The Theory of p-Groups

David A. Craven

Hilary Term, 2008

Contents

Chapter 1

Motivation

1.1 Soluble Groups

A *nilpotent* group G is a finite group that is the direct product of its Sylow p-subgroups.

Theorem 1.1 (Fitting's Theorem) Let G be a finite group, and let H and K be two nilpotent normal subgroups of G. Then HK is nilpotent.

Hence in any finite group there is a unique maximal normal nilpotent subgroup, and every nilpotent normal subgroup lies inside this; it is called the *Fitting subgroup*, and denoted by $\mathrm{F}(G)$.

Theorem 1.2 Let G be a finite soluble group. Then

$$\mathrm{C}_G(\mathrm{F}(G)) \leqslant \mathrm{F}(G).$$

Note firstly that if G is not a soluble group, we may well have $\mathrm{F}(G) = 1$, and even if $\mathrm{F}(G) \neq 1$, then we need not have $\mathrm{C}_G(\mathrm{F}(G)) \leqslant \mathrm{F}(G)$.

Recall that for any group G and subgroup H, we have that $\mathrm{N}_G(H)/\mathrm{C}_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$; since $\mathrm{C}_G(\mathrm{F}(G))$ is a normal nilpotent subgroup of the finite soluble group G, this implies that any soluble group has a normal nilpotent subgroup K such that G/K is a group of automorphisms of K.

Proposition 1.3 Let G be a finite nilpotent group, and let $G = P_1 \times P_2 \times \cdots \times P_n$, where the P_i are the Sylow p-subgroups of G. Then

$$\mathrm{Aut}(G) = \mathrm{Aut}(P_1) \times \mathrm{Aut}(P_2) \times \cdots \times \mathrm{Aut}(P_n).$$

This focuses attention on the structure of p-groups and the automorphisms of p-groups.

1.2 Lie Algebras

Definition 1.4 A *Lie ring* is a set R with two binary operations—addition and the Lie bracket—such that

(i) $(R, +)$ is an abelian group;

(ii) the bracket operation distributes over addition;

(iii) $[x, x] = 0$ for all $x \in R$; and

(iv) $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ for all $x, y, z \in R$.

If F is a field, and R is an F-vector space, with $a[x, y] = [ax, y]$ then R is a *Lie algebra*.

To every finite p-group one can associate a Lie ring $L(G)$, and if G/G' is elementary abelian then $L(G)$ is actually a Lie algebra over the finite field $\mathrm{GF}(p)$.

Proposition 1.5 Let ϕ be an automorphism of the finite p-group G. Then ϕ induces an automorphism on $L(G)$, and if ϕ has order prime to p, then the induced automorphism has the same order.

There is a correspondence between a subset of Lie algebras over $\mathrm{GF}(p)$, called p-restricted Lie algebras, and p-groups. Thus studying one is equivalent to studying the other.

1.3 The Number of Groups

Lemma 1.6 Let $g(n)$ denote the number of groups of order n.

(i) $g(p) = 1$ for p a prime.

(ii) if $p < q$, then $g(pq) = 1$ if $q \not\equiv 1 \mod p$, and $g(pq) = 2$ otherwise.

(iii) $g(p^2) = 2$.

(iv) $g(p^3) = 5$.

From this we can see that the number of groups of order n depends more on the prime structure of n then on its size. We can make this explicit with the following table of n against $g(n)$.

n	$g(n)$	n	$g(n)$	n	$g(n)$	n	$g(n)$
1	1	11	1	21	2	31	1
2	1	12	5	22	2	32	51
3	1	13	1	23	1	33	1
4	2	14	2	24	15	34	2
5	1	15	1	25	2	35	1
6	2	16	14	26	2	36	14
7	1	17	1	27	5	37	1
8	5	18	5	28	4	38	2
9	2	19	1	29	1	39	2
10	2	20	5	30	4	40	14

The result $g(32) = 51$ should make one believe that if one picks a group G of order at most n at random, then as n tends to infinity, the probability that G is a p-group tends to 1, and even more that G is a non-abelian 2-group with probability 1. This looks true, but there is still no proof of it yet.

Hence we should be interested in p-groups if only for the fact that almost all groups are p-groups!

1.4 Sylow Structure of Groups

Theorem 1.7 (Sylow's Theorem) Let G be a finite group and let p^n be the p-part of $|G|$. Then G possesses a single G-conjugacy class of subgroups of order p^n of length congruent to 1 modulo p, and every p-subgroup is contained in one of them.

This implies that there are always p_i-subgroups P_i of largest possible order for the various primes p_i. Let π be a set of primes, and define a π-subgroup in the obvious way; that is, a π-subgroup is a subgroup whose order is divisible only by primes present in π. If G is a finite group and n is the π-part of $|G|$, then a subgroup of order n is called a *Hall π-subgroup*.

Theorem 1.8 (Philip Hall's Theorem) Let G be a finite group. Then G is soluble if and only if, for all sets of primes π, the group G contains a Hall π-subgroup. In this case, all Hall π-subgroups of are conjugate, and any π-subgroup is contained within one of them.

Thus Sylow's Theorem is special, in the sense that in an arbitrary group, not only are we not guaranteed Hall π-subgroups, if the group is insoluble there is guaranteed to be sets of primes for which they don't exist. What this means is that the only Hall subgroups that we are really guaranteed in a finite simple group, for example, are the Sylow p-subgroups.

The structure of the Sylow p-subgroups of a finite group place considerable constraints on the structure of the finite group itself. For example, the following theorem characterizes all groups with abelian Sylow 2-subgroup.

Theorem 1.9 (Walter) Let G be a group with abelian Sylow 2-subgroups. Then there is a normal subgroup K and a normal subgroup H with $K \leqslant H$, such that K has odd order, H has odd index, and H/K is a direct product of an abelian 2-group and simple groups with abelian Sylow 2-subgroups, namely:

(i) the projective special linear group $\mathrm{PSL}_2(q)$, $q \equiv 3, 5 \mod 8$;

(ii) the projective special linear group $\mathrm{PSL}_2(2^n)$ for $n \geqslant 3$;

(iii) the twisted Dickson group (or Ree group) $R(3^{2n+1})$ where $n \geqslant 1$; and

(iv) the first Janko group J_1.

In the final chapter we will look at how the Sylow p-subgroups of a finite group can be embedded in it.

Chapter 2

Introduction to the Structure of p-Groups

Definition 2.1 A *central series* is a chain of normal subgroups

$$1 = H_0 \leqslant H_i \leqslant \cdots \leqslant H_r = G$$

such that $H_i/H_{i-1} \leqslant \mathrm{Z}\left(G/H_{i-1}\right)$ for all $1 \leqslant i \leqslant r$.

It can be shown that a finite group is nilpotent if and only if it possesses a central series. In fact, this is traditionally the definition of a (possibly infinite) nilpotent group.

Definition 2.2 Let G be a group. Define

(i) $G^{(1)} = G'$, the derived subgroup, and $G^{(r)} = [G^{(r-1)}, G^{(r-1)}]$;

(ii) $\mathrm{Z}_1\left(G\right) = \mathrm{Z}\left(G\right)$, and $\mathrm{Z}_r\left(G\right)$ by $\mathrm{Z}_r\left(G\right)/\mathrm{Z}_{r-1}\left(G\right) = \mathrm{Z}\left(G/\mathrm{Z}_{r-1}\left(G\right)\right)$, the *upper central series*; and

(iii) $\gamma_1(G) = G$, $\gamma_2(G) = G'$, and $\gamma_r(G) = [\gamma_{r-1}(G), G]$ the *lower central series.*

Lemma 2.3 Suppose that

$$1 = H_0 \leqslant H_i \leqslant \cdots \leqslant H_r = G$$

is a central series for G. Then $\mathrm{Z}_i\left(G\right) \geqslant H_i$ and $\gamma_i(G) \leqslant H_{r-i+1}$ for all i.

This lemma implies that if c is the smallest integer such that $\mathrm{Z}_c\left(G\right) = G$ then $\gamma_{c+1}(G) = 1$ and $\gamma_c(G) \neq 1$, and any central series has length at least c. This integer c is called the (nilpotence) *class* of a nilpotent group.

Proposition 2.4 Let G be a group of order p^n. Then G is nilpotent, and if c denotes its class, then $0 \leqslant c \leqslant n-1$, $c = 0$ if and only if G is trivial, and $c = 1$ if and only if G is abelian.

Thus there is an easy characterization of p-groups of class 1. However, 'most' p-groups are of class 2, in the sense that as $n \to \infty$, the number of p-groups of class 2 gets unmanageably large. Notice, however, that there is a largest possible class for each order.

Definition 2.5 Let G be a finite p-group, of order p^n. If c denotes the class of G, then the *coclass* of G is the quantity $n - c$.

Having failed completely to classify p-groups by class, we can try to classify them by coclass. In particular, we ask the question 'can we classify the groups of coclass 1?'

Definition 2.6 Let G be a finite abelian group. Then G is called *elementary abelian* if every non-identity element has order p.

The elementary abelian groups are actually the groups $C_p \times C_p \times \cdots \times C_p$, where C_n is the cyclic group of order n. If the elementary abelian group P has order p^n, then the *rank* of P is n. The *p-rank* of a finite group is the maximum of the ranks of all elementary abelian p-subgroups.

Having failed completely to describe the p-groups by class, how about trying to classify them by rank?

Lemma 2.7 Let G be a non-abelian group of order p^3. Then $\mathrm{Z}(G)$ has order p, and $G/\mathrm{Z}(G)$ is elementary abelian.

We define an *extraspecial group* to be a p-group for which $G/\mathrm{Z}(G)$ is elementary abelian, and $\mathrm{Z}(G)$ has order p. Extraspecial groups appear frequently in representation theory; can we classify them?

2.1 Commutators

We start with the very basic results in p-group theory.

Definition 2.8 Let x and y be elements of a group G. Then the *commutator* $[x, y]$ is given by

$$[x, y] = x^{-1}y^{-1}xy.$$

The *commutator subgroup* or *derived subgroup* is the subgroup

$$G' = [G, G] = \langle\, [x, y] \,:\, x, y \in G \rangle.$$

If H and K are subgroups of G, then $[H,K] = \langle\, [h,k] \,:\, h \in H,\, k \in K \rangle$.

Lemma 2.9 Let G be a group. If ϕ is any homomorphism from G, then for all $x, y \in G$, $[x,y]\phi = [x\phi, y\phi]$. Consequently, G' is a fully invariant subgroup of G.

Proof: Let ϕ be a homomorphism from the group G. Then for any two elements x and y of G, we have

$$([x,y])\phi = \left(x^{-1}y^{-1}xy\right)\phi = (x\phi)^{-1}(y\phi)^{-1}x\phi y\phi = [x\phi, y\phi],$$

and so if $\phi : G \to G$ is an endomorphism, then $G'\phi \leqslant G'$, as required. □

Lemma 2.10 Let G be a group, and H any normal subgroup of G.

(i) The quotient group G/G' is abelian (the quotient group G/G' is called the *abelianization* of G);

(ii) If G/H is also abelian then $G' \leqslant H$.

Proof: Suppose that x and y are two elements of G. Then $[x,y] = g$ for some element g of G'. But then from the definition of $[x,y]$, we have that $x^{-1}y^{-1}xy = g$, whence $xy = yxg$, and so since $1 \in G'$, xy and yx are in the same coset of G'. Therefore

$$(xG')(yG') = (xy)G' = (yx)G' = (yG')(xG'),$$

proving assertion (i).

If G/H is abelian, then for any two elements x and y of G, we have that xy and yx are in the same coset of H, whence $xy = yxh$ for some element h of H. In a similar fashion to the proof of (i), we have $x^{-1}y^{-1}xy = h \in H$, and so since all generators of G' lie inside H, we have $G' \leqslant H$, proving (ii). □

We will give a notation to extended commutators – by this we mean an object like $[[x,y],z]$ – which we denote by $[x,y,z]$. We extend this notation by induction, so that

$$[x_1, x_2, x_3, \ldots, x_{n-1}, x_n] = \left[[x_1, x_2, \ldots, x_{n-1}], x_n\right].$$

Lemma 2.11 Let G be a group, and x, y, z be elements of G.

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

(ii) $[x, yz] = [x,z][x,y]^z = [x,z][x,y][x,y,z]$.

(iii) $[x,y] = [y,x]^{-1}$.

(iv) (Hall–Witt's Identity) $[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1$.

Proof: To prove (i), notice that

$$[xy, z] = y^{-1}x^{-1}z^{-1}x(zyy^{-1}z^{-1})yz = y^{-1}(x^{-1}z^{-1}xz)yy^{-1}z^{-1}yz = [x, z]^y[y, z],$$

and

$$[x, z][x, z, y] = x^{-1}z^{-1}xz[x^{-1}z^{-1}xz, y] = (x^{-1}z^{-1}xzz^{-1}x^{-1}zx)y^{-1}x^{-1}z^{-1}xzy = y^{-1}x^{-1}z^{-1}xzy = [x, z]^y,$$

giving $[x, z][x, z, y][y, z] = [x, z]^y[y, z]$. The proof of (ii) is similar.

The proof of (iii) is obvious: $[y, x]^{-1} = (y^{-1}x^{-1}yx)^{-1} = x^{-1}y^{-1}xy = [x, y]$.

To prove Witt's Identity is harder: let $u = xzx^{-1}yx$, $v = yxy^{-1}zy$ and $w = zyz^{-1}xz$. Then

$$[x, y^{-1}, z]^y = [x^{-1}yxy^{-1}, z]^y = y^{-1}(yx^{-1}y^{-1}xz^{-1}x^{-1}yxy^{-1}z)y = (x^{-1}y^{-1}xz^{-1}x^{-1})(yxy^{-1}zy) = u^{-1}v,$$

and similarly $[y, z^{-1}, x]^z = v^{-1}w$ and $[z, x^{-1}, y]^x = w^{-1}u$, giving

$$[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = u^{-1}vv^{-1}ww^{-1}u = 1,$$

as required. □

The Hall–Witt Identity has the following consequence, which is often of use in group theory.

