On the Burnside Ring of a Finite Group

by

Donald Macleod Nicolson

Department of Mathematics,

Imperial College of Science and Technology.

Abstract

On the Burnside ring of a finite group

The material contained herein is based on work by A. Dress, notably his paper "A Characterisation of Solvable Groups" (Math Z. 110, 1969, pages 213-217).

Chapter 1, the introduction, contains a summary of the above paper, together with a detailed statement of other unpublished results of Dress's which are relevant to this dissertation. Also contained are definitions of my own which will be used in later chapters.

My own work falls into two distinct sections. The first section concerns the embedding of the Burnside ring, $\Omega(G)$, of a finite group G into a direct product of copies of the integers, and is covered in Chapters 2 and 3. The second section concerns the graph of prime ideals of $\Omega(G)$, and is covered in Chapters 4 and 5.

Chapter 2 We have the homomorphism $\phi_U : \Omega(G) \longrightarrow Z$ for each $U \leqslant G$ defined on the transitives of $\Omega(G)$ by $\phi_U(S) = |S^U|$, for S a transitive G-set, where $S^U = (s \in S : us = s, \text{ all } u \in U)$; Dress shows that $\phi_U = \phi_V$ if and only if $U \sim V$ and that $\theta = \prod_{U \in \mathfrak{J}} \phi_U : \Omega(G) \longrightarrow \prod_1^n Z$ is an embedding, where $\mathfrak{J}$ is a complete set of representatives of the n conjugacy classes of subgroups of G.

We define $y_U \in \prod_1^n Z$ to be such that y_U has zero component in $V \leqslant G$ unless $V \sim U$, and component 1 if $V \sim U$; we denote the least positive integer a such that $ay_U \in \Omega(G)$ by λ_U^G, and the product $\lambda_U^G y_U$ by x_U^G. The main results of Chapter 2 can be stated:

Theorem (a) If G is a finite group, whose maximal normal subgroups have index $p_1, p_2, \ldots, p_s$, then $\lambda_G^G = p_1 p_2 \ldots p_s$

(b) If $U \leqslant G$, then $\lambda_U^G = (N_G(U):U)\lambda_U^U$.

Chapter 3 We apply the results of Chapter 2 to a consideration of the regular G-set, G/e; we have $G/e = x_e^G$, and $\lambda_e^G = |G|$. Our results are:

Theorem If G has odd order, and $U \leqslant G$, with $\lambda_U^G = |G|$, then the following conditions are equivalent:

(1) G has no other subgroup of the same order as U.

(2) There is an automorphism of $\Omega(G)$ sending x_U^G to x_e^G.

Theorem If G has even order, and $U \leqslant G$ with $\lambda_U^G = |G|$, then the following conditions are equivalent. (U necessarily has square-free order)

(1) G has no other subgroup of order p for any odd prime p dividing $|U|$, and there is no subgroup of G of order 4 which does not contain the Sylow 2-subgroup of U.

(2) There is an automorphism of $\Omega(G)$ sending x_U^G to x_e^G.

Chapters 4 and 5 Further definitions are necessary to introduce our results: firstly, $\mathcal{P}_{U,p}$ for p zero or prime is the kernel of the map $\Omega(G) \xrightarrow{\phi_u} Z \longrightarrow Z_p$ (see Dress's paper). If U, $V \leqslant G$, then a chain c from U to V is a sequence $U = U_0, U_1, \ldots, U_n = V$ such that

$$\mathcal{P}_{U_0,p_1} = \mathcal{P}_{U_1,p_1}, \mathcal{P}_{U_1,p_2} = \mathcal{P}_{U_2,p_2}, \ldots, \mathcal{P}_{U_{n-1},p_n} = \mathcal{P}_{U_n,p_n}.$$

The width $W(c)$ of the above chain is the number of steps, n; the diameter, $d(c)$, is $p_1p_2\cdots p_n$. If $C(U,V)$ is the set of chains from U to V, we define $W(U,V) = \min\ (W(C) : c \in C(U,V))$; $d(U,V) = \text{h.c.f.}\ (d(c) : c \in C(U,V))$.

Finally, we define $W(G)$, the <u>width</u> of G, and $d(G)$, the <u>diameter</u> of G, as follows:

$$W(G) = \max\ (W(U,V) : U,\ V \leq G)$$

$$d(G) = \text{l.c.m.}\ (d(U,V) : U,\ V \leq G)$$

The results of Chapters 4 and 5 include the following:

<u>Theorem</u> If the prime divisors of the order of the group G are $p_1, p_2, \ldots, p_r$, then the following conditions are equivalent:

(1) G is nilpotent

(2) $W(G) = r$

(3) $d(G) = p_1p_2\cdots p_r$.

<u>Theorem</u> If G is a finite soluble group of order divisible by exactly r distinct primes, then if $W(G) = r + n$, then G has at most n non-normal Sylow subgroups.

<u>Theorem</u> If $d(G) = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then

$$W(G) \geq a_1 + a_2 + \cdots + a_r.$$

Acknowledgements

I would like to thank Dr. O. Pretzel for his encouragement, advice and patience, and also Dr. B. Baumslag for help in the early stages of my research. I am also grateful to the S.R.C. for their financial support.

Contents

		Page
Chapter 1	Introduction	7
1.1	The Burnside ring $\Omega(G)$ of a finite group	7
1.2	The prime ideals of $\Omega(G)$	8
1.3	The transitive G-sets; induction and restriction	9
1.4	The width and diameter of G	13
Chapter 2	The embedding of $\Omega(G)$ in a direct product of copies of the integers	16
Chapter 3	A characterisation of the regular G-set	24
Chapter 4	Some results on the width of a finite group	38
Chapter 5	The diameter of a finite group	57
Appendix		69
References		73

Chapter 1

Introduction

The basis for the work embodied in this dissertation is the paper "A Characterisation of Soluble Groups", [1], by A. Dress, concerning the relationship between a finite group, and its Burnside ring. Further relevant material is contained in a lecture course by Dress and Küchler at Bielefeld University in 1970, and since this is not generally available, its relevant results are summarised in this Introduction. Also the introduction includes a brief summary of the definitions and results of Dress's paper, [1], and various definitions to facilitate the development of my own results.

1.1 The Burnside Ring $\Omega(G)$ of a finite group G

In the following results and definitions, G is a finite group.

A finite set S is said to be a G-set if G acts as a (left) permutation group on S, i.e. we have a map $G \times S \longrightarrow S$: $(g,s) \longrightarrow gs$: such that $(g_1g_2)s = g_1(g_2s)$, and $es = s$, for $g_1, g_2 \in G$, $s \in S$, e the identity element of G. If S_1, S_2 are G-sets, then $f: S_1 \longrightarrow S_2$ is a G-map if, for all $g \in G$, $s \in S_1$, $f(gs) = gf(s)$.

Given two G-sets M, N, the disjoint union $M \cup N$, and the Cartesian product $M \times N$, are also G-sets in a natural way; and with this addition and multiplication, the isomorphism classes of G-sets (under G-maps) form a commutative half-ring $\Omega^+(G)$. Its associated ring is the Burnside ring, $\Omega(G)$, of G.

The transitive G-sets can be shown easily to be the set $(G/U\colon U \leqslant G)$, where G/U is the set of left cosets of U in G; also $G/U \cong G/V$ if and only if U is conjugate to V. Finally, the distinct (i.e. non-isomorphic) G-sets G/U, for $U \leqslant G$, form a basis for $\Omega(G)$ as a free Z-module.

1.2 The Prime Ideals of $\Omega(G)$

For each $U \leqslant G$, we define the map $\phi^+_U\colon \Omega^+(G) \longrightarrow Z$ by $\phi^+_U(S) = |S^U|$, for S a G-set, where $S^U = (s \in S\colon us = s,$ all $u \in U)$; we have $\phi^+_U = \phi^+_V$ if and only if U is conjugate to V, and ϕ^+_U extends to a homomorphism $\phi_U\colon \Omega(G) \longrightarrow Z$.

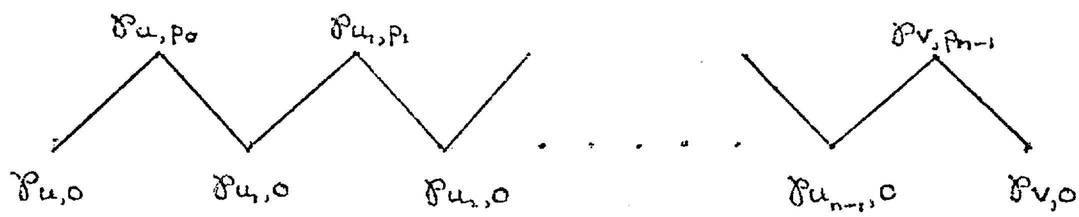
For p zero or prime, and $U \leqslant G$, we define $\mathscr{Y}_{U,p} = (x \in \Omega(G)\colon \phi_U(x) = 0 \bmod p)$. The $\mathscr{Y}_{U,p}$ are prime ideals (since $\Omega(G)/\mathscr{Y}_{U,p} \cong Z$ or Z_p) and Dress shows, either by considering a minimal transitive G-set not belonging to a prime ideal, or by using a theorem of Cohen-Seidenburg, that these are the only prime ideals.

It follows that $\mathscr{Y}_{U,p}$ is maximal, $\mathscr{Y}_{U,0}$ minimal, for $p \neq 0$ $(\mathscr{Y}_{U,p} \supseteq \mathscr{Y}_{U,0})$; and $\mathscr{Y}_{U,0} = \mathscr{Y}_{V,0}$ if and only if U is conjugate to V.

The conditions under which $\mathscr{Y}_{U,p} = \mathscr{Y}_{V,p}$, are more complicated, and require a further definition.

For $U \leqslant G$, we define $K_p(U)$ to be the minimal normal subgroup of U such that $U/K_p(U)$ is a p-group, i.e. $K_p(U) = \bigcap(V\colon V \lhd U,\ U/V$ is a p-group). $K_p(U)$ is a characteristic subgroup of U; and $\mathscr{Y}_{U,p} = \mathscr{Y}_{V,p}$ if and only if $K_p(U)$ is conjugate to $K_p(V)$.

In his paper, [1], Dress considers the graph of prime ideals of $\Omega(G)$, and defines two minimal prime ideals $\gamma_{U,0}$, $\gamma_{V,0}$ to be connected if there is a chain $U = U_0, U_1, \ldots, U_{n-1}, U_n = V$ of subgroups of G, and non-zero primes $p_0, p_1, \ldots, p_{n-1}$ such that $\gamma_{U_i,p_i} = \gamma_{U_{i+1},p_i}$, for i = 0 to n-1, i.e. we have the diagram



Dress's result in his paper [1] is that the following conditions are equivalent:

(1) G is a soluble group

(2) The graph of prime ideals of $\Omega(G)$ is connected (i.e. any 2 minimal prime ideals are connected)

(3) $\Omega(G)$ has no non-trivial idempotents.

1.3 The Transitive G-sets; Induction and Restriction

In defining the Burnside ring $\Omega(G)$ of a finite group G, the transitive G-sets G/U, where U runs through the conjugacy classes of subgroups of G, play an important role, being a basis for $\Omega(G)$ over the integers, Z.

Chapter 3 considers the problem of characterising this basis; given that a ring is the Burnside ring of a finite group, can we determine its transitive basis? The regular G-set, G/e, is determined (up to automorphism of $\Omega(G)$), but the problem of characterising the other transitives has not been solved.

The following results and definitions contained in Dress's unpublished work are used in Chapters 2 and 3.

<u>Definition 1</u> Suppose the finite group G has n distinct conjugacy classes of subgroups. We define $\Theta : \Omega(G) \to \prod_1^n Z$ by $\Theta = \prod_{U \leqslant G} \phi_U$, where ϕ_U is as defined in 1.2, and U runs through the conjugacy classes of subgroups of G.

Θ can be shown to be an embedding of $\Omega(G)$ in $\prod_1^n Z$; we now identify $\Omega(G)$ with its image under Θ.

<u>Lemma 1</u> $|G|\prod_1^n Z \subseteq \Omega(G)$.

<u>Proof</u> Define $y_U = (0, 0, \ldots, 1, \ldots, 0)$, i.e. the component of y_U corresponding to $V \leqslant G$ is zero unless $V \sim U$, in which case the component is 1. It is sufficient to show that $|G|y_U \in \Omega(G)$ for each subgroup U of G. We use induction on $|U|$.

For $|U| = 1$, that is $U = e$, we have $\phi_U(G/e) = \begin{cases} 0 & U \neq e \\ |G| & U = e \end{cases}$

So $|G|\, y_e \in \Omega(G)$.

So suppose $U \neq e$, and that for $V \leqslant G$ with $|V| < |U|$, $|G|\, y_V \in \Omega(G)$. Consider G/U; $\phi_V(G/U) = \begin{cases} 0 & V \not\lesssim U \\ |N_G(U):U| & V = U \\ a_V & V \lesssim U,\ V \neq U. \end{cases}$

So $G/U = |N_G(U):U|y_U + \sum_{|V|<|U|} a_V y_V$.

Hence $|G|y_U = (|G|/|N_G(U):U|)G/U - \sum_{|V|<|U|} (a_V/|N_G(U):U|)|G|y_V$.

It can be shown that $\phi_U(G/U)$ divides $\phi_U(G/V)$, so $|N_G(U):U|$ divides a_V. Hence $|G|y_U \in \Omega(G)$, and the result follows by induction.

<u>Definition 2</u> We denote the least positive integer a such that $a\, y_U \in \Omega(G)$ by λ_U^G, and the product $\lambda_U^G y_U$ by x_U^G. The superscript G is omitted if $U = G$; we write x_G and λ_G.

We call x_U^G, for $U \leqslant G$, a <u>quasi-idempotent</u> of $\Omega(G)$.

<u>Definition 3</u> (a) Suppose H,G are groups, and $\phi : H \longrightarrow G$ is a homomorphism. Let N be a G-set; we define an H-operation on N by $h \circ n = \phi(h).n$, for all $h \in H$, $n \in N$. Under this operation, we obtain an H-set, which we denote by $(N)_H$. In the case where H is a subgroup of G, and $\phi : H \longrightarrow G$ is the inclusion homomorphism, (the case with which we are concerned) $(N)_H$ is termed the <u>restriction of N to H</u>.

(b) Suppose H,G are groups, and $\phi : H \longrightarrow G$ is a homomorphism. Let M be an H-set; we define by $(h,(g,m)) \longrightarrow (g\,\phi(h^{-1}),hm)$, an H-operation on $G \times M$. We denote by $G \times_H M$ the set of equivalence classes of $G \times M$ under this action by H, that is $(h,(g,m)) \sim (g,m)$; and finally we define G to act on $G \times_H M$ by $g_1\overline{(g,m)} = \overline{(g_1 g,m)}$. Under this action, $G \times_H M$ becomes a G-set, the <u>induced G-set</u>, denoted by $(M)^G$.

<u>Lemma 2</u> Let $\phi : H \longrightarrow G$ be a group homomorphism, M_1 and M_2 H-sets, and N a G-set. Then

(a) $G \times_H (M_1 + M_2) = G \times_H M_1 + G \times_H M_2$

(b) $G \times_H ((N)_H \times M) = N \times (G \times_H M)$

(c) $\mathrm{Hom}_H (M,(N)_H) = \mathrm{Hom}_G ((M)^G,N)$ where M is an H-set.

<u>Definition 4</u> With ϕ, H and G as above, we define additive homomorphisms $\Omega(\phi)$, $\mho(\phi)$ from $\Omega(G)$ to $\Omega(H)$, and from $\Omega(H)$ to $\Omega(G)$ respectively, by $\Omega(\phi)$: $N \longrightarrow (N)_H$, for N a G-set, and $\mho(\phi)$: $M \longrightarrow G \times_H M$, for M an H-set.

Finally, for $U \leqslant G$, i: $U \longrightarrow G$ the inclusion, $x \in \Omega(G)$, $y \in \Omega(U)$, we define $(x)_U = \Omega(i)(x)$, and $(y)^G = \mho(i)(y)$.

<u>Lemma 3</u> For $U \leqslant G$, $(1_U)^G = G/U$, where 1_U is the U-set with 1 element.

<u>Corollary</u> For $U \leqslant G$, $x \in \Omega(G)$, $((x)_U)^G = G/U.x$.

<u>Proof</u> $((x)_U)^G = (1_U(x)_U)^G = (1_U)^G . x = G/U.x.$

<u>Lemma 4</u> Let N be a V-set, where $V \leqslant U \leqslant G$. Then

$$G \times_U (U \times_V N) = G \times_V N.$$

<u>Corollary 1</u> If $U \leqslant G$, and $N = U/V$ is a transitive U-set, then $(N)^G = G/V$, a transitive G-set.

<u>Proof</u> $(N)^G = ((1_V)^U)^G = (1_V)^G = G/V.$

<u>Corollary 2</u> For $U \leqslant G$, $\mho(i)$: $\Omega(U) \longrightarrow \Omega(G)$ is injective if and only if for every V_1, V_2 with $V_1 \sim V_2$ in G, then $V_1 \sim V_2$ in U.

<u>Corollary 3</u> For $U \leqslant G$, $(x_U)^G = bx_U^G$, where $b \in Z^+$.

