \varepsilon_i^j = 0 ,$$

and, if $\varepsilon_i \neq 0$, then

$$\sum_{j=1}^{k} \binom{k}{j} \varepsilon_i^{j-1} = 0 .$$

Therefore, if $\varepsilon_i \neq 0$, then

$$\sum_{j=0}^{k-1} \binom{k}{j+1}^{\#} (\varepsilon_i^j)^{\#} = \binom{k}{1}^{\#} = 0 .$$

That is, if $\varepsilon_i \neq 0$, then $k \in \underline{p}$. But k is a rational integer and, being a divisor of $|H|$, is certainly not divisible by p, so that, in fact, $k \notin \underline{p}$. Therefore $\varepsilon_i = 0$ and $\lambda_i = 1$, $1 \leq i \leq t$. Since, if $\lambda_i^{\#} \neq 1$ then clearly $\lambda_i \neq 1$, it follows that

$$\phi_M(h) = t = \phi_{M^{\#}}(h)$$

and the proof is complete.

Now the main item of this section can be completed without pain.

Proof of Theorem 4. By the corollary following Lemma 7.1, we may assume that F is the algebraic closure of its prime field, and then by Lemma 7.2, it is sufficient to prove the theorem when F is the field of algebraic numbers. Suppose therefore that M is an FH-module (F now the algebraic numbers) for which $\psi(h) \geq \frac{1}{2}$ for all $h \in H$, and let $\theta: H \to F$ be the character of M. Then, for $h \in H$,

$$\theta(h) = \sum_1^m \lambda_i ,$$

where $\lambda_1, \ldots, \lambda_m$ are the eigenvalues of h on M. Of these, $\phi(h) = t \geq \frac{1}{2}m$ are equal to 1 by assumption; and all the λ_i are k^{th} roots of unity, where k is the order of h, so that $\mathrm{Re}(\lambda_i) \geq -1$. Therefore

$$\mathrm{Re}(\theta(h)) = \sum \mathrm{Re}(\lambda_i) \geq t - (m - t) = 2t - m \geq 0 .$$

Now estimate the inner product of θ with the trivial character χ_1:

$$(\theta, \chi_1) = \mathrm{Re}(\theta, \chi_1) = |H|^{-1} \sum_{h \in H} \mathrm{Re}(\theta(h)\chi_1(h^{-1}))$$

$$= |H|^{-1} \sum_{h \in H} \mathrm{Re}(\theta(h))$$

$$> 0 .$$

Strict inequality holds because $\theta(1) = m > 0$. Thus the inner product of θ with the trivial character is not zero, and so ([CR] § 31) M contains a non-zero trivial submodule, and the proof of Theorem 4 is complete.

Remark. By using the Brauer character of M we could have treated the case where $\mathrm{char}(F) = p > 0$, $p \nmid |H|$ directly, in precisely the same way. However, it requires all the machinery sketched in the proof of Lemma 7.2 to obtain and use Brauer characters. More generally, the character relations between Brauer characters ([CR], p.600) do produce, in the same way as above, the result that, if M has property C then M is in the principal p-block, but when $p \mid |H|$ I have been quite unable to exploit this information usefully.

In the rest of this section we turn our attention to the group H.

Lemma 7.3 Let N be a non-trivial normal subgroup of H, let M be a faithful irreducible FH-module, and let $\Omega = \{1, 2, \ldots, r\}$ be the H-space implicit in clause (iii) of Clifford's Theorem, 3.9, (that is, $M_1, \ldots, M_r$ are the characteristic N-submodules of M described there, and, for all $h \in H$, $M_i h = M_{ih}$ $i = 1, \ldots, r$). Then for all $h \in H$,

$$a_\Omega(h) \leq \psi_M(h)^{-1}.$$

Proof. Let $h \in H$, and let $\Gamma_1, \Gamma_2, \ldots, \Gamma_t$ be the distinct cycles of h on Ω. That is, $\Omega = \bigcup_1^t \Gamma_j$, if $j_1 \neq j_2$ then

Γ_{j_1} and Γ_{j_2} are disjoint, and, if $i_1, i_2 \in \Gamma_j$ then, for some integer q, $i_2 = i_1 h^q$. Put

$$V_j = \sum_{i \in \Gamma_j} M_i \qquad j = 1, \ldots, t$$

so that

$$M = V_1 \oplus V_2 \oplus \ldots \oplus V_t$$

and the subspaces V_j are invariant under h. If $U = \mathrm{fix}(h)$ and $U_j = U \cap V_j$, then

$$U = U_1 \oplus U_2 \oplus \ldots \oplus U_t .$$

For, certainly,

$$U \geq U_1 \oplus U_2 \oplus \ldots \oplus U_t ;$$

but on the other hand, if $u \in U$, say, $u = \sum_1^t v_j$ with $v_j \in V_j$, then

$$u = uh = \sum v_j h$$

with $v_j h \in V_j$, and, since the sum of the V_j is direct, comparison of the two expressions for u gives that $v_j = v_j h$, $j = 1, \ldots, t$. Thus $v_j \in U_j$, and

$$U \leq U_1 \oplus U_2 \oplus \ldots \oplus U_t .$$

The two inclusions give the stipulated equality.

Next we prove that, for all j, $\dim(U_j) \leq m/r$. To this end, suppose that $\Gamma_j = \{i_1, \ldots, i_{s-1}, i_s\}$, where $i_k h = i_{k+1}$ for $1 \leq k \leq s-1$, and $i_s h = i_1$. Let

$$X_j = M_{i_1} \oplus M_{i_2} \oplus \ldots \oplus M_{i_{s-1}} ,$$

or $X_j = 0$ if $s = 1$. If $u \in U \cap X_j$ then, say, $u = \sum_1^{s-1} m_k$, $m_k \in M_{i_k}$, and

$$u = uh = \sum m_k h$$

with $m_k h \in M_{i_{k+1}}$. Therefore, since the sum of the subspaces M_i is direct, this gives

$$m_1 = 0 \; ; \quad m_2 = m_1 h \; ; \quad \ldots \; ; \quad m_{k+1} = m_k h \; ; \quad \ldots \; ; \quad m_{s-1} = m_{s-2} h \; ;$$

and so

$$m_1 = m_2 = \ldots = m_{s-1} = 0 \; ;$$

$u = 0$, and thus $U \cap X_j = 0$. Since M_{i_s} is one complement for X_j in V_j , it follows that

$$\dim(U_j) \leq \dim(M_{i_s}) = m/r \; .$$

Finally, therefore,

$$\psi(h).m = \phi(h) = \dim(U) = \sum_1^t \dim(U_j) \leq tm/r \; .$$

That is,

$$r/t = a_\Omega(h) \leq 1/\psi(h) \; .$$

For the purposes of the next lemma let us call H "bad" if there is an FH-module M having property C .

Lemma 7.4 If H is a minimal bad group, minimal in that all its proper subnormal factors are not bad, then

(i) H is a simple group; and

(ii) H cannot be generated by two elements.

Proof. Let M be an FH-module having property C : then M is faithful, for otherwise $H/C_H(M)$ would be a bad proper subnormal factor of H .

(i) Let N be a non-trivial normal subgroup of H , and let Ω be the transitive H-space of degree r given by Theorem 3.9 (iii) , as in the preceding lemma. If $r > 1$ then there is an element $h \in H$

which has no fixed points on Ω . Every cycle of h on Ω has length 2 or more, hence $a_{\Omega}(h) \geq 2$, and, by Lemma 7.3 , $\psi(h) \leq \frac{1}{2}$. This contradicts the assumed property of M that for all $h \in H$, $\psi(h) > \frac{1}{2}$. It follows that $r = 1$ and therefore M , as N-module, is a direct sum of, say, s N-submodules all isomorphic to a fixed irreducible N-module U . For all $h \in N$,

$$\dim \mathrm{fix}_M(h) = s \dim \mathrm{fix}_U(h) ,$$

while

$$\dim(M) = s \dim(U) ,$$

so that $\psi_U(h) = \psi_M(h) > \frac{1}{2}$. Moreover, U is not trivial, otherwise N would centralize M . Thus U enjoys property C , N cannot be a proper subnormal factor, that is, a proper normal subgroup of H , and so $N = H$. This shows that H is simple.

(ii) If $h_1, h_2 \in H$, then

$$\dim \mathrm{fix}(h_1) > \tfrac{1}{2} \dim(M)$$

$$\dim \mathrm{fix}(h_2) > \tfrac{1}{2} \dim(M) ,$$

and therefore

$$\mathrm{fix}(h_1) \cap \mathrm{fix}(h_2) \neq 0 .$$

Thus M contains a non-zero trivial $gp(h_1, h_2)$-submodule, and since M contains no non-zero trivial H-submodule, it follows that h_1 and h_2 do not generate H . This completes the proof.