Theorem 2.12 (Three Subgroup Lemma) Let X, Y and Z be three subgroups of a group G, and let N be a normal subgroup of G. If $[X, Y, Z]$ and $[Y, Z, X]$ are both contained within N, then so is $[Z, X, Y]$.

Proof: Let $x \in X$, $y \in Y$ and $z \in Z$. Since $[X, Y, Z]$ and $[Y, Z, X]$ are both contained in N, then $[x, y^{-1}, z]^y$ and $[y, z^{-1}, x]^z$ are elements of N (since N is normal), and so

$$\left([x, y^{-1}, z]^y [v, z^{-1}, x]^z\right)^{-1} = [z, x^{-1}, y]^x \in N,$$

by Witt's Identity. Since N is normal, we can conjugate by x^{-1} to get $[z, x^{-1}, y] \in N$. But by writing $x' = x^{-1}$, we have $[z, x', y] \in N$ for all $z \in Z$, $x' \in X$ and $y \in Y$. Since $[Z, X, Y]$ is generated by such elements, $[Z, X, Y] \leqslant N$. □

Proposition 2.13 Let H and K be subgroups of a group G.

(i) $[H, K] \leqslant K$ if and only if $H \leqslant \mathrm{N}_G(K)$.

(ii) If H and K normalize one another then $[H, K] \trianglelefteqslant HK$, and $[H, K] \leqslant H \cap K$.

(iii) If K is a normal subgroup of G and $H \geqslant K$ then $[H, G] \leqslant K$ if and only if $H/K \leqslant \mathrm{Z}(G/K)$.

Proof: Suppose that $H \leqslant \mathrm{N}_G(K)$. Then $h^{-1}k^{-1}h = k' \in K$ and so $h^{-1}k^{-1}hk = k'k \in K$. Thus $[H, K] \leqslant K$. Conversely, suppose that $[H, K] \leqslant K$, but that $H \not\leqslant \mathrm{N}_G(K)$. Then there exist h and k such that $h^{-1}k^{-1}h \notin K$. Then certainly $h^{-1}k^{-1}hk \notin K$, contradicting $[H, K] \leqslant K$.

Now suppose that H and K are mutually normalizing subgroups. Then for $h \in H$, $k \in K$ and $[h', k'] \in [H, K]$, we have that $h \mapsto h^g$ is an endomorphism of G and so by Lemma 2.9,

$$[h', k']^{hk} = [(h')^{hk}, (k')^{hk}] \in [H, K],$$

and thus $[H, K] \trianglelefteqslant HK$. By part (i), $[H, K] \leqslant H$ and $[H, K] \leqslant K$, yielding the second assertion of (ii).

Finally, suppose that $[H, G] \leqslant K$. Then for all $g \in G$ and $h \in H$, $h^{-1}g^{-1}hg \in K$; i.e., $hgK = ghK$, or that $h \in \mathrm{Z}(G/K)$. Conversely, if $hK \in \mathrm{Z}(G/K)$, then for all $g \in G$, $ghK = hgK$, and so $[h, g] \in K$. This means that $[h, G] \subseteq K$, and thus if this is true for all $h \in H$ then $[H, G] \leqslant K$ as required. □

Corollary 2.14 Suppose that H, K and L are normal subgroups of G. Then

$$[HK, L] = [H, L][K, L], \qquad [L, HK] = [L, H][L, K].$$

Theorem 2.15 (Fitting's Theorem) Suppose that G is a group, and H and K are nilpotent normal subgroups, of classes c and d respectively. Then HK is a nilpotent subgroup of G, of class at most $c + d$.

Proof: Consider the commutator

$$X = [HK, HK, \ldots, HK],$$

where there are $c + d + 1$ terms. By Corollary 2.14, this can be written as

$$X = \prod_{M_i \in \{H,K\}} [M_1, M_2, \ldots, M_{c+d+1}].$$

Let $A = [M_1, M_2, \ldots, M_{c+d+1}]$ be one of these multiplicands. Notice that if a of the M_i are equal to H, then $A \leqslant \gamma_{a+1}(H)$. Since there are $c + d + 1$ of the M_i, either $c + 1$ of them are H or $d + 1$ of them are K. Either way, since $\gamma_{c+1}(H) = \gamma_{d+1}(K) = 1$, we have that $A = 1$, and so $X = 1$, proving that $\gamma_{c+d+1}(HK) = 1$, as required. □

2.2 The Frattini Subgroup

Definition 2.16 Let G be a finite group. The *Frattini subgroup* is the intersection of all maximal subgroups of G. It is denoted by $\Phi(G)$.

This subgroup has the curious property that it contains all of the elements of G that do not generate G, in a sense that will be made precise now.

Definition 2.17 Let G be a group, and $x \in G$. Then x is said to be a *non-generator* if whenever G is generated by x and a set X, then $G = \langle X \rangle$.

What this says is that you can remove all non-generators from a generating set and still generate the group. We now give the strange-looking result.

Proposition 2.18 Let G be a group. Then $\Phi(G)$ is the set of all non-generators of G. Consequently, if $G = H\,\Phi(G)$ for some H, then $H = G$.

Proof: Suppose that x is a non-generator of G, and let M be a maximal subgroup of G. Then $\langle M, x \rangle \geqslant M$, and so, since M is a maximal subgroup of G, $\langle M, x \rangle = M$ or $\langle M, x \rangle = G$. If $\langle M, x \rangle = G$, then, since x is a non-generator, $\langle M \rangle = G$, a clear contradiction. Thus $\langle M, x \rangle = M$; i.e., $x \in M$. This is true for all maximal subgroups, and so $x \in \Phi(G)$.

Conversely, suppose that x is an element of $\Phi(G)$. Let G be generated by some set X, together with x, so $G = \langle X, x \rangle$. Denote by N the group $\langle X \rangle$. If $N \neq G$, it is contained in a maximal subgroup, say M. But $x \in M$, since x is an element of $\Phi(G) \leqslant M$, and so $\langle X, x \rangle \leqslant M < G$, a contradiction. Thus $\langle X \rangle = G$ for all sets X for which $\langle X, x \rangle = G$; i.e., x is a non-generator, as required.

Finally, notice that $G = H\,\Phi(G) = \langle H, \Phi(G) \rangle$, so $G = \langle H \rangle = H$, as needed. □

There is an interplay between the Fitting and Frattini subgroups, which we will examine briefly now. The following result has several interesting corollaries.

Theorem 2.19 Let G be a finite group, and suppose that N is a normal subgroup of G containing $\Phi(G)$. If $N/\,\Phi(G)$ is nilpotent, then N is nilpotent.

Proof: A finite group is nilpotent if and only if its Sylow p-subgroups are normal. We will show that the Sylow p-subgroups of N are normal, thus proving that N is nilpotent. Let P be a Sylow p-subgroup of N. Then $P\,\Phi(G)/\,\Phi(G)$ is a Sylow p-subgroup of $G/\,\Phi(G)$, since if $|P| = p^d$ and $|\,\Phi(G)| = p^e a$, where $p \nmid a$, then

$$\left| \frac{P\,\Phi(G)}{\Phi(G)} \right| = p^{d-e},$$

which is the power of p dividing $N/\Phi(G)$. Now $N/\Phi(G)$ is nilpotent, so $P\Phi(G)/\Phi(G)$, being a Sylow p-subgroup of $N/\Phi(G)$, is normal. If a Sylow p-subgroup of G is normal, it is also characteristic; thus $P\Phi(G)/\Phi(G)\,\mathrm{char}\,N/\Phi(G)$, and so

$$P\Phi(G)\,\mathrm{char}\,N \trianglelefteq G,$$

showing that $P\Phi(G) \trianglelefteq G$.

Now we can use the Frattini Argument: P is a Sylow p-subgroup of N, so is certainly a Sylow p-subgroup of $P\Phi(G)$, and therefore

$$G = \mathrm{N}_G(P)P\Phi(G).$$

Now $P \leqslant \mathrm{N}_G(P)$, so $\mathrm{N}_G(P)P = \mathrm{N}_G(P)$. Thus $G = \mathrm{N}_G(P)\Phi(G)$. Now Proposition 2.18 proves that $G = \mathrm{N}_G(P)$, so $P \trianglelefteq G$, which clearly implies that $P \trianglelefteq N$, as required. □

This theorem gives us several important corollaries, so in this sense it is very useful. The first is a result of Frattini.

Corollary 2.20 The Frattini subgroup of a finite group is nilpotent.

Proof: Take $N = \Phi(G)$ in Theorem 2.19. □

Corollary 2.21 Let G be a finite group. Then $\Phi(G) \leqslant \mathrm{F}(G)$.

Proof: $\Phi(G)$ is a normal nilpotent subgroup of G. □

Corollary 2.22 If G is a finite group and $G/\Phi(G)$ is nilpotent, then G is nilpotent.

Proof: Take $N = G$ in Theorem 2.19. □

Corollary 2.23 If G is a finite group, then $\mathrm{F}(G/\Phi(G)) = \mathrm{F}(G)/\Phi(G)$.

Proof: Any normal nilpotent subgroup $N/\Phi(G)$ of $G/\Phi(G)$ lifts to a nilpotent subgroup N of G, and so $N \leqslant \mathrm{F}(G)$, showing $\mathrm{F}(G/\Phi(G)) \leqslant \mathrm{F}(G)/\Phi(G)$. Certainly $\mathrm{F}(G)/\Phi(G)$ is nilpotent, so $\mathrm{F}(G)/\Phi(G) \leqslant \mathrm{F}(G/\Phi(G))$, and we have the result. □

So Theorem 2.19 is indeed very useful.

Proposition 2.24 Let G be a finite p-group. Then $G/\Phi(G)$ is elementary abelian, and if H is another normal subgroup of G such that G/H is elementary abelian, then $\Phi(G) \leqslant H$.

Proof: Firstly notice that every maximal subgroup of a p-group is normal, and of index p. This means that if M is a maximal subgroup of G, then G/M is cyclic of order p. Hence $G' \leqslant M$ for all maximal subgroups M; consequently $G' \leqslant \Phi(G)$, and so $G/\Phi(G)$ is abelian. Also, since G/M has order p (for M a maximal subgroup of G), we know that $(Mx)^p = M$ for all $x \in G$; i.e., $x^p \in M$ for all $x \in G$ and all maximal subgroups M. Thus $x^p \in \Phi(G)$, and so if $\Phi(G)x \in G/\Phi(G)$, then $\Phi(G)x$ has order p, proving that $G/\Phi(G)$ is elementary abelian.

Now suppose that G/H is elementary abelian of order p^n. Then G/H is generated by n cosets Hx_i of G/H, each of order p. We know then that

$$G/H \cong \langle Hx_1 \rangle \times \cdots \times \langle Hx_n \rangle.$$

Now, this group has n maximal subgroups, H_i/H, each generated by $\{Hx_j : j \neq i\}$. Since this is a direct product, the intersection satisfies

$$\bigcap_{1 \leqslant j \leqslant n} H_j/H = 1.$$

This means that the intersection of all H_j is H (where H_j is the corresponding subgroup in G to H_j/H, the preimage of H_j/H). But the H_j are maximal subgroups of G/H, and hence of G. This clearly implies that their intersection contains $\Phi(G)$: hence

$$H = \bigcap_{1 \leqslant j \leqslant n} H_j \geqslant \Phi(G),$$

as we wanted. □

This has the following consequence.

Proposition 2.25 Let G^p denote the group generated by the set $\{g^p : g \in G\}$; i.e., the smallest group containing all elements of order p. Then $\Phi(G) = G'G^p$.

Proof: Since $\Phi(G)$ contains all x^p, as we saw in the proof of Proposition 2.24, $G^p \leqslant \Phi(G)$. Also, $G' \leqslant \Phi(G)$ since $G/\Phi(G)$ is abelian: thus $G'G^p \leqslant \Phi(G)$.

To prove the converse, notice that $G/G'G^p$ is elementary abelian: it is abelian certainly, since $G' \leqslant G'G^p$. Also, $x^p \in G^p \leqslant G'G^p$ for all $x \in G$, and so every element of $G/G'G^p$ has order either 1 or p. Thus $G/G'G^p$ is elementary abelian, and so $G'G^p \leqslant \Phi(G)$ by Proposition 2.24. □

The subgroup G^p is important enough to be given a special notation. In fact, we can generalize these notions.

Definition 2.26 Let G be a finite p-group. Then the subgroup $\Omega_i(G)$ is the subgroup generated by all elements of order dividing p^i; that is,

$$\Omega_i(G) = \langle\, g \,:\, g^{p^i} = 1 \rangle.$$

The subgroup $\mho^i(G)$ is the subgroup generated by all elements of the form g^{p^i}; that is,

$$\mho^i(G) = \langle\, g^{p^i} \,:\, g \in G \rangle.$$

The Proposition 2.25 can be written as $\Phi(G) = G'\mho^1(G)$. In fact, the subgroups $\Omega_i(G)$ and $\mho^i(G)$ are all characteristic in G: this is true since the elements by which they are generated are left fixed by any automorphism of G.

Quickly, we notice the following lemma.

Lemma 2.27 Let G be a finite group with p dividing $|G|$. Then $\Omega_1(G) \neq 1$.

Proof: Obvious from Cauchy's Theorem. □

This seems a rather obvious lemma, but it can come in very handy.

Now we prove two important, yet not difficult, results on finite p-groups. These tell us that the Frattini subgroup is even more interesting than we had previously thought.

Theorem 2.28 (Burnside Basis Theorem) Let G be a finite p-group, and suppose that $|G : \Phi(G)| = p^d$. If $G/\Phi(G)$ is generated by elements $\Phi(G)x_i$, for $1 \leqslant i \leqslant d$, then G is generated by the x_i. Furthermore, any generating set of G contains a subset Y such that $G = \langle Y \rangle$ and $G/\Phi(G)$ is generated by the images of the elements of Y.