<u>Proof</u> Look at $(x_U^G)_U$. For $V \leqslant U$, clearly

$$\phi_V((x_U^G)_U) = \phi_V(x_U^G) = \begin{cases} \lambda_U^G & V = U \\ 0 & V \neq U \end{cases}$$

Hence $(x_U^G)_U = ax_U$, $a \in Z^+$. Induce up to G:

$$a(x_U)^G = ((x_U^G)_U)^G = G/U.x_U^G \qquad \text{(Lemma 3, Corollary)}$$

$$= |N_G(U):U|x_U^G.$$

Since $(x_U)^G$ is in $\Omega(G)$, a must divide $|N_G(U):U|$, by the definition of x_U^G. Hence $(x_U)^G = bx_U^G$, where $b = (1/a)|N_G(U):U|$.

Chapter 2 involves an analysis of x_U^G and λ_U^G for $U \leqslant G$. We prove that λ_U^G can be calculated exactly in terms of the structure of U, and the index of U in its normaliser (Propositions 2.5 and 2.6).

Chapter 3 applies this analysis to a consideration of the regular G-set, G/e. This uses the fact that $G/e = x_e^G$, and we prove that G/e is unique up to automorphism of $\Omega(G)$.

1.4 <u>The Width, and the Diameter of G</u>

Further results can be obtained by considering the number of steps required to connect the graph of prime ideals of $\Omega(G)$; and by considering which primes occur in a chain. To facilitate this, we introduce some notation and definitions.

<u>Notation</u> Suppose U,V are subgroups of G, and $\gamma_{U,p} = \gamma_{V,p}$ for some non-zero prime p. Then $K_p(U) \sim K_p(V)$, so $|U|$ and $|V|$ differ only by a power of p.

We write $U \overset{p}{\searrow} V$ if $|U| \geqslant |V|$,

$U \overset{p}{\nearrow} V$ if $|U| \leqslant |V|$,

$U \overset{p}{\longrightarrow} V$ if the relative orders of U,V are not known.

<u>Definition 5</u> Suppose $U,V \leqslant G$. A <u>chain</u> c from U to V (which may not exist if G is not soluble) is a sequence $U = U_0, U_1, \ldots$ $\ldots, U_n = V$ such that

$$U = U_0 \overset{p_1}{\longrightarrow} U_1 \overset{p_2}{\longrightarrow} U_2 \longrightarrow \cdots\cdots \overset{p_n}{\longrightarrow} U_n = V,$$

where the p_i's are primes (not necessarily distinct), and $p_i = 1$ if $U_{i-1} \sim U_i$.

The <u>width</u>, W(c), of the above chain c, is the number of steps, n; the diameter, d(c), of the above chain c, is $p_1 p_2 \cdots\cdots p_n$.

<u>Definition 6</u> Let C(U,V) be the set of chains from U to V, for $U,V \leqslant G$. We define

$$W(U,V) = \min(w(c) : c \in C(U,V))$$

$$d(U,V) = \text{h.c.f.}(d(c) : c \in C(U,V)).$$

<u>Definition 7</u> Define W(G), the <u>width</u> of G, and d(G), the <u>diameter</u> of G, as follows:

$$W(G) = \max\,(w(U,V) : U,V \leqslant G),$$

$$d(G) = \text{l.c.m.}(d(U,V) : U,V \leqslant G).$$

Chapter 4 deals with some results concerning the width of G. Its main result, Proposition 4.8, is that if the order of G has r distinct prime divisors, and $W(G) = r + n$, then G has at most n non-normal Sylow subgroups.

Chapter 5 deals firstly with results concerning the diameter of G; Proposition 5.3 shows how d(G) may be determined from a consideration of normal series of subgroups of G. Chapter 5 concludes with Proposition 5.4 relating d(G) and W(G): if $d(G) = p_1^{a_1} \ldots\ldots p_r^{a_r}$, then $W(G) \geqslant a_1 + a_2 + \ldots\ldots + a_r$.

Chapter 2

The embedding of $\Omega(G)$ in a direct product of copies of the integers

In this chapter, we consider the map θ , defined in Definition 1, Chapter 1, embedding $\Omega(G)$ in $\prod_1^n Z$, where n is the number of distinct conjugacy classes of subgroups of G. In particular, we analyse the values of λ_U^G (see Definition 2, Chapter 1) for U a subgroup of G. This analysis begins with the case where G is a p-group, and uses the Mobius function $\mu(U,G)$ of G, introduced by P. Hall (see [2]).

$\mu(H,G)$ is defined as follows: $\mu(G,G) = 1$ and $\sum_{H \leqslant K} \mu(K,G) = 0$ for $H < G$.

Lemma 2.1

(a) $\mu(H,G) = 0$ unless H is an intersection of maximal subgroups of G.

(b) If G is an elementary abelian p-group, and $|G/H| = p^a$, then $\mu(H,G) = (-1)^a p^{a(a-1)/2}$.

Proof (a) is standard; for (b), see P. Hall [2].

Proposition 2.2

If G is a p-group, then $\lambda_G = p$.

Proof By (a) of the above Lemma, $\mu(H,G) = 0$ unless $F(G) \leqslant H$, where F(G) is the Frattini subgroup of G. G/F(G) is elementary abelian since G is a p-group, so if $F(G) \leqslant H$, then $H \lhd G$; and if $|G/H| = p^a$, then by (b) of the above Lemma, $\mu(G,H) = (-1)^a p^{a(a-1)/2}$.

Now $p\mu(H,G) = (-1)^a p^{a(a-1)/2 + 1}$, and for $a \in Z^+$, we have $a(a-1)/2 + 1 \geqslant a$. Hence p^a divides $p\mu(H,G)$; that is, $|G/H|$ divides $p\mu(H,G)$. So suppose $p\mu(H,G) = k_H|G/H|$; clearly this holds for any $H \leqslant G$, with $k_H = 0$ unless $F(G) \leqslant H$.

Now put $x = \sum_{V \leqslant G} k_V G/V$; then $\phi_U(x) = \sum_{U \leqslant V \leqslant G} |G/V|\ k_V = p \sum_{U \leqslant V \leqslant G} \mu(V,G)$

$$= \begin{cases} p & U = G \\ 0 & U \neq G \end{cases}$$

Hence x_G divides x, so λ_G divides p. But if $\lambda_G = 1$, then x_G is an idempotent, which is impossible since G is soluble (see 1.2). Hence $x = x_G$, and $\lambda_G = p$.

<u>Proposition 2.3</u>

Suppose that $K \lhd G$; let G_1 be the quotient group G/K. Suppose that in $\Omega(G_1)$, $x_{G_1} = \sum_{V \leqslant G} a_V G_1 \big/ VK/K$. Define y in $\Omega(G)$ by:

$$y = \sum_{V \leqslant G} a_V G/VK.$$

Then for $U \leqslant G$, $\phi_U(y) = \begin{cases} 0 & UK \neq G \\ \lambda_{G_1} & UK = G \end{cases}$

<u>Proof</u> We prove that $\phi_{UK}(G/VK) = \phi_{UK/K}\left(G/K \big/ VK/K\right) = \phi_U(G/VK)$.

For: $UKgVK = gVK \iff UK(gK)VK = (gK)VK$

$\iff UK/K(gK)VK/K = (gK)VK/K$,

and also: $UKgVK = gVK \iff (UK)^g \leqslant VK \iff U^g \leqslant VK$ (since $K \lhd G$)

$\iff UgVK = gVK$.

Hence $\phi_U(y) = \phi_{UK}(y) = \phi_{UK/K}(x_{G_1}) = \begin{cases} 0 & UK = G \\ \lambda_{G_1} & UK \neq G \end{cases}$

Corollary 1 If $K_p(G) \neq G$, there exists y in $\Omega(G)$ such that $\phi_G(y) = p$, and $\phi_U(y) = 0$ if $UK_p(G) \neq G$.

Proof Put $K = K_p(G)$ in the above Proposition. $G/K_p(G)$ is a p-group, and so $\lambda_{G_1} = p$, by Proposition 2.2.

Proposition 2.4

If G is nilpotent of order $p_1^{n_1} p_2^{n_2} \ldots\ldots p_r^{n_r}$, then $\lambda_G = p_1 p_2 \ldots\ldots p_r$.

Proof By Proposition 2.3, Corollary 1, there exists, for $i = 1$ to r, y_i in $\Omega(G)$ such that $\phi_U(y_i) = p_i$ if $US_{p_i} = G$, and 0 otherwise, where S_{p_i} is the (normal) Sylow p_i-complement of G.

So put $z = y_1 y_2 \ldots\ldots y_r$. Then $\phi_U(z) \neq 0$ implies that $US_{p_i} = G$ for $i = 1$ to r, and hence that U contains all the Sylow p_i-subgroups of G. But this is only possible for $U = G$. Clearly, $\phi_G(z) = p_1 p_2 \ldots\ldots p_r$, hence $z = p_1 p_2 \ldots\ldots p_r + \sum_{V \lneqq G} a_V G/V$. We now show that z is not divisible.

G has a normal subgroup U, say, of index p_1; we have:

$0 = \phi_U(z) = p_1 p_2 \ldots\ldots p_r + a_U \phi_U(G/U) = p_1 p_2 \ldots\ldots p_r + a_U p_1$.

Hence $a_U = -p_2 \ldots\ldots p_r$, so p_1 does not divide z. Similarly, we can show that z is not divisible by $p_2, \ldots\ldots, p_r$; so z is not divisible, hence $z = x_G$, and $\lambda_G = p_1 p_2 \ldots\ldots p_r$.

Proposition 2.5

Suppose G is a group of order $p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$, and that $K_{p_i}(G) \neq G$ for i = 1 to s, and $K_{p_i}(G) = G$ for i = s+1 to r where $s \leqslant r$. Then $\lambda_G = p_1 p_2 \ldots p_s$.

Proof Put $K = \bigcap_{i=1 \text{ to } r} K_{p_i}(G)$; K is a normal (characteristic) subgroup of G. Suppose $|G/K| = p_1^{b_1} p_2^{b_2} \ldots p_s^{b_s}$; G/K is nilpotent, and by hypothesis, $b_i \neq 0$, for i = 1 to s.

Hence, by Propositions 2.3 and 2.4, we can find z in $\Omega(G)$ such that $\phi_U(z) = \lambda_{G/K} = p_1 p_2 \ldots p_s$ if UK = G, and 0 otherwise. We now show the existence of an element y in $\Omega(G)$ which satisfies $\phi_G(y) = 1$, and $\phi_U(y) = 0$ if UK = G, $U \neq G$; and then we show that $x_G = zy$.

Let I be the ideal of $\Omega(G)$ generated by the x_U^G's for $K \leqslant U$, and $U \neq G$; consider the quotient ring $\Omega(G)/I$. Its minimal prime ideals are $\mathscr{P}_{G,0}/I$, and $\mathscr{P}_{V,0}/I$, for $K \nleqslant V$. Hence $\mathscr{P}_{G,0}/I$ is isolated in the spectrum of prime ideals of $\Omega(G)/I$; hence, since $\Omega(G)/I$ is commutative with a 1, there is an idempotent in $\bigcap_{K \nleqslant V} \mathscr{P}_{V,0}/I$.

Hence there is an element y of $\Omega(G)$ such that $y \in \bigcap_{K \nleqslant V} \mathscr{P}_{V,0}$ mod I, and $y^2 = y$ mod I. If $K \nleqslant V$, then $I \leqslant \mathscr{P}_{V,0}$, so $y \in \bigcap_{K \nleqslant V} \mathscr{P}_{V,0}$. Since $I = (\sum a_U x_U^G : K \leqslant U < G,\ a_U \in Z)$, we have $y^2 = y + \sum_{K \leqslant U < G} a_U x_U^G$, and therefore

$$\phi_U(y)^2 = \phi_U(y^2) = \phi_U(y) + \sum_{K \leqslant V < G} a_V \phi_U(x_V^G).$$

So if U = G, or if $K \nleqslant U$, $\phi_U(y)^2 = \phi_U(y)$, and since $\phi_U(y)$ is integral, this implies that $\phi_U(y) = 0$ or 1. But

$y \in \bigcap_{K \nleq V} \gamma_{V,0}$, so $\phi_U(y) = 0$ for $K \nleq U$; a fortiori, $\phi_U(y) = 0$ if $UK = G$, $U \neq G$. Finally, $\phi_G(y) = 1$, since $y \notin I$.

Now, $\phi_U(zy) = \phi_U(z)\phi_U(y) = \begin{cases} 0 & U = G \\ p_1p_2\cdots p_s & U \neq G \end{cases}$

and by an argument similar to that used in Proposition 2.4, p_i divides λ_G for $i = 1$ to s. Hence $x_G = zy$, and $\lambda_G = p_1p_2\cdots p_s$.

We now know λ_G exactly in terms of the group structure of G; we now consider λ_U^G, for U G. By considering the induced element $(x_U)^G$ of $\Omega(G)$ and the restricted element $(x_U^G)_U$ of $\Omega(U)$, it is easy to see that $\lambda_U \mid \lambda_U^G \mid |N_G(U):U|\lambda_U$. The next proposition shows that $\lambda_U^G = |N_G(U):U|\lambda_U$; the results of 1.3 on induction and restriction are assumed.

<u>Proposition 2.6</u>

Suppose G is a group, and U a subgroup of G. Then $\lambda_U^G = |N_G(U):U|\lambda_U$, and $(x_U)^G = x_U^G$.

<u>Proof</u> By Lemma 4, Corollary 3, of Chapter 1, we know that $(x_U)^G = b\, x_U^G$, so we need to show that $b = 1$. By Proposition 2.5, we know x_U precisely: $x_U = p_1p_2\cdots p_s + \sum_{V \neq U} a_V\, U/V$, where the summation is taken over a set of representatives of the conjugacy classes of subgroups of U, and the p_i's are precisely the primes such that $K_{p_i}(U) \neq U$. Hence by Lemma 4, Corollary 1, of Chapter 1,

$$(x_U)^G = p_1p_2\cdots p_s\, G/U + \sum_{V \neq U} a_V\, G/V .$$

However, the total coefficient of G/V is not necessarily a_V, since there may be subgroups of U conjugate to V in G, but not conjugate in U (that is, $\mho(i)$ is not necessarily injective, see Lemma 4, Corollary 2, Chapter 1). The term in G/U in $(x_U)^G$ is certainly $p_1p_2\dots p_s\ G/U$; so to prove that $b = 1$, it is sufficient to show that p_1 does not divide $(x_U)^G$.

Consider the coefficient a_V in x_U of U/V for V a maximal subgroup of U. Since $\phi_U(U/V) = 0$, we have $x_U.U/V = 0$. This gives the equation $p_1p_2\dots p_s + |N_U(V):V|\,a_V = 0$.

So if V is normal in U of index p_i (where $1 \leq i \leq s$ by hypothesis), then $a_V = -p_1p_2\dots p_s/p_i$; whilst otherwise $a_V = -p_1p_2\dots p_s$ (since V is then self-normalising).

Hence p_1 divides a_V for maximal V unless V is normal in U of index p_1. The number c of maximal normal subgroups of U of index p_1 is equal to the number of maximal subgroups of $U/K_{p_1}(U)$, a nilpotent p_1-group; by standard theory, $c \equiv 1 \bmod p_1$. Therefore,

$$x_U = p_1p_2\dots p_s - p_2p_3\dots p_s \sum_{1}^{c} U/V_i + \sum_{\substack{V \neq V_i \\ V \neq U}} a_V\, U/V\ ,$$

where $V_1, V_2, \dots, V_c$ are the normal subgroups of U of index p_1. Hence

$$(x_U)^G = p_1p_2\dots p_s\ G/U - p_2p_3\dots p_s \sum_{W} a_W\, G/W + \sum_{V} a_V\, G/V\ ,$$

where the first sum is taken over a set of representatives of the conjugacy classes of $V_1, V_2, \dots, V_c$, a_W = the number of V_i's conjugate to W, and the second sum is over the remaining subgroups V of U, where $V \neq U$.

Hence $\sum_W a_W = c = 1 \mod p_1$, so at least one a_W is not divisible by p_1; so p_1 does not divide $(x_U)^G$.

Therefore $(x_U)^G = x_U^G$, and $\lambda_U^G = |N_G(U):U| \; p_1 p_2 \ldots p_s$

$$= |N_G(U):U| \lambda_U.$$

Corollary 1

For $U \leqslant V \leqslant G$, $(x_U^V)^G = x_U^G$, and $\lambda_U^G = |N_G(U):N_V(U)| \lambda_U^V$.

Proof $(x_U)^V = x_U^V$, $(x_U^V)^G = ((x_U)^V)^G$

$$= (x_U)^G$$
$$= x_U^G.$$

Also, $\lambda_U^V = |N_V(U):U| \lambda_U$, $\lambda_U^G = |N_G(U):U| \lambda_U$, and the result follows since $N_G(U) \geqslant N_V(U)$.

Corollary 2

For $U \leqslant V \leqslant G$, $(x_U^G)_V = \sum_{W \leqslant V} a_W x_W^V$, where $a_W = |N_G(W):N_V(W)|$ if W is conjugate to U in G (and W appears only once for each conjugacy class in V), $a_W = 0$ otherwise.