As a corollary, if H is any bad group, then H has a composition factor which cannot be generated by 2 elements. Consequently, if H is soluble then H is not bad, and if M is any non-trivial irreducible FH-module, then there is an element $h \in H$ for which $\phi(h) \leq \frac{1}{2} m$. The next section is devoted to improving this result.

8. Soluble groups.

We have already seen, in Lemmas 3.7 and 3.8 , how a primitive soluble permutation group gives rise to a faithful irreducible representation of one of its stabilizers; and, using Lemma 3.6 , Theorem 3(i) is an immediate consequence of Theorem 5(i) . The first part of this section is concerned with proving the latter theorem. In the second half we consider another problem about soluble permutation groups, a problem which arises out of the representation theory, and which gives an alternative, more promising but less successful, approach to Conjecture D .

For present purposes H will denote a non-trivial finite soluble group, F a field, and N a non-trivial abelian normal subgroup of H . M will denote a faithful irreducible FH-module, and I will assume the whole of the notation of Clifford's Theorem (3.9). In addition, I will write N_i for $C_N(M_i)$ $[= C_N(M_i^*)]$, and $\Omega = \{1, \ldots, r\}$ for the transitive H-space implicit in the third clause of 3.9 . Thus, if $h \in H$ and $1 \leq i \leq r$, then

$$M_{ih} = M_i h$$

and

$$N_{ih} = h^{-1} N_i h \ .$$

Notice that

$$\bigcap_1^r N_i \leq C_H(M) = 1$$

since M is a faithful H-module.

The first lemma will determine the structure of N for us:

Lemma 8.1 If N has exponent q, then there is an element $h \in N$ such that $\psi_M(h) < \frac{1}{q}$.

Proof. Since $\bigcap N_i = 1$, and since the N_i are all conjugate in H, their common index in N is, say, $q_o > 1$, and q divides q_o. Lemma 3.4 guarantees an element h contained in fewer than r/q_o of the groups N_i, and we put $U = \mathrm{fix}_M(h)$. Since N is abelian, U is an N-submodule of M, and, by Clause (ii) of 3.9,

$$U = U_1 \oplus U_2 \oplus \ldots \oplus U_r$$

where $U_i = U \cap M_i$, $i = 1, \ldots, r$. If $h \in N_i$ then $M_i \leq U$. Conversely, if $M_i \cap U \neq 0$ then $M_i \cap U$ is a sum of non-zero submodules isomorphic to M_i^*, therefore

$$h \in C_N(M_i \cap U) = C_N(M_i^*) = N_i .$$

Thus if $h \notin N_i$ then $M_i \cap U = 0$. This shows that U is the direct sum of those M_i for which $h \in N_i$, and therefore, since the spaces M_i all have the same dimension m/r, we have

$$m\,\psi(h) = \phi(h) = \dim(U) < \frac{r}{q_o} \cdot \frac{m}{r} = \frac{m}{q_o} .$$

that is, $\psi(h) < \frac{1}{q_o} \leq \frac{1}{q}$, and the lemma is proved.

Theorem 5 (ii) is an immediate consequence, for, if F has characteristic 2 then H, a group with a faithful irreducible representation over F, can contain no non-trivial normal 2-subgroup; hence the Fitting subgroup of H is of odd order, and the exponent of N is at least 3.

From now we add to our hypotheses that, for all $h \in H$,

$\psi_M(h) \geq \frac{1}{3}$, and then we have

Corollary 8.2 (i) H contains no non-trivial normal subgroup of odd order;

(ii) N is elementary abelian of exponent 2 ;

(iii) $|N:N_i| = 2$, $i = 1, \ldots, r$;

(iv) the H-space consisting of the N_i on which H operates by conjugation is H-isomorphic to Ω : in fact, for all $i \in \Omega$,

$$N_H(N_i) = H_i .$$

Parts (i), (ii) and (iii) follow directly from the lemma, since the hypothesis implies that $q \leq q_o < \psi(h)^{-1} \leq 3$. Part (iv) is just the fact that, since N is elementary abelian of exponent 2 , an irreducible representation of N is completely determined by its kernel. In fact, every element of N not contained in N_i ($1 \leq i \leq r$) operates on M_i as multiplication by -1 . Consequently, if $N_i = N_j$ then $M_i \cong M_j$ as N-modules, and so, from the definition of these modules, $M_i = M_j$. [Of course it is quite generally true that the H-space consisting of the groups N_i is an H-epimorphic image of Ω , but except when N has exponent 2 we cannot be sure that several of the modules M_i do not share the same centralizer.]

Lemma 8.3 r is not a power of 2 .

Proof. Take N , which is already elementary abelian of exponent 2 , to be a minimal non-trivial normal subgroup of H , and let K be the kernel of the permutation representation of H on Ω , so that,

by 8.2 (iv), $K = \bigcap_{i=1}^{r} N_H(N_i)$. I show first that $K = C_H(N)$. Certainly,

$$C_H(N) \leq \bigcap_{1}^{r} N_H(N_i) = K .$$

However, K normalizes all of $N_1, \ldots, N_r$; a suitable intersection of some of these groups is cyclic of order 2 and is also normalized - hence centralized - by K; therefore $C_N(K) \neq 1$. But $C_N(K)$ is normal in H and is contained in N. Minimality of N gives that $C_N(K) = N$, hence that $K \leq C_H(N)$: and so $K = C_H(N)$, as claimed.

Now N, being a minimal normal subgroup of H, is an irreducible H-module, hence a faithful irreducible $G = H/C_H(N)$-module over $GF(2)$. Consequently, G contains no non-trivial normal 2-subgroup. If G itself were trivial then r would be 1, N would be cyclic of order 2, and for the non-trivial element h of N we would have $\phi_M(h) = 0$, contradicting our assumptions. Therefore G is not trivial and, being soluble, must contain a non-trivial abelian normal subgroup A, whose order must then be odd. Now $G = H/K$ is a faithful permutation group on Ω, and so G_α ($\alpha \in \Omega$) contains no non-trivial normal subgroup of G. In particular, $A \not\leq G_\alpha$; therefore $|G_\alpha A : G_\alpha| > 1$; and

$$|G_\alpha A : G_\alpha| = |A : G_\alpha \cap A|$$

is an odd number which divides $|G : G_\alpha| = r$. Thus r is not a power of 2 and the proof is complete.

Proof of Theorem 5(i). The first step is to find an element $x \in H$, of odd order, and such that

$$\chi_\Omega(x) = |\mathrm{fix}_\Omega(x)| < \tfrac{1}{3}r .$$

To do this, let p be an odd prime which divides r (Lemma 8.3), and let P be a Sylow p-subgroup of H. Then P is not contained in any of the stabilizers H_ω, and therefore, for all $\omega \in \Omega$, $|P : P \cap H_\omega| \geq p \geq 3$. By Lemma 3.4, there is an element $x \in P$ contained in fewer than $r/3$ of the stabilizers H_ω, and of course x has odd order.

Next we need an element $y \in N$ which commutes with x and which is contained in fewer than a half of all those N_i which are normalized by x. The proof that such an element exists is as follows. Let $X = C_N(x)$, $Y = [N, x] = \mathrm{gp}(\{z^{-1}x^{-1}zx \mid z \in N\})$, so that both X and Y are x-invariant subgroups of N, and, because the order of x is odd, $N = X \times Y$. This is easiest to show if we again write N additively as an H-module over $GF(2)$, and consider conjugation by x as a linear transformation $\underline{x}$ of N. Then X is the null space, Y is the image space, of the linear transformation $1 - \underline{x}$. If $u \in X \cap Y$, say $u = v(1 - \underline{x})$ with $v \in N$, then

$$0 = u(1 - \underline{x}) = v(1 - \underline{x})^2 = v(1 - \underline{x}^2) ,$$

so that $v\underline{x}^2 = v$. But the order of $\underline{x}$ is, say, $2k + 1$, and it follows that $v = v\underline{x}^{2k+1} = v\underline{x}$. Hence $u = 0$; X and Y generate their direct sum; and since $\dim(X) + \dim(Y) = \dim(N)$, we have $N = X \oplus Y$. Or, back in the group H, $N = X \times Y$. Now, if x

normalizes N_i - that is, by 8.2 (iv), if $i \in fix(x)$ - then x acts trivially on N/N_i and so $N_i \geq Y$; conversely, if $N_i \geq Y$ then clearly N_i is normalized by x. Since no subgroup N_i can contain both X and Y it follows that, if N_i is normalized by x, then $N_i \cap X$ has index 2 in X. Therefore, by Lemma 3.4, there is an element $y \in X$ which is contained in fewer than $\frac{1}{2}|fix(x)|$ of the subgroups N_i which are normalized by x. And, since $y \in X$, x and y commute.