Proof: Suppose that $\langle x_1, \ldots, x_d \rangle$ is not the whole of G, say it is H. Since we are in a finite p-group, we have maximal subgroups, and so H is contained within some maximal subgroup M. Now $\Phi(G) \leqslant M$, and so

$$\langle \Phi(G)x_1, \ldots, \Phi(G)x_d \rangle \leqslant M/\Phi(G) < G/\Phi(G).$$

This contradicts the fact that the cosets $\Phi(G)x_i$ generate $G/\Phi(G)$, so

$$G = \langle x_1, \ldots, x_d \rangle.$$

Now suppose that X is any generating set. Then the images of X under the quotient $G \to G/\Phi(G)$ must generate $G/\Phi(G)$. Now we can pick a subset $\{y_1, \ldots, y_d\}$ of d elements of X such that

$$G/\Phi(G) = \langle \Phi(G)y_1, \ldots, \Phi(G)y_d \rangle,$$

and thus $G = \langle y_1, \ldots, y_d \rangle$. □

The Burnside Basis Theorem tells us that G can be generated with d elements, and this is also the *smallest* number of elements you can generate G with. We are led to the following definition.

Definition 2.29 A group is said to be *d-generator* if $G = \langle X \rangle$ for some subset $X \subseteq G$ of size d. A group is said to be *finitely generated* if G is generated by a finite subset X of G.

Then the only 1-generator groups are cyclic, for example. Dihedral groups, symmetric and alternating groups, the quaternion group, and direct products of two cyclic groups are 2-generator. $\mathbb{Q}$ is an example of a group that is not finitely generated.

The second of the promised results is the Hall–Burnside Theorem. This deals with automorphisms of p-groups. Notice that if H is a characteristic subgroup of G, then any automorphism ϕ induces an automorphism of G/H, by permuting the cosets as

$$Hx \mapsto H(x\phi).$$

Theorem 2.30 (Hall–Burnside Theorem) Let G be a finite p-group, and A be a subgroup of $\mathrm{Aut}(G)$, with $p \nmid |A|$. If every element of A acts as the identity on $G/\Phi(G)$, then $A = 1$.

Proof: Suppose that q is a prime dividing $|A|$, and let ϕ be an element of A of order q. Now ϕ acts as the identity on $G/\Phi(G)$, so ϕ acts on each coset of $\Phi(G)$. The orbits of ϕ are each of length either 1 or q, which tells us that $\Phi(G)x$ contains a fixed point; i.e., there is an element in each coset of $\Phi(G)$ which is left fixed by ϕ. Now take their images under the quotient map. This is clearly a generating set of $G/\Phi(G)$, since it is the whole quotient group! We can now choose a basis of $G/\Phi(G)$, and apply the Burnside Basis Theorem, to get that G is generated by elements that are fixed by ϕ. Hence $\phi = 1$, and we are done. □

2.3 Some Automorphism Groups

Proposition 2.31 Let G denote the elementary abelian group of order p^n. Then $\mathrm{Aut}(G) \cong \mathrm{GL}_n(p)$, the group of $n \times n$ matrices over $\mathrm{GF}(p)$.

Proof: Notice that there are $p^n - 1$ elements of order p in G. Suppose that G is generated by $x_1, \ldots, x_n$. An automorphism of a finite group is determined uniquely by its action on the generators of a group, so if we know where to send the x_i, we have nailed down our automorphism. Write ϕ for this automorphism.

We also need to see that any element of G can be expressed as a product

$$\prod_{i=1}^{n} x_i^{b_i},$$

where the b_i are unique integers between 0 and $p-1$. Then G cannot be generated by fewer than n elements, so we cannot 'waste' a generator by mapping it to somewhere that we can already express in terms of the other generators. Borrowing a term from linear algebra, we would like the images of the generators to be 'linearly independent'.

Notice that x_1 can be sent to any element of order p, so there are $p^n - 1$ choices for $x_1\phi$. Now we have to decide what to do with x_2; we cannot send it into $\langle x_1 \rangle$, since we would then be wasting a generator, and so there are $p^n - p$ choices for $x_2\phi$. Then $\langle x_1, x_2 \rangle$ has order p^2, and so there are $p^n - p^2$ choices for $x_3\phi$, and so on, until we get

$$|\operatorname{Aut}(G)| = (p^n - 1)(p^n - p)\dots(p^n - p^{n-1}),$$

which is the order of $\mathrm{GL}_n(p)$. So if we can find a homomorphism from $\operatorname{Aut}(G)$ to $\mathrm{GL}_n(p)$, and show that it is injective, we will be done.

Using the fact that any element of G can be expressed as a multiple of the basis elements, we proceed to write down a matrix for ϕ: let $A_\phi = (a_{i,j}^{(\phi)})$, where

$$x_j\phi = \sum_{i=1}^{n} a_{i,j}^{(\phi)} x_i.$$

So A_ϕ is uniquely determined. Then

$$(x_1, x_2, \dots, x_n)A_\phi = (x_1\phi, x_2\phi, \dots, x_n\phi).$$

The function $\Phi : \operatorname{Aut}(G) \to \mathrm{GL}_n(p)$ given by $\phi \mapsto A_\phi$ is injective, since the coefficients $a_{i,j}^{(\phi)}$ are uniquely determined. We must show that it is a homomorphism. If ϕ and ψ are two elements of $\operatorname{Aut}(G)$, then

$$\begin{aligned}
(x_i)(\phi\Phi)(\psi\Phi) &= \left(\sum_{i=1}^{n} a_{i,j}^{(\phi)} x_i\right)\psi \\
&= \sum_{i=1}^{n}\sum_{k=1}^{n} a_{i,j}^{(\phi)} a_{i,j}^{(\psi)} x_k \\
&= \sum_{k=1}^{n}\left(\sum_{i=1}^{n} a a_{i,j}^{(\phi)} a_{i,j}^{(\psi)}\right) x_k \\
&= \sum_{k=1}^{n} a_{i,j}^{(\phi\psi)} x_k \\
&= (x_i)(\phi\psi)\Phi,
\end{aligned}$$

so $(\phi\psi)\Phi = (\phi\Phi)(\psi\Phi)$ as required. Thus $\operatorname{Aut}(G) \cong \mathrm{GL}_n(p)$. □

Proposition 2.32 Let G denote the cyclic group of order n. Then $\operatorname{Aut}(G)$ is abelian, and has order $\phi(n)$, where ϕ denotes Euler's ϕ-function.

Proof: Let $G = \langle x \rangle$. Then an automorphism of G must send x to another generator of G, which obviously must have order n, and so it reduces to finding out how many elements of C_n have order n. If n and m are coprime, with $1 \leqslant m \leqslant n$, then the first integer k for which $x^{mk} = 1$ is $k = n$. Hence, if m and n are coprime, then x^m has order n. Conversely, let d denote $\gcd(m, n)$, and suppose that x^m has order n. Then since $(x^m)^{n/d} = 1$ (since mn/d is divisible by n, $n \leqslant n/d$; this clearly implies that $d = 1$, and so m and n are coprime.

We have proved that x^m has order n if and only if m and n are coprime, and hence $|\operatorname{Aut}(G)| = \phi(n)$, since Euler's ϕ-function is simply the amount of numbers $m \leqslant n$ that are coprime to n.

To see that $\operatorname{Aut}(G)$ is abelian, notice that all automorphisms are of the form $x \mapsto x^m$; if $\phi : x \mapsto x^m$ and $\psi : x \mapsto x^k$ are two automorphisms, then

$$x(\phi\psi) = (x\phi)\psi = x^m\psi = x^{mk} = x^{km} = x^k\phi = x(\psi\phi),$$

and so $\operatorname{Aut}(G)$ is abelian. □

We have the following improvement to the previous proposition in the case where the cyclic group is of prime order.

Proposition 2.33 Let $G \cong C_p = \langle x \rangle$. Then $\operatorname{Aut}(G)$ is cyclic of order $p - 1$.

Proof: We already know that $\operatorname{Aut}(G)$ is abelian of order $p-1$ (since every number less than p is coprime to p), so we simply need to show that $\operatorname{Aut}(G)$ is cyclic. To see this, we will notice that $\operatorname{Aut}(G)$ is the same as multiplying the non-zero integers modulo p. Then since the integers modulo a prime form a field, $\operatorname{Aut}(G)$ is cyclic.

Consider two automorphisms $\phi_m : x \mapsto x^m$ and $\phi_k : x \mapsto x^k$, where m and k lie between 1 and $p - 1$. Then $\phi_m\phi_k$ is given by

$$\phi_{mk} : x \mapsto x^{mk},$$

so we get a homomorphism from $\operatorname{Aut}(G)$ to the multiplicative group of the integers modulo p by

$$\Phi : \operatorname{Aut}(G) \to (\mathbb{Z}/p\mathbb{Z})^\star, \qquad \Phi : \phi_m \mapsto m.$$

[Here, $F^\star = F \setminus \{0\}$ denotes the multiplicative subgroup of F.] Hence $\operatorname{Aut}(G)$ is cyclic of order $p - 1$, as required. □

Before we analyze the structure of $\operatorname{Aut}(G)$ further, note that $\phi(p^n) = p^{n-1}(p - 1)$.

Proposition 2.34 Let $G = \langle x \rangle$ be a cyclic 2-group, and write $A = \operatorname{Aut}(G)$.

(i) If $G = C_4$, then $A = C_2$, and is generated by $x \mapsto x^{-1}$.

(ii) If $G = C_{2^n}$ where $n \geqslant 3$, then $A = C_{2^{n-2}} \times C_2$, and is generated by $\phi : x \mapsto x^{-1}$ and $\psi : x \mapsto x^5$.

Proof: The proof of (i) is obvious, and so we examine (ii). Note that

$$5^{2^{n-2}} = (1+4)^{2^{n-2}} \equiv 1 \mod 2^n, \quad 5^{2^i} \not\equiv \pm 1 \mod 2^n,$$

if $0 < i < n-2$. Hence the automorphism $x \mapsto x^5$ has order 2^{n-1}. Since 5^{2^j} is not congruent to -1 modulo 2^n either, there is no power of ϕ that is equal to ψ, whence they form a generating set for A, as $\langle \phi, \psi \rangle$ has then correct order. □

In particular, notice that there are exactly three subgroups of $\mathrm{Aut}(C_{2^n})$ of order 2.

Proposition 2.35 Let G be a cyclic p-group with p odd, and write $A = \mathrm{Aut}(G)$. Then A is cyclic.

Proof: Since $|A| = p^{n-1}(p-1)$, where $|G| = p^n$, if we can prove that A contains an element of order $p-1$ and the Sylow p-subgroup of A is cyclic, then we are done.

We firstly claim that the automorphism $\phi : x \mapsto x^{p+1}$ is a generator for the Sylow p-subgroup of A. To see this, notice that

$$(1+p)^{p^i} \equiv 1 \mod p^{i+1}, \quad (1+p)^{p^i} \not\equiv 1 \mod p^{i+2},$$

and hence ϕ has order p^{n-1}, as we need.

To prove that A contains an element of order $p-1$, recall that this is true if $n = 1$. Next, we have a surjective homomorphism $A \to \mathrm{Aut}(C_p)$ given by the following: if x is a generator for G and y is a generator for C_p, then the function

$$(x \mapsto x^a) \mapsto (y \mapsto y^{a \bmod p})$$

is a homomorphism, and clearly is surjective. Hence A contains an element of order a multiple of $p-1$ to map onto a generator of $\mathrm{Aut}(C_p)$, and hence has an element of order $p-1$. □

In particular, notice that there is exactly one subgroup of order p, generated by $x \mapsto x^{p^{n-1}+1}$.

With the information in Propositions 2.34 and 2.35 we can determine $\mathrm{Aut}(G)$ for any cyclic group G.

Corollary 2.36 Let G be a cyclic group, and write $|G| = 2^n p_1^{n_1} \dots p_r^{n_r}$. For $n = 0$ or $n = 1$, we have

$$\mathrm{Aut}(G) = \left(\prod_{i=1}^{r} C_{p_i^{n_i-1}(p_i-1)} \right).$$

If $n \geqslant 2$, then we have

$$\mathrm{Aut}(G) = C_2 \times C_{2^{n-2}} \times \left(\prod_{i=1}^{r} C_{p_i^{n_i-1}(p_i-1)} \right).$$

Chapter 3

Extraspecial Groups

Definition 3.1 Let G be a finite p-group. Then G is defined to be *special* if either G is elementary abelian or G is of class 2 and $G' = \Phi(G) = \mathrm{Z}(G)$ is elementary abelian. If G is a non-abelian special group with $|\mathrm{Z}(G)| = p$, then G is said to be *extraspecial*.

Example 3.2 The dihedral and quaternion groups D_8 and Q_8 are extraspecial. More generally, if G is a non-abelian group of order p^3 then G is extraspecial.

We now give some examples of p-groups that we will use in this chapter and the next. We will actually give the definition of more groups than we need for this chapter, because it is sometimes useful to have them all in one place.