Proof For $W \leqslant V$, $\phi_W((x_U^G)_V) = \phi_W(x_U^G)$

$$= \begin{cases} \lambda_U^G & \text{if } W = U \\ 0 & \text{otherwise} \end{cases}$$

So $(x_U^G)_V = \sum_i \lambda_U^G / \lambda_{W_i}^V \; x_{W_i}^V$, where the W_i are a complete set of representatives of the conjugacy classes in V of those conjugates in G of U which are contained in V,

$$= \sum_i |N_G(W_i):N_V(W_i)| x_{W_i}^V$$

Corollary 3

$\lambda_U^G = |G|$ if and only if U is an abelian normal subgroup of square-free order.

Proof $\lambda_U^G = |N_G(U):U|\lambda_U$; λ_U divides $|U|$, and by Proposition 6, $\lambda_U = |U|$ if and only if U is abelian of square-free order. If U is not normal in G, then $|N_G(U):U| < |G/U|$, so the result follows clearly.

Chapter 3

A characterisation of the regular G-set

In this chapter, we investigate the possibility of distinguishing the regular G-set, G/e, where e is the identity element of the group G, from the other elements of $\Omega(G)$. Now $\phi_U(G/e) = 0$, for $U \neq e$, $U \leqslant G$, and $\phi_e(G/e) = |G|$; hence $G/e = x_e^G$, and $\lambda_e^G = |G|$. So we only need to consider elements of the same type, that is, elements of the form x_U^G with $\lambda_U^G = |G|$, where $U \leqslant G$. From Proposition 2.6, Corollary 3, $\lambda_U^G = |G|$ if and only if U is a normal Abelian subgroup of square-free order.

The cases for G of even and odd order require separate treatment. In the odd case, x_e^G can be distinguished from x_U^G (where $\lambda_U^G = |G|$) if G has another subgroup of the same order as U (Proposition 3.3); in any case, the regular G-set is unique up to automorphism of $\Omega(G)$ (Proposition 3.5). The even case is slightly more complicated (Proposition 3.6), but G/e is again unique up to automorphism of $\Omega(G)$ (Proposition 3.7).

Proposition 3.1

If p divides $(x_U^G + x_V^G)$, $V \neq U$, then $U \cap V \lhd U$, $U \cap V \lhd V$, and either $|U/U \cap V| = |V/U \cap V| = p$, or $U \geqslant V$, $|U/V| = p$ (or $V \geqslant U$, $|V/U| = p$) where suitable conjugates of U and V are chosen.

Proof Suppose that $U \not\leqslant V$ (without loss of generality)

$$x_U^G = p_1 \ldots p_s G/U - \sum a_W G/W.$$

x_V^G has no term in G/U, so $p = p_1$, say.

Now $x_U^G = p_1 \dots p_s G/U - p_2 \dots p_s \sum_{\substack{W \lhd U \\ |U/W| = p}} a_W G/W - \sum a_K G/K$

As before, for some $W_1 \lhd U$, $|U/W_1| = p_1$, $a_{W_1} \not\equiv 0 \bmod p_1$, so there must be a non-zero term in G/W_1 in x_V^G.

Therefore $V \geqslant W_1$, choosing suitable conjugates. So either $V = W_1$, or $V \not\leqslant U$. If $V \not\leqslant U$, then, by a similar argument, there exists $W' \lhd V$ such that $|V/W'| = p_1$, and $W' \leqslant U$.

Thus $U \cap V \geqslant W_1$, and $U \cap V \geqslant W'$; so $W_1 = W'$, and $U \cap V = W_1$.

Corollary 1 p divides $(x_U^G + x_e^G)$ if and only if $|U| = p$.

Proof If $|U| = p$, then $x_U^G = pG/U - G/e$

$$= pG/U - x_e^G$$

The converse follows from the proposition.

By the above corollary, the number of subgroups U for which p divides $(x_U^G + x_e^G)$ is precisely the number of conjugacy classes of subgroups of G of order p; we attempt to distinguish between x_e^G and x_V^G, where $\lambda_V^G = |G|$, by considering the number of conjugacy classes of subgroups U such that p divides $(x_V^G + x_U^G)$. The next proposition is stated in greater generality than is necessary for our immediate needs, but will be useful later.

Proposition 3.2

If $G = UP$, where $|P| = p$, P is normal in G, and $(|U|,p) = 1$,

$$\text{then } x_G = \begin{cases} pz_H - x_U^G & \text{if } U \lhd G \\ z_H - x_U^G & \text{if } U \ntriangleleft G \end{cases}$$

where $H = G/P$, and z_H is defined from x_H, by

$z_H = \sum a_V G/VP$, where $x_H = \sum a_V H/V$.

<u>Proof</u> By Proposition 2.3, $\phi_V(z_H) = \begin{cases} 0 & VP \neq G \\ \lambda_H & VP = G \end{cases}$

So if U is normal in G, then

$$\phi_U(pz_H - x_U^G) = p\lambda_H - \lambda_U^G = p(\lambda_H - \lambda_U) = 0$$

$$\phi_G(pz_H - x_U^G) = p\lambda_H = \lambda_G$$

$$\phi_V(pz_H - x_U^G) = 0 \text{ otherwise.}$$

Hence $x_G = pz_H - x_U^G$.

If U is not normal in G, then $\lambda_U^G = \lambda_U$, so

$\phi_U(z_H - x_U^G) = 0$, and the result follows.

<u>Proposition 3.3</u>

Let G have odd order, and U be a subgroup of G with $\lambda_U^G = |G|$; then if G has another subgroup of the same order as U, x_U^G can be distinguished from x_e^G.

<u>Proof</u> By Proposition 2.6, Corollary 3, $|U| = p_1 \ldots p_s$, say, where the p_i's are distinct primes, $U \lhd G$, and U is abelian.

Suppose there is another subgroup V, say, of order $p_1 \ldots p_s$. Then without loss of generality, there are 2 subgroups of order p_1, say P_1, P_1', where $P_1 \leqslant U$ $(P_1 \lhd G)$, $P_1' \leqslant V$.

Clearly, $x_{P_1}^G \neq x_{P_1'}^G$, and $p_1 \mid x_{P_1}^G + x_e^G$, $p_1 \mid x_{P_1'}^G + x_e^G$.

We show that $p_1 \mid x_U^G + x_W^G$ only if $W = K_{P_1}(U)$.

Suppose $U = P_1 \times P_2 \times \ldots \times P_s$, where $|P_i| = p_i$, and $P_i \lhd G$.

$p_1 \mid x_U^G + x_W^G$ implies either (a) $W \rhd P_2 \ldots P_s = M$, say, and either $|W/M| = p_1$, or $W = M$, or (b) $W \geqslant U$, $|W/U| = p_1$, by Proposition 3.1.

(a) Suppose $|W/M| = p_1$. Now, $P_2 \lhd W$, and if $W = P'M$, where $|P'| = p$, then by Proposition 3.2, putting $N = P'P_3 \ldots P_s$

$$x_W^G = \begin{cases} p_2 z_{W/P_2} - x_N^G & \text{if } N \lhd W, \\ z_{W/P_2} - x_N^G & \text{if } N \not\lhd W \end{cases}$$

$$\text{Hence } x_U^G + x_W^G = \left(\begin{bmatrix} p_2 z_{W/P_2} \\ z_{W/P_2} \end{bmatrix} + p_2 z_{U/P_2} \right) - \left(x_N^G + x^G_{P_1 P_3 \ldots P_s}\right)$$

The two brackets above are disjoint, since all the transitives in the first bracket are of the form $G/U'P_2$, whilst those in the second are of the form G/U' for $U' \not\geq P_2$.

So $p_1 \mid (x^G_{P'P_3 \ldots P_s} + x^G_{P_1 P_3 \ldots P_s})$. Continue inductively, to arrive at $p_1 \mid x^G_{P'} + x^G_{P_1} = p_1 G/P' + p_1 G/P_1 - 2G/e$.

Since $p_1 \neq 2$, this is a contradiction.

So $W = M$ only.

(b) $|W/U| = p_1$, $U \lhd W$

$x_W^G = \lambda_W G/W + \sum a_{W'} G/W'$, and p_1 divides λ_W since $K_p(W) = M$, so the coefficient of G/U in x_W^G is λ_W/p_1, which is not divisible by p_1. So p_1 does not divide $x_U^G + x_W^G$.

Hence p_1 divides $x_U^G + x_W^G$ only if $W = M$. So x_U^G cannot be confused with x_e^G.

The case for G of even order is slightly different, and is more readily considered after further work on the case where G has odd order.

We now show that for G of odd order, and if G has exactly one subgroup of order $p_1 \ldots p_s$, which is (normal) and Abelian (so that $\lambda^G_U = |G|$), then there is an automorphism of $\Omega(G)$ which sends x^G_e to x^G_U. It is sufficient to show that there is an automorphism θ_i of $\Omega(G)$ acting on the set $(x^G_U: \; U \leqslant G)$ as follows:

If $U = P_1 \times P_2 \times \ldots \times P_s$, then $\theta_i : x_e \longrightarrow x_{P_i}$, $x_{VP_i} \longrightarrow x_V$, $x_V \longrightarrow x_{VP_i}$ for $(|V|, p_i) = 1$.

For then $\theta_1 \theta_2 \ldots \theta_s$ sends x^G_e to x^G_U.

<u>Proposition 3.4</u>

(a) Let S be the set of quasi-idempotents x^G_U in $\Omega(G)$ (as defined in Definition 2, Chapter 1), and Γ the subring of B consisting of integral combinations of elements of S. Then

$\Gamma \supseteq |G| \, \Omega(G)$.

(b) Let θ be a permutation of S; then θ extends to an automorphism of Γ if and only if $x^G_U \theta = x^G_V$ implies $\lambda^G_U = \lambda^G_V$.

(c) Let θ be an automorphism of Γ, then θ extends to an automorphism of $\Omega(G)$ if and only if for all $a \in \Gamma$, any factor of $|G|$ dividing a in $\Omega(G)$ divides $a\theta$ in $\Omega(G)$.

<u>Proof</u> (a) is immediate from the fact that λ^G_U divides $|G|$ for each $U \leqslant G$.

(b) θ is obviously additive, and bijective (since Γ is additively a free abelian group on its generators), and the condition implies that it is multiplicative.

(c) If Θ' is an automorphism of $\Omega(G)$, then $(|G|a)\Theta' = |G|(a\Theta')$ for $a \in \Omega(G)$. Hence, if Θ' is an extension of Θ, Θ' must satisfy $a\Theta' = \frac{1}{|G|}((|G|\, a)\Theta)$.

Proposition 3.5

Suppose p is a prime, and P' is the only subgroup of G of order p; let Θ be the product of the transpositions $(x_U^G, x_{UP'}^G)$, where $(|U|,p) = 1$ on S, the set of quasi-idempotents of $\Omega(G)$. Then Θ extends to an automorphism of $\Omega(G)$.

Proof (a) We prove that if $(|U|,p) = 1$, $\lambda_U^G = \lambda_{UP'}^G$, and hence that Θ extends to an automorphism of Γ, by Proposition 3.4 (b). First, we note that by Schur's theorem, if $V \geqslant P'$, and $p^2 \nmid |V|$, then V has a p-complement.

Clearly $N_G(UP') \supseteq N_G(U).P'$; suppose $x \in N_G(UP')$. Then $(UP')^x = UP'$, and so U^x is another complement of P' in UP'; hence, by a theorem of Zassenhaus, $U^x = U^y$ for $y \in UP'$, and so $xy^{-1} \in N_G(U)$, that is, $x \in N_G(U).P'$. So $N_G(UP') = N_G(U).P'$. Now if $U \ntriangleleft UP'$, then $\lambda_{UP'} = \lambda_U$, and $|N_G(UP'):UP'| = |N_G(U):U|$, and so $\lambda_U^G = \lambda_{UP'}^G$. Whilst if $U \triangleleft UP'$, $\lambda_{UP'} = p\,\lambda_U$, and $|N_G(U):U| = p|N_G(UP'):UP'|$, so again $\lambda_U^G = \lambda_{UP'}^G$ (Proposition 2.6).

(b) Let m be a factor of $|G|$ dividing $y = \sum a_U x_U^G$ in $\Omega(G)$; we need to show (Proposition 3.4(c)) that $m \mid y\Theta$.

We split the sum as follows:

$$y = \sum_{p^2 \mid |U|} a_U x_U^G + \sum_{p \nmid |U|} a_U x_U^G + \sum_{p \nmid |U|} a_{UP'} x_{UP'}^G \qquad (1)$$

(c) Now, using the notation of Proposition 3.2,

$$x^G_{UP'} = \begin{cases} (z_{UP'/P'})^G - x^G_U & \text{if } U \ntriangleleft UP' \\ (pz_{UP'/P'})^G - x^G_U & \text{if } U \triangleleft UP' \end{cases}$$

We simplify this notation by writing z_U for $(z_{UP'/P'})^G = \sum s_V \, {}^G\!/_{VP'}$, where $x_U = \sum s_V \, {}^U\!/_V$. Then the last sum in (1) splits thus:

$$\sum_{p \nmid |U|} a_{UP'} x^G_{UP'} = \sum_{\substack{U \ntriangleleft UP' \\ p \nmid |U|}} a_{UP'} z_U + p \sum_{\substack{U \triangleleft UP' \\ p \nmid |U|}} a_{UP'} z_U - \sum_{p \nmid |U|} a_{UP'} x^G_U$$

So if we put $b_U = a_U - a_{UP'}$, we have:

$$\sum_{p \nmid |U|} (a_U x^G_U + a_{UP'} x^G_{UP'}) = \sum_{U \ntriangleleft UP'} a_{UP'} z_U + p \sum_{U \triangleleft UP'} a_{UP'} z_U + \sum b_U x^G_U$$

Rewriting (1), we obtain:

$$y = \sum_{p^2 \mid |U|} a_U x^G_U + \sum_{U \ntriangleleft UP'} a_{UP'} z_U + p \sum_{U \triangleleft UP'} a_{UP'} z_U + \sum b_U x^G_U \qquad (2)$$

(d) If $P' \nleq V$, then the coefficient of ${}^G\!/_V$ in the second and third sums in (2) is zero. The same holds in the first sum; for if $p^2 \mid |U|$, and M is maximal in U with $P' \nleq M$, then $MP' = U$, would imply that M contains a subgroup of order p distinct from P'. Hence P' is a subgroup of the Frattini group of U.

Hence $m \mid y$ implies $m \,\Big|\, \sum_{p \nmid |U|} b_U x^G_U$

(e) Now if $p \nmid |U|$, $z_U = x^G_U + x^G_{UP'}$, if $U \ntriangleleft UP'$

$pz_U = x^G_U + x^G_{UP'}$, if $U \triangleleft UP'$

Hence Θ fixes the z_U's, and hence the terms in the first 3 sums of (2), so

$$y - y\Theta = \sum b_U (x^G_U - x^G_{UP'}).$$

Hence we can assume that in (1), the only non-zero sum is $\sum_{p \nmid |U|} a_U x_U^G$, and we now have to show that for any factor m of $|G|$, $m \mid \sum_{p \nmid |U|} a_U x_U^G$ implies $m \mid \sum_{p \nmid |U|} a_U x_{UP'}^G$. We may obviously take m to be a prime power; suppose $m = q^s$, where q is prime, s an integer.

To do this, we split the sum into further smaller summands.

(f) Consider $[\Omega(G)]_{q'} = (x/n : x \in \Omega(G),\ n \in Z,\ (n,q) = 1)$

This is a ring with 1 and has minimal prime ideals $\wp'_{U,0}$, say, and maximal prime ideals $\wp'_{U,q}$ only. Hence its graph of prime ideals splits into components of the form $(\wp'_{U,0} : K_q(U) = K)$ for the different subgroups K of G with $K_q(K) = K$.

Hence there is an idempotent e in $[\Omega(G)]_{q'}$ such that $e \in \bigcap_{K_q(U) \neq K} \wp'_{U,0}$ for a given $K \leq G$ with $K_q(K) = K$. So by taking a suitable integral multiple n of e, with $(n,q) = 1$ we obtain $z \in \Omega(G)$ such that

$$\phi_U(z) = \begin{cases} 0 & K_q(U) \neq K \\ n & K_q(U) = K \end{cases}$$

We now consider $z.\left(\sum_{(|U|,p)=1} a_U x_U^G\right)$. This becomes $n \sum_{K_q(U)=K} a_U x_U^G$, and since $(n,q) = 1$, $m \mid \sum_{K_q(U)=K} a_U x_U^G$.

(g) We observe that if $K = K_q(U)$, with $p \nmid |K|$, then $K \triangleleft KP'$ if and only if $U \triangleleft UP'$. So now, $m \mid \sum_{p \nmid |U|} a_U x_U^G$ implies, using (f), that $m \mid \sum_{U \triangleleft UP'} a_U x_U^G$, and $m \mid \sum_{U \ntriangleleft UP'} a_U x_U^G$.

(h) Now notice that if $m \mid \sum_{p \nmid |U|} a_U x_U^G = \sum_{\substack{V \leq G \\ p \nmid |V|}} c_V \, G/V,$

say, then $m \mid \sum_{\substack{V \leq G \\ p \nmid |V|}} c_V \, G/VP' = \sum a_U z_U.$

But $\sum a_U x_{UP'}^G = p \sum_{U \triangleleft UP'} a_U z_U + \sum_{U \ntriangleleft UP'} a_U z_U - \sum_{p \nmid |U|} a_U x_U^G$, and m divides each partial sum, and hence the left-hand side. This concludes the proof.