Lastly, we put $h = xy$ and calculate $\phi_M(h)$. Define

$$U = \sum_{i \in fix(x)} M_i \; ; \quad V = \sum_{i \notin fix(x)} M_i \; ,$$

so that U, V are x-invariant N-submodules of M, and $M = U \oplus V$. As a permutation of $\Omega - fix(x)$, x consists of cycles all of length 3 or more: therefore, as Lemma 7.3 shows,

$$\dim(fix_M(x) \cap V) \leq \frac{1}{3} \dim(V) \; .$$

Since x and y commute and their orders are coprime, they are both powers of h and so $fix(h) = fix(x) \cap fix(y)$. In particular,

$$\dim(fix_M(h) \cap V) \leq \frac{1}{3} \dim(V) \; .$$

Moreover, since y centralizes fewer than a half of all the M_i contained in U, we have

$$\dim(fix_M(y) \cap U) < \frac{1}{2} \dim(U)$$

and therefore also,

$$\dim(fix_M(h) \cap U) < \frac{1}{2} \dim(U) \; .$$

Now U, V are both h-invariant, so that

$$\mathrm{fix}_M(h) = (\mathrm{fix}_M(h) \cap U) \oplus (\mathrm{fix}_M(h) \cap V)$$

and so

$$\begin{aligned} \dim \mathrm{fix}_M(h) &< \tfrac{1}{2}\dim(U) + \tfrac{1}{3}(m - \dim(U)) \\ &= \tfrac{1}{3}m + \tfrac{1}{6}\dim(U) \ . \end{aligned}$$

However, x was chosen to ensure that

$$\dim(U) < \tfrac{1}{3}\dim(M) = \tfrac{1}{3}m \ ,$$

and so, finally,

$$\phi_M(h) < \tfrac{1}{3}m + \tfrac{1}{18}m = \tfrac{7}{18}m \ .$$

This completes the proof of the theorem.

An alternative approach to Conjecture D is suggested by Lemma 7.3 . In fact, it seems to be quite a strong restriction on a transitive soluble permutation group that the average orbit length of all its permutations is small. I shall use the rest of this section to prove

Theorem 8.4 If G is a transitive soluble permutation group, and if $\lambda(G) < 12/5$, then the degree n of G is a power of 2 .

As a corollary, from Lemmas 7.3 and 8.3 , if M is an irreducible FH-module, then for some $h \in H$, $\psi(h) \leq 5/12$, but, since $7/18 < 5/12$, this gives no great joy in practice. For the remainder of this section G denotes a faithful transitive soluble permutation group on Ω ; and, as usual, $\alpha \in \Omega$, and $|\Omega| = n$.

Lemma 8.5 Every prime divisor p of n satisfies

$$p^2/(2p - 1) < \lambda(G)$$

(and therefore $p < 2\lambda(G)$).

[This is true quite generally: G need not be soluble].

Proof. Let p be a prime divisor of n, and P a Sylow p-subgroup of G. Then P cannot be contained in any stabilizer, and so, for all $\omega \in \Omega$, $|P : P \cap G_\omega| \geq p$. Lemma 3.4 guarantees an element $g \in P$ contained in fewer than n/p of these groups $P \cap G_\omega$, - that is, $\chi(g) < n/p$. Now the length of a non-trivial cycle of g in Ω is a power of p, and therefore

$$\begin{aligned} t(g) &\leq \chi(g) + \frac{1}{p}(n - \chi(g)) \\ &= \frac{n}{p} + \frac{p - 1}{p}\chi(g) \\ &< \frac{n}{p}\left(1 + \frac{p - 1}{p}\right) = n.\frac{2p - 1}{p^2} . \end{aligned}$$

Hence

$$\lambda(G) \geq a(g) = \frac{n}{t(g)} > \frac{p^2}{2p - 1} ,$$

which is the desired inequality.

This lemma is, in general, not a bad generalisation of Theorem 8.4, but for small values of $\lambda(G)$ it is not nearly delicate enough: it would require $\lambda(G) \leq 9/5$ to exclude 3 as a divisor of the degree, but we know that, if G is non-trivial, then it contains fixed-point free permutations g, and so $\lambda(G) \geq a(g) \geq 2 > 9/5$. However, we do have the corollary:

Corollary 8.6 If $\lambda(G) < 25/9$, and *a fortiori* if $\lambda(G) < 12/5$, then the only primes which can divide n are 2 and 3.

For, if $p \geq 5$, then $p^2/(2p - 1) \geq 25/9 > 12/5$.

The next step is to study 2-groups in greater detail.

Lemma 8.7 If G is a 2-group and if $\lambda(G) < 8/3$, then G is elementary abelian of exponent 2 (therefore regular, and $\lambda(G) = 2$).

Proof. Suppose the lemma to be false, and let G denote a counterexample of smallest order, and, among counterexamples of that order, of least degree. If $g \in G$, then, since

$$a(g) \leq \lambda(G) < \frac{8}{3} < 4,$$

and since every cycle of g on G has length a power of 2, g must contain cycles of length 2 or 1. Consequently g^2 has fixed points. Therefore $G_\alpha \neq 1$, otherwise G would have exponent 2, would therefore be abelian, and would not be a counterexample. Now

(i) $G_\alpha \leq \Phi(G)$, the Frattini subgroup of G. For, if M is a maximal proper subgroup of G and if $G_\alpha \not\leq M$, then, since M is normal in G, $G_\alpha \cdot M = G$ and so M is transitive. As M-space Ω certainly inherits all the properties assumed for Ω as G-space, but M is smaller than G. Therefore M is elementary abelian and must be regular on Ω: $G_\alpha \cap M = 1$. Since M is normal, all stabilizers intersect M trivially, and therefore squares in G, which lie both in some stabilizers and in M, are trivial. Thus G has exponent 2 and is no counterexample, contradicting our original assumptions. So $G_\alpha \leq M$, and this for all maximal subgroups M, so that therefore $G_\alpha \leq \Phi(G)$.

(ii) $N_G(G_\alpha) \leq \Phi(G)$. Again, suppose not. Then there is a maximal subgroup M such that $N_G(G_\alpha) \not\leq M$. This implies that $N_G(G_\alpha).M = G$; and, by (i) , we also have $G_\alpha \leq M$. By Lemma 4.6 , if Ω_1 is the M-orbit in Ω containing α , then

$$\lambda_{\Omega_1}(M) = \lambda_\Omega(M) \leq \lambda_\Omega(G) < \frac{8}{3} .$$

The supposed minimality of G implies therefore that M acts as an elementary abelian 2-group on Ω_1 : and, in particular, $M_\alpha = G_\alpha$ is normal in M . However, since $N_G(G_\alpha) \not\leq M$, it follows that $N_G(G_\alpha) > M$, and therefore G_α is normal in G , and G is regular, which is not so. This contradiction shows that $N_G(G_\alpha) \leq \Phi(G)$.

(iii) $N_G(G_\alpha) = \Phi(G) = G_\alpha \times Z$, where $Z = \zeta(G)$ is cyclic of order 2 . For, if $z \neq 1$ is any element of the centre $\zeta(G)$, then since z^2 is contained in some stabilizer and is central in G , it must be 1 ; therefore, if $Z = gp(z)$, then Z is cyclic of order 2 , $Z \cap G_\alpha = 1$, and certainly

$$gp(G_\alpha, z) = G_\alpha \times Z \leq N_G(G_\alpha) \leq \Phi(G) .$$

On the other hand, if Ω_2 is the coset space $\Omega(G_\alpha \times Z)$ then, by Lemmas 3.1 and 4.5 , $\lambda_{\Omega_2}(G) \leq \lambda_\Omega(G) < 8/3$. By minimality of Ω , G then acts as an elementary abelian 2-group on Ω_2 . That is, $G_\alpha \times Z$ is normal in G and $G/(G_\alpha \times Z)$ is elementary abelian. Consequently, $G_\alpha \times Z \geq \Phi(G)$, and so

$$G_\alpha \times Z = \Phi(G) = N_G(G_\alpha) .$$

There remains only to show that $Z = \zeta(G)$. But we know that $\zeta(G) \leq N_G(G_\alpha) = \Phi(G)$, that $G_\alpha \cap \zeta(G) = 1$, and that the index of

G_α in $\Phi(G)$ is $|Z|$, which is 2. From this it follows that $|\zeta(G)| \leq 2$, and hence $\zeta(G) = Z$.

(iv) Both $\Phi(G)$ and G are elementary abelian of exponent 2. For,

$$\Phi(\Phi(G)) = \Phi(G_\alpha \times Z) = \Phi(G_\alpha) \times \Phi(Z) = \Phi(G_\alpha),$$

and so $\Phi(G_\alpha)$, being a normal subgroup of G contained in G_α, is trivial. Therefore G_α is elementary abelian, and so is $\Phi(G)$.