Definition 3.3 The *dihedral group* D_{2n} is given by the generators and relations

$$D_{2n} = \langle\, x, y \,:\, x^n = y^2 = 1,\ x^y = x^{-1} \rangle = \langle\, a, b \,:\, a^2 = b^2 = 1,\ (ab)^n = 1 \rangle.$$

The *quaternion group* Q_{4n} is given by

$$Q_{4n} = \langle\, x, y \,:\, x^{2n} = y^4 = 1,\ x^y = x^{-1},\ y^2 = x^n \rangle$$

The *semidihedral* or *quasidihedral* group SD_{2^n} is given by

$$\mathrm{SD}_{2^n} = \langle\, x, y \,:\, x^{2^{n-1}} = y^2 = 1,\ x^y = x^{2^{n-2}-1} \rangle.$$

The *modular p-group* $\mathrm{Mod}_n(p)$ is given by the generators and relations

$$\mathrm{Mod}_n(p) = \langle\, x, y \,:\, x^{p^{n-1}} = y^p = 1,\ x^y = x^{1+p^{n-2}} \rangle.$$

Define

$$p_+^{1+2} = \langle\, x, y, z \,:\, x^p = y^p = z^p = 1,\ [x, z] = [y, z] = 1,\ [x, y] = z \rangle.$$

In the case where $n = 3$, we also write $\mathrm{Mod}_3(p) = p_-^{1+2}$. We will not prove that these groups are well-defined or unique up to isomorphism. The groups D_{2n} are of order $2n$, and are split extensions of C_n by C_2. The groups SD_{2^n} are of order 2^n, and are split extensions of $C_{2^{n-1}}$ by C_2. The groups Q_{4n} are non-split extensions of C_{2n} by C_2. The groups $\mathrm{Mod}_n(p)$ have order p^n and are a split extension of $C_{p^{n-1}}$ by C_p. Finally, the group p_+^{1+2} has order p^3.

Notice that the groups D_{2^n}, Q_{2^n}, SD_{2^n} and Mod_{p^n} all have a cyclic subgroup of index p.

Lemma 3.4 There are five non-isomorphic groups of order p^3, namely the three abelian groups, D_8 and Q_8 if $p = 2$ and $p_\pm^{1+2}$ when p is odd.

Proof: The three abelian groups are obvious, and so we only need to consider the non-abelian groups. Firstly, let $p = 2$, and let G be a non-abelian group of order 8. Since any group of exponent 2 is abelian, G contains an element x of order 4. If $G \setminus \langle x \rangle$ contains an element of order 2, then G is a split extension of C_4 by C_2, and since G is non-abelian, the homomorphism $C_2 \to \mathrm{Aut}(C_4) = C_2$ is non-trivial, and hence an isomorphism. Thus there is exactly one non-abelain split extension of C_4 by C_2, and this is D_8.

Thus suppose that $G \setminus \langle x \rangle$ contains only elements of order 4, and let y be one of these. It is clear that G possesses a single element of order 2, and so $x^2 = y^2$. Also, since $\langle x \rangle$ has index 2 and is hence normal in G, x^y is either x or x^{-1}. If $x^y = x^{-1}$ then $G = Q_8$, as defined above. If $x^y = x$ then x and y commute and so G is abelian.

Now let p be odd, and suppose that G contains an element x of order p^2, and write $X = \langle x \rangle$. Since G is non-abelian, $\mathrm{C}_G(X) = X$, and so if $y \in G \setminus X$, then y induces a non-trivial automorphism of X, and as $y^p \in X$, this automorphism has order p. By Lemma 2.35, $\mathrm{Aut}(X)$ possesses a unique subgroup of order p, generated by $x \mapsto x^{1+p}$, so that y can be chosen so that $x^y = x^p x = xz$ for $z = x^p$ of order p, lying in $\mathrm{Z}(G)$. Since $y^p \in X$, we must have $y^p = x^p \alpha$ for some α; write $g = yx^{-\alpha}$. Then

$$g^p = (yx^{-\alpha})^p = y^p x^{-\alpha p} = 1,$$

(by the fact that G is of class 2 and $G/\mathrm{Z}(G)$ is elementary abelian) so that the extension splits, and we see that $G \cong \mathrm{Mod}_3(p)$.

Now let G be a group of exponent p, and choose a subgroup of index p. Let x be a non-central element of this subgroup, and y be an element not in this subgroup. Then $[x, y] = z \in \mathrm{Z}(G)$, and so $[x, z] = [y, z] = 1$, yielding the presentation of p_+^{1+2}. □

This has dealt with the groups of order p^3. To deal with the larger extraspecial groups, we need central products and alternating forms.

3.1 Central Products

This section will outline the construction of a central product. Let G and H be groups with isomorphic centres Z. Then we aim to construct a group with centre Z and a quotient of $G \times H$.

Proposition 3.5 Let G be a finite group, and let $G_1, \ldots, G_r$ be subgroups of G. The following are equivalent:

(i) $G = \langle G_i : 1 \leqslant i \leqslant r \rangle$ and $[G_i, G_j] = 1$ for $i \neq j$; and

(ii) the map ϕ given by

$$\phi : G_1 \times G_2 \times \cdots G_r \to G, \qquad \phi(x_1, x_2, \ldots, x_r) \mapsto x_1 x_2 \ldots, x_r$$

is a surjective homomorphism and, if H_i denotes the subgroup of the domain of ϕ consisting of all elements in the ith co-ordinate, then $H_i\phi = G_i$, and $G_i \cap \ker \phi = 1$.

Proof: Suppose that G is generated by the G_i, and $[G_i, G_j] = 1$. Clearly, since G is generated by the G_i, the map ϕ is surjective, and it is a homomorphism since G_i and G_j commute. Again, certainly $H_i\phi \leqslant G_i$, and since G is a finite group, this map is a bijection. Finally, suppose that $G_i \cap \ker \phi \neq 1$, and let $1 \neq x \in \ker \phi$. Again, we see that $G_i \cap \ker \phi = 1$ trivially.

Conversely, suppose that (ii) holds. Since ϕ is a surjective homomorphism, every element of G is of the form $g = x_1 x_2 \ldots x_r$, and so G is generated by the G_i. Now suppose that $g_i \in G_i$ and $g_j \in G_j$, and consider $[g_i, g_j]$. Let h_i and h_j be the preimage of g_i and g_j in H_i and H_j; since $G_i \cap \ker \phi = 1$, this element is uniquely determined. Then $[h_i, h_j] = 1$, and so

$$[g_i, g_j] = [h_i, h_j]\phi = 1,$$

as required. □

If a group G satisfies either (and hence both) of the conditions in the proposition above, then G is said to be a *central product* of the groups G_i.

Theorem 3.6 Let $\{G_i : 1 \leqslant i \leqslant r\}$ be a family of subgroups such that $\mathrm{Z}(G_i) = \mathrm{Z}(G_j)$, and such that

$$\mathrm{Aut}(\mathrm{Z}(G_i)) = \mathrm{Aut}_{\mathrm{Aut}(G_i)}(\mathrm{Z}(G_i))$$

for all i. Then there exists up to isomorphism a unique group G that is the central product of the G_i, such that, if H_i denotes the subgroup isomorphic with G_i lying in G, then $\mathrm{Z}(H_i) = \mathrm{Z}(H_j)$ for all i and j.

We will not prove this theorem here.

3.2 Alternating Forms

Let F be a field, and let V be a vector space over F. Then a *form* ϕ is simply a map $\phi : V \times V \to F$; we often require that ϕ is bilinear, so that

$$\phi(ax_1 + x_2, by_1 + y_2) = ab\phi(x_1, y_1) + b\phi(x_2, y_1) + a\phi(x_1, y_2) + \phi(x_2, y_2),$$

for $x_i, y_j \in V$ and $a, b \in F$.

Definition 3.7 Suppose that ϕ is a bilienar form on the vector space V, which is over a field F.

(i) If $\phi(x, y) = \phi(y, x)$, then ϕ is said to be *symmetric*.

(ii) If $\phi(x, y) = -\phi(y, x)$, then ϕ is said to be *skew-symmetric*.

(iii) If $\phi(x, x) = 0$, then ϕ is said to be *alternating*.

If a bilinear form is alternating then it is skew-symmetric, and if $\operatorname{char} F \neq 2$ then a skew-symmetric bilinear form is alternating.

Definition 3.8 Suppose that V is a vector space over F, and that ϕ is a bilinear form. If two vectors v and w have the property that $\phi(v, w) = 0$, then v and w are said to be *orthogonal*, and it is written $v \perp w$. Write $v^\perp$ for the set of all vectors w such that $v \perp w$. A vector v, is called *singular* if $v^\perp = V$, and V is singular and non-singular according as V contains a singular vector or not.

Theorem 3.9 Let V be a vector space over a field F, supporting a non-singular alternating form. Then $\dim_F(V) = 2n$ is even, and there exists a basis $u_1, v_1, u_2, v_2, \ldots, u_n, v_n$, such that

(i) $(u_i, u_j) = (v_i, v_j) = 0$, and

(ii) $(u_i, v_j) = \delta_{ij}$.

This theorem requires a few lemmas from which it will become clear. If U is a subspace of the vector space V with form ϕ, then write $U^\perp$ for the set

$$\bigcap_{u \in U} u^\perp.$$

Lemma 3.10 Suppose that $v \in V$, where V is a vector space with form ϕ. Write $\theta : y \mapsto \phi(y, v)$. Then $v^\perp = \ker \theta$, and $\dim v^\perp \geqslant n - 1$, with equality exactly when $v \in V^\perp$.

This will be used to prove the next lemma in the chain.

Lemma 3.11 Let V be a non-singular vector space, and let U be a subspace of V. Then $\dim U^\perp = \operatorname{codim} U$.

Proof: We proceed by induction on $m = \dim U$, where $n = \dim V$. We can assume that U is non-trivial, so let $x \in V \setminus U^\perp$, which exists since ϕ is non-singular. The space $X = U \cap x^\perp$ is of dimension $m-1$, whence by induction we have

$$\dim_F X^\perp = n - m + 1.$$

Suppose that v is an element of $U \setminus X$; then $U^\perp = X^\perp \cap v^\perp$, and since $x \in X^\perp \setminus v^\perp$, the space $U^\perp$ is of codimension 1 in $X^\perp$, yielding $\dim U^\perp = n - m$, as required. □

Lemma 3.12 Let U be a subspace of the vector space V, and suppose that ϕ is non-singular. Then $\phi|_U$ is non-singular if and only if $U = U \oplus U^\perp$.

Proof: This follows easily from Lemma 3.11. □

Now let V be a vector space with an alternating bilinear form, and proceed by induction on $\dim_F V$; choose the non-trivial element u_1 arbitrarily. Since f is non-singular, V contains a vector w_1 such that $\phi(u_1, w_1) \neq 0$, so let $v_1 = (\phi(u_1, w_1))^{-1} w_1$. Then $\phi(u_1, v_1) = 1$, and $V_1 = \langle u_1, v_1 \rangle$ is a non-singular subspace of V. Thus, by Lemma 3.12, we see that $V = V_1 \oplus V_1^\perp$, which by induction is a sum of 2-dimensional spaces of the form stated in Theorem 3.9, whence we are done.

3.3 Extraspecial Groups of Order p^{1+2n}

Let $A = \mathrm{Mod}_3(p)$ and $B = p_+^{1+2}$. Suppose that G and H are extraspecial p-groups, and form their central product $X = G * H$. Then $\mathrm{Z}(X)$ has order p, and since $G \times H$ has a derived subgroup equal to its centre, so does X, and in fact this is the Frattini subgroup. Hence X is also extraspecial. In fact, these are the only extraspecial groups. Before we prove this, we need some specific central products. We will not prove this proposition completely, although we will prove most of it.

Proposition 3.13 Let A and B be defined as above. Then

(i) $D_8 * D_8 \cong Q_8 * Q_8 \ncong D_8 * Q_8$, and

(ii) $A * B \cong A * A \ncong B * B$.

Proof: Firstly suppose that $p = 2$; we will prove that $D_8 * D_8$ and $Q_8 * Q_8$ are isomorphic. Suppose that $P = Q_8 * Q_8$; then $P = \langle x_1, y_1, x_2, y_2 \rangle$, with $\langle x_1, y_1 \rangle$ centralizing $\langle x_2, y_2 \rangle$, with $x_i^{y_i} = x_i^{-1}$, and $x_i^2 = y_i^2 = z$, the central element of order 2. Let $H_1 = \langle x_1, x_2 y_1 \rangle$, and let $H_2 = \langle x_2, x_1 y_2 \rangle$. Then $x_1 y_2$ and $x_2 y_1$ are of order 2, and conjugate x_2 and x_1 respectively into their inverses, proving that $H_i \cong D_8$, and that $Q_8 * Q_8 \cong D_8 * D_8$.

Now we show that $Q_8 * Q_8$ and $D_8 * Q_8$ are different, by proving that they have different numbers of elements of order 4. Suppose that $G_1 = D_8$ and $G_2 = Q_8$, where

$$G_1 = \langle\, a, b \,:\, a^4 = b^2 = 1,\ a^b = a^{-1} \rangle, \qquad G_2 = \langle\, x, y \,:\, x^4 = 1,\ x^2 = y^2,\ x^y = x^{-1} \rangle.$$

The elements in $H = G_1 \times G_2$ of order 4 are $(a^{\pm 1}, g_2)$ for $g_2 \in G_2$, and (g_1, g_2) where $g_1 \in G_1$ and g_2 has order 4. In particular, there are 52 elements of order 4. The central subgroup of order 2 that will be quotiented out to form the central product is $\langle z \rangle$, where $z = (a^2, x^2)$, and so an element of order 4 in $G = G_1 * G_2$ is the image of an element of order 4 in H. The 12 elements $(a^{\pm 1}, g_2)$, where $g_2 \in G_2$ has order 4, square to z, and so these have order 2 in G. The remaining elements $h \in H$ are identified with the elements hz, and so there are $(52 - 12)/2 = 20$ elements of order 4 in $D_8 * Q_8$.