<u>Proposition 3.6</u>

Suppose G has even order, and suppose U is a subgroup of G with $\lambda_U^G = |G|$; then if there are 2 subgroups of G of order p for any odd prime p dividing the order of U, or if there is a subgroup of G of order 4 which does not contain the Sylow 2-subgroup of U, then x_U^G can be distinguished from x_e^G.

<u>Proof</u> (a) The first part, for $p \neq 2$, follows as in Proposition 3.3. So assume $U = P'Q_1 \ldots Q_r$, where $|P'| = 2$, $|Q_i| = q_i \neq 2$, for i = 1 to r, and $Q_1 \ldots Q_r$ is the unique subgroup of G of order $q_1 \ldots q_r$. By Proposition 3.5, there is an automorphism of $\Omega(G)$ which maps x_e^G to $x_{Q_1 \ldots Q_r}^G$, mapping $x_{P'}^G$ to $x_{P'Q_1 \ldots Q_r}^G$. Hence, without loss of generality, we may assume that $U = P'$.

(b) Now suppose that G has a subgroup W of order 4. If W is cyclic, then $x_W^G = 2G/W - G/V$, say, where $|V| = 2$, and so $4G/W = 2x_W^G + x_V^G + x_e^G$. If W is not cyclic, then $x_W^G = 2G/W - \sum_{i=1}^{3} a_i \, G/V_i + G/e$, where $|V_i| = 2$, $a_i = 0, 1, 2$ or 3, for i = 1 to 3, and $\sum_{i=1}^{3} a_i = 3$. In this case, $4G/W = 2x_W^G + \sum_{i=1}^{3} a_i x_{V_i}^G + x_e^G$. So in each case, $4 \mid 2x_W^G + \sum a_i x_{V_i}^G + x_e^G$, and $2 \mid x_{V_i}^G + x_e^G$, for suitable integral a_i.

(c) We now show that if $4 \mid 2x_H^G + \sum b_i x_{K_i}^G + x_U^G$, and $2 \mid x_{K_i}^G + x_U^G$, with $x_{K_i}^G \neq x_U^G$, then $H \geqslant U$, and $|H| = 4$.

Suppose $2 \mid x_V^G + x_U^G$; by Proposition 3.1, $U \cap V \lhd U$, $U \cap V \lhd V$, and either $U \cap V = e$, and $|V| = 2$, or $V = e$, or $V \geqslant U$ with $|V/U| = 2$. But if $U \cap V = U$, then $x_V^G = 2^G/_V - {}^G/_U + \sum_{K \neq U} a_K {}^G/_K$, since $U \lhd G$; so $2 \nmid x_V^G + x_U^G$. Hence $U \cap V = e$; and $2 \mid x_V^G + x_U^G$ if and only if $V = e$ or $|V| = 2$.

So our condition becomes $4 \mid 2x_H^G + \sum b_i x_{V_i}^G + x_U^G$, where $V_i = e$, or $|V_i| = 2$. (1)

Now if $H \not\geqslant U$, the only contribution to ${}^G/_U$ in (1) is 2 from x_U^G; so $H \geqslant U$. If $|H| > 4$, then there is a term $2a_K {}^G/_K$ in (1) from x_H^G, where K is a maximal subgroup of W, and a_K is odd, and no other term in (1) contributes to ${}^G/_K$; hence $|H| = 4$.

(d) Hence $4 \mid 2x_H^G + \sum b_i x_{V_i}^G + x_U^G$, and $2 \mid x_{V_i}^G + x_U^G$, $x_{V_i}^G \neq x_U^G$, only if $H \geqslant U$, and $|H| = 4$, whereas the same equations with x_U^G replaced by x_e^G can be solved for any subgroup H of order 4.

Hence if G has a subgroup $W \not\geqslant U$, $|W| = 4$, then x_U^G can be distinguished from x_e^G.

<u>Proposition 3.7</u>

If P' is a normal subgroup of G of order 2, and every subgroup of G of order 4 contains P', then there is an automorphism of $\Omega(G)$ which maps x_e^G onto $x_{P'}^G$.

<u>Proof</u> The method is similar to that of Proposition 3.5. We show that the product θ of the transpositions $(x_U^G, x_{UP'}^G)$, where $(|U|,2) = 1$, on S, the set of quasi-idempotents of $\Omega(G)$, can be extended to an automorphism of G.

(a) $\lambda_U^G = \lambda_{UP'}^G$, if $2 \nmid |U|$, as in 3.5.

(b) Let m be a factor of $|G|$ dividing $y = \sum a_U x_U^G$ in $\Omega(G)$; we need to show that m divides $y\Theta$. We split the sum as follows:

$$y = \sum_{4 | |U|} a_U x_U^G + \sum_{\substack{2 | |U| \\ U \not\geq P'}} a_U x_U^G + \sum_{2 \nmid |U|} a_{UP'} x_{UP'}^G + \sum_{2 \nmid |U|} a_U x_U^G \qquad (1)$$

(c) The sums in (1) are no longer disjoint; for if U = VP, say, where $|P| = 4$, $(|V|,2) = 1$, then x_U^G may have a non-zero term in G/V.

However, as in Proposition 3.4 (f), we can assume that $m = q^s$, where q is a prime, and by multiplying by suitable elements of $\Omega(G)$, we can deduce that $q^s \Big| \sum_{K_q(U)=K} a_U x_U^G$, for each $K \leq G$ with $K_q(K) = K$.

(d) Suppose $q \neq 2$. Then clearly, if U,V are subgroups appearing in different sums in (1), $K_q(U) \neq K_q(V)$, and hence q^s divides each sum in (1).

Now $x_{UP'}^G = 2z_U - x_U^G$, for $(|U|, 2) = 1$.

So $q^s \,\Big|\, \sum a_{UP'} x_{UP'}^G$ implies that $q^s \,\Big|\, \sum a_{UP'} x_U^G$ (since z_U and x_U^G are disjoint); and $q^s \,\Big|\, \sum a_U x_U^G$ implies that $q^s \,\Big|\, \sum a_U z_U$, and hence $q^s \,\Big|\, \sum a_U x_{UP'}^G$.

$$y\Theta = \sum_{4 | |U|} a_U x_U^G + \sum_{\substack{2 | |U| \\ U \not\geq P'}} a_U x_U^G + \sum_{2 \nmid |U|} a_{UP'} x_U^G + \sum_{2 \nmid |U|} a_U x_{UP'}^G$$

and clearly q^s divides each sum, and hence divides y .

(e) q = 2. We have

$$2^s \,\Big|\, y_1 = \sum_{K_2(U)=K} a_U x_U^G \qquad (2)$$

This is only affected by Θ if $2 \nmid |K|$. So we may suppose that $2 \nmid |K|$.

We split the sum (2) as follows:

$$y_1 = \sum_{K_2(U)=K} a_U x_U^G = a_K x_K^G + a_{KP'} x_{KP'}^G + \sum a_U x_U^G \qquad (3)$$

$$y_1\theta = a_K x_{KP'}^G + a_{KP'} x_K^G + \sum a_U x_U^G ;$$

So $y_1 - y_1\theta = (a_{KP'} - a_K)(x_{KP'}^G - x_K^G)$.

Now $x_{KP'}^G - x_K^G = 2(z_K - x_K^G)$, so it suffices to show that $2^{s-1} \mid a_{KP'} - a_K$. We do this by considering the coefficient in (3) of G/K, and G/KP_i, where $|P_i| = 2$, $P_i \neq P'$.

(f) If $8 \mid |U|$, then G/V has a non-zero coefficient in x_U^G only if $V \geq P'$; for the Frattini subgroup of U contains P'.

Hence x_U^G can only contribute to G/K, or G/KP_i, if $|U/K| = 2$, or $U/K \cong Z/2 \times Z/2$; if $U/K \cong Z/4$, then again, the Frattini subgroup of U contains P'.

(g) Let $U_1,\ldots,U_s$ be representatives of the conjugacy classes of the subgroups of G such that $K \lhd U_i$, $U_i/K \cong Z/2 \times Z/2$; let $KP', V_1,\ldots,V_t$ represent the subgroups such that $K \lhd V_i$, $V_i/K = 2$. Clearly, for such a V_i, $V_iP' = U_j$ (up to conjugacy), for some j, and V_i is contained in exactly one U_j.

U_i contains KP', and 2 other subgroups of index 2, which may, or may not, be conjugate. So suppose $U_1,\ldots,U_n$ are those U_i's containing a single V_j; let $U_1 \geq V_1$, $U_2 \geq V_2,\ldots,U_n \geq V_n$. Then $U_{n+1} \geq V_{n+1}, V_{t+1}$, say, $U_{n+2} \geq V_{n+2}, V_{t+2}$ etc.

In $x_{U_1}^G$, the coefficient of G/V_1 is $-\lambda_{U_1} G/V_1$, and the coefficient of G/K is $+ 1/2\, \lambda_{U_1}$ G/K. Hence the coefficient of G/V_1 in (3) is $(-\lambda_{U_1}a_{U_1} + \lambda_{V_1}a_{V_1})G/V_1$, so $2^s \mid \lambda_{V_1}a_{V_1} - \lambda_{U_1}a_{U_1}$.

The coefficient in (3) of G/V_{n+1} is

$$(-1/2\ \lambda_{U_{n+1}}\, a_{U_{n+1}} + \lambda_{V_{n+1}}\, a_{V_{n+1}})\ G/V_{n+1}, \text{ and so}$$

$$2^s \mid \lambda_{V_{n+1}}\, a_{V_{n+1}} - 1/2\ \lambda_{U_{n+1}}\, a_{U_{n+1}}\ . \quad \text{Similarly,}$$

$$2^s \mid \lambda_{V_{t+1}}\, a_{V_{t+1}} - 1/2\ \lambda_{U_{n+1}}\, a_{U_{n+1}}\ , \text{ and hence}$$

$$2^s \mid \lambda_{V_{n+1}}\, a_{V_{n+1}} + \lambda_{V_{t+1}}\, a_{V_{t+1}} - \lambda_{U_{n+1}}\, a_{U_{n+1}}\ .$$

(h) Now the coefficient of G/K in (3) is

$$-1/2\,\lambda_{KP'}\, a_{KP'} + \lambda_K\, a_K - \sum_i 1/2\ \lambda_{V_i}\, a_{V_i} + \sum_j 1/2\ \lambda_{U_j}\, a_{U_j}\ .$$

The sums can be reordered into

$$\sum_{i=1}^{n} 1/2\ (\lambda_{U_i} a_{U_i} - \lambda_{V_i} a_{V_i}) + \sum_{i=1}^{t-n} 1/2\ (\lambda_{U_{n+i}} a_{U_{n+i}} - \lambda_{V_{n+i}} a_{V_{n+i}} - \lambda_{V_{t+i}} a_{V_{t+i}})$$

2^{s-1} divides each sum, and since $\lambda_{KP'} = 2\lambda_K$, and $(\lambda_K, 2) = 1$,

$2^{s-1} \mid a_K - a_{KP'}$. By (e), this is sufficient to show that $2^s \mid y_1\theta$.

Hence $2^s \mid y\theta$, and our result follows.

<u>Note</u>

In his paper [3], H. Krämer restricts most of his results to the case where G is an abelian p-group. He considers the automorphism group of $\Omega(G)$, Aut $\Omega(G)$; if G is an abelian p-group, then Aut $L(G) \leq$ Aut $\Omega(G)$, where $L(G)$ is the subgroup lattice of G.

He proves in this special case that $\lambda_U^G = p\,|G/U|$, using our notation (4.1 in his paper; this is a special case of Propositions 2.2 and 2.6), and uses this to show that if $\phi \in$ Aut $\Omega(G)$, then if

$p^2 \mid |U|$, ϕ maps G/U onto G/V, where $|U| = |V|$. He then shows that an automorphism of $\Omega(G)$ which fixes G/e induces an automorphism of L(G). His result is then as follows:

Let G be an abelian p-group. Then: if G is cyclic, Aut $\Omega(G) \cong Z/2$. If G is not cyclic and $p \neq 2$, then Aut $\Omega(G)$ = Aut L(G). Suppose p = 2; let F be the Frattini subgroup of G. If $|G : F| \geq 8$, or $|G : F| = 4$ and $G = Z/2^m \times Z/2^n$, with m, $n \geq 2$, then Aut $\Omega(G)$ = Aut L(G). If G is elementary abelian of order 4, then Aut $\Omega(G) = S_4$, Aut $L(G) = S_3$. If G is $Z/2^n \times Z/2$, $n \geq 2$, then Aut $\Omega(G) = Z/2 \times Z/2 \times Z/2$, and Aut $L(G) = Z/2 \times Z/2$.

The above conditions for Aut L(G) $\neq$ Aut $\Omega(G)$ i.e. for the existence of an automorphism of $\Omega(G)$ which does not fix G/e, are clearly special cases of Propositions 3.4, 3.5, 3.6 and 3.7.

Chapter 4

Some results on the width of a finite group

We recall the definition of the width $W(G)$ of G defined in Definitions 5 to 7, Chapter 1:

A chain c from U to V, where $U,V \leq G$, is a sequence $U = U_0, U_1, \ldots, U_n = V$ such that

$$U = U_0 \xrightarrow{p_1} U_1 \xrightarrow{p_2} U_2 \longrightarrow \;\ldots \xrightarrow{p_n} U_n = V,$$

where the p_i's are primes (not necessarily distinct), and $p_i = 1$ if $U_{i-1} \sim U_i$.

The width, $W(c)$, of the above chain c is the number of steps, n; if $C(U,V)$ is the set of chains from U to V, we define $W(U,V) = \min\,(W(c) : c \in C(U,V))$.

Finally the width, $W(G)$, of G is defined by:

$$W(G) = \max\,(W(U,V) \;:\; U,V \leq G).$$

We find that $W(G)$ depends closely on the order of G, and in particular on the number of distinct primes dividing $|G|$. Firstly, an immediate corollary of Dress's paper [1] is that $W(G)$ is finite if and only if G is soluble, and in this case we can obtain an upper bound on $W(G)$ in terms of $|G|$:

Proposition 4.1

If G is soluble, and has order $p_1^{n_1} \ldots p_r^{n_r}$, then $W(G) \leq 2(n_1 + n_2 + \ldots + n_r) - 1$.

Proof G is soluble, so G has a series

$$G = A_0 \rhd A_1 \rhd \;\ldots\; \rhd A_s = e$$

such that A_i / A_{i-1} is a p-group, for $i = 1,\ldots s$; we may assume the series is of minimal length, so ${}^{A_i}/{A_{i-1}}$ is non-trivial, for $i = 1, \ldots s$. So we have the chain

$$G \searrow A_1 \searrow A_2 \searrow \cdots \searrow A_s = e$$

The length of this chain is at most $n_1 + n_2 + \ldots + n_r$.

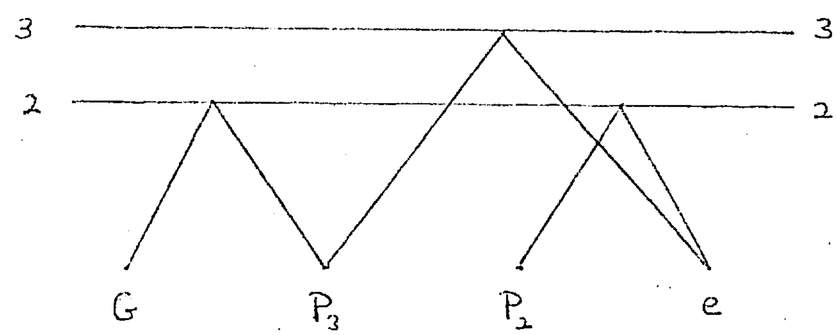
If $U \neq G$, we have the chain

$$U \searrow U \cap A_1 \searrow U \cap A_2 \cdots \searrow U \cap A_s = e,$$

which has length at most $(n_1 + n_2 + \ldots + n_r) - 1$.

Hence any two (distinct) subgroups of G can be connected via e by a chain of length at most $2(n_1 + n_2 + \ldots + n_r) - 1$; hence our result follows.

Example (see Appendix) G is the non-abelian group of order 6. Its graph is:



i.e. $K_2(G) = P_3$, the Sylow 3-subgroup, $K_3(P_3) = e$, etc. Clearly $W(G) = 3$, so our bound is attained in this case.

After the next set of results, we can improve this bound under certain conditions. Lemmas 4.2 and 4.3 are used repeatedly in the following chapter.

Lemma 4.2

Suppose P is a Sylow p-subgroup of G, and we have a chain

$$P \xrightarrow{q_1} A_1 \xrightarrow{q_2} A_2 \rightarrow \dots \xrightarrow{q_r} G, \text{ where } q_i \neq p,\ i = 1,\dots,n.$$

Then P is normal in G.

Proof p does not occur in the chain, so if $|P| = p^r$, then $|A_i| = p^r m_i$. Hence we may choose A_i (by taking a suitable conjugate) such that $A_i \geq P$.

We show by induction on i that $P \lhd A_i$.

Firstly, $P \xrightarrow{q_1} A_1$ implies that $P = K_{q_1}(P) \sim K_{q_1}(A_1) \lhd A_1$.

So $P \lhd A_1$ since $P \leq A_1$.

Assume that $P \lhd A_i$. $A_i \xrightarrow{q_{i+1}} A_{i+1}$ implies that $K_{q_{i+1}}(A_i) \sim K_{q_{i+1}}(A_{i+1})$.