To complete the proof, choose $x \neq 1$, $x \in G_\alpha \cap \zeta_2(G)$. Such a choice is possible because $(G_\alpha \times Z)/Z$ is normal in G/Z, and every non-trivial normal subgroup of the nilpotent group G/Z has non-trivial intersection with its centre: and thus $G_\alpha \cap \zeta_2(G) \neq 1$. Let y be an element of G which does not commute with x. Such an element exists because x is not central in G. Then

$$[x,y] = x^{-1}y^{-1}xy \in \zeta_1(G) = Z,$$

and so we have $[x,y] = z$.

Now $y \notin \Phi(G)$ since, by (iv), $\Phi(G)$ centralizes x; and therefore also $xy \notin \Phi(G)$. In particular, neither y nor xy has any fixed points on Ω. Moreover, by (iv), G has exponent 4, so that both y and xy, as permutations of Ω, consist entirely of 2-cycles and 4-cycles. Let s_1, s_2 be the numbers of 2-cycles in y and in xy respectively: then it is easy to calculate that, since $a(y) < 8/3$, $s_1 > \frac{1}{4}n$, and similarly, $s_2 > \frac{1}{4}n$. Consequently,

$$\chi(y^2) = 2s_1 > \tfrac{1}{2}n;$$

$$\chi((xy)^2) = 2s_2 > \tfrac{1}{2}n;$$

so that $\mathrm{fix}(y^2) \cap \mathrm{fix}((xy)^2)$ is not empty. Thus

$$y^2.(xy)^2 = x^2y^4[x,y] = [x,y] = z$$

has at least one fixed point on Ω, and Z is contained in one of the stabilizers in G. This impossibility proves the lemma. In § 10 there is a sketch of an example which shows that this lemma cannot be improved.

Proof of Theorem 8.4. Again, assume the theorem to be false, and let G be a minimal counterexample and of least degree. Thus G is soluble, transitive and faithful on Ω, for all $g \in G$, $a(g) < 12/5$, and yet n is divisible by an odd prime. This prime, by Corollary 8.6 can only be 3. Actually, the minimality of G usefully restricts its structure still further.

(i) If N is a minimal normal subgroup of G then N is an elementary abelian 3-group, $|G : G_\alpha.N|$ is a power of 2, and $|G_\alpha N : G_\alpha| = |N : N \cap G_\alpha| = 3$.

Let $A = G_\alpha.N$ and let Ω_2 be the coset space $\Omega(A)$. Then, since $N \not\leq G_\alpha$, the degree of Ω_2 is $n/q < n$, where q, the index of G_α in A, is the index of $N_\alpha = N \cap G_\alpha$ in N. Since, by Lemma 4.5, $\lambda_{\Omega_2}(G) \leq \lambda_\Omega(G)$, it follows from the minimality of G and n that $|\Omega_2| = |G : G_\alpha N|$ is a power of 2. Therefore q, which is certainly a prime-power, must be a power of 3 and N is an elementary abelian 3-group. The intersections of N with the stabilizers in G are the conjugates in G of N_α and so they all have

index q in N. Some element g of N is contained (Lemma 3.4) in fewer than n/q of the stabilizers therefore, and since g consists then of $\chi(g) < n/q$ fixed points and $\frac{1}{3}(n - \chi(g))$ 3-cycles on Ω, we have

$$t(g) = \chi(g) + \frac{1}{3}(n - \chi(g)) = \frac{1}{3}n + \frac{2}{3}\chi(g) < \frac{n}{3}\frac{q+2}{q},$$

so that

$$\frac{12}{5} > \lambda(G) \geq a(g) = \frac{n}{t(g)} > \frac{3q}{q+2}.$$

This gives $q < 8$, and therefore $q = 3$.

(ii) N is complemented by a Sylow 2-subgroup in G.

Let Q be a Sylow 2-subgroup of G_α, P a Sylow 2-subgroup of G which contains Q. Then Q is also a Sylow 2-subgroup of A, and, since the index of A in G is a power of 2, $AP = G$. Thus $G_\alpha \cdot NP = G$, and so NP is a transitive subgroup of G. By minimality of G it follows that $G = NP$; and so also $G_\alpha = N_\alpha Q$; $A = NQ$.

(iii) $Q = \Phi(P)$.

Since N is contained in the kernel of G on $\Omega_2 = \Omega(A)$, it follows from (ii) that G acts on Ω_2 as a 2-group, and, since $\frac{12}{5} < \frac{8}{3}$, by Lemma 8.7, as an elementary abelian 2-group. Therefore $Q \lhd P$, and $Q \geq \Phi(P)$. On the other hand, if M is any maximal proper subgroup of P, and if $Q \not\leq M$, then $QM = P$,

$$G_\alpha NM = QNM = NQM = NP = G,$$

and so NM is a transitive proper subgroup of G, whereas, by minimality, G contains no such thing. Therefore $Q \leq M$ for all maximal proper subgroups M of P; hence $Q \leq \Phi(P)$; and so $Q = \Phi(P)$ as claimed.

(iv) As P-module over $GF(3)$, N is faithful and irreducible.

Irreducibility is simply the minimality of N as a normal subgroup of G. If $C = C_P(N)$ then $C \cap Q$ is normal in P, is centralized by N, and therefore is normal in $NP = G$, but is contained in G_α. Hence

$$C \cap Q = C \cap \Phi(P) = 1 .$$

If $Q \leq B \leq P$ and B/Q is a complement for CQ/Q in P/Q (B exists because P/Q is elementary abelian), then $B \cap C \leq Q \cap C = 1$, so that $P = B \times C$, and $G = BN \times C$. Now $G_\alpha \leq BN$ and $C \leq N_G(G_\alpha)$, so that, as BN-space, Ω is the union of $|C|$ isomorphic BN-orbits Ω_c, $c \in C$, for all of which $\lambda_{\Omega_c}(BN) = \lambda_\Omega(BN) < \frac{12}{5}$ (Lemmas 3.2 and 4.6). The degree of each orbit Ω_c is $n/|C|$ and is therefore not a power of 2. By minimality of G, $G = BN$, and so $C = 1$. Hence N is faithful as P-module.

(v) Q is elementary abelian.

For, N_α is a Q-invariant subspace of N, and by Maschke's Theorem ([CR], Theorem 10.8, p.41) is complemented in N: say $X \leq N$ is a Q-invariant complement for N_α. Then of course, $|X| = q = 3$, and the centralizer of X in Q must have cyclic factor group of order (dividing) 2. By Clifford's Theorem (3.9), N is the sum of Q-submodules conjugate to X, their centralizers conjugate in P to $C_Q(X)$, and intersecting trivially. Hence Q is elementary abelian.

To complete this portrait of G :

(vi) $\mathcal{Z}(P)$ is cyclic; and if z is the element of order 2 in $\mathcal{Z}(P)$, then z acts on N as multiplication by -1.

This is, of course, a familiar consequence of Schur's Lemma. But in any case, if z is any element of order 2 in $\mathcal{Z}(P)$, then the eigenvalues of z on N are $+1$ and -1, and since z is central in P, the corresponding eigenspaces are P-invariant. Since N is irreducible, one of these eigenspaces is 0, the other is N; and since N is a faithful P-module it is the eigenspace corresponding to $+1$ which is 0. Thus z acts as multiplication by -1 on N. If now z_o is any (other) element of order 2 in $\mathcal{Z}(P)$, then also z_o multiplies by -1; therefore $z_o z^{-1} \varepsilon C_P(N) = 1$, and so $z_o = z$. Thus z is the only element of order 2 in the centre of P, which is therefore cyclic.

(vii) $Q \geq Z = gp(z)$.

For, Q is not trivial, as otherwise P would be elementary abelian (by (iii)), hence cyclic of order 2 (by (vi)), and G would be the symmetric group of degree 3, which is certainly not a counterexample to the theorem. Therefore, as Q is normal in P, its intersection with $\mathcal{Z}(P)$ is not trivial, and so $z \varepsilon Q$. In particular, $\alpha z = \alpha$.

(viii) On Ω, z has $\frac{1}{3}n$ fixed points and $\frac{1}{3}n$ 2-cycles.

If T is a transversal - a complete set of right coset representatives - for Q in P, then XT is a transversal for G_α in G:

$$G_\alpha XT = QN_\alpha XT = QNT = NQT = NP = G.$$

Therefore if $\omega \in \Omega$ then there is a unique element xt, $x \in X$, $t \in T$, such that $\alpha xt = \omega$. Then $\omega z = \omega$ if and only if

$$\alpha xt = (\alpha xt)z = \alpha xzt = \alpha z.z^{-1}xzt = \alpha x^{-1}t$$

(the last equality depends on (vi) and (vii)); that is, $\omega z = \omega$ if and only if $x = x^{-1}$, or, since x has odd order, if and only if $x = 1$. Hence z fixes precisely $|T| = \frac{1}{3}n$ of the points of Ω, and has $\frac{1}{2}(n - \frac{1}{3}n) = \frac{1}{3}n$ 2-cycles on Ω.