Now let $G_1 = D_8$ and $G_2 = D_8$, where

$$G_1 = \langle\, a, b \,:\, a^4 = b^2 = 1,\ a^b = a^{-1} \rangle, \qquad G_2 = \langle\, x, y \,:\, x^4 = y^2 = 1,\ x^y = x^{-1} \rangle.$$

The elements in $H = G_1 \times G_2$ of order 4 are $(a^{\pm 1}, g_2)$ and $(g_1, x^{\pm 1})$, where $g_i \in G_i$. In particular, there are 28 elements of order 4. The central subgroup of order 2 that will be quotiented out to form the central product is $\langle z \rangle$, where $z = (a^2, x^2)$, and so an element of order 4 in $G = G_1 * G_2$ is the image of an element of order 4 in H. The 4 elements $(a^{\pm 1}, x^{\pm 1})$ square to z, and so these have order 2 in G. The remaining elements $h \in H$ are identified with the elements hz, and so there are $(28 - 4)/2 = 12$ elements of order 4 in $D_8 * D_8$. Hence $D_8 * D_8 \ncong D_8 * Q_8$, proving (i).

Since B has exponent p and the elements of each subgroup commute, we see that $B * B$ has exponent p, whereas $A * B$ and $A * A$ have exponent p^2. Now suppose that $G = A * A$, with generators x_1, y_1, x_2, and y_2, where $\{x_1, y_1\}$ centralizing $\{x_2, y_2\}$, $o(x_i) = p^2$, $o(y_i) = p$, and $x_i^{y_i} = x_i^{1+p}$. Finally, $\langle x_i^p \rangle = \mathrm{Z}(P)$, and we can suppose that $x_1^p = x_2^p$. Let $a = x_2 x_1^{-1}$; we have

$$a^p = (x_2 x_1^{-1})^p = 1,$$

and y_2 does not centralize a. Hence $\langle a, y_2 \rangle$ is a non-abelian group of order p^3, and is of exponent p, and so is isomorphic with B. It turns out that there is another non-abelian subgroup of order p^3 that centralizes the subgroup isomorphic with B, and so it is a central

product involving B and another group, which has to be A, as we know that it cannot be B. Hence all parts are proved. □

Now we use our knowledge of alternating forms to prove the following result.

Theorem 3.14 Let G be an extraspecial p-group.

(i) If p is odd, then either $G \cong B^{*n}$ or $G \cong A^{*n}$, and in either case, $|G| = p^{2n+1}$.

(ii) If $p = 2$, then either $G \cong D_8^{*n}$ or $G \cong Q_8 * D_8^{*(n-1)}$, and in either case, $|G| = 2^{2n+1}$.

Proof: By Proposition 3.13, we see that all we need to show is that G is the central product of non-abelian groups of order p^3, and then we are done. Thus let G be any extraspecial group, and let $Z = \mathrm{Z}(G)$. Identify Z with $\mathrm{GF}(p)$, so that if $Z = \langle z \rangle$, then z^i is associated with $i \in \mathrm{GF}(p)$. If x and y are elements of G, then $[x, y] \in \mathrm{GF}(p)$.

Writing $\bar{G} = G/Z$, we see that commutation of elements induces a map $\phi : \bar{G} \times \bar{G} \to \mathrm{GF}(p)$. If x lies in G, write $\bar{x}$ for the image of x (a coset of Z) in $\bar{G}$. Notice that if $z_1, z_2 \in \mathrm{Z}(P) = \Phi(P)$, then $[xz_1, yz_2] = [x, y]$, that $[xx', y] = [x, y][x', y]$ since $[x, y] \in \mathrm{Z}(P)$, and so the map is bilinear.

Write $\phi(\bar{x}, \bar{y}) = [x, y] \in \mathrm{GF}(p)$. Thus ϕ becomes a bilinear form, and since $\phi(x, x) = 0$, the form ϕ is alternating. If $\bar{x} \neq 1$, so that $Zx \neq Z$, then there exists $y \notin Z$ such that $[\bar{x}, \bar{y}] \neq 0$, and so ϕ is non-singular.

We can view $\bar{G}$, which is elementary abelian, as a vector space, and can write

$$\bar{G} = \bar{G}_1 \oplus \cdots \oplus \bar{G}_n,$$

where $\bar{G}_i = \langle \bar{x}_i, \bar{y}_i \rangle$ has dimension 2, and $\phi(\bar{x}_i, \bar{y}_i) = 1$ and all G_i and G_j are orthogonal for $i \neq j$. Hence, in particular, $\dim_{\mathrm{GF}(p)} \bar{G} = 2n$ is even.

Let $G_1, \ldots, G_n$ be preimages of $\bar{G}_1, \ldots, \bar{G}_n$ in G. Then $G_1, \ldots, G_n$ are non-abelian groups of order p^3, generating G, such that any two of them intersect in $\mathrm{Z}(G)$. Also $[G_i, G_j] = 1$ if $i \neq j$. Thus G is a central product

$$G = G_1 * G_2 * \cdots * G_n,$$

as required. □

Theorem 3.15 Let P be extraspecial of order p^{2n+1}.

(i) If $\alpha \in \mathrm{Aut}(P)$ induces the identity on $P/\Phi(P)$, then α is inner.

(ii) Let $\mathrm{Aut}_C(P) = \{\alpha \in \mathrm{Aut}(P) : \alpha|_{\mathrm{Z}(P)} = 1\} \trianglelefteqslant \mathrm{Aut}(P)$, and put $\mathrm{Out}_C(P) = \mathrm{Aut}_C(P)/\mathrm{Inn}(P)$. Then

$$\mathrm{Out}_c(P) \hookrightarrow \mathrm{Sp}_{2n}(p),$$

and we get an isomorphism if and only if $\exp(P) = p$.

Proof: Let B be the group of all such automorphisms. Consider $\beta \in B$, and its action on a 'basis' for P (i.e., a minimal generating set $\{g_1, \ldots, g_{2n}\}$). Then the total number of automorphisms is at most p^{2n}, which is $|\mathrm{Inn}(P)| = |P/\mathrm{Z}(P)|$. But $B \leqslant \mathrm{Inn}(P)$, so $B = \mathrm{Inn}(P)$.

Now let $\alpha \in \mathrm{Aut}_c(P)$. Then for $x, y \in P$,

$$[x\alpha, y\alpha] = [x, y]\alpha = [x, y] \in \mathrm{Z}(P),$$

so α induces an automorphism on $P/\Phi(P)$ that preserves the form $[\,,\,]$, induced by commutation. Now consider

$$\psi : \mathrm{Aut}_c(P) \to \mathrm{Sp}_{2n}(p).$$

Now $\ker\psi = \mathrm{Inn}(P)$ by the previous part. If $\exp(P) = p$, then effectively one can choose any element of $\mathrm{Sp}_{2n}(P)$ and inflate. Otherwise, we need to preserve the pth-power map, so that in particular $\mathrm{Aut}_c(P)$ is not transitive on the non-zero elements of $P/\Phi(P)$. □

Notice that if $\exp(P) = p^2$, then $\mathrm{Out}_c(P)$ is an orthogonal group. [If p is odd, then only one of the two orthogonal groups occurs (since one of the two extraspecial groups is of exponent p). However, if $p = 2$, then both groups are of exponent p^2, and so both types of orthogonal group occur.]

We now prove a generalization of a special case of a theorem of P. Hall: this theorem discussed p-groups in which every normal abelian subgroup is cyclic.

Theorem 3.16 Let P be a non-abelian p-group in which every characteristic abelian subgroup is central and cyclic. Then $P = \mathrm{Z}(P)E$, where E is extraspecial.

Proof: The proof of this will go in stages. Firstly, we will show that $\mathrm{cl}(P) = 2$. Let $\gamma_i = \gamma_i(P)$ be the ith term in the lower central series, so that $\gamma_{i+1} = [\gamma_i, P]$. Then the Three Subgroup Lemma implies

$$[\gamma_i, \gamma_j] \leqslant \gamma_{i+j}.$$

[This is a general theorem about groups.] Suppose $c = \mathrm{cl}(P) \geqslant 3$. Then $2(c-1) \geqslant c+1$, so that

$$[\gamma_{c-1}, \gamma_{c-1}] \leqslant \gamma_{2c-1} \leqslant \gamma_{c+1} = 1.$$

Thus γ_{c-1} is a characteristic abelian subgroup, so is central, a contradiction.

Next we show that $\Phi(P) \leqslant \mathrm{Z}(P)$. It is enough to show that $\Phi(P)$ is abelian, since it is already characteristic. We have $\mathrm{Z}(\Phi(P)) \leqslant \mathrm{Z}(P)$ since $\mathrm{Z}(\Phi)(P)$ is characteristic and abelian. Now $\Phi(P)$ is characteristic, and so hits the centre non-trivially. Suppose that $\Phi(P)$ is non-abelian: if we put $\bar{P} = P/Z$, then $\overline{\Phi(P)}$ is a non-trivial normal subgroup of P/Z, so hits the centre of $\bar{P}$ non-trivially. Let $N \geqslant Z$ such that $|\bar{N}| = p$ and

$$\bar{N} \leqslant \mathrm{Z}\left(\bar{P}\right) \cap \overline{\Phi(P)}.$$

Now N is a normal abelian subgroup, so either N is cyclic or $N \cong Z \times N_1$ for some N_1 of order p. If N is cyclic, then $|P : \mathrm{C}_P(N)| \leqslant p$, because a subgroup of N of index p lies in $\mathrm{Z}(P)$. The same is true in the p-rank 2 case. In any case, $\mathrm{C}_P(N)$ contains a maximal subgroup of P. Thus,

$$\mathrm{C}_P(N) \geqslant \Phi(P),$$

i.e., $N \leqslant \mathrm{Z}(\Phi(P)) = Z$, a contradiction.

We now prove that $P' = \Omega_1(\mathrm{Z}(P))$. For $x \in P$, we have $x^p \in \Phi(P) \leqslant \mathrm{Z}(P)$, and for $x, y \in P$ (since P has class 2),

$$[x, y]^p = [x^p, y] = 1.$$

Thus $(P')^p = 1$.

Finally, we prove the conclusion. Notice that if $|\mathrm{Z}(P)| = p$, then P is extraspecial. Now suppose that $|\mathrm{Z}(P)| \geqslant p^2$. Put $\bar{P} = P/P'$, the abelianization of P. Since $P' \leqslant \Phi(P) \cong C_{p^n}$, $\Phi(P)$ is cyclic. Thus $\overline{\Phi(P)} = \Phi(\bar{P})$. But $\bar{P}$ is abelian, and so

$$\bar{P} = A_1 \times \cdots \times A_r,$$

with the A_i cyclic; then $|A_i| = p$ except for A_1 (since $\Phi(P)$ is cyclic). If $|A_1| \geqslant p^2$, then

$$\mathfrak{V}^1(\bar{P}) = \langle\, \bar{g}^p \,:\, \bar{g} \in \bar{P} \rangle = \mathfrak{V}^1(A_1) \operatorname{char} \bar{P}.$$

Notice importantly that $\mathfrak{V}^1(A_1) = \Phi(\bar{P})$. In any case consider $\Omega_1(\bar{P})$ and its lift $\widehat{\Omega_1(\bar{P})}$ to P; call this P_1.

We can apply the same arguments to P_1 as to extraspecial groups. Now $P_1 \operatorname{char} P$, so $\mathrm{Z}(P_1) \operatorname{char} P$, implying that $\mathrm{Z}(P_1)$ is cyclic. So the form $[\,,\,]$ on $\Omega_1(\bar{P})$ induced by commutation has a 1-dimensional singular subspace. Hence $P_1 = Z_1 E$, where $Z_1 = \mathrm{Z}(P_1) \cong C_{p^2}$ and E is extraspecial.

If $|A_1| = p$, we are done. If not, then $E \trianglelefteq P$ and $P = E\,\mathrm{C}_P(E)$ by Theorem 3.15(i). Now, looking at $\bar{P}$, the rank of $\mathrm{C}_P(E)$ is 1, so $\mathrm{C}_P(E)$ is cyclic, and $\mathrm{C}_P(E) = \mathrm{Z}(P)$. $\square$

Chapter 4

Maximal Class and p-Rank

4.1 Cyclic Subgroups of Index p

Recall the definitions of the dihedral, quaternion, semidihedral and modular groups from the previous chapter.

Theorem 4.1 Let G be a p-group with a cyclic subgroup of index p. If p is odd then G is isomorphic with one of the following:

(i) C_{p^n};

(ii) $C_{p^{n-1}} \times C_p$; or

(iii) $\mathrm{Mod}_n(p)$;

If $p = 2$ then G is isomorphic with one of the groups

(i) C_{2^n};

(ii) $C_{2^{n-1}} \times C_2$;

(iii) $\mathrm{Mod}_n(2)$ for $n \geqslant 4$;

(iv) D_{2^n} for $n \geqslant 3$;

(v) SD_{2^n} for $n \geqslant 4$; or

(vi) Q_{2^n} for $n \geqslant 3$.

Proof: We may assume that G is a non-abelian group with an element x of order p^{n-1}. Let y denote an element of $G \setminus X$. Since $y^p \in X$, the automorphism induced by conjugation by y is of order p.

Suppose firstly that p is odd. Then y can be chosen so that $x^y = x^{1+p^{n-2}}$, and $G = \langle x, y \rangle$. Now

$$(x^p)^y = (x^y)^p = x,$$

and so $x^p \in \mathrm{Z}(G)$. Since $G/\mathrm{Z}(G)$ cannot be cyclic and G is non-abelian, we see that $\mathrm{Z}(G) = \langle x^p \rangle$. Since G is 2-generator, we find that $\Phi(G) = \mathrm{Z}(G)$, and so G has class 2. Write $y^p = x^{\alpha p}$ for some α, and set $z = yx^{-\alpha}$. Since $G/\mathrm{Z}(G)$ is elementary abelian, we have

$$z^p = (yx^{-\alpha})^p = y^p x^{-\alpha p} = 1,$$

(since if G has class two and $G' = \Phi(G)$ then $x^p y^p = (xy)^p$) and so $\langle x, z \rangle = \mathrm{Mod}_n(p)$. Thus we have proved the result for p odd.