$|A_{i+1}| = q_{i+1}^s |K_{q_{i+1}}(A_i)|$, so $P \lhd K_{q_{i+1}}(A_i)$. Similarly,

$P \lhd K_{q_{i+1}}(A_{i+1})$, so $P \lhd K_{q_{i+1}}(A_{i+1}) \lhd A_{i+1}$. Hence, by the Frattini argument, $P \lhd A_{i+1}$. It follows that $P \lhd G$.

Lemma 4.3

Suppose p occurs only once in a chain between P and G. Then the p-step is redundant.

Proof We have $P \xrightarrow{q_1} U_1 \xrightarrow{q_2} U_2 \xrightarrow{q_3} \dots \rightarrow U_i \xrightarrow{p} U_{i+1} \rightarrow \dots \rightarrow G$, say; $|U_i| = |U_{i+1}|$ since p occurs only once.

$U_i \xrightarrow{p} U_{i+1}$ implies that $K_p(U_i) \sim K_p(U_{i+1})$. By taking suitable conjugates, we may assume that $K_p(U_i) = K_p(U_{i+1}) = V$, say.

$|U_i| = |U_{i+1}| = p^s m$, where $|P| = p^s$.

Consider $N_G(V)/V$. U_i/V and U_{i+1}/V are Sylow p-subgroups of this quotient, hence are conjugate. So $U_i = (U_{i+1})^g$, for some g in $N_G(V)$; thus the p-step may be omitted.

Proposition 4.4

If G is a finite group of order divisible by r distinct primes, then G is nilpotent if and only if W(G) = r.

Proof (a) Suppose G is nilpotent.

Let U,V be subgroups of G. U,V are nilpotent, so, if $p_1,\ldots,p_r$ are the r distinct prime divisors of $|G|$, then

$$U = U_1 \times U_2 \times \ldots \times U_r, \quad V = V_1 \times V_2 \times \ldots \times V_r,$$

where U_i is a p_i-group (possibly consisting of the identity element only) and V_i is a p_i-group, for i = 1 to r.

Put $A_i = V_1 \times V_2 \times \ldots \times V_{i-1} \times U_i \times \ldots \times U_r$.

$$K_{p_i}(A_i) = V_1 \times V_2 \times \ldots \times V_{i-1} \times U_{i+1} \times \ldots \times U_r$$
$$= K_{p_i}(A_{i+1}).$$

Hence $A_i \xrightarrow{p_i} A_{i+1}$.

So we have $U = A_1 \xrightarrow{p_1} A_2 \xrightarrow{p_2} \ldots \xrightarrow{p_{i-1}} A_i \xrightarrow{p_i} A_{i+1} \xrightarrow{p_{i+1}} \ldots \xrightarrow{p_r} A_{r+1} = V$, i.e., U can be connected to V in r steps. U,V are arbitrary subgroups of G, so $W(G) \leqslant r$.

Clearly, we need r steps to connect e to G; so W(G) = r.

(b) Suppose G is not nilpotent.

Then at least one Sylow subgroup is not normal in G. Suppose P is a non-normal Sylow p-subgroup of G. Consider a chain connecting P to G. By Lemma 4.2, p must occur at least once in any such chain, and by Lemma 4.3, p must occur at least twice.

Every other prime must occur at least once, so at least r+1 steps are necessary.

Hence W(G) is at least (r+1).

This completes the proof.

<u>Corollary</u>

If G is soluble, and $|G| = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$, then $W(G) \leq 2(m - \left[{(m-1)}/{(2r+1)}\right]) - 1$ where $[\ ]$ denotes the integer part, and $m = n_1 + n_2 + \dots + n_r$.

<u>Proof</u> As in Proposition 4.1, we have a normal series of minimal length $G \rhd A_1 \rhd \dots \rhd A_s = e$, such that $|A_i/A_{i+1}| = p(i)^{a_i}$.

If $a_i = 1$ for each i, then G is supersoluble. In this case, the derived group G' of G is nilpotent, and we have the chain

$$G \overset{p_1}{\searrow} \dots \overset{p_r}{\searrow} G' \overset{p_1}{\searrow} \dots \overset{p_r}{\searrow} e ,$$

since G/G' and G' are nilpotent. So G can be connected to e in at most 2r steps.

Hence, if in our chain

$$G \searrow A_1 \searrow \dots \searrow A_s = e,$$

there are 2r+1 consecutive steps $A_i \searrow A_{i+1}$, such that

$|A_i/A_{i+1}| = p(i)$, for $i = k, k+1, \dots, k+2r+1$, then A_k/A_{k+2r+1} is supersoluble, and hence A_k can be connected to A_{k+2r+1} in 2r steps.

Thus within every 2r+1 steps, some prime must occur squared, so G can be connected to e in at most $n_1 + n_2 + \dots + n_r - [m/(2r+1)]$ steps, where $m = n_1 + n_2 + \dots + n_r$.

For $U \underset{r}{\lneq} G$, U can be connected to e in at most $m - 1 - \left[(m-1)/(2r+1)\right]$ steps.

Therefore $W(G) \leq m - \left[m/(2r+1)\right] + m-1 - \left[(m-1)/(2r+1)\right]$

$$\leq 2\left(m - \left[(m-1)/(2r+1)\right]\right) - 1$$

<u>Proposition 4.5</u>

If G has order $p^r q^s$, where p,q are distinct primes, then G has Fitting length n if and only if W(G) is 2n-1 or 2n.

<u>Proof</u> (a) Let G have Fitting length n.

We have the chain

$$G = N_0 \trianglerighteq N_1 \trianglerighteq \dots \trianglerighteq N_n = e,$$

defined by $N_i = \bigcap (M \lhd N_{i-1} ; N_{i-1}/M \text{ is nilpotent})$, i=1,..,n. The N_i's are characteristic subgroups of G.

Define X_i, Y_i to be subgroups of G such that X_i/N_i, Y_i/N_i are respectively the Sylow p and q-subgroups of N_{i-1}/N_i, for i = 1,...n.

We have two chains from G to e:

$$G \overset{q}{\searrow} X_1 \overset{p}{\searrow} N_1 \overset{q}{\searrow} X_2 \overset{p}{\searrow} N_2 \overset{q}{\searrow} \dots \searrow e,$$

$$G \overset{p}{\searrow} Y_1 \overset{q}{\searrow} N_1 \overset{p}{\searrow} Y_2 \overset{q}{\searrow} N_2 \overset{p}{\searrow} \dots \searrow e.$$

These can be combined to give two further chains:

$$G \overset{q}{\searrow} X_1 \overset{p}{\searrow} N_1 \overset{p}{\searrow} Y_2 \overset{q}{\searrow} N_2 \overset{q}{\searrow} \dots \searrow e,$$

$$G \overset{p}{\searrow} Y_1 \overset{q}{\searrow} N_1 \overset{q}{\searrow} X_2 \overset{p}{\searrow} N_2 \overset{p}{\searrow} \dots \searrow e,$$

which give $G \overset{q}{\searrow} X_1 \overset{p}{\searrow} Y_2 \overset{q}{\searrow} X_3 \overset{p}{\searrow} Y_4 \overset{q}{\searrow} \dots \searrow e$ (x)

$$G \overset{p}{\searrow} Y_1 \overset{q}{\searrow} X_2 \overset{p}{\searrow} Y_3 \overset{q}{\searrow} X_4 \overset{p}{\searrow} \dots \searrow e. \qquad (y)$$

Both the chains (x),(y) have length at most n+1, and at least n. Both chains cannot have length n, otherwise we would have $N_{n-1} = e$, since $X_i \cap Y_i = N_i$. We have two cases; firstly, one of (x),(y) has length n, the other length n+1, and secondly, both have length n+1.

Suppose one of (x),(y) has length n, and w.l.o.g. that its last term is a q-group i.e. we have the chains

$$G \searrow A_1 \searrow \dots \overset{q}{\searrow} A_{n-2} = Q'P_1 \overset{p}{\searrow} Q' \overset{q}{\searrow} e \qquad (X)$$

$$G \searrow B_1 \searrow \dots \searrow B_{n-2} \overset{q}{\searrow} B_{n-1} = Q_1'P_1' \overset{p}{\searrow} Q_1' \overset{q}{\searrow} e, \qquad (Y)$$

where $Q' \geqslant Q_1'$, $P_1 \geqslant P_1'$.

Consider $N_G(P_1)$; $Q'P_1 \lhd G$, so $P_1 \lhd P$, the Sylow p-subgroup of G. Hence $N_G(P_1) = PQ_2$, where Q_2 is a q-group.

Now $P_1 \leq P_1Q' \lhd G$, so by the Frattini argument, $N_G(P_1).P_1Q' = G$, so $Q_2Q' = Q$, the Sylow q-subgroup of G (since $Q' \lhd G$).

Now consider connecting $K = N_G(P_1)$ to e; we have two chains, (X') of length n-1 and (Y') of length n, as follows:

$$K \searrow K \cap A_1 \searrow \dots \searrow K \cap A_i \searrow \dots \overset{p}{\searrow} K \cap Q'P_1 \overset{q}{\searrow} P_1 \overset{p}{\searrow} e \qquad (X')$$

$$K \searrow K \cap B_1 \searrow \dots \searrow K \cap B_i \searrow \dots \overset{q}{\searrow} P_1' \overset{p}{\searrow} e \qquad (Y')$$

(since $P_1 \lhd K \cap Q'P_1$, and $P_1' \lhd K \cap Q_1'P_1'$). (X') and (Y') are not necessarily the characteristic chains from K to e whose terms have minimal order. However, since any chain from K to e can be made into a chain from G to e by multiplying each term by the normal subgroup Q' ($KQ' = G$), we can see that (X'),(Y') have minimal length, and P_1 and P_1' are the last terms in the 2 minimal characteristic chains from K to e. Hence P_1 is normal in the first (n-1) terms of any chain from K starting with the same prime as (X'), whereas P_1' is normal in the first n terms of any chain from K starting with the same prime as (Y').

Now suppose we can connect K to G in 2n-2 steps, i.e. we have a chain

$$\underbrace{K \to \dots \to A}_{n-2} \to \underbrace{B \to \dots \to G}_{n}$$

Suppose the first step involves the same prime as the first step in (X'). There is an even number of steps, so the last step corresponds to the first step in (Y).

So $A \rhd P_1$, and also $A \rhd Q_1'$. Hence $P_1 \lhd P_1Q_1'$, and since $P_1' \leq P_1$, $P_1' \lhd P_1'Q_1'$. This contradicts (Y), since $K_q(B_{n-1}) = B_{n-1}$.

If the first step involves the same prime as the first step in (Y'), then the last step corresponds to the first step in (X).

Then $B \rhd P_1'$, $B \rhd Q'$, so $P_1' \lhd P_1'Q'$, hence $P_1' \lhd P_1'Q_1'$ (since $Q_1' \leq Q'$) and this contradicts (Y) again.

Thus we cannot connect K to G in less than 2n-1 steps i.e. $W(G) \geq 2n-1$.

If both (x),(y) have n+1 steps, then obviously we can find in a similar manner a subgroup K' which cannot be connected to G in less than 2n-1 steps.

Finally, we show that $W(G) \leq 2n$.
For we have the chains (x),(y) of length at most n+1; relabel (x), (y) to obtain

$$G \searrow Z_1 \searrow Z_2 \searrow \ldots \searrow Z_n \searrow e \qquad (x)$$

$$G \searrow Z_1' \searrow Z_2' \searrow \ldots \searrow Z_n' \searrow e \qquad (y), \text{ and } (|Z_n|, |Z_n'|) = 1.$$

Suppose U,V are subgroups of G. The subgroups $U \cap Z_n$, $V \cap Z_n'$ are subgroups of $Z_n \times Z_n'$, so $(U \cap Z_n) \times (V \cap Z_n')$ is a subgroup.

Therefore we have the chain

$$U \searrow U \cap Z_1 \searrow \ldots \searrow U \cap Z_{n-1} \rightarrow (U \cap Z_n) \times (V \cap Z_n')$$
$$\rightarrow V \cap Z_{n-1}' \nearrow \ldots \nearrow V \cap Z_1' \nearrow V.$$

This has width 2n.

Hence $W(G) = 2n$ or $2n-1$.

(b) The converse is immediate.

Proposition 4.6

If G has order $p^r q^s$, where p,q are distinct primes, and G has Fitting length n, then W(G) = 2n if and only if the shortest chain from G to e has n+1 steps.

Proof (a) Suppose that G cannot be connected to e in less than n+1 steps.

As in Proposition 4.5, we have two minimal chains of length n+1:

$$G \searrow A_1 \searrow \dots \searrow A_{n-1} = P'Q_1 \overset{q}{\searrow} P' \overset{p}{\searrow} e$$

$$G \searrow B_1 \searrow \dots \searrow B_{n-1} = P_1Q' \overset{p}{\searrow} Q' \overset{q}{\searrow} e,$$

where $P_1 \geqslant P'$, $Q_1 \geqslant Q'$.

Consider connecting $N_G(P_1)$ to $N_G(Q_1)$; suppose this can be done in 2n-1 steps. We have two chains:

$$(1) \quad N_G(P_1) \searrow N_G(P_1) \cap A_1 \searrow \dots \searrow N_G(P_1) \cap A_i \searrow \dots \overset{p}{\searrow} P'Q_2 \overset{q}{\searrow} P' \overset{p}{\searrow} e,$$

$$(2) \quad N_G(P_1) \searrow N_G(P_1) \cap B_1 \searrow \dots \searrow N_G(P_1) \cap B_i \searrow \dots \overset{q}{\searrow} P_1 \overset{p}{\searrow} e,$$

where (1) has n+1 steps, and (2) has n steps. As in Proposition 4.5, these chains have minimal length, given that one must start with a p-step, one with a q-step, and P' and P_1 are the last terms in the 2 minimal characteristic chains (otherwise by multiplying each term by Q', we would form chains from G to e contradicting the minimality of the above chains).

$$(1') \quad N_G(Q_1) \searrow N_G(Q_1) \cap A_1 \searrow \dots \searrow N_G(Q_1) \cap A_i \searrow \dots \overset{p}{\searrow} Q_1 \overset{q}{\searrow} e,$$

$$(2') \quad N_G(Q_1) \searrow N_G(Q_1) \cap B_1 \searrow \dots \searrow N_G(Q_1) \cap B_i \searrow \dots \searrow P_2Q' \overset{p}{\searrow} Q' \overset{q}{\searrow} e,$$

where (1') has n steps, and (2') has n+1 steps, and $P_2 \leqslant P_1$.

Without loss of generality, we have the chain

$$\underbrace{N_G(P_1) \to \dots \overset{q}{\to} A}_{n-1} \underbrace{\overset{p}{\to} B \overset{q}{\to} \dots \to N_G(Q_1)}_{n}$$

Hence $A_1 \trianglerighteq P_1$, $B \trianglerighteq Q'$, and $A \geqslant Q'$ since $A \overset{p}{\to} B$.

So $P_1 \lhd P_1Q'$. This contradicts the minimality of (y) above

Hence $N_G(Q_1)$ to $N_G(P_1)$ takes at least 2n steps.

(b) If $W(G) = 2n$, then G has Fitting length n, by Proposition 4.5.

If G can be connected to e in n steps, suppose the minimal chain is

$$G \searrow A_1 \searrow \dots \overset{q}{\searrow} A_{n-1} = P' \overset{p}{\searrow} e,$$

Suppose U,V are subgroups of G. We have the chains

$$U \searrow U \cap A_1 \searrow \dots \searrow U \cap P'$$

$$V \searrow V \cap A_1 \searrow \dots \searrow V \cap P',$$

and both have n-1 steps.

Also $U \cap P' \xrightarrow{p} V \cap P'$.

So $W(G) = 2n-1$, a contradiction.

Hence G cannot be connected to e in less than n+1 steps.

We now consider the general finite soluble group G of order $p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$, say, where the p_i's are distinct primes. P_i will denote the Sylow p_i-subgroup of order $p_i^{n_i}$, for $i = 1,2,\dots,r$.

If P_i is not normal in G, then the chain from P_i to G involves p_i at least twice, by Propositions 4.2 and 4.3; if the non-normal Sylow subgroups of G are exactly $P_1, P_2, \dots, P_s$, say, then for each p_i, $i = 1,2,\dots,s$, there is a chain which involves p_i twice (at least). It seems plausible to suppose that there might be a chain which involves each prime $p_1, p_2, \dots p_s$ twice (at least), making $W(G)$ at least $(2s + (r-s))$ i.e. at least $s+r$.

This is indeed the case; the proof is inductive on the order of G. First we prove:

Proposition 4.7

Suppose P is a normal Sylow p-subgroup of G, and $W(G) = m$. Then $W(G/P) \leq m - 1$.

Proof Certainly $W(G/P) \leq m$.

Suppose U/P, V/P are subgroups of G/P, where $U, V \geq P$.

G is soluble, so $U = PM$, where M is the p-complement of U. Consider connecting M to V; this can be done in m steps, and p must occur at least once, since $p \mid |V|$, $p \nmid |M|$.

Further, if $A \xrightarrow{p} B$, then AP is conjugate to BP in G (A, B subgroups of G).

So if our chain is

$$M \longrightarrow A_1 \longrightarrow \dots \longrightarrow A_i \xrightarrow{p} A_{i+1} \longrightarrow \dots \longrightarrow V,$$

then the chain

$$U = MP \longrightarrow A_1P \longrightarrow \dots \longrightarrow A_iP \xrightarrow{p} A_{i+1}P \longrightarrow \dots \longrightarrow VP = V,$$

has at most $(m-1)$ irredundant steps, since $A_iP \sim A_{i+1}P$.