(ix) $Q \neq Z$, and $Z = \zeta(P)$.

Suppose that z had a square root in P, say $u^2 = z$. Then $u \notin Q$, for otherwise u^2 would be contained in $C_Q(X)$ and we know that it is not. Therefore u has no fixed points on Ω, and it follows from (viii) that u consists of $\frac{1}{2}.\frac{1}{3}n$ 2-cycles, and $\frac{1}{2}.\frac{1}{3}n$ 4-cycles. That is, $t(u) = \frac{1}{3}n$ and $a(u) = 3$, contradicting our original assumptions. Hence z can have no square root in P. It follows then that $Z = \zeta(P)$, and that $Q = \Phi(P) > Z$.

The structure of P has now been shown to be similar to that of the group G in the proof of Lemma 8.7 : the final step in the argument is also similar to the last part of the proof of that lemma. Choose $x \in (Q \cap \zeta_2(P)) - Z$: such an element exists because the non-trivial normal subgroup Q/Z of P/Z has non-trivial intersection with the centre $\zeta_2(P)/Z$ of P/Z. Choose $y \in P$ so that y does not commute with x, and then $[x,y] = z$. Then $y \notin Q$ (by (v)), therefore $xy \notin Q$, and so neither y nor xy has fixed points on Ω. Since P has exponent 4 (see (iii) and (v)), both y and xy consist

entirely of 2-cycles and 4-cycles . If the numbers of 2-cycles in y and in xy are s_1 and s_2 respectively, then

$$t(y) = s_1 + \frac{1}{4}(n - 2s_1) = \frac{n}{4} + \frac{1}{2}s_1 ,$$

and it follows from the assumption that $a(y) < \frac{12}{5}$, that $s_1 > \frac{1}{3}n$; and similarly $s_2 > \frac{1}{3}n$. Therefore $\chi(y^2) > \frac{2}{3}n$, and $\chi((xy)^2) > \frac{2}{3}n$, so that

$$\chi(y^2.(xy)^2) > \frac{1}{3}n$$

But $y^2(xy)^2 = z$, and, by (viii) , $\chi(z) = \frac{n}{3}$. This contradiction establishes the theorem.

I doubt very much that $12/5$ is the 'right' upper bound in Theorem 8.4 . In fact I know of no transitive group G whose degree is divisible by an odd prime number, and for which $\lambda(G) < 3$.

9. Primitive groups containing regular normal subgroups.

This section is devoted to proving Clause (ii) of Theorem 3 . We suppose that G is a primitive group containing a regular normal subgroup A , so that (Lemma 3.7) $G_\alpha = H$ operates faithfully as a group of automorphisms of A in such a way that A is H-simple, and H is a complement for A in G . There are three cases to be considered: A is non-abelian and not simple, or A is a non-abelian simple group, or A is abelian.

Case 1. If A is non-abelian and not simple then, since A is characteristically simple, $A = S_1 \times S_2 \times \ldots \times S_r$, say, where $r > 1$

and $S_i \cong S$, $i = 1, \ldots, r$, and S is a non-abelian simple group. Now, as is well-known (see [H], pp 127-131 , or [S], p.84) any automorphism of A permutes the factors S_i , and thus, since A is H-simple, H acts as a transitive permutation group on the factors. From here the proof is very similar to the proof of Lemma 7.3 .

Let $\Delta = \{1, \ldots, r\}$ be the H-space such that, for all $h \in H$, $S_i^h = S_{ih}$ $i = 1, \ldots, r$. Let $h \in H$ be an element with no fixed points on Δ (Corollary to 3.4), let $\Gamma_1, \ldots, \Gamma_t$ be the cycles of h on Δ , and put

$$T_j = \prod_{i \in \Gamma_j} S_i \qquad j = 1, \ldots, t .$$

Then h normalizes each of $T_1, \ldots, T_t$, so that

$$C_A(h) = C_{T_1}(h) \times C_{T_2}(h) \times \ldots \times C_{T_t}(h) .$$

However,

$$|C_{T_j}(h)| \leq |S| \qquad 1 \leq j \leq t ,$$

hence

$$|C_A(h)| \leq |S|^t ;$$

while

$$|T_j| \geq |S|^2 \qquad 1 \leq j \leq t ,$$

so that

$$|A| \geq |S|^{2t} .$$

Therefore

$$|C_A(h)| \leq |A|^{\frac{1}{2}} ,$$

and, by Lemma 3.6 ,

$$\mu(G) \leq \chi(h) = |C_A(h)| \leq |A|^{\frac{1}{2}} = n^{\frac{1}{2}} < n(\log n)^{-\frac{1}{2}} .$$

Case 2. A is a non-abelian simple group. In this case, if $1 \neq h \in H$, and $|A : C_A(h)| = k$, then $k! \geq n$, for otherwise the homomorphism of A into the symmetric group S_k which describes the permutation representation of A on the coset space $\Omega(C_A(h))$ would have non-trivial kernel, and A would not be simple. Hence $k^k > n$, and

$$k^2 > k \log k > \log n ,$$

$$k > (\log n)^{\frac{1}{2}}$$

and so

$$|C_A(h)| = |A|/k < n(\log n)^{-\frac{1}{2}} .$$

Again then, by Lemma 3.6, $\mu(G) < n(\log n)^{-\frac{1}{2}}$.

Case 3. A is abelian, elementary abelian of exponent p, say. In this case, if $h \in H$, $h \neq 1$, then certainly $|C_A(h)| \leq n/p$, so that (3.6)

$$(*) \qquad \mu(G) \leq n/p .$$

On the other hand, A is an irreducible H-module over GF(p) (3.7 , note 1) of dimension m, where $n = |A| = p^m$. If $u \in A$, $u \neq 0$, then the set $\{uh \mid h \in H\} = uH$ spans an H-submodule of A, and therefore spans A itself. Consequently, $|uH| \geq m$ - and in fact, $|uH| > m$, since if uH contained precisely m elements then their sum, which is clearly invariant under H, would not be zero. However, $|uH| = |H : C_H(u)|$, and so $|H : C_H(u)| \geq m + 1$ for all non-zero $u \in A$. By Lemma 3.4, there is an element $h \in H$

contained in fewer than $\frac{|A| - 1}{m + 1}$ of the centralizers of non-zero elements of A. That means,

$$|C_A(h)| < \frac{|A| - 1}{m + 1} + 1 = \frac{n + m}{m + 1} \leq \frac{n}{m} .$$

This last inequality holds whenever $m^2 \leq n$. But if $m^2 > n = p^m$, then $p = 2$, $m = 3$, $n = 8$, and actually $\mu(G) = 1$. In every case therefore, by Lemma 3.6,

$$(**) \qquad \mu(G) < \frac{n}{m} = n \frac{\log p}{\log n} .$$

From (*) and (**) we get

$$\mu(G) \leq \min\left(\frac{n}{p}, n \frac{\log p}{\log n}\right) .$$

As functions of p, n/p is decreasing, $n \log p / \log n$ is increasing. therefore

$$\min\left(\frac{n}{p}, n\frac{\log p}{\log n}\right) \leq \frac{n}{q} ,$$

where q satisfies the equation

$$\frac{n}{q} = \frac{n \log q}{\log n} ,$$

that is,

$$\log n = q \log q < q^2 .$$

Thus in this case also,

$$\mu(G) \leq \frac{n}{q} < n(\log n)^{-\frac{1}{2}} .$$

The three cases cover every possibility, and so $f_{rn}(n) < n(\log n)^{-\frac{1}{2}}$ The proof clearly gives that, as $n \to \infty$,

$$\frac{f_{rn}(n)}{n(\log n)^{-\frac{1}{2}}} \to 0 ,$$

a strengthening of Theorem 3 (ii), but cold comfort all the same.

CHAPTER III: EXAMPLES

10. Some transitive groups.

There are very many transitive groups G in which $\mu(G)$ is near $\frac{1}{2}n$. The following three examples give some indication of their variety. We begin by proving Clause (ii) of Theorem 1.

Example 1. Let A be any group and let G be the split extension of $A \times A$ by its automorphism of order 2 which interchanges the two factors, that is, G is isomorphic to the wreath product A wr C_2. Denote the factors of the direct square by A_1 and A_2, and define Ω to be $\Omega(A_1)$ as G-space. This is certainly a faithful permutation representation of G, and there are just two distinct stabilizers, namely A_1 and A_2: $S(G) = A_1 \cup A_2$, and, if $g \in S(G) - \{1\}$ then $\omega g = \omega$ ($\omega \in \Omega$) if and only if $\omega = A_1 x$ with $x \in A_1 \times A_2$. Thus $\chi(g) = |A|$ for $g \in S(G) - \{1\}$, while $n = |\Omega| = 2|A|$. That is, every non-trivial element of $S(G)$ has precisely $\frac{1}{2}n$ fixed points, and so $\mu(G) = \frac{1}{2}n$.