Now suppose that $p = 2$. If $y \in G \setminus X$, then x^y is one of the following three elements: $x^{1+2^{n-2}}$; x^{-1}; and $x^{2^{n-2}-1}$. Since $x^{2^{n-2}}$ is the unique element of order 2 in X, write a for this element. Then $x^y = x^\delta a^\varepsilon$, where $\delta = \pm 1$ and ε is equal to either 0 or 1.

Since $y^2 = x^{2\alpha}$ for some α, the element y^2 centralizes both y and x, and so lies in the centre of G. We will compute the order of the centre of G in each of the three cases for δ and ε. If $\delta = -1$ and $\varepsilon = 0$, we clearly have that $|\mathrm{Z}(G)| = 2$, and with slightly more work, one can see that $|\mathrm{Z}(G)| = 2$ in the case where $\delta = -1$ and $\varepsilon = 1$. Thus y has order 2 or 4 in either of these cases.

If $o(y) = 2$, then the extension splits, and G is isomorphic to $\mathrm{Mod}_n(2)$, D_{2^n}, and SD_{2^n} in each of the three cases outlined above, so we assume that $o(y) = 4$. If $(\delta, \varepsilon) = (-1, 0)$, then $G = Q_{2^n}$, so we are left with the case where $o(y) = 4$ and $x^y = x^{-1}a$. Since $a = y^2 \in \mathrm{Z}(G)$, we have

$$(yx)^2 = y^2 x^y x = z x^{-1} z x = 1,$$

and so there is an element of order 2, proving that the extension does split.

Hence, we are left with the case where $x^y = xa$, where $y^2 = x^{2\alpha}$. Consider the element yx^β, for some β; then

$$(yx^\beta)^2 = y^2 (x^\beta)^y x^\beta = x^{2\alpha} x^{\beta(1+2^{n-2})} x^\beta = x^{2\alpha + 2\beta(1+2^{n-3})}.$$

One can choose β to satisfy $2\alpha + 2\beta(1 + 2^{n-3}) \equiv 0 \mod 2^{n-2}$, proving that yx^β has order 2, giving a split extension $\mathrm{Mod}_2(n)$. □

Notice that the centre of $\mathrm{Mod}_n(2)$ has order 4, and that the derived subgroup of $\mathrm{Mod}_n(2)$ has order 2.

4.2 The 2-Groups of Maximal Class

Theorem 4.2 Let G be a 2-group of maximal class, with $|G| \geqslant 8$. Then G is either dihedral, semidihedral, or quaternion.

Proof: Since G is of maximal class, $|\operatorname{Z}_i(G)/\operatorname{Z}_{i-1}(G)| = 2$ for all $1 \leqslant i \leqslant n-1$. Thus $G/\operatorname{Z}(G)$ has order 2^{n-1} and is of maximal class $n-2$. Hence $G/\operatorname{Z}(G)$ is dihedral, semidihedral, or quaternion. Let $\bar{x}$ denote an element of order 2^{n-2} in $\bar{G} = G/\operatorname{Z}(G)$, and let $\bar{X} = \langle \bar{x} \rangle$. Write X for its preimage in G. Since $X \trianglelefteqslant G$, and $\operatorname{Z}(G)$ has order 2, $\operatorname{Z}(G) \leqslant X$, whence $\bar{X} = X/\operatorname{Z}(G)$ is cyclic, so that X is abelian. We know that X has an element of order 2^{n-2}, so either $X \cong C_{2^{n-2}} \times C_2$ or it is cyclic. If X is cyclic, then G contains a maximal cyclic subgroup, and we are done by Theorem 4.1, so we assume that X is not cyclic. In this case, $X = \langle x, z \rangle$, where $\operatorname{Z}(G) = \langle z \rangle$. Then

$$\langle x^{2^{n-3}} \rangle = \Omega^1(X) \cap \mho^1(X) \operatorname{char} X \trianglelefteqslant G,$$

whence $x^{2^{n-3}} \in \operatorname{Z}(G) = \{1, z\}$, contrary to the fact that $X = \langle x, z \rangle$, yielding the result. □

In fact, the 2-groups of maximal class can be characterized in another way.

Theorem 4.3 Let G be a 2-group. Then G/G' is of order 4 if and only if G is of maximal class.

Proof: Let G be a 2-group of maximal class. The quotient G/G' has order at least 4 since the rank of $G/\Phi(G)$ is the number of generators of G, which is at least 2. Since G has class $n-1$, $\gamma_n(G) = 1$, and since $\gamma_i(G) > \gamma_{i+1}(G)$ for all $i < n$, we must have that $|G : \gamma_2(G)| \leqslant 4$.

Thus suppose that G is a 2-group such that $|G/G'| = 4$. Since $1 \neq G' \trianglelefteqslant G$, we have $1 \neq z \in \operatorname{Z}(G) \cap G'$. Write $\bar{G} = G/\langle z \rangle$, and note that $|\bar{G}/(\bar{G})'| = 4$. Hence $\bar{G}$ is of maximal class, by induction, and so $|\operatorname{Z}(G)| \leqslant 4$. If $|\operatorname{Z}(G)| = 2$, then G has maximal class, and so we assume that $|\operatorname{Z}(G)| = 4$.

Let x be an element of G whose image $\bar{x}$ in $\bar{G}$ has order 2^{n-2}; and write X for the preimage of $\bar{X} = \langle \bar{x} \rangle$. If X is cyclic, then G contains a cyclic subgroup of index 2, and we easily see that G has maximal class, so we assume that $X = \langle x, z \rangle$ is isomorphic with $C_{2^{n-2}} \times C_2$. As with the previous theorem, we get $x^{2^{n-3}} \in \operatorname{Z}(G)$, and so $\operatorname{Z}(G)$ is a Klein four-group, generated by $x^{2^{n-3}} = y$ and z.

Now consider $H = G/\langle y \rangle$. This is again of maximal class, and the image of X in H is isomorphic with $C_2 \times C_{2^{n-3}}$. Since no group of maximal class has a non-cyclic abelian subgroup of order 8, this forces $n = 4$.

Hence we have a group G with $\mathrm{Z}(G) = G'$ of order 4, and $G = \langle \mathrm{Z}(G), a, b \rangle$ for some a, b. Thus

$$G' = \langle [a, b] \rangle$$

is cyclic, a contradiction. □

4.3 Groups of p-Rank 1

The case where p is odd is very easy.

Proposition 4.4 Suppose that p is odd, and let G be a p-group of p-rank 1. Then G is cyclic.

Proof: Suppose that G has p-rank 1. Let H be a subgroup of index p, which also has p-rank 1. Then H is cyclic by induction, and so G has a cyclic subgroup of index p. By Theorem 4.1, G is either cyclic, isomorphic with $\mathrm{Mod}_n(p)$, or is isomorphic with $C_{p^{n-1}} \times C_p$. The last two are clearly not of p-rank 1, and so G must be cyclic, as required. □

For the case where $p = 2$, we start off with Philip Hall's original theorem, about which we had a generalization of a special case earlier. The proof will be omitted.

Theorem 4.5 (P. Hall) Let G be a p-group in which every characteristic abelian subgroup is cyclic. Then G is the central product of an extra-special group E and a p-group R, where R is either cyclic, dihedral, semidihedral, or quaternion.

This is a characterization of p-groups of *characteristic p-rank* 1; that is, those groups whose characteristic elementary abelian subgroups are all of size p. We will refine this by determining those groups whose normal p-rank is 1, and finally to those whose p-rank is 1.

Theorem 4.6 Let G be a p-group with normal p-rank 1. Then G is cyclic, dihedral (of order at least 16), semidihedral, or generalized quaternion.

Proof: Suppose that G is a group with normal p-rank 1. Then G has characteristic p-rank 1, and so G is the central product $E * R$. If $E = 1$ then the theorem is true, and so we assume that $E \neq 1$.

Suppose firstly that p is odd. Then $E = H * K$, with H isomorphic with either p_-^{1+2} or p_+^{1+2}, both of which contain a normal subgroup L isomorphic with $C_p \times C_p$. Since $[H, K] = 1$, we see that $L \trianglelefteq E$, and similarly $L \trianglelefteq G$, proving that $E = 1$, and G is cyclic.

Hence we reduce to the case where $p = 2$. Certainly if $E \cong D_8 * H$ for some subgroup H, then E contains a normal subgroup isomorphic with $C_2 \times C_2$, and since $Q_8 * Q_8 = D_8 * D_8$

by Proposition 3.13, we see that $E = Q_8$. Thus G can only be the central product of Q_8 and a cyclic, dihedral, semidihedral or quaternion subgroup.

Let H be a normal subgroup of E of order 4, and let K be a normal subgroup of R of order 4, both containing the central element $z \neq 1$. Then HK has order 8 and exponent 4, since $[H, K] = 1$, and so HK is a non-cyclic, abelian normal subgroup, contrary to hypothesis. Thus $E = 1$, as required. □

Corollary 4.7 Let G be a group of 2-rank 1. Then G is cyclic or generalized quaternion.

Proof: Certainly dihedral and semidihedral groups are of 2-rank 2, and so the only groups left on the list given in Theorem 4.6 are cyclic and quaternion, both of which do indeed have p-rank 1. □

Chapter 5

Fixed-Point-Free Automorphisms

Definition 5.1 Let ϕ be an automorphism of the group G. Then ϕ is *fixed-point-free* if $x^\phi = x$ implies $x = 1$.

As easy examples of fixed-point-free automorphisms, we have the non-trivial automorphism of C_3, and the automorphism of V_4 of order 3. Clearly, if a finite group G has a fixed-point-free automorphism of order p, then $|G| \equiv 1 \mod p$.

Lemma 5.2 Let G be a group, and let ϕ be a fixed-point-free automorphism of order n. Then

$$x(x^\phi)(x^{\phi^2}) \dots (x^{\phi^{n-1}}) = 1.$$

The proof of this is obvious, since the left-hand side is invariant under ϕ.

Lemma 5.3 Let G be a finite group, and let ϕ be a fixed-point-free automorphism of G. If p is a prime dividing $|G|$, then ϕ fixes a unique Sylow p-subgroup P of G.

Proof: If P is a Sylow p-subgroup of G, then $P\phi$ is also a Sylow p-subgroup of G. Therefore, $P\phi = x^{-1}Px$ for some $x \in G$. Then for any $y \in G$,

$$(y^{-1}Py)\phi = (y^\phi)^{-1}x^{-1}Px(y^\phi).$$

However, every element of G can be expressed as $x^\phi x^{-1}$ (G is finite and $x \mapsto x^\phi x^{-1}$ is an injection) and so choose y such that $(y^\phi)y^{-1} = x^{-1}$. Then P^y is fixed under ϕ, as required.

Now suppose that P and P^x are fixed by ϕ. Therefore, $(x^\phi)x^{-1} \in \mathrm{N}_G(P)$. Again, since $(x^\phi)x^{-1}$ is in $\mathrm{N}_G(P)$, we see that (as $\mathrm{N}_G(P)$ is ϕ-invariant) there is an element $y \in \mathrm{N}_G(P)$ such that

$$(x^\phi)x^{-1} = (y^\phi)y^{-1}.$$

Since the map $x \mapsto (x^\phi)x^{-1}$ is a bijection, $x = y$, and so $P^x = P$, as needed. □

Lemma 5.4 Let G be a finite abelian group, and suppose that H is a subgroup of $\mathrm{Aut}(G)$ of the form $K \rtimes \langle \phi \rangle$. Suppose that, for all $k \in K$, the element $k\phi$ is fixed-point-free and or prime order, and that $|K|$ and $|G|$ are coprime. Then K fixes some non-trivial element of G.

Proof: The elements of $H \setminus K$ are of the form $(k\phi)^i$, where $k \in K$ and $1 \leqslant i \leqslant p-1$. If $x \in G$, then

$$\begin{aligned} 1 &= \prod_{k \in K} \prod_{i=0}^{p-1} x^{(k\phi)^i} \\ &= x^{|K|} \prod_{i=1}^{p-1} \prod_{k \in K} x^{(k\phi)^i} \\ &= x^{|K|} \prod_{i=1}^{p-1} \prod_{k \in K} x^{k\phi^i} \end{aligned}$$

Clearly,

$$\prod_{k \in K} x^{k\phi^i}$$

is a fixed point of G under the action of $k \in K$, and since $x^{|K|}$ is not the identity, one of the terms in the product must also not be the identity. Hence there is a fixed point of G under the action of K. □

Corollary 5.5 Let G be a finite abelian group, and let A be a homocyclic group of automorphisms of G, all of whose non-trivial elements act fixed-point-freely. Then A is cyclic.

If G is a group, then the map $x \mapsto x^{-1}$ is an *anti-automorphism*; that is, it is a map ϕ such that $(xy)\phi = (y^\phi)(x^\phi)$. If G is abelian, then all anti-automorphisms are automorphisms, and so any abelian group of odd order has a fixed-point-free automorphism of order 2.

Lemma 5.6 Suppose that $\phi : G \to G$ is a bijection that is both an automorphism and an anti-automorphism. Then G is abelian.

Proof: Let x and y be elements of G. Since ϕ is a bijection, there are elements x' and y' such that $x'\phi = x$ and $y'\phi = y$. Since ϕ is both an automorphism and an anti-automorphism, we have

$$xy = (x'\phi)(y'\phi) = (x'y')\phi = (y'\phi)(x'\phi) = yx,$$

as G is abelian. □

Corollary 5.7 Suppose that G has a fixed-point-free automorphism ϕ of order 2. Then G is an abelian group of odd order.

Proof: The map ϕ satisfies $x(x^\phi) = 1$, by Lemma 5.2. This implies that $x^\phi = x^{-1}$, and so this map is an automorphism. It is also an anti-automorphism, and so G possesses an automorphism that is also an anti-automorphism; thus G is abelian. □

Theorem 5.8 (B. Neumann, 1956) Let ϕ be a fixed-point-free automorphism of G, and suppose that ϕ has order 3. Then G is nilpotent of class at most 2.