Thus $W(G/P) \leq m-1$.

Note With the above conditions, $W(G/P)$ is not necessarily $m-1$. For example, if G is the non-abelian group of order 6, then $W(G) = 3$, but $W(G/P) = 1$, where P is the normal Sylow 3-subgroup of G.

Proposition 4.8

Suppose G is a finite soluble group, of order $p_1^{n_1}p_2^{n_2}\dots p_r^{n_r}$; if $W(G) = r+n$, then G has at most n non-normal Sylow subgroups.

Proof If $n \geq r$, the result is trivial.

So suppose $n < r$, and that G is a counter-example of minimal order to our Proposition.

$W(G) = r+n$, G has at least $(n+1)$ non-normal Sylow subgroups; and if U is a non-trivial normal subgroup of G, then $W(G/U) \leq r+n$, and hence G/U has at most n non-normal Sylow subgroups.

Let the normal Sylow subgroups of G be $P_1,\dots,P_t$, where $t \geq 0$; and suppose there are non-trivial normal p_i-subgroups for $i = 1,2,\dots,s$, and no others. $s \geq 1$, since G is soluble, and $s \geq t$.

If there is a non-trivial normal p_i-subgroup, there is a unique maximal such (since, if X_1 and X_2 are normal p_i-subgroups, so is X_1X_2). Denote this unique maximal p_i-subgroup by P_i', for $i = 1,2,\dots,s$ (where $P_i' = P_i$ for $i = 1,\dots,t$).

By Proposition 4.7, $W(G/P_1) \leq (r-1)+n$, so G/P_1 has at most n non-normal Sylow subgroups (G is a counter-example of minimal order, so G/P_1 satisfies our Proposition), hence $Q_iP_1 \lhd G$, for some non-normal Sylow subgroup Q_i of G.

If $s > t$, G/P_{t+1}' satisfies our Proposition: $W(G/P_{t+1}') \leq n + r$ and G/P_{t+1}' has r distinct Sylow subgroups (since $P_{t+1}' \neq P_{t+1}$), and is a non-trivial quotient of G. Hence G/P_{t+1}' has at most n non-normal Sylow subgroups, so $Q_jP_{t+1}' \lhd G$, for some non-normal Sylow subgroup Q_j of G.

Let $Q_1, Q_2, \ldots, Q_a$ be a set of representatives of the conjugacy classes of the non-normal Sylow subgroups of G which satisfy $Q_i P_j^! \lhd G$, for some $P_j^!$, $j = 1,2,\ldots,s$. Since $Q_1 \ntriangleleft G$, $Q_1 P_i^! \lhd G$ implies $Q_1 P_j^! \ntriangleleft G$, if $i \neq j$; so $a \geqslant s$.

Now consider $N = \bigcap_{i=1}^{a} N_G(Q_i)$.

Suppose $Q_{j_1}, \ldots, Q_{j_k}$ are the Q's which satisfy $Q_i P_j^! \lhd G$. Then, by the Frattini argument, $Q_{j_1} Q_{j_2} \ldots Q_{j_k}$ is nilpotent, and since $Q_{j_1} \ldots Q_{j_k} P_j^! \lhd G$, $N_G\,(Q_{j_1} \ldots Q_{j_k}) = P_1 \ldots P_{j-1} P_j^* P_{j+1} \ldots P_r$, say, where $P_j^* P_j^! = P_j$ (by the Frattini argument).

Hence $N = \bigcap_{i=1}^{a} N_G(Q_i) = P_1^* \ldots P_s^* P_{s+1} \ldots P_r$, where

$P_i^* P_i^! = P_i$, $i = 1,\ldots,s$, and $P_i^* \neq e$, for $i = t+1,\ldots,s$ (since $P_i^! \neq P_i$, $i = t+1,\ldots,s$).

Now suppose $P_i^* \geqslant X_i$, where X_i is a non-trivial normal p_i-subgroup of G. By the minimality of G, G/X_i has at most n non-normal Sylow subgroups, so $QX_i \lhd G$ for some non-normal Sylow subgroup Q of G. But $X_i \leqslant P_i^!$, so $QP_i^! \lhd G$, and hence, by the definition of P_i^*, $Q \lhd QP_i^*$, so $Q \lhd QX_i \lhd G$. This implies $Q \lhd G$, a contradiction.

So P_i^* contains no normal subgroups, so neither does N.

We now connect $N_1 = P_{t+1}^* \ldots P_s^* P_{s+1} \ldots P_r$ to G; we show that each prime $p_{t+1}, \ldots p_r$ must occur twice, and obtain a contradiction to the choice of G.

Suppose the chain is

$$N_1 = P_{t+1}^* \ldots P_s^* P_{s+1} \ldots P_r \xrightarrow{\alpha_1} A_1 \xrightarrow{\alpha_2} A_2 \xrightarrow{\alpha_3} \ldots \xrightarrow{\alpha_k} G. \qquad (1)$$

$p_1, p_2, \ldots, p_t$ must each occur at least once. Suppose $Q_1 P_i^! \lhd G$;

Q_1 is one of $P_{t+1},\ldots,P_r$. If $Q_1 = P_j$ for $j > s$, then $Q_1 \triangleleft N_1$, so q_1 occurs twice (where Q_1 is the Sylow q_1-subgroups); if $Q_1 = P_j$ for some $j = t+1,\ldots,s$, then form the chain

$$N_1P_j' \xrightarrow{\alpha_1} A_1P_j' \xrightarrow{\alpha_2} A_2P_j' \xrightarrow{\alpha_3} \cdots \longrightarrow A_{k-1}P_j' \xrightarrow{\alpha_k} G \qquad (2)$$

$Q_1(=P_j)$ is normal in N_1P_j', so q_1 must occur twice in (2), and hence twice in (1).

So q_i occurs twice, for $i = 1,2,\ldots,a$.

The remaining primes are those p_i such that $i > t$, and $p_i \neq q_j$, $j = 1,\ldots,a$. Suppose p_i is such, with $i > s$ and that it doesn't occur in (1) (since $P_i \leq N_1$, p_i must occur twice if it occurs in a non-trivial step).

Then $K_{\alpha_1\alpha_2\cdots\alpha_k}(G)$ is normal in G, and contains P_i, since p_i does not occur, and is contained in N_1. But N_1 contains no non-trivial normal subgroups, so this is impossible. So p_i must occur twice.

The remaining p_i's are those such that $t+1 \leq i \leq s$, $p_i \neq q_j$, $j = 1,\ldots,a$. So suppose p_i is such, and it occurs only once (it must occur once, since $P_i^* \neq P_i$). Form the chain

$$N_1P_i' \xrightarrow{\alpha_1} A_1P_i' \xrightarrow{\alpha_2} \cdots \longrightarrow A_{k-1}P_i' \xrightarrow{\alpha_k} G. \qquad (3)$$

Each term in this chain includes P_i, so the p_i-step is trivial. Remove it, to form the chain

$$N_1P_i' \xrightarrow{\beta_1} B_1 \xrightarrow{\beta_2} B_2 \longrightarrow \cdots \longrightarrow B_{k-2} \xrightarrow{\beta_{k-1}} G.$$

Hence $K_{\beta_1\beta_2\cdots\beta_k}(G) \leq N_1P_i'$, and is normal in G; suppose $K = K_{\beta_1\beta_2\cdots\beta_k}(G) = X_{t+1}\cdots X_{i-1}P_iX_{i+1}\cdots X_r$.

From (3), it follows that $K_{\alpha_1\alpha_2\cdots\alpha_k}(G) = e$, since N_1 contains no normal subgroups of G; so e can be connected to G by a chain which involves p_i only once. Hence we must have a subgroup Z of G such that $(|Z|,p_i) = 1$, $Z \triangleleft G$, and $ZP_i \triangleleft G$. $Z \neq e$, since $P_i \ntriangleleft G$.

So $Z \cap K \lhd ZP_i \cap K \lhd G$. $Z \cap K$ is normal in G, and is also a subgroup of N_1; hence $Z \cap K = e$. But this implies $P_i \lhd G$, since $P_i = ZP_i \cap K$; a contradiction.

So every prime $p_{t+1}, \ldots, p_r$ occurs (at least) twice; hence the number of steps in (1) is at least $t + 2(r-t)$.

Hence $t + 2(r-t) \leq n+r$, i.e. $r - t \leq n$.

Thus the number of non-normal Sylow subgroups of G is at most n; this finally contradicts the choice of G and proves our result.

Proposition 4.9

Suppose G has order $p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$. Then $W(G) = r + 1$ if and only if G has exactly one non-normal Sylow subgroup.

Proof (a) Suppose $W(G) = r + 1$.

By Proposition 4.8, G has at most one non-normal Sylow subgroup, and by Proposition 4.4, if G has no non-normal Sylow subgroups (i.e. G is nilpotent), then $W(G) = r$.

So G has exactly one non-normal Sylow subgroup.

(b) Suppose G has exactly one non-normal Sylow subgroup.

Let this non-normal Sylow subgroup be P_1, say, the Sylow p_1-subgroup. $P_2, P_3, \ldots, P_r \lhd G$, so $P_2 P_3 \ldots P_r$ is normal in G, and nilpotent.

So for $U, V \leq G$, we have $U \overset{p_1}{\searrow} K_{p_1}(U) \leq P_2 P_3 \ldots P_r$, and similarly $K_{p_1}(V) \overset{p_1}{\searrow} P_2 P_3 \ldots P_r$. $K_{p_1}(U)$ can be connected to $K_{p_2}(V)$ in $(r-1)$ steps by the nilpotency of $P_2 P_3 \ldots P_r$ (Proposition 4.4), so U can be connected to V in $(r+1)$ steps.

Hence $W(G) = r + 1$.

<u>Examples</u>

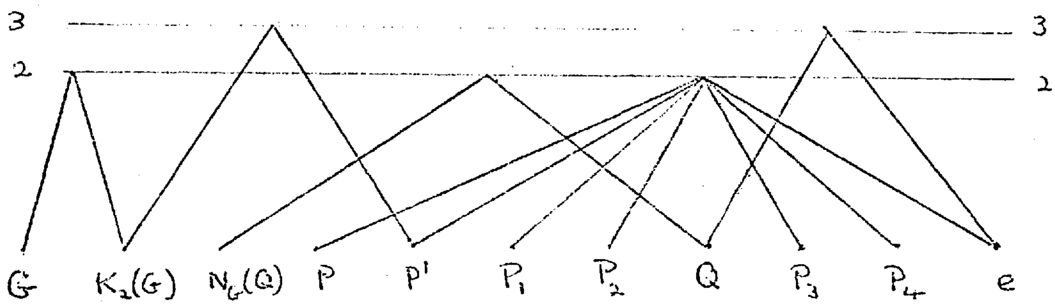
(1) $G = S_4$ (see appendix for details)

$|P| = 8, |Q| = 3$. P is self-normalising, $|N_G(Q)| = 6$, $K_3(G) = G$, and $|K_2(G)| = 12$. We have the chains

$$G \overset{2}{\searrow} K_2(G) \overset{3}{\searrow} P' \overset{2}{\searrow} e, \quad |P'| = 4,$$

$$G \overset{3}{\searrow} G \overset{2}{\searrow} K_2(G) \overset{3}{\searrow} P' \overset{2}{\searrow} e.$$

The graph is:



$N_G(Q)$ to G takes 5 steps, and $W(G) = 5$.

(2) $G = (x,y,z,a,b)$, where $P = (x,y,z)$ is elementary abelian of order 8, and $Q = (a,b)$, elementary abelian of order 9, and the relations are $x^a = y$, $y^a = z$, $z^a = x$, $b^x = b^y = b^z = b^2$.

$N_G(P) = (P,a)$, $N_G(Q) = (Q,xyz)$,

$K_3(G) = (P,b)$, $K_2(G) = (Q,xy,yz)$,

so $K_2(G) \cap K_3(G) = P' \times Q'$, where $P' = (xy,yz)$, $Q' = (b)$.

Hence G has Fitting length 2.

We now show that G is 4-step connected.

If $U \leqslant G$, and U has a normal Sylow p-subgroup, where $p = 2$ or 3, then U can be connected to V in 4 steps for any subgroup V of G; for $V \overset{2}{\searrow} K_2(V) \overset{3}{\searrow} P^*$, where P^* is a 2-subgroup, and $V \overset{3}{\searrow} K_3(V) \overset{2}{\searrow} Q^*$, Q^* is a 3-subgroup.

If $|U| = 2,3,4,8,6,12$, or 18, then U has a normal Sylow subgroup.

The other possibilities are $|U| = 36$, or 24.

If $|U| = 36$, then $U \geq Q$, so possibilities are $U = (a,b,xyz)$, or (a,b,xy,yz): both have a normal Sylow subgroup.

If $|U| = 24$, then $U \geq P$. The only possibilities are (P,a), (P,b): again, both have a normal Sylow subgroup.

Hence G is 4-step connected. ($N_G(P)$ to $N_G(Q)$ takes 4 steps)

We now consider the case where $W(G) = r+2$, where as usual G has order $p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$; we already know the condition for $r = 2$, so we assume $r \geq 3$.

In this case, as one might expect, G has exactly 2 non-normal Sylow subgroups; but this is not a sufficient condition, as can be seen from the case $r = 2$.

Proposition 4.10

If G has order $p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$, where $r \geq 3$, then $W(G) = r + 2$ if and only if G has exactly 2 non-normal Sylow subgroups, P_1 and P_2 say, and either G has Fitting length 2, or one of the Sylow p_1- and p_2-complements is normal in G.

Proof (a) Suppose $W(G) = r + 2$.

By Proposition 4.8, G has at most 2 non-normal Sylow subgroups, and by Proposition 4.9, G has exactly 2 non-normal Sylow subgroups.

Let these be P_1, P_2, say; so $P_3, \dots, P_r$ are normal in G. Suppose neither the p_1- nor the p_2-Sylow complement is normal in G.

We use induction on r, and reduce to the case $r = 3$.

By Proposition 4.7, $W(G/P_r) \leq r + 1$, and hence G/P_r satisfies the Proposition. So, if $K_{p_i}(G) = P_1 \dots P_{i-1} P_i' P_{i+1} \dots P_r$, $i = 1, \dots, r$ then $P_1' P_r$, $P_2' P_r \triangleleft G$; for G/P_r must have Fitting length 2, since $P_1', P_2' \neq e$.

If $P_{r-1} \triangleleft G$, then similarly $P_1'P_{r-1}, P_2'P_{r-1} \triangleleft G$, so $P_1', P_2' \triangleleft G$, and our result follows.

We are left with the case $r = 3$; $P_1, P_2 \ntriangleleft G$, $P_3 \triangleleft G$, and $W(G) = 5$, with $P_1P_3, P_2P_3 \ntriangleleft G$.

Firstly, $W(G/P_3) \leq 4$, by Proposition 4.7, and by Proposition 4.9, $w(G/P_3) = 4$, since G/P_3 has no normal Sylow subgroups.

So by Proposition 4.6, $P_1'P_3, P_2'P_3 \triangleleft G$, with the above notation. We must show $P_1', P_2' \triangleleft G$ (by supposition, $P_1', P_2' \neq e$).

Suppose G has no normal p_1- or p_2-subgroups. Consider the chain

$$P_1P_2 \xrightarrow{q_1} A_1 \xrightarrow{q_2} A_2 \xrightarrow{q_3} \dots \xrightarrow{q_5} G.$$

P_1P_2 contains no normal subgroups, so $K_{q_1 \dots q_5}(G) = e$. Hence p_1 and p_2 must occur twice, so p_3 can occur only once. By our assumption about the normal subgroups of G, p_3 must occur in the first 2 steps; so $P_1' \triangleleft P_1'P_3$ ($\triangleleft G$), and this is a contradiction.

So G has a normal p_1-subgroup, X_1 say, so by induction on the order of G, either $P_1'X_1, P_2'X_1 \triangleleft G$, or $X_1P_2P_3 \triangleleft G$. Both these give $P_1' \triangleleft G$.

So now suppose G has no normal p_2-subgroups.

We have $P_1'P_2P_3 \triangleleft G$, so $N_G(P_2) = P_1^*P_2P_3^*$, where $P_1^*P_1' = P_1$. Consider the chain

$$P_1^*P_2 \xrightarrow{q_1} A_1 \xrightarrow{q_2} A_2 \xrightarrow{q_3} \dots \xrightarrow{q_5} G. \qquad (1)$$

p_2 must occur twice. Suppose p_1 occurs only once; then the chain $P_1'.P_1^*P_2 = P_1P_2 \xrightarrow{q_1} P_1'A_1 \xrightarrow{q_2} \dots \xrightarrow{q_5} G$ has a trivial p_1-step, and so can be shortened to

$$P_1P_2 \xrightarrow{\alpha_1} B_1 \xrightarrow{\alpha_2} B_2 \xrightarrow{\alpha_3} B_3 \xrightarrow{\alpha_4} G,$$

where p_1 does not appear. Hence $K_{\alpha_1 \dots \alpha_4}(G) = P_1X_2$; $X_2 \neq e$, since $P_1 \ntriangleleft G$, and $X_2 \leq P_2'$. But $P_2'P_3 \triangleleft G$, so $X_2 \triangleleft G$, a contradiction.