If n is a given even integer, we may take for A any group of order $\frac{1}{2}n$, and the example then shows that $f_{trans}(n) \geq \frac{1}{2}n$. By Theorem 1(i), therefore, if n is even, then $f_{trans}(n) = \frac{1}{2}n$.

Next a sketch of some transitive groups in which the unions of the stabilizers are subgroups - the situation which appeared in the proof given in §5.

Example 2. Let N be an elementary abelian group of order p^m, let r be an integer, $0 < r < m$, and let X be a group of automorphisms of N which acts transitively on the subgroups of order p^r: the full automorphism group of N is one example. Let G be the split extension $N.X$ of N by X, let $A < N < G$ be any subgroup of order p^r in N, and put $\Omega = \Omega(A)$. Then G is faithful and transitive on Ω, and clearly, $S(G) = N$

In the special case where $p = 2$, $r = m-1$ and X is the cyclic group of automorphisms of N of order $2^m - 1$, every subgroup of order 2^{m-1} in N occurs as the stabilizer of precisely two elements of Ω, and every non-trivial element of N lies in $2^{m-1} - 1$ distinct subgroups of order 2^{m-1}. Therefore $\mu(G) = 2^m - 2$, while $n = 2^{m+1} - 2$. In this case therefore, $\mu(G) = \frac{1}{2}n - 1$.

A similar, slightly more sophisticated construction gives groups which show Lemma 8.7 to be best possible.

Example 3. Let m be a natural number, and let N be an elementary abelian group of order 2^{m+1}:

$$N = gp(g_0, g_1, \ldots, g_m \mid g_i^2 = [g_i, g_j] = 1, \ 0 \le i \le m, \ 0 \le j \le m).$$

Let x_i, $1 \le i \le m$, be the automorphism of N such that

$$g_i^{x_i} = g_0 g_i$$

$$g_j^{x_i} = g_j \quad \text{if} \quad j \neq i.$$

Then $X = gp(x_1, \ldots, x_m)$ is an elementary abelian subgroup of the automorphism group of N, of order 2^m. Let G be any extension

of N by X acting as described, considered as permutation group on the coset space $\Omega = \Omega(A)$, where $A = gp(g_1, \ldots, g_m) < N$.

The centre of G is the subgroup generated by g_o, for certainly, no element outside N centralizes the whole of N; and the element

$$g_o^{\varepsilon} g_{i_1} g_{i_2} \cdots g_{i_r}$$

$\varepsilon = 0$ or 1, $r > 0$, $1 \leq i_1 < i_2 < \ldots < i_r \leq m$, does not commute with an element $x \in G$ such that $xN/N = x_{i_1} \in X$. Consequently A contains no non-trivial normal subgroup of G and Ω is a faithful G-space. A very similar calculation shows that $N_G(A) = N$. There are therefore precisely $2^m = |G:N|$ distinct conjugates of A in G, none of which contain g_o, all of them contained in N. However, N contains precisely 2^m subgroups of order 2^m which do not contain g_o, and each of these must therefore be a stabilizer in G. Each stabilizer is the stabilizer of precisely 2 elements of Ω: the stabilizer of $Ag \in \Omega$ is also the stabilizer of Agg_o. Now if $g \in N - \{g_o, 1\}$, then there are precisely 2^{m-1} distinct subgroups of N of order 2^m which contain g and do not contain g_o. Therefore $S(G) = N - \{g_o\}$, and if $g \in S(G) - \{1\}$, then $\chi(g) = 2^m = \frac{1}{2}n$, for the degree n is 2^{m+1}. Thus here are more groups G for which $\mu(G) = \frac{1}{2}n$.

Furthermore, if g_o has no square root in G, then $\lambda(G) = \frac{8}{3}$. For, if $g \in G$ has order 2 then certainly $a(g) \leq 2 < \frac{8}{3}$. If g has order 4, then $g \notin N$, but $g^2 \in N$. Consequently, since

$g^2 \neq 1$, and $g^2 \neq g_0$, g^2 has precisely $\frac{1}{2}n$ fixed points. Thus g consists of $\frac{1}{2}\cdot\frac{1}{2}n$ 2-cycles and $1/4\cdot\frac{1}{2}n$ 4-cycles on Ω; that is, $t(g) = \frac{3}{8}n$ and $a(g) = \frac{8}{3}$.

To ensure that g_0 has no square root it is sufficient (and necessary) that every element of $G/gp(g_0)$ not contained in $N/gp(g_0)$ has order 4. Such an extension of N by X does exist whenever $m \geq 3$ (and not for $m = 1, 2$), but I have not been able to find a proof of this which is free of unilluminating, lengthy calculations. However, for $m = 3$ such an extension can be described quite easily as a permutation group on $\{1, 2, \ldots, 16\}$. Namely, let h_1, h_2, h_3 be elements of G which map onto x_1, x_2, x_3 respectively, under the canonic homomorphism of G onto X. Then we can take

$$g_0 = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)(11\ 12)(13\ 14)(15\ 16)$$
$$g_1 = (1\ 2)(3\ 4)(5\ 6)(7\ 8)$$
$$g_2 = (1\ 2)(3\ 4)(9\ 10)(11\ 12)$$
$$g_3 = (1\ 2)(5\ 6)(9\ 10)(13\ 14)$$
$$h_1 = (1\ 9\ 2\ 10)(3\ 11\ 4\ 12)(5\ 13)(6\ 14)(7\ 15)(8\ 16)$$
$$h_2 = (3\ 7\ 4\ 8)(9\ 13\ 10\ 14)(1\ 5)(2\ 6)(11\ 15)(12\ 16)$$
$$h_3 = (1\ 3\ 2\ 4)(5\ 7\ 6\ 8)(9\ 11)(10\ 12)(13\ 15)(14\ 16).$$

It is straightforward to check that $N = gp(g_0, g_1, g_2, g_3)$ is a normal elementary abelian subgroup of $G = gp(h_1, h_2, h_3)$, and that conjugating with h_1, h_2, h_3 does give the specified automorphisms of N. A similar calculation shows that

$$h_1^2 = g_2 \qquad [h_2, h_3] = g_2$$
$$h_2^2 = g_1 g_3 \qquad [h_1, h_3] = g_3$$
$$h_3^2 = g_1 \qquad [h_1, h_2] = g_1 g_2 .$$

From these relations it is equally easy to verify that the elements of order 2 in $G/gp(g_o)$ are indeed contained in $N/gp(g_o)$. Therefore G is a non-abelian 2-group for which $\lambda(G) = \frac{8}{3}$, as required.

Of course, from this one extension in which the non-trivial central element has no square root one can make arbitrarily large examples simply by forming generalised direct products of several copies of this group G amalgamating their centres.

11. Some primitive groups.

The following is a polished version due to Dr Wiegold of the examples which first aroused our interest in the problems described in this thesis.

Example 4. Let G be the direct square $A \times A$ of a group A, let H be the diagonal, $H = \{(a, a) \mid a \in A\}$, and consider G as permutation group on the coset space $\Omega = \Omega(H)$. If A is simple then it follows directly from the converse of Lemma 3.7 that G is primitive, for then either direct factor is a regular normal subgroup in G and H acts as its group of inner automorphisms. Professor Higman has suggested the following elegant direct treatment:

(i) As G-space Ω is isomorphic to A on which G operates as the group of all permutations of the form $x \to a^{-1}xb$, $x \in A$, $(a, b) \in G$;

(ii) Ω is faithful if and only if the centre of A is trivial;

(iii) Ω is primitive (and faithful) if and only if A is simple.

The first statement is merely the observation that the stabilizer of $1 \in A$ is the diagonal $H \leq G$. Then (ii) follows because, if $a^{-1}xb = x$ for all $x \in A$, then in particular, $a^{-1}1b = 1$, so that $a = b$, and then $a^{-1}xa = x$ for all $x \in A$ if and only if $a \in \zeta(A)$. The reason for (iii) is that the equivalence class E containing $1 \in A$ under an equivalence relation $\underline{e}$ which is G-invariant, is a normal subgroup of A. For, if $x, y \in E$, then $1 \underline{e} x$ and $1 \underline{e} y$, so that (operating with the element $(x, 1)$ of G) $x^{-1} \underline{e} 1$, and (operating with $(1, y)$) $y \underline{e} xy$. By symmetry and transitivity of $\underline{e}$ we get $x^{-1} \in E$ and $xy \in E$ - and therefore E is a subgroup of A. And, if $a \in A$ then operating with (a, a) gives $1 \underline{e} a^{-1}xa$, that is, $a^{-1}xa \in E$. Hence E is a normal subgroup of A. Conversely, the cosets of a normal subgroup are clearly the equivalence classes of an equivalence relation on A invariant under G.