Proof: By Lemma 5.2, we see that $xx^\phi x^{\phi^2} = 1$ for all $x \in G$. Let $y = x^{-1}$, so that

$$y^{\phi^2} y^\phi y = 1$$

for all $y \in G$. Therefore

$$[x, x^\phi] = yy^\phi xx^\phi = x^{\phi^2} xx^\phi = 1.$$

Clearly if ϕ is fixed-point-free, then $\phi\tau_g$ is fixed-point-free, where τ_g is conjugation by g. Therefore x^g commutes with x^ϕ and x^{ϕ^2} for all g and x, and so x commutes with x^g.

We now note that G can have no elements of order 3: if it were to, then since x and x^ϕ commute, $\langle x, x^\phi \rangle$ is a ϕ-invariant elementary abelian of order 9, and contains a fixed point under ϕ, which is demonstrably impossible.

We finish by quoting a standard result. If G is a group such that $[g, x, x] = 1$ for all $g, x \in G$ and G contains no 3-torsion, then G is nilpotent of class at most 2. □

There is a substantial generalization of this theorem, which was Thompson's Ph.D. thesis.

Theorem 5.9 (Thompson) Suppose that a finite group G possesses a fixed-point-free automorphism ϕ of prime order. Then G is nilpotent.

This in turn rests upon Thompson's normal p-complement theorem.

Theorem 5.10 (Thompson, 1959) Let G be a group, and let p be an odd prime with $p \mid |G|$; write $P \in \mathrm{Syl}_p(G)$ and write $J^*(P)$ for the subgroup of P generated by all abelian subgroups of maximal rank. Then G has a normal p-complement if and only if both $\mathrm{C}_G(\mathrm{Z}(P))$ and $\mathrm{N}_G(J^*(P))$ have normal p-complements.

We will reduce Thompson's Theorem 5.9 to soluble groups first. We therefore assume that G is a minimal counterexample, and prove that G is soluble. If G is a 2-group, then G is nilpotent, and so choose q to be an odd prime dividing $|G|$, and let P denote a ϕ-invariant Sylow q-subgroup of G. Since both $Z = \mathrm{Z}(G)$ and $J = J^*(P)$ are characteristic in P, they are ϕ-invariant. If either Z or J is normal in G, then ϕ induces a fixed-point-free automorphism on G/Z or G/J, which are by induction nilpotent, and thus G is soluble.

The other possibility is that $\mathrm{N}_G(J)$ and $\mathrm{N}_G(Z)$ are both proper in G. By choice of minimal counterexample, both $\mathrm{C}_G(Z)$ and $\mathrm{N}_G(J)$ are nilpotent (as normalizers and centralizers of ϕ-invariant subgroups are ϕ-invariant), and so have normal q-complements. Therefore, G has a normal q-complement, say Q. Since Q is characteristic (a normal Hall q'-subgroup is characteristic) it is ϕ-invariant, and so is nilpotent by induction, and G is soluble.

For Thompson, this was enough, since the soluble case was proved by then. However, we haven't, and so let's do that now.

Theorem 5.11 Let G be a soluble group admitting a fixed-point-free automorphism of prime order. Then G is nilpotent.

Proof: Let ϕ be a fixed-point free automorphism of order p of the soluble group G, and let Q be a minimal ϕ-invariant normal subgroup of G (lying in $G \rtimes \langle\phi\rangle$). Then Q is an elementary abelian q-subgroup, and clearly $p \neq q$.

If G is a q-group, then G is nilpotent, so let $r \neq q$ be a prime dividing $|G|$, and let R be the ϕ-invariant Sylow r-subgroup. Consider the group QR; if $QR \neq G$, then by induction QR is nilpotent, and so Q and R centralize each other. This is true for all $r \neq q$ dividing $|G|$, and so $\mathrm{C}_G(Q)$ has index a power of q. Then $\mathrm{Z}(G) \neq 1$.

Thus $G = QR$ for some R. Let K be the subgroup of $\mathrm{Aut}(Q)$ induced by the action of R on it, and let H be the semidirect product of K by $\langle\phi\rangle$. Then it is clear that $k\phi$ acts fixed-point-freely and has the same order as ϕ itself, and so K fixes a point of R. Equivalently, there is a non-identity element $z \in Q$ such that $R \leqslant \mathrm{C}_G(z)$; clearly, $z \in \mathrm{Z}(G)$, and by induction $G/\mathrm{Z}(G)$ is nilpotent, whence G is nilpotent. □

We finish discussing fixed-point-free automorphisms with a result on the structure of groups of automorphisms all elements of which act fixed-point-freely.

Theorem 5.12 (Burnside) Let G be a finite group and suppose that G accepts a group A of automorphisms, each (non-trivial) element of which acts fixed-point-freely. Then $|G|$ and $|A|$ are coprime, and all Sylow p-subgroups of A are of p-rank 1.

Proof: Suppose that p divides both $|G|$ and $|A|$, and let ϕ be an element of A of order p. Then ϕ fixes a Sylow p-subgroup of G, and so acts fixed-point-freely on P. However, counting ϕ-orbits yields an easy contradiction.

Now let P be a Sylow p-subgroup of A, and let S be a subgroup of P of order p^2. We will show that S is cyclic, proving our result. We claim that G possesses an S-invariant Sylow q-subgroup Q, where $q \mid |G|$ is a prime. If this is true, then let $K = \mathrm{Z}(Q)$, and apply Corollary 5.5: then S is an homocyclic group of automorphisms of an abelian group K, whence it is cyclic, as required.

It remains to prove that if P is a p-group acting on a group G with $p \nmid |G|$, then there is a P-invariant Sylow q-subgroup Q for all primes q dividing $|G|$. To see this, let R be any Sylow q-subgroup of G, and write $H = G \rtimes P$. Then, by the Frattini argument, $H = \mathrm{N}_H(R)G$. A Sylow p-subgroup $\bar{P}$ of $\mathrm{N}_H(R)$ is a Sylow p-subgroup of H, and hence there is an element g such that $\bar{P}^g = P$. Then

$$P = \bar{P}^g \leqslant \mathrm{N}_H(R^g),$$

and so $Q = R^g$ is a P-invariant Sylow q-subgroup, finishing the proof. □

Since nilpotent groups are direct products of their Sylow p-subgroups, each of which is clearly characteristic, we see that we need to understand fixed-point-free automorphisms of p-groups. The nilpotency class was proved to be finite by Higman, and the bound below was given by Kreknin and Kostrikin.

Theorem 5.13 (Higman, Kreknin, Kostrikin) Let G be a nilpotent group possessing a fixed-point-free automorphism of order p. Then the nilpotency class is bounded by the function $h(p)$, where

$$h(p) \leqslant \frac{(p-1)^{2^{p-1}-1} - 1}{p-2}.$$

Chapter 6

The Critical Subgroup Theorem

Proposition 6.1 Let G be a group, and ϕ be an automorphism of G. Let $H = G \rtimes \langle \phi \rangle$ be the semidirect product of G and $\langle \phi \rangle$. Write $\bar{G}$ for the image of G in H, and similarly $\bar{\phi}$ for the image of ϕ in H. Then

$$\overline{\mathrm{C}_G(\phi)} = \mathrm{C}_{\bar{G}}(\bar{\phi}).$$

Proof: Suppose that we have the setup described in the proposition, and let $x \in \mathrm{C}_G(\phi)$. Write $\bar{x}$ for the image of x in H. We have $x\phi = x$, and so, inside H,

$$\bar{x}\bar{\phi} = (x, 1_{\langle\phi\rangle}) \cdot (1_G, \phi) = ((x\phi)1_G, \phi) = (x, \phi),$$

and

$$\bar{\phi}\bar{x} = (1_G, \phi) \cdot (x, 1_{\langle\phi\rangle}) = ((1_G\phi)x, \phi) = (x, \phi).$$

Thus $\bar{x} \in \mathrm{C}_{\bar{G}}(\bar{\phi})$.

Conversely, if $\bar{x} \in \mathrm{C}_{\bar{G}}(\bar{\phi})$, then $\bar{x}\bar{\phi} = \bar{\phi}\bar{x}$. But we calculated above what $\bar{x}\bar{\phi}$ and $\bar{\phi}\bar{x}$ are: they are

$$\bar{x}\bar{\phi} = (x\phi, \phi), \qquad \bar{\phi}\bar{x} = (x, \phi).$$

This clearly implies that ϕ centralizes x; that is, $x \in \mathrm{C}_G(\phi)$, as required. □

Notice that in a group $[x, y] = x^{-1}x^y$. If we identify x^y with $x\tau_y$, where τ_y represents conjugation by y, then we have a very good candidate for the notion of a commutator with an automorphism. We define

$$[x, \phi] = x^{-1}(x\phi).$$

Notice that $[x, \phi] = 1$ if and only if $x \in \mathrm{C}_G(\phi)$, which is analogous to the statement $[x, y] = 1$ if and only if $x \in \mathrm{C}_G(y)$, which holds for any group. Consider the group $G \rtimes \langle \phi \rangle$ again, and write $\bar{X}$ for the image of X in this semidirect product. We need

$$\overline{[x, \phi]} = [\bar{x}, \bar{\phi}].$$

The proof of this is in the exercises.

Suppose that this is true: what good does it do us? Well, all of the commutator relations that we have will work equally well for commutators involving automorphisms. For example, let $\phi \in \mathrm{Aut}(G)$ and $x, y \in G$. Then

$$[xy, \phi] = [x, \phi]^y [y, \phi].$$

To see this, take the image of $[xy, \phi]$ in $G \rtimes \langle \phi \rangle$, and calculate there. Since

$$\overline{[xy, \phi]} = [\bar{x}\bar{y}, \bar{\phi}],$$

we can use the fact that the identity works for the usual definition of commutator, and then pull back. In particular, it should be noted that the Three Subgroup Lemma still works with groups of automorphisms instead of subgroups: this is important, as it will be needed in this section.

We have an opportunity to test out our new notation in the next result.

Theorem 6.2 Let G be a finite group, and $A \leqslant \mathrm{Aut}(G)$ be a group of automorphisms. Suppose N a normal subgroup that is A-invariant, and suppose that $|N|$ and $|A|$ are coprime. Then

$$\mathrm{C}_{G/N}(A) = \mathrm{C}_G(A)N/N.$$

Proof: Suppose that xN is an element of $\mathrm{C}_G(A)N/N$; then $x \in \mathrm{C}_G(A)$, and so A acts trivially on x, so acts trivially on xN. Thus

$$\mathrm{C}_{G/N}(A) \geqslant \mathrm{C}_G(A)N/N.$$

It suffices to show the reverse inclusion; that is, we need to find an element $x \in \mathrm{C}_g(A)$ lying in every A-invariant coset gN of N. Proceed by induction on the number of factors of $|A|$, noting that the case where $|A|$ is a prime is clear: for then, gN is split up into orbits of size 1 or p, and the fact that $|N|$ and p are coprime proves that there is an orbit of size 1.

The proof of this will be omitted. □

Theorem 6.2 has an important corollary, for which we first need a defintion.

Definition 6.3 Let G be a finite group, and ϕ an automorphism of G. If

$$1 = H_0 \trianglelefteqslant H_1 \trianglelefteqslant \cdots \trianglelefteqslant H_i = G$$

is a series, then ϕ is said to *stabilize* the series if ϕ acts trivially on each H_i/H_{i-1}.

Corollary 6.4 Suppose that G is a finite group, and A is a group of automorphisms with $|G|$ and $|A|$ coprime. If A stabilizes some normal series, then $A = 1$.

Proof: Let

$$1 = H_0 \trianglelefteqslant H_1 \leqslant \cdots \trianglelefteqslant H_r = G$$

be a series, and suppose that $\phi \in A$ stabilizes this series. Then $H_1 \leqslant \mathrm{C}_G(\phi)$. We will show that if $H_i \leqslant \mathrm{C}_G(\phi)$, then $H_{i+1} \leqslant \mathrm{C}_G(\phi)$, proving the result, since if $G = \mathrm{C}_G(\phi)$, $\phi = 1$. Now if $H_i \leqslant \mathrm{C}_G(\phi)$, then (by Theorem 6.2)

$$H_{i+1}/H_i = \mathrm{C}_{H_{i+1}/H_i}(\phi) = \mathrm{C}_{H_{i+1}}(\phi)H_i/H_i = \mathrm{C}_{H_{i+1}}(\phi)/H_i,$$

since $H_i \leqslant \mathrm{C}_G(\phi) \cap H_{i+1}$. Thus

$$H_{i+1} = \mathrm{C}_{H_{i+1}}(\phi) \leqslant \mathrm{C}_G(\phi),$$

as required. □

Theorem 6.5 (Thompson's Critical Subgroup Theorem) Let G be a finite p-group. Then there is a characteristic subgroup C of G such that:

(i) every non-trivial p'-automorphism of G induces a non-trivial p'-automorphism on C;

(ii) $\mathrm{C}_G(C) = \mathrm{Z}(C)$;

(iii) $[G, C] \leqslant \mathrm{Z}(C)$ (or equivalently $[G, C, C] = 1$); and

(iv) C has class at most 2, and $C/\mathrm{Z}(C)$ is elementary abelian.

Proof: Suppose that A is a maximal abelian normal subgroup of G, and firstly assume that A is characteristic. Then, since $A = \mathrm{C}_G(A)$ (proof an exercise), we have (ii). Certainly,

$$[G, A] \leqslant A = \mathrm{Z}(A),$$

and so we have (iii). Any abelian subgroup satisfies (iv), and so we only need to satisfy (i). We will delay this, however, and deal with the case where A is not characteristic.