So p_1 occurs twice in (1), and hence p_3 only occurs once.

If P_1^* contains X_1, a non-trivial normal p_1-subgroup, then by induction either $X_1P_2' \triangleleft G$, which gives $P_2' \triangleleft G$, or $X_1P_2P_3 \triangleleft G$, i.e. $X_1 \geqslant P_1'$. This gives $P_1^* = P_1$; but $P_2P_3 \ntriangleleft G$, so $P_2 \ntriangleleft P_2P_1$.

Hence $P_1^*P_2$ does not contain any normal subgroups of G, so $K_{q_1 \ldots q_5}(G) = e$. $P_1 \ntriangleleft P_1P_3$, $P_2 \ntriangleleft P_2P_3$, so p_3 cannot occur in the last 2 steps, or in the first 2 steps in (1). $P_2' \ntriangleleft P_2'P_3$, so $P_2' \nleqslant A_2$, $P_2' \nleqslant A_3$. So $q_1 = q_5 = p_1$, $q_2 = q_4 = p_2$. But then $P_1' \leqslant A_1$, so $P_2 \triangleleft P_2P_1'$; hence $P_2 \triangleleft P_2P_1$, contrary to our assumption.

Hence G has a normal p_2-subgroup X_2, say, and by induction, $P_2' \triangleleft G$, as proved above for P_1'.

So $P_1'P_2'P_3$ is nilpotent and normal in G; so G has Fitting length 2. This completes the proof.

(b) The converse.

$P_3, P_4, \ldots P_r$ are normal in G; if $P_1P_3 \ldots P_r$, the Sylow p_2-complement is normal in G, then for $U, V \leqslant G$, we have $K_{p_1p_2}(U)$, $K_{p_1p_2}(V)$ contained in $P_3 \ldots P_r$, which is nilpotent and hence $W(P_3 \ldots P_r) = r-2$. Hence U can be connected to V in (r+2) steps.

If, on the other hand, G has Fitting length 2, then P_1', $P_2' \triangleleft G$, so we have the chain

$$U \overset{p_1}{\searrow} U \cap P_1'P_2 \ldots P_r \overset{p_2}{\searrow} U \cap P_1'P_2'P_3 \ldots P_r \overset{p_2}{\rightarrow} \ldots \overset{p_1}{\longrightarrow} V \cap P_1'P_2'P_3 \ldots P_r$$
$$\ldots \overset{p_1}{\nearrow} V \cap P_1P_2'P_3 \ldots P_r \overset{p_2}{\nearrow} V,$$

using the nilpotency of $P_1'P_2'P_3 \ldots P_r$. This can be shortened to (r+2) steps.

So in both cases $W(G) = r + 2$.

Chapter 5

The diameter of a finite group

The number of times a given prime must occur in a chain between 2 subgroups of G is not determined in general by the number of times it occurs in a path of minimal width, since there may not be a unique minimal path. For example, if G has order $p^r q^s$, and $W(G) = 4$, then by the results of Chapter 4, G has fitting length 2, and no normal Sylow subgroups. Hence there is no chain from G to e with 2 steps, but 2 chains of length 3, one involving p once and q twice, the other involving q once and p twice.

Recall the definition of d(G), the diameter of G, defined in Definitions 5 to 7, Chapter 1:

A chain c from U to V, where $U,V \leqslant G$, is a sequence $U = U_0, U_1, \ldots\ldots, U_n = V$ such that

$$U_0 = U_0 \xrightarrow{p_1} U_1 \xrightarrow{p_2} U_2 \longrightarrow \ldots\ldots \xrightarrow{p_n} U_n = V,$$

where the p_i's are prime (not necessarily distinct), and $p_i = 1$ if $U_{i-1} \sim U_i$.

The diameter, d(c), of the above chain c is defined by $d(c) = p_1 p_2 \ldots\ldots p_n$; if $C(U,V)$ is the set of chains from U to V, for $U,V \leqslant G$, we define $c(U,V) = \text{h.c.f.}(d(c): c \in C(U,V))$.

Finally, the diameter, d(G), of G is defined by:

$$d(G) = \text{l.c.m.}(d(U,V): U,V \leqslant G).$$

Proposition 5.1

Suppose G is a soluble group. Then:

(a) p divides the order of G if and only if p divides d(G).

(b) G has a normal Sylow p-subgroup if and only if p^2 does not divide d(G).

(c) G is nilpotent if and only if d(G) is square-free.

Proof

(a) Any chain from G to e (G is soluble, so there is a chain from G to e) involves every prime divisor of the order of G; so if G has order $p_1^{n_1} p_2^{n_2} \ldots . p_r^{n_r}$, then $p_1 p_2 \ldots . p_r$ divides d(G).

The converse is trivial.

(b) Suppose P is a normal Sylow p-subgroup of G. If $U \leqslant G$, then $U \cap P \lhd U$, and there is a normal chain

$$U = A_0 \overset{q_1}{\searrow} A_1 \overset{q_2}{\searrow} A_2 \overset{q_3}{\searrow} \ldots . . \overset{q_s}{\searrow} A_s = U \cap P,$$

where each A_i is normal in U, and the q_i's are distinct from p. Similarly, we have a chain

$$V \cap P = B_0 \overset{q'_1}{\nearrow} B_1 \overset{q'_2}{\nearrow} B_2 \overset{q'_3}{\nearrow} \ldots . . \nearrow B_t = V. \quad (q'_i \neq p)$$

Combining these two chains with the p-step $U \cap P \xrightarrow{p} V \cap P$, we obtain a path from U to V which involves p exactly once.

Hence $d(U,V) = pm$, where $(p,m) = 1$; and since this holds for all $U,V \leqslant G$, $d(G) = pm'$, where $(p,m') = 1$.

Conversely, if the Sylow p-subgroup P is not normal in G, then by Propositions 4.2 and 4.3, p must occur twice in any path from P to G; so p^2 divides d(P,G), and hence divides d(G).

(c) This follows from (b): d(G) is square-free if and only if every Sylow subgroup of G is normal, i.e. if and only if G is nilpotent.

Proposition 5.2

If G has Fitting length f, then d(G) divides $(p_1 p_2 \ldots p_r)^f$.

Proof

We have the chain

$G = N_0 \rhd N_1 \rhd N_2 \rhd \ldots\ldots \rhd N_f = e$, where N_i/N_{i+1} is nilpotent for $i = 0, 1, \ldots, f$.

(a) Suppose f is even. We have the chain:

$$G \searrow^{p_r} \searrow^{p_{r-1}} \searrow \ldots \searrow^{p_1} N_1 \searrow^{p_1} \ldots \searrow^{p_r} N_2 \searrow^{p_r} \ldots$$

$$\searrow^{p_1} N_3 \searrow^{p_1} \ldots \searrow^{p_1} N_{f-1} . \qquad (1)$$

So if U is a subgroup of G, by intersecting U with the above chain, we obtain

$$U \searrow \ldots\ldots \searrow^{p_1} U \cap N_{f-1} , \qquad (2)$$

in which p_1 occurs at most f/2 times (combining adjacent p_1 steps).

For V a subgroup of G, $U \cap N_{f-1}$, and $V \cap N_{f-1}$ are subgroups of N_{f-1}, which is nilpotent; hence we have the chain

$$U \cap N_{f-1} \xrightarrow{p_1} A_1 \xrightarrow{p_2} \cdots\cdots \xrightarrow{p_r} V \cap N_{f-1}, \qquad (3)$$

in which each prime occurs at most once.

Hence combining the chains (2) and (3), and the chain

$$V \cap N_{f-1} \overset{p_1}{\nearrow} \cdots\cdots \overset{p_r}{\nearrow} V,$$

obtained by intersecting (1) with V (and reversing the order), we obtain a chain from U to V involving p_1 at most f times (since the last step of (2) and the first of (3) combine).

(b) Suppose f is odd.

We have the chain

$$G \overset{p_r}{\searrow} \cdots \overset{p_1}{\searrow} N_1 \overset{p_1}{\searrow} \cdots \overset{p_r}{\searrow} N_2 \overset{p_r}{\searrow} \cdots \overset{p_1}{\searrow} N_{f-2} \overset{p_1}{\searrow} \cdots \overset{p_r}{\searrow} N_{f-1}.$$

p_1 occurs $(f-1)/2$ times in this, so for $U,V \leqslant G$, we can obtain the chain:

$$U \overset{p_r}{\searrow} \cdots \overset{p_r}{\searrow} U \cap N_{f-1} \xrightarrow{p_1} \cdots \xrightarrow{p_r} V \cap N_{f-1} \overset{p_r}{\nearrow} \cdots \overset{p_r}{\nearrow} V,$$

in which p_1 occurs $2(f-1)/2 + 1$ times i.e. f times.

So in both cases, d(G) divides $(p_1 p_2 \ldots p_r)^f$.

<u>Remark</u> In the example given at the beginning of this chapter, i.e. G has order $p^r q^s$, 4-step connected, (and hence no normal Sylow subgroups, Fitting length 2) $d(G,e) = pq$ (so if $d(U,V) = p_1^{m_1} \ldots p_r^{m_r}$, there is not in general a chain of length $(m_1 + \ldots. + m_r)$ between U and V). However, from the above results, $d(G) = p^2 q^2$; alternatively, this can be shown using the fact that a chain from P^*Q^* to G must involve both p and q twice, where $N_G(P) = PQ^*$, and $N_G(Q) = P^*Q$ (see Proposition 4.6).

Neither is it true in general that $d(G) = p_1^{a_1} \ldots p_r^{a_r}$ implies that $W(G) = a_1 + a_2 + \ldots. + a_r$, but it is possible to derive some relationships between d(G) and W(G). To further this end, we introduce another definition:

Definition Suppose p is a prime dividing the order of G. For a subgroup U of G, define

$$K_{p'}(U) = \bigcap (V \lhd U : (|U/V|, p) = 1).$$

The following lemma shows the motivation for this definition:

Lemma 5.3

For G soluble, $K_{p'}(U)$ is the (unique up to conjugacy) minimal subgroup of G to which U can be connected by a chain not involving p.

Proof Suppose

$$V \xrightarrow{q_1} A_1 \xrightarrow{q_2} A_2 \xrightarrow{q_3} \cdots\cdots \xrightarrow{q_s} A_s = U,$$

is a chain from V to U not involving p.

Then $K_{q_1 q_2 \ldots q_s}(U) \lhd V$ (picking as usual a suitable conjugate of V if necessary)

But $K_{q_1 q_2 \ldots q_s}(U) \geqslant K_{p'}(U)$, so $V \geqslant K_{p'}(U)$.

Finally, U can certainly be connected to $K_{p'}(U)$, by a chain not involving p, for $U/K_{p'}(U)$ is a soluble group of order prime to p.

This completes the proof.

Lemma 5.4

If

$$G \rightarrow \cdots \rightarrow A_1 \xrightarrow{p} B_1 \rightarrow \cdots \rightarrow A_2 \xrightarrow{p} B_2 \rightarrow \cdots\cdots$$

$$\rightarrow A_m \xrightarrow{p} B_m \rightarrow \cdots\cdots \rightarrow e,$$

is a chain from G to e, where $A_i \xrightarrow{p} B_i$ is the i^{th} occurrence of p, for i = 1,2, ..., m, and p occurs exactly m times, then

$A_1 \geqslant K_{p'}(G)$, $A_2 \geqslant K_{p'pp'}(G) = K_{p'}(K_p(K_{p'}(G)))$, and so on.

So if the chain

$$(*) \quad G \overset{q_1}{\searrow} \cdots \overset{q_a}{\searrow} K_{p'}(G) \overset{p}{\searrow} K_{pp'}(G) \overset{q_1'}{\searrow} \cdots\cdots \overset{q_k'}{\searrow} K_{p'pp'}(G) \overset{p}{\searrow} \cdots\cdots$$

$$\cdots\cdots \searrow e,$$

involves p exactly n times, then any chain from G to e must involve p at least n times.

Proof The proof is obvious.

Proposition 5.5

If the least number of times p_1 occurs in a chain from G to e is n, then if the last term in the chain (*) above (for $p=p_1$) is a p_1-group, then $d(G) = p_1^{2n-1} m$, where $(m,p_1) = 1$; whilst if the last term is not a p_1-group, $d(G) = p_1^{2n} m'$, where $(m', p_1)=1$.

Proof Suppose (*) for p_1 is

$$G \searrow \cdots \searrow K_{p_1'}(G) = X_1 \overset{p_1}{\searrow} Y_1 \searrow \cdots \searrow X_n \overset{p_1}{\searrow} Y_n \searrow \cdots\cdots \searrow e,$$

where the i^{th} occurrence of P_1 is from X_i to Y_i, for i=1,2,..., n.

Case 1 $Y_n = e$.

Suppose $X_n = P_1'$, say, and look at the $(n-1)^{th}$ occurrence of p_1, i.e. $X_{n-1} \overset{p_1}{\searrow} Y_{n-1}$. Put $Y_{n-1} = P_1'Z_n$, say, where $P_1' \cap Z_n = e$.

$Z_n \triangleleft G$ implies $K_{p_1}(Y_{n-1}) = Z_n$, which gives $P_1' = e$, a contradiction. So $Z_n \ntriangleleft G$, and hence, by the Frattini argument,

$N_G(Z_n) = P_1^*P_2 \cdots P_r$, where $P_1^* \neq P_1$, and $P_1^*P_1' = P_1$.

Connect $N_G(Z_n)$ to G; suppose this can be done by a chain involving p_1 only (2n-2) times, i.e.

$$P_1^*P_2 \cdots P_r \underbrace{\xrightarrow{q_1} \cdots\cdots \xrightarrow{q_s}}_{n-2} A \xrightarrow{p_1} B \underbrace{\longrightarrow \cdots\cdots \longrightarrow}_{n-1} G,$$

where $A \xrightarrow{p_1} B$ is the $(n-1)^{th}$ occurrence of p_1.

Firstly, $A \overset{char}{\rhd} K_{q_s \ldots q_1}(N_G(Z_n)) \overset{char}{\rhd} Z_n$; otherwise, by forming the product of each term in the chain

$$N_G(Z_n) \overset{q_1}{\searrow} \ldots\ldots\ldots \overset{q_s}{\searrow} K_{q_s \ldots q_1}(N_G(Z_n))$$

by P_1', we would obtain a contradiction to Lemma 5.4. Hence $Z_n \lhd B$.

But also by Lemma 5.4, $B \geqslant P_1' Z_n$, and hence $Z_n \lhd Z_n P_1' \lhd G$, which implies $Z_n \lhd G$, a contradiction.

So p_1^{2n-1} divides $d(G)$.

Finally, if $U, V \leqslant G$, then we have chains

$$U \searrow \ldots\ldots \searrow U \cap P_1',$$

$$V \searrow \ldots\ldots \searrow V \cap P_1',$$

each involving p_1 $(n-1)$ times, formed by intersecting U,V with (*). Connecting these via the p_1-step $U \cap P_1' \overset{p_1}{\longrightarrow} V \cap P_1'$, we obtain a chain involving p_1 $(2n-1)$ times.

Hence $d(G) = p_1^{2n-1} m_1$, where $(p_1, m_1) = 1$.

<u>Case 2</u> $Y_n \neq e$.

$Y_n \lhd G$; suppose $X_n = P_1' Y_n$. $K_{p_1'}(X_n) = X_n$, so $P_1' \ntriangleleft G$.

Hence, by the Frattini argument, $N_G(P_1') = P_1 Y_n^*$, say, where $Y_n Y_n^* = P_2 \ldots P_r$.

Connect $N_G(P_1')$ to G, and suppose p_1 only occurs $(2n-1)$ times.

We have

$$N_G(P_1') \longrightarrow \ldots\ldots \longrightarrow A \overset{p_1}{\longrightarrow} B \rightarrow \ldots\ldots \longrightarrow G,$$

where $A \overset{p_1}{\longrightarrow} B$ is the n^{th} occurrence of p_1.

As in Case 1, $A \overset{char}{\rhd} K_{q_s \ldots q_1}(N_G(P_1')) \overset{char}{\rhd} P_1'$, so $P_1' \lhd A$.

Moreover, $B \geqslant X_n = Y_n P_1'$, so $A \geqslant Y_n$. Hence $P_1' \lhd P_1' Y_n$, which gives $Y_n = e$, a contradiction.

So p_1 occurs at least 2n times.

Finally, for $U,V \leqslant G$, we can connect each to e in chains involving p_1 n times (at most); joining these chains gives the required one from U to V.

Hence $d(G) = p_1^{2n}m$, where $(p_1,m) = 1$.

<u>Corollary 1</u>

If G has order $p_1^{n_1}p_2^{n_2}$, and $W(G) = m$, then $d(G) = p_1^{a}p_2^{b}$, where $a=b=m/2$ if m is even, and $a=(m-1)/2$, $b=(m+1)/2$ if m is odd, (or $a=(m+1)/2$, $b=(m-1)/2$).

<u>Proof</u> By Propositions 4.5 and 4.6, if $W(G) = 2n$ then there are two minimal chains of length (n+1) from G to e.

If (n+1) is odd, then the chain (*) of Lemma 5.4 for $p=p_1$ contains p_1 n/2 times, and the last term is a p_2-group. So by the above Proposition, $d(G) = p_1^{n}p_2^{n}$, since the situation is symmetric in p_1 and p_2.