As has already been observed, the direct factors

$$A_1 = \{(a, 1) \mid a \in A\}, \qquad A_2 = \{(1, a) \mid a \in A\}$$

are always regular normal subgroups in G; H acts on these as their groups of inner automorphisms (in fact, G was first constructed as the split extension of the simple group A by its group of inner

automorphisms). It is easy to calculate, and is in any case a consequence of Lemma 3.6 , that if $g \in G$ is conjugate to, say, $(a, a) \in H$, then

$$\chi_{\Omega}(g) = |C_A(a)| .$$

From now we assume that A is a finite simple group. In this case G is primitive on Ω , and A_1, A_2 are the only regular normal subgroups in G - which illustrates Note 3 of Lemma 3.7 . If Conjecture A_{rn} is correct, then G contains some element g for which

$$1 \leq \chi_{\Omega}(g) \leq n^{\frac{1}{2}} = |A|^{\frac{1}{2}} .$$

Therefore A contains an element a for which $|C_A(a)| < |A|^{\frac{1}{2}}$. Thus Conjecture W is indeed a consequence of Conjecture A_{rn} .

A second, closely related application of this construction uses simple groups with relatively large centralizers to show that $\gamma \geq \gamma_{rn} \geq \frac{1}{3}$. Specifically, take for A the group $PSL(2, p)$ where p is prime and $p \geq 5$. This is the factor group of the group of all non-singular 2 by 2 matrices over $GF(p)$ whose determinants are squares in the field, by its centre, the group of non-zero scalar matrices. As is well-known, $PSL(2, p)$ is simple, its order is $\frac{1}{2}(p - 1)\, p\, (p + 1)$, and maximal cyclic subgroups have orders $\frac{1}{2}(p - 1)$, p, and $\frac{1}{2}(p + 1)$ (see [B], § 318 , p.440). In particular therefore, if $a \in A$, then $|C_A(a)| \geq \frac{1}{2}(p - 1)$. In this case then,

$$\mu(G) = \min_{a \in A} |C_A(a)| = \tfrac{1}{2}(p - 1) .$$

Consequently, if $n = \frac{1}{2}(p-1)p(p+1)$ and $p \geq 5$, then

$$f(n) \geq f_{rn}(n) \geq \tfrac{1}{2}(p-1) > (\tfrac{1}{8}n)^{1/3},$$

and since there are infinitely many prime numbers [Euclid] this gives

$$\gamma \geq \gamma_{rn} \geq \tfrac{1}{3}.$$

In the next section we describe examples which give a better (i.e., bigger) lower bound for f, f_{rn}, and also for f_{sol}, but the construction embodied in Example 4 gives a portmanteau example with other uses besides. I give two more of its applications in §13, and Dr Olaf Tamaschke has used it in yet another context (oral communication).

12. Some linear groups and primitive soluble permutation groups.

According to a well-known theorem - known as Euler's Theorem in Rigid Body Mechanics - every rotation in euclidean 3-dimensional space has an axis. Consequently the finite groups of rotations of 3-space, the dihedral groups, the tetrahedral group (isomorphic to A_4, the alternating group of degree 4), the octahedral group (isomorphic to S_4) and the icosahedral group (isomorphic to A_5), all have representations of degree 3 over the real numbers in which every element fixes a subspace of dimension 1. These representations of the dihedral groups are reducible; the representations of A_4, S_4 and A_5 are irreducible. The procedures described in §7 can

be used to obtain further representations with similar properties, over fields of characteristic $p > 0$, at least when $p \nmid |A_4|$, $p \nmid |S_4|$ or $p \nmid |A_5|$, respectively. Actually, since A_4 and S_4 are already the groups of rotations of r a t i o n a l 3-space leaving invariant a regular tetrahedron and a regular octahedron respectively, we can get in this way irreducible representations of degree 3 of A_4 and S_4 over the prime field $GF(p)$, at least if $p \geq 5$ (and actually, even if $p = 3$). And, since A_5 is the group of rotations of 3-space leaving invariant a regular icosahedron, over a quadratic extension of the rationals (namely, with $\sqrt{5}$ adjoined), we can obtain irreducible representations of A_5 of degree 3 over $GF(p^2)$ at least if $p \geq 7$ (and actually also for $p = 3$), and over $GF(p)$ for suitable primes p (namely, $p \equiv \pm 1 \ (5)$).

As illustration we consider only the case of A_4 in greater detail:

Example 5. The matrices

$$a = \begin{pmatrix} 1 & & \\ & -1 & \\ & & -1 \end{pmatrix} \qquad b = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

generate a group H isomorphic to A_4. For, b, a permutation matrix, has order 3;

$$b^{-1}ab = \begin{pmatrix} -1 & & \\ & 1 & \\ & & -1 \end{pmatrix} \qquad b^{-2}ab^2 = \begin{pmatrix} -1 & & \\ & -1 & \\ & & 1 \end{pmatrix}$$

so that the conjugates of a by the powers of b form, with the

unit matrix, an elementary abelian group of order 4. (Clearly H leaves invariant the octahedron whose six vertices are at the points $(\pm 1, 0, 0)$, $(0, \pm 1, 0)$, $(0, 0, \pm 1)$. The rotation of order 4,

$$c = \begin{pmatrix} 1 & & \\ & 0 & 1 \\ & -1 & 0 \end{pmatrix}$$

whose square is a, also leaves this octahedron invariant, and, with b generates the group of all rotations leaving it invariant. H is the subgroup consisting of all rotations leaving invariant the two regular tetrahedra which can be inscribed, their vertices at the midpoints of faces, in the octahedron.) Since all that is required in the above proof that $H \cong A_4$ is that $1 \neq -1$, the matrices a, b, interpreted as matrices over any field F of characteristic $p \neq 2$, generate a group, which we also denote by H, isomorphic to A_4.

The corresponding H-module M, spanned by, say, u_1, u_2, u_3 over F, with

$$u_1 a = u_1 \qquad u_1 b = u_2$$
$$u_2 a = -u_2 \qquad u_2 b = u_3$$
$$u_3 a = -u_3 \qquad u_3 b = u_1$$

is irreducible. For, the only 1-dimensional subspaces invariant under N, the normal closure of a in H, are the subspaces spanned by u_1, by u_2 and by u_3, and these are generators for M as $gp(b)$-module.

Any element of order 2 in H is conjugate to a, whose fixed space has dimension 1, spanned by u_1. Similarly, an element of order 3 in H is conjugate to b or b^2, whose fixed point space also has dimension 1, spanned by $u_1 + u_2 + u_3$. Therefore, for all $h \in H$,

$$\phi_M(h) \geq 1 = \frac{1}{3}\dim(M) .$$

We get directly:

Example 6. Let G be the split extension of (the additive group of) M, defined over $GF(p)$, $p \geq 3$, by H, and consider the permutation representation of G on the coset space $\Omega = \Omega(H)$. Then G is soluble because H is soluble, primitive on Ω, of degree $n = p^3$, and

$$\mu(G) = p = n^{1/3} .$$

Consequently, if $n = p^3$ and $p \geq 3$, then

$$f(n) \geq f_{rn}(n) \geq f_{sol}(n) \geq n^{1/3} ,$$

and so

$$\gamma \geq \gamma_{rn} \geq \gamma_{sol} \geq \frac{1}{3} .$$

Thus Theorem 2(ii) and Theorem 3(iii) are proved.

Next a sketch of how Example 5 may be used to construct soluble groups X with irreducible representations of arbitrarily large degree m for which $\phi_M(x) \geq \frac{1}{6}m$ for all $x \in X$.

Example 7. Let Y be an elementary abelian group of order 2^k, $k > 0$, let M be the direct sum of 2^k vector spaces M_y $y \in Y$, of dimension 3 over the field F (char$(F) \neq 2$), let H_1 be the group of linear automorphisms of M which centralizes M_y, $y \neq 1$,

and acts as described in Example 5 on M_1. Identify Y with the group of linear transformations of M which permute its direct summands: $M_{y_o} y = M_{y_o y}$ for all y_o, $y \in Y$; and let X be the group of automorphisms of M generated by H_1 and Y. Then it is not hard to see that X is isomorphic to the wreath product H wr Y, that is, A_4 wr Y, and that M is irreducible as X-module. The degree of M is $m = 3.2^k$, and, for all $x \in X$, $\phi(x) \geq \frac{1}{6}m$.

Finally, some remarks on Theorem 4. If $\mathrm{char}(F) \neq 2$, H is an elementary abelian group of order 2^k ($k \geq 2$), and M is the complement of the trivial submodule in the regular representation module FH of H over F, then since in FH,

$$\dim \mathrm{fix}_{FH}(h) = \tfrac{1}{2} \dim(FH)$$

for $1 \neq h \in H$, it follows that

$$\phi_M(h) = \dim \mathrm{fix}_M(h) = \tfrac{1}{2}(\dim(M) - 1) .$$

But of course, M contains no trivial H-submodule. This shows that Theorem 4 cannot be improved merely by weakening the condition on $\phi_M(h)$.