Suppose that A is a maximal abelian *characteristic* subgroup, and let B be a maximal normal abelian subgroup contianing it. Now $B \leqslant \mathrm{C}_G(A)$ and so $A \neq \mathrm{C}_G(A)$; since $A \operatorname{char} G$, we see that $\mathrm{C}_G(A) \operatorname{char} G$. We quotient out by A, then, and notice that $\mathrm{C}_G(A)/A$ is non-trivial. Let C be the preimage of the group

$$\Omega_1(\mathrm{C}_G(A)/A \cap \mathrm{Z}(G/A)) = \mathrm{C}_G(A)/A \cap \Omega_1(\mathrm{Z}(G/A)),$$

(which is non-trivial by Lemma 2.27).

Notice firstly that $\mathrm{C}_G(A)/A$ and $\Omega_1(\mathrm{Z}(G/A))$ are both characteristic in G/A, and therefore their intersection is also characteristic: hence $C \operatorname{char} G$. Now what is $\mathrm{Z}(C)$? Notice that $C \operatorname{char} G$, so

$$\mathrm{Z}(C) \operatorname{char} G$$

and since $\mathrm{Z}(C)$ is a characteristic abelian subgroup that contains A (since certainly A centralizes C), $A = \mathrm{Z}(C)$. Then $C/A \leqslant \Omega_1(\mathrm{Z}(G/A))$, and so is elementary abelian; hence C is of class 2, with $C/\mathrm{Z}(C)$ elementary abelian, proving (iv).

Let ϕ denote the quotient homomorphism from G into G/A. By Lemma 2.9, we have

$$([G, C])\phi = [G\phi, C\phi] = [G/A, C/A] \leqslant [G/A, \mathrm{Z}(G/A)] = 1,$$

and so $[G, C] \leqslant \ker \phi = A$, proving (iii). We are left to prove (ii). Let $X = \mathrm{C}_G(C)$; then we must show $X = A$. Now

$$\mathrm{Z}(C) = \mathrm{C}_C(C),$$

and so $\mathrm{C}_G(C) \cap C = A$.

Let us work in G/A. Then $X/A \cap C/A$ is trivial. We are aiming, in fact, to show that X/A itself is trivial. Now $X \trianglelefteqslant G$, so $X/A \trianglelefteqslant G/A$; if X/A were non-trivial, then it would intersect $\mathrm{Z}(G/A)$ non-trivially. By taking Ω_1, we must show that

$$X/A \cap \Omega_1(\mathrm{Z}(G/A)) = 1.$$

Now $X = \mathrm{C}_G(C) \leqslant \mathrm{C}_G(A)$, since every element of G that centralizes C must centralize A. Hence

$$X/A \cap \Omega_1(\mathrm{Z}(G/A)) \leqslant \mathrm{C}_G(A)/A \cap \Omega_1(\mathrm{Z}(G/A)) = C/A.$$

But $X/A \cap C/A = 1$, a clear contradiction. Thus $X = A$, and we have proved (ii). Thus in any case we have proved that there is a subgroup C satisfying (ii), (iii) and (iv). We will show that this subgroup satisfies (i),

Let A be a group of p'-automorphisms of G that act trivially on C. Then $[C, A] = 1$, so certainly $[C, A, G] = 1$. (We are clearly planning to use the Three Subgroup Lemma here!) Also, we know that $[G, C] \leqslant \mathrm{Z}(C)$, and since A acts trivially on C, A acts trivially on $\mathrm{Z}(C)$: this gives $[G, C, A] = 1$. Then the Three Subgroup Lemma gives

$$[A, G, C] = 1.$$

Then $[A, G] \leqslant \mathrm{C}_G(C) = \mathrm{Z}(C) \leqslant C$. Then we have a series

$$1 \trianglelefteqslant C \trianglelefteqslant G,$$

which A stabilizes. Hence, by Corollary 6.4, $A = 1$. Thus we have (i), and we are done. □

We let C, the characteristic subgroup of G in this theorem, be called the *critical subgroup*.

Chapter 7

How are p-Groups Embedded in Finite Groups?

Theorem 7.1 (Cayley) Let G be a group with a cyclic Sylow 2-subgroup P. Then G posseses a normal Hall $2'$-subgroup.

Proof: This is easy: consider the regular representation. Then a generator x for P is an odd permutation, and so G has a subgroup of index 2, the set of all even permutations. By induction, this subgroup has a normal (and hence characteristic) Hall $2'$-subgroup, and so G has a normal Hall $2'$-subgroup. □

Theorem 7.2 Let G be a soluble group, and suppose that G possesses a V_4 Sylow 2-subgroup P. Then G possesses a normal subgroup H of odd order such that G/H is either V_4 or A_4.

Proof: Let $H = \mathrm{O}_{2'}(G)$. Then G/H is a soluble group, and so has non-trivial Fitting subgroup, and this subgroup is a 2-group Q. If $|Q| = 4$ then G/Q is a subgroup of $\mathrm{Aut}(Q) = S_3$ of odd order, so is either trivial or C_3, and in the first case G/H is V_4 and in the second G/H is A_4. If $|Q| = 2$, then $\mathrm{Aut}(Q)$ is trivial, and this is a contradiction. □

More generally, if G is a soluble group is with abelian Sylow 2-subgroup then $G/\mathrm{O}_{2'}(G)$ is the extension of the abelian Sylow 2-subgroup by an odd subgroup of its automorphism group.

Proposition 7.3 Let G be the semidirect product of H by P. If x and y are conjugate in G then x and y are conjugate in P.

Proof: Let h be an element of H, and let x be an element of P. Then

$$x^h = h^{-1}xh = h^{-1}xhx^{-1}x = (h^{-1}h')x,$$

which lies in P precisely when $h = h'$, in which case h centralizes x. If $g \in G$, then $g = yh$ for some $y \in P$ and $h \in H$, whence x^g is $(x^y)^h$, and the result follows. □

The converse of Proposition 7.3 is also true, and it is a result of Frobenius.

Theorem 7.4 (Frobenius' Normal p-complement Theorem) Let G be a finite group, and let P be a Sylow p-subgroup. Then the following are equivalent:

(i) any two elements of P that are conjugate in G are conjugate in P; and

(ii) G possesses a normal Hall p'-subgroup.

We will not prove this theorem here, since it involves considerable finite group theory. We will discuss fusion briefly now, though.

Definition 7.5 Let H and K be subgroups of G with $H \leqslant K \leqslant G$. Then K is said to *control fusion* in H with respect to G if any two elements of H that are G-conjuate are also H-conjugate.

The following result of Burnside is well-known.

Proposition 7.6 (Burnside) Suppose that G is a finite group with an abelian Sylow p-subgroup P. Then $\mathrm{N}_G(P)$ controls fusion in P with respect to G.

Proof: Let x and y be elements of P, and suppose that there is $g \in G$ such that $x^g = y$. Thus

$$P^g \leqslant \mathrm{C}_G(x)^g = \mathrm{C}_G(x^g) = \mathrm{C}_G(y).$$

Thus both P and P^g are Sylow p-subgroups of $\mathrm{C}_G(y)$, whence they are conjugate by some element $h \in \mathrm{C}_G(y)$. Thus $P^{gh} = P$, and so $gh \in \mathrm{N}_G(P)$, and $x^{gh} = y$, as required. □

As a corollary of Frobenius' normal p-complement theorem, we get Burnside's normal p-complement theorem.

Corollary 7.7 (Burnside's Normal p-complement Theorem) Let G be a finite group, and let P be a Sylow p-subgroup of G. Suppose that P is contained within the centre of its normalizer. Then G possesses a normal Hall p'-subgroup.

Proof: Since P is abelian, $\mathrm{N}_G(P)$ controls fusion in P. Since P lies in the centre of its normalizer, all $\mathrm{N}_G(P)$-conjugacy classes of P are of size 1, and so actually P controls fusion in P. Hence, by Frobenius' normal p-complement theorem, G possesses a normal Hall p'-subgroup, as required. □

We can also easily get Cayley's result, given earlier in this chapter.

Corollary 7.8 Let G be a group with cyclic Sylow 2-subgroups. Then $\mathrm{O}_{2'}(G)$ has index a power of 2.

Proof: Let P denote a Sylow 2-subgroup of G, and recall that $\mathrm{Aut}(P)$ is a 2-group. Since $\mathrm{N}_G(P)/\mathrm{C}_G(P)$ is an odd-order subgroup of $\mathrm{Aut}(P)$, it is trivial, whence P lies in the centre of its normalizer. Thus $\mathrm{O}_{2'}(P)$ is a normal Hall $2'$-subgroup, as required. □

To demonstrate the fusion in finite groups, we prove the characterization of simpel groups of order 168. To do this, we need the following lemma.

Lemma 7.9 Let G be a subgroup of A_7 such that $|G|$ is a multiple of 14. Then $G = A_7$ or $G = \mathrm{GL}_3(2) = \mathrm{PSL}_2(7)$.

Proof: This proof is a case-by-case analysis. Since 14 divides $|G|$, we know that G contains a 7-cycle and a double transposition. Without loss of generality, we may assume that the 7-cycle x is $(1,2,3,4,5,6,7)$, and by raising x to an appropriate power, we may assume that $y = (1,2)(a,b)$.

To prove that $G = A_7$, it suffices to find an element of order 3 and an element of order 5, since then $|A_7 : G| \leqslant 4$. It originally appears as though there are ten possibilities for (a,b), but by relabelling we see that $(3,4)$ and $(6,7)$ yield isomorphic groups, as do $(4,5)$ and $(5,6)$. Again, relabelling and raising x to a power gives that $(3,7)$ and $(4,6)$ yield isomorphic groups, as do all four of the remaining pairs.

We reduce to the four possibilities $(3,4)$, $(3,5)$, $(3,7)$, and $(4,5)$. Three of these yield A_7, as outlined below.

(a,b)	Order 3	Order 5
$(3,4)$	$(x^3y)^2$	xy
$(3,7)$	$(x^2y)^2$	$[x,y]$
$(4,5)$	$[x,y]$	xy

Since $\mathrm{GL}_3(2)$ (whose order is a multiple of 14) acts on the seven non-zero vectors and it is a simple group, we must have that the remaining possibility is $\mathrm{GL}_3(2)$, as required. □

Theorem 7.10 Let G be a simple group of order 168. Then $G \cong \mathrm{GL}_3(2)$.

Proof: We will prove that G possesses a subgroup of index 7, whence the previous lemma will prove our result. (Note that this is equivalent to proving that G possesses a subgroup of index at most 7.) Therefore we will assume that the index of any proper subgroup of G is at least 8, and derive a contradiction.

Since G possesses no subgroups of index 3 or 7, the number of Sylow 2-subgroups is 21. Thus a Sylow 2-subgroup is self-normalizing, and so is non-abelian. Let P and Q denote distinct Sylow 2-subgroups, and consider $P \cap Q$. If this has order 4, then both P and Q normalize their intersection, and so the order of the normalizer of this intersection is at least 24, a contradiction. Thus the intersection of any two Sylow 2-subgroups is of order at most 2.

If the Sylow 2-subgroups of G were quaternion, then they must intersect trivially, else the normalizer of the intersection $P \cap Q$ would contain both P and Q, and so have order at least 24. However, in this case there must be $21 \times 7 = 147$ non-trivial elements lying in Sylow 2-subgroups. There are clearly eight Sylow 7-subgroups, contributing 48 elements of order 7, and so this contradiction implies that P is dihedral of order 8.

Let z denote the non-trivial central element of P. Then all conjugates of z lie in the centre of some Sylow 2-subgroup, and so there are at most 21 of them. Conversely, if some conjugate of z lies in two different Sylow 2-subgroups, then the centralizer of z has order at least 24, a contradiction. Thus $\mathrm{C}_G(z) = P$.

We will prove that there are no other elements of order 2 in G. If this is true, then the theorem follows easily from this: let R denote a subgroup of P isomorphic with V_4, and consider $\mathrm{N}_G(R)$, which we claim has order (at least) 24. Each Sylow 2-subgroup contains two V_4 subgroups, and either one of them (without loss of generality R) lies in two different Sylow 2-subgroups, or there are 42 different V_4 subgroups. However, each involution appears in exactly two V_4 subgroups, and so there are fourteen V_4 subgroups. Thus R lies in two different Sylow 2-subgroups, and so its normalizer had order at least 24, as required.

It remains to prove that there are exactly twenty-one elements of order 2, and we will prove this by counting. We have 48 elements of order 7, as seen above. There must also be at least eight Sylow 3-subgroups (since G possesses no subgroups of index less than 8), and so there must be twenty-eight Sylow 3-subgroups, yielding 56 elements of order 3. Together with the identity and 21 elements of order 2, that leaves 42 elements to find.

Let x denote an element of order 4 in P. Then $\mathrm{C}_G(x)$ has order an odd multiple of 4, but above we calculated the normalizers of the Sylow 3- and 7-subgroups. It was shown that 4 does not divide the order of the normalizer of either a Sylow 3- or a Sylow 7-subgroup, and so no odd element can centralize x. Thus there are 42 elements of order 4, and we have identified all elements of the group. □

Here we see a good example of Frobenius' normal p-complement theorem in action. The normalizer of a Sylow 3-subgroup has order 6, and since the centralizer of an involution has order 8, the Sylow 3-subgroups are self-centralizing. Therefore the two non-trivial elements in a Sylow 3-subgroup are conjugate, as predicted by Frobenius' theorem. All elements of

order 3 are conjugate, as are all elements of orders 2 and 4.

Finally, consider the elements of order 7. Then the normalizer of a Sylow 7-subgroup has order 21, and since no elements of order 3 centralize an element of order 7, we see that the Sylow 7-subgroups are self-centralizing as well. Let g be an element of order 7. Thus the normalizing element of order 3 must make g, g^2 and g^4 conjugate (as the automorphism group of order 3 of C_7 is generated by the map $g \mapsto g^2$), and make g^3, g^5 and g^6 conjugate. Thus there are two conjugacy classes of elements of order 7, each with 24 elements in it. Again, this agrees with Frobenius' theorem.

We can see that the simplicity of G causes great constraints on the fusion of conjugacy classes of p-elements. This is used extensively in finite group theory.