If (n+1) is even, then (*) for p_1 contains p_1 (n+1)/2 times, and ends with a p_1-group. Hence the p_1-factor of d(G) is $p_1^{2(n+1)/2-1} = p_1^{n}$. So $d(G) = p_1^{n}p_2^{n}$, again by symmetry.

If $W(G) = 2n+1$, then the two minimal chains from G to e have lengths (n+1) and (n+2); these minimal chains are the chains (*) for p_1 and p_2. Suppose the shorter chain is (*) for p_1.

If n is odd, p_1 occurs (n+1)/2 times in (*) (for p_1) and the last term is a p_1-group; so the p_1-factor is p_1^{n+1-1}. The chain (*) for p_2 involves p_2 $(n+1)/2$ times, and ends in a p_1-group, so the p_2-factor is $p_2^{\,n+1}$. Hence $d(G) = p_1^{\,n} p_2^{\,n+1}$.

If n is even, p_1 occurs $n/2$ times in (*) for p_1, and the last step is a p_2-step; whilst p_2 occurs $(n+2)/2$ times in (*) for p_2, the last step being a p_2-step. So $d(G) = p_1^{\,n} p_2^{\,n+1}$.

This completes the result.

<u>Corollary 2</u>

If $U \leqslant G$, then $d(U)$ divides $d(G)$ and if U is normal in G, then $d(G/U)$ divides $d(G)$.

<u>Proof</u> If the chain (*) for G for p is

$$G \searrow \ldots\ldots \searrow K_{p'}(G) \overset{p}{\searrow} K_{pp'}(G) \searrow \ldots\ldots \searrow e,$$

then by forming the intersection of this chain with U, we obtain a chain from U to e (of subgroups of U, choosing suitable conjugates in (*) to ensure that each term is a subgroup of the preceding one). By Lemma 5.4, the (*) chain for U for p is "contained" in this; so, by the above Proposition, the p-factor of $d(U)$ divides the p-factor of $d(G)$.

If U is normal in G, by forming the product of each term of (*) with U, and taking the quotient by U, we obtain a chain from G/U to e. This again is "contained" in the chain (*) for G/U and p, so again $d(G/U)$ divides $d(G)$.

<u>Remark</u> If $W(G) = m$ then certainly $W(G/U) \leqslant m$ for any normal subgroup U of G; but for U a subgroup of G, with $W(U) = n$ it seems difficult to say anything useful about the relation between m and n, although it seems likely that $n \leqslant m$. This is because we

have not found a natural way of determining m for an arbitrary finite group, unlike d(G), which follows as above from a consideration of the chains (*), for the primes dividing the order of G. It may well be that two subgroups of G can be chosen in a natural way so that the shortest chain between them has m steps, but this also seems difficult.

We can say, however, that $m \geqslant n$, if G is either nilpotent, has exactly one non-normal Sylow subgroup, or satisfies the conditions of Proposition 4.10. For U also satisfies the same conditions (or stronger conditions).

The difficulty, of course, is that two subgroups of U, whilst being conjugate in G, may no longer be conjugate in U, and so chains of subgroups of G, although consisting of subgroups of U, may no longer be chains when considered as subgroups of U.

<u>Proposition 5.6</u>

If $d(G) = p_1^{a_1} \dots p_r^{a_r}$, then $W(G) \geqslant (a_1 + \dots + a_r)$.

<u>Proof</u> Suppose G is a counter-example of minimal order.

Suppose the normal p-subgroups of G are p_i-subgroups, for $i = 1,2, \dots, t$ $(t \geqslant 1)$.

If X_1 is a minimal normal p_1-subgroup, then if $d(G/X_1) = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$, then by the minimality of G, $W(G/X_1) \geqslant a_1 + \dots + a_r$, so $W(G) \geqslant a_1 + \dots + a_r$. This is a contradiction, so $d(G/X_1) < d(G)$.

The only (*)-chain (see Lemma 5.4) which can be shorter in G/X_1 than in G is the p_1 chain; and this can only be shorter if the last term is contained in X_1. So X_1 is the unique minimal normal p_1-subgroup, and is the last term of the (*)-chain for G and p_1.

Let X_i, i = 1,2, ..., t, be the unique minimal p-subgroups of G.

Suppose the (*) chain for p_1 and G is:

$$G \searrow \dots \searrow K_{p_1'}(G) \overset{p_1}{\searrow} \dots \searrow P_1' Z_1 \overset{p_1}{\searrow} X_1 Z_1 \dots \searrow X_1 \overset{p_1}{\searrow} e.$$

$Z_1 \not\triangleleft G, Z_1 \cap X_1 = e$; $N_G(Z_1) = X_1^* P_2 \dots P_r$, where $X_1^* X_1 = P_1$.

Connect $N_G(Z_1)$ to G; by the proof to Proposition 5.5, p_1 occurs at least a_1 times.

Define Z_i and X_i^* in a similar way for i = 1, ..., t.

Form $\bigcap_1^t N_G(Z_i) = X_1^* X_2^* \dots X_t^* P_{t+1} \dots P_r = Z$ say; any chain from Z to G involves p_i at least a_i times, for i = 1,2, ..., t, since by forming the product of each term with $X_1 \dots X_{i-1} . X_{i+1} \dots X_t$ ($\triangleleft$ G), we obtain a chain from $N_G(Z_i)$ to G.

Suppose p_r occurs $(a_r - 1)$ times (a_r is even, otherwise there would be a normal p_r-subgroup, by Proposition 5.5); suppose $a_r = 2b$, and the chain is

$$Z = X_1^* \dots X_t^* P_{t+1} \dots P_r \to \dots \to A \overset{p_r}{\to} B \to \dots \to G,$$

where $A \overset{p_r}{\to} B$ is the b^{th} occurrence of p_r.

Suppose the (*)-chain for p_r from G to e is

$$G \searrow \dots \searrow P_r' Z_r \overset{p_r}{\searrow} Z_r \searrow \dots \searrow e, \qquad (1)$$

where $Z_r \cap P_r' = e$, and p_r occurs b times.

Suppose the (*) chain for p_r from Z to e is

$$Z \searrow \dots \searrow P_r' Y_r \overset{p_r}{\searrow} Y_r \searrow \dots \searrow e,$$

where $Y_r \cap P_r' = e$, and p_r occurs b times. The chain must be of this form, otherwise, by forming the product of each term with $X_1 \dots X_t$, we would get a chain from G to $X_1 \dots X_t$ contradicting (1).

Hence $P_r'Z_r \lhd B$, and $P_r'Y_r \lhd A$.

We now show that $Y_r = e$; Y_r is a characteristic subgroup of A, and hence of B. Also $Y_r \leqslant Z_r \leqslant B$, so Y_r is characteristic in Z_r, which is normal in G. Hence $Y_r \lhd G$. A normal subgroup of G must contain a minimal normal p-subgroup; but $Z \not\geqslant X_i$, $i = 1, \ldots, t$: hence $Y_r = e$.

But now $P_r' \lhd A$, and $Z_r \leqslant A$, so $P_r' \lhd P_r'Z_r$, which is not so.

Hence p_r must occur at least a_r times, and similarly for $i = t+1, \ldots, r-1$.

So p_i must occur at least a_i times for $i=1, \ldots, r$, so $W(G) \geqslant a_1 + \ldots\ldots + a_r$.

Appendix

We give here further details of examples mentioned in Chapter 4, and also an example to show that $\Omega(G) \cong \Omega(G')$ does not imply that $G \cong G'$.

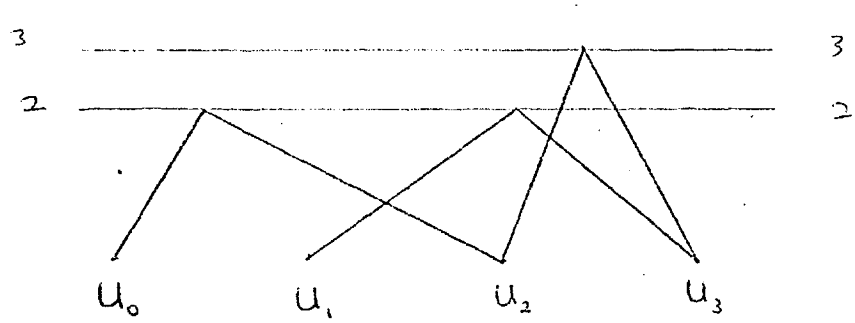
(1) The symmetric group on 3 elements

The conjugacy classes of subgroups of S_3 are $U_0 = S_3$, U_1 = a Sylow 2-subgroup, U_2 = the Sylow 3-subgroup, and $U_3 = e$. Put $T_i = {}^{S_3}/_{U_i}$.

Multiplication Table

	T_0	T_1	T_2	T_3
T_0	T_0	T_1	T_2	T_3
T_1	T_1	$T_1 + T_3$	T_3	$3T_3$
T_2	T_2	T_3	$2T_2$	$2T_3$
T_3	T_3	$3T_3$	$2T_3$	$6T_3$

Graph



Quasi-idempotents If we put $x_i = x^G_{U_i}$, $\lambda_i = \lambda^G_{U_i}$, then:

$$x_0 = 2 - T_2 - 2T_1 + T_3 \; ; \quad \lambda_0 = 2$$

$$x_1 = 2T_1 - T_3 \; ; \quad \lambda_1 = 2$$

$$x_2 = 3T_2 - T_3 \; ; \quad \lambda_2 = 6$$

$$x_3 = T_3 \; ; \quad \lambda_3 = 6$$

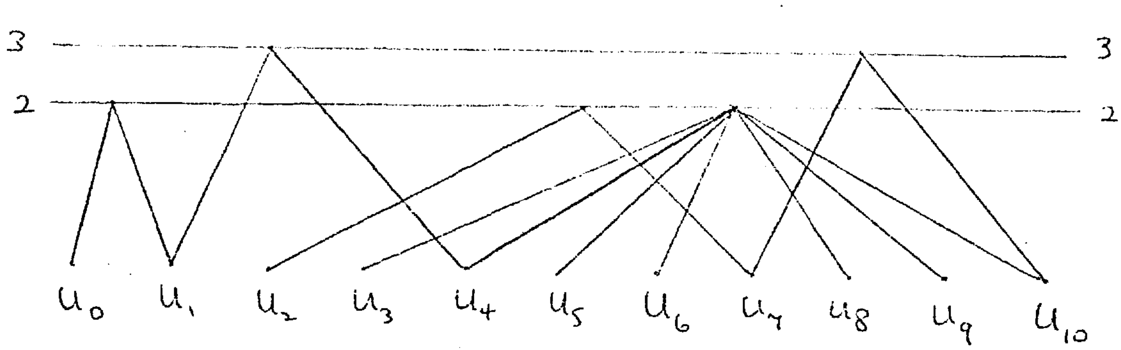
<u>Automorphisms</u> The permutation of $(x_i : i = 0,1,2,3)$ defined by multiplying the transpositions (x_0x_1), (x_2x_3) gives the automorphism $T_3 \longrightarrow 3T_2 - T_3$, $T_2 \longrightarrow T_2$, $T_1 \longrightarrow 1 - T_1 + T_2$, and T_0 fixed.

It is easy to see that this is the only possible non-identity automorphism of $\Omega(G)$ (for the above is the only possible image for T_3, and T_3 fixed implies x_2 and hence T_2 fixed, and it follows easily that T_1 must be fixed).

(2) <u>The symmetric group on 4 elements</u>

There are 11 conjugacy classes of subgroups of S_4, as follows:

U_0 , order 24 : $U_0 = S_4$
U_1 , order 12 : $U_1 = A_4 \triangleleft S_4$
U_2 , order 6 : $\langle(12),(123)\rangle$ self-normalising
U_3 , order 8 : Sylow 2-subgroup, self-normalising
U_4 , order 4 : $\langle(12)(34),(13)(24)\rangle \triangleleft S_4$
U_5 , order 4 : $\langle(12),(34)\rangle \precsim U_3$
U_6 , order 4 : $\langle(1234)\rangle \precsim U_3$
U_7 , order 3 : $\langle(123)\rangle \precsim U_2$
U_8 , order 2 : $\langle(12)\rangle \precsim U_5$
U_9 , order 2 : $\langle(12)(34)\rangle \precsim U_3$
U_{10}, order 1 : $U_{10} = e$



Multiplication Table

T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}
T_1	$2T_1$	T_7	T_4	$2T_4$	T_9	T_9	$2T_7$	T_{10}	$2T_9$	$2T_{10}$
T_2		T_2+T_8	T_8	T_{10}	$2T_8$	T_{10}	T_7+T_{10}	$2T_8+T_{10}$	$2T_{10}$	$4T_{10}$
T_3			T_3+T_4	$3T_4$	T_5+T_9	T_6+T_9	T_{10}	T_8+T_{10}	$3T_9$	$3T_{10}$
T_4				$6T_4$	$3T_9$	$3T_9$	$2T_{10}$	$3T_{10}$	$6T_9$	$6T_{10}$
T_5					$2T_5+T_{10}$	T_9+T_{10}	$2T_{10}$	$2T_8+2T_{10}$	$2T_9+2T_{10}$	$6T_{10}$
T_6						$2T_6+T_{10}$	$2T_6$	$3T_{10}$	$2T_9+2T_{10}$	$6T_{10}$
T_7							$2T_7+T_{10}$	$4T_{10}$	$4T_{10}$	$8T_{10}$
T_8								$2T_8+T_{10}$	$6T_{10}$	$12T_{10}$
T_9									$4T_9+4T_{10}$	$12T_{10}$
T_{10}										$24T_{10}$

Quasi-idempotents

$x_0 = 2 - T_1 - 2T_2 - 2T_3 + T_4 + T_7 + 2T_8 - T_{10}$; $\lambda_0 = 2$

$x_1 = 6T_1 - 2T_4 - 6T_7 + T_{10}$; $\lambda_1 = 12$

$x_2 = 2T_2 - T_7 - 2T_8 + T_{10}$; $\lambda_2 = 2$

$x_3 = 2T_3 - (T_4 + T_5 + T_6) + T_9$; $\lambda_3 = 2$

$x_4 = 2T_4 - 3T_9 + T_{10}$; $\lambda_4 = 12$

$x_5 = 2T_5 - 2T_8 - T_9 + T_{10}$; $\lambda_5 = 4$

$x_6 = 2T_6 - T_9$; $\lambda_6 = 4$

$x_7 = 3T_7 - T_{10}$; $\lambda_7 = 6$

$x_8 = 2T_8 - T_{10}$; $\lambda_8 = 4$

$x_9 = 2T_9 - T_{10}$; $\lambda_9 = 8$

$x_{10} = T_{10}$; $\lambda_{10} = 24$

(3). We define $G(\mu)$ as follows:

$G(\mu) = (a,b,c : a^p=b^p=c^q=e,\ ab=ba,\ cac^{-1}=a^r,\ cbc^{-1}=b^{r^\mu})$,

where p, q are prime with $p - 1 = nq$, $r \not\equiv 1$, $r^q \equiv 1 \mod p$, and $\mu \not\equiv 0, 1 \mod q$.

The conjugacy classes of subgroups of G are as follows:

$U_0 = G$, $U_1 = \langle a,b\rangle \lhd G$, $U_2 = \langle a,c\rangle$, $U_3 = \langle b,c\rangle$,
$U_4 = \langle a\rangle \lhd G$, $U_5 = \langle b\rangle \lhd G$, $U_{6,j} = \langle a b^{\alpha_j}\rangle$, for $j = 1,\ldots,n$, and α_j is chosen such that ab^{α_j} are the generators of a set of representatives of the n conjugacy classes of subgroups of $\langle a,b\rangle$ different from $\langle a\rangle$ and $\langle b\rangle$, $U_7 = \langle c\rangle$, $U_8 = e$.

Multiplication Table

T_0	T_1	T_2	T_3	T_4	T_5	$T_{6,j}$	T_7	T_8
T_1	qT_1	T_4	T_5	qT_4	qT_5	$qT_{6,j}$	T_8	qT_8
T_2		T_2+nT_4	T_7	pT_4	T_8	T_8	T_7+nT_8	pT_8
T_3			T_3+nT_5	T_8	pT_5	T_8	T_7+nT_8	pT_8
T_4				pqT_4	qT_8	qT_8	pT_8	pqT_8
T_5					pqT_5	qT_8	pT_8	pqT_8
T_6						$pT_{6,j}+(q-1)T_8$	pT_8	pqT_8
T_7							$T_7+n(p+1)T_8$	p^2T_8
T_8								p^2qT_8

and $T_{6,j} \cdot T_{6,i} = qT_8$ for $i \neq j$.

Clearly $\Omega(G(\mu)) \cong \Omega(G(\mu'))$; but $G(\mu) \cong G(\mu')$ if and only if $\mu\mu' = 1 \mod q$. This example was given by Rottländer in the paper "Nachweis der Existenz nicht-isomorphic Gruppen von gleicher Situation der Untergruppen" Math. Z. 28 (1928); see Suzuki, "The Structure of a Group and its Subgroup Lattice", p.57.

References

1. A. Dress, A characterisation of solvable groups, Math. Z. 110 (1969), 213-217.

2. P. Hall, The Eulerian functions of a group, Quarterly Journal of Maths. 7, 1936.

3. H. Krämer, Über die Automorphismengruppe des Burnsideringes endlicher abelscher Gruppen, J. Alg. 30, No. 1-3, 1974, 279-293.