A deduction from Theorem 4 is, by Corollary 4(ii), that if the group H has a faithful module M of dimension m over the field F whose characteristic is zero or does not divide $|H|$, and if $\phi_M(h) \geq m - 1$ for all $h \in H$, then M contains an $(m - 1)$-dimensional trivial submodule, which must be complemented then by a 1-dimensional faithful module: and since H has a 1-dimensional faithful module, H itself must be cyclic. The situation is completely

different when $\mathrm{char}(F) \mid |H|$. If F has characteristic $p > 0$, H is elementary abelian of order p^k , and M is the module of dimension $m = k + 1$ over F , similar to that used in Example 3 : namely, M is spanned by elements $u_0, u_1, \ldots, u_k$, and H is generated by elements $h_1, \ldots, h_k$, where

$$\left.\begin{aligned} u_i h_i &= u_0 + u_i \\ u_j h_i &= u_j \quad \text{if } j \neq i \end{aligned}\right\} \quad 1 \leq i \leq k ,$$

then it is easy to see that, for all $h \in H$, if $h \neq 1$ then

$$\phi_M(h) = k = m - 1 .$$

Nevertheless, M is a faithful H-module, it is even indecomposable, and its trivial submodule is only 1-dimensional, spanned by u_0 .

CHAPTER IV: MISCELLANY

These last two sections contain some brief remarks which have very little connection with the rest of this essay.

13. An unfortunate theorem of Cauchy, and a question of Wielandt.

In [1] Cauchy stated (in a quite different language):

13.1 If G is a primitive permutation group of degree $p + 1$, where p is prime and $p > 2$, then G is 2-fold transitive.

He deduced this from

13.2 If G is a transitive group of degree n, and if G is not 2-fold transitive, then either G is primitive or the order of a stabilizer is the order of a transitive group whose degree is smaller than $n - 1$ and divides $n - 1$,

which he announced, but for which he gave no proof. Frobenius ([3], p.353) and later de Séguier ([de S], p.86, footnote 4) drew attention to counterexamples to 13.2, but they both pointed out hopefully that 13.1 is nevertheless true for $p \leq 13$. Huppert ([4], p.304) raises 13.1 to the status of a conjecture:

"Die folgende, bisher unbewiesene Vermutung stammt schon von CAUCHY . . . "

and he proves it under the assumption that G is soluble. And W.R. Scott gives (in [S], §§ 13.7, 13.8) a verification for $p \leq 37$ in the special case of groups G which contain regular subgroups.

If, in Example 4 , we take for A the simple group A_5 of order 60 , then the resulting permutation group G is primitive, its degree is $60 = 59 + 1$, and it is not 2-fold transitive: but 59 is prime and $59 > 2$. The simple groups of orders 168, 360, ... give rise to similar counterexamples to Cauchy's statement.

There is considerable interest in primitive permutation groups containing regular subgroups (see, for example, [W] Chapter 4 , or [S] Chapter 13). In this context, if G is constructed from the simple group A according to the recipe of Example 4 , then every factorisation of A as a product, $A = XY$, $X \cap Y = 1$, with X and Y subgroups of A , gives rise to a regular subgroup in G , namely, in the obvious notation, to the subgroup $X_1 \times Y_2$ with $X_1 \leq A_1$, $Y_2 \leq A_2$. So, for example, if, as above, A is $A_5 = A_4 . C_5$, then $A_4 \times C_5$ appears as a regular subgroup in the resulting primitive group G of degree 60 . This suggests that a question of Wielandt should be slightly modified: on page 64 of [W] he defines a group H to be a "B-group" if every primitive permutation group G containing H as a regular subgroup is 2-fold transitive, and on page 69 he asks "Is the direct product of a B-group and a group of relatively prime order always a B-group?" Since A_4 is a B-group (every primitive group of degree 12 , whether or not it contains a regular subgroup, is 2-fold transitive - Frobenius, and de Séguier, attribute this to Jordan), while $A_4 \times C_5$ appears as a regular

subgroup in the group G described above, which is not 2-fold transitive, the answer to Wielandt's question is, in general, no. John Macdermott has kindly pointed out to me that another example comes directly from Theorem 25.7 on page 67 in [W], for $C_6 \times C_6$ is not a B-group, whereas $C_6 \times C_6 \cong (C_2 \times C_2) \times (C_3 \times C_3)$ and $C_2 \times C_2$, the elementary abelian group of order 4, is a B-group. Perhaps the question should read:

"Is the direct product of a B-group and a B-group of relatively prime order always a B-group?"

There is some connection between B-groups and the structure of factorisable groups (see [S], Chapter 13) and, in fact, Example 4 and the remarks above show that if there is a simple group factorisable as the product of two B-groups of relatively prime order, then the answer to the modified question would also be negative.

14. Remarks on Lemma 3.5.

I am indebted to Professor Higman for the proof given on page 17. Wielandt gives a slightly different proof of the result ([W], Theorem 18.2, p.49). Curiously, he claims in the preface of [W], on page viii, that this theorem is new, whereas it appears already as Théorème 395 in Jordan's work ([J], pp 281-284) stated there in the language of the 19th Century Theory of Equations. De Séguier ([de S], p.85) states a stronger theorem - which he ascribes to Jordan (l.c.) - namely that, in the notation of Lemma 3.5,

every composition factor of G_α is also a composition factor of G_α^Δ. However, his proof is incomplete, and his theorem is false.

Example 8. S_8, the symmetric group on $\Omega = \{1, 2, \ldots, 8\}$, has a primitive representation of degree 56 on $\Omega = \{\omega \mid \omega \subset \Omega, |\omega| = 3\}$. Certainly S_8, being 3-fold transitive on Ω, acts as a transitive permutation group which we will denote by G on Ω. If $\alpha = \{1, 2, 3\}$, then $G_\alpha = S_3 \times S_5$ where $S_3 \leq S_8$ is the subgroup fixing 4, 5, 6, 7 and 8, and $S_5 \leq S_8$ is the subgroup fixing 1, 2 and 3. Now

$$\Omega = \{\alpha\} \cup \Delta_1 \cup \Delta_2 \cup \Delta_3$$

where

$$\Delta_i = \{\omega \in \Omega \mid |\omega \cap \alpha| = 3 - i\},$$

and these sets $\{\alpha\}$, Δ_1, Δ_2, Δ_3 can easily be seen to be the G_α-orbits in Ω. Also, $|\Delta_1| = 15$, $|\Delta_2| = 30$, and $|\Delta_3| = 10$, and if G were imprimitive then the equivalence class containing α would consist of complete G_α-orbits. Since the only unions of G_α-orbits giving sets whose cardinals divide 56 are $\{\alpha\}$ and Ω itself, G is primitive. Finally, G_{α,Δ_3} is the subgroup of S_8 consisting of those permutations which fix all of 4, 5, 6, 7, 8, and this is the direct factor S_3 of G_α. Thus $G_\alpha / G_{\alpha,\Delta_3} \cong S_5$, whose only composition factors are A_5 and C_2. On the other hand, G_α has a composition factor isomorphic to C_3. Thus de Séguier's statement is not correct.

BIBLIOGRAPHY

Books.

[B] W. Burnside, Theory of groups of finite order.
Second edition reprinted, Dover Publications Inc., 1955.

[CR] C.W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras.
Interscience, New York, 1962.

[H] M. Hall, Jr., The theory of groups.
Macmillan, New York, 1959.

[J] C. Jordan, Traité des substitutions et des équations algébriques.
Gauthier-Villars, Paris, 1870.

[S] W.R. Scott, Group theory.
Prentice-Hall, Englewood Cliffs, N.J., 1964.

[de S] J.-A. de Séguier, Éléments de la théorie des groupes de substitutions.
Gauthier-Villars, Paris, 1912.

[W] H. Wielandt, Finite permutation groups.
Academic Press, New York, 1964.

Articles.

[1] A. Cauchy, Note sur la réduction des fonctions transitives aux fonctions intransitives, et sur quelques propriétés remarquables des substitutions qui n'altèrent pas la valeur d'une fonction transitive.
C.R.Acad.Sci. Paris, 21 (1845), 1199-1201
= Œuvres complètes d'Augustin Cauchy, 1re Série, 9, 442-444.

[2] W. Feit and J.G. Thompson, Finite groups which contain a self-centralizing subgroup of order 3 .
Nagoya Math. J., 21 (1962), 185-197.

[3] G. Frobenius, Über Gruppen des Grades p oder p + 1 .
Sitzungsberichte der Preuss. Akad. Wiss. (1902), 351-369.

[4] B. Huppert, Primitive, auflösbare Permutationsgruppen.
Arch. Math. 6 (1955), 303-310.

[5] Z. Janko, A new finite simple group with abelian Sylow 2-subgroups and its characterization.
J. Alg. 3 (1966), 147-186.

==========