Topics in Finite p-groups

Martin van Beek

Contents

Chapter 0

Prerequisites

This space is used for recounting and revising some elementary group theory you should be reasonably familiar with. You may not have encountered everything in this chapter, but you should have all the tools to be able to understand the various definitions, and prove the various upcoming results. The content of this chapter will be used freely through the remainder of this course, and so anything that is unclear should be queried before moving onto the actual content of the course.

Definition 0.1. A (finite) group is a (finite) set G along with a binary operation (called a multiplication) $* : G \times G \to G$ satisfying the following properties:

(i) For each $x, y, z \in G$ we have that $(x * y) * z = x * (y * z)$.

(ii) There is $e \in G$ such that $x * e = e * x = x$ for all $x \in G$. Say that e is an *identity* element in G.

(iii) For each $x \in G$ there is $y \in G$ such that $x * y = y * x = e$. Say that y is an *inverse* of x.

We suppress the $*$ notation and represent multiplication of elements by concatenation. From now on, we will generally just say that "G is a group" without explicitly referring to the multiplication.

Proposition 0.2. *The following hold in a group G:*

(i) *G has a unique identify element, which we write as e.*

(ii) *For each $x \in G$, x has a unique inverse element, which we write x^{-1}.*

(iii) $(x^{-1})^{-1} = x$.

Definition 0.3. For G a group, $n \in \mathbb{N}$ and $x \in G$ we write $x^n = xx \ldots x$ with the convention that $x^0 = e$. By x^{-n} we mean $(x^{-1})^n$.

The order of G, written $|G|$, is the cardinality of the underlying set of G.

Let i be the smallest natural number such that $x^i = e$. Then i is the *order* of x. If no such number exists then x has infinite order.

In this course, we will primarily be concerned with finite groups and so every element will be of finite order.

Definition 0.4. Say H is a *subgroup* of G, written $H \leq G$, if H is a subset of G which is a group in its own right with the same multiplication, identity and inverses as G.

For $H, K \leq G$, the intersection of H and K, written $H \cap K$ is also a subgroup of G.

For S a non-empty subset of G, write $\langle S \rangle$ to be the subgroup *generated* by S. That is, $\langle S \rangle$ is the smallest subgroup of G containing S. You should check that $\langle S \rangle = \bigcap_{S \subseteq H \leq G} H$ so that $\langle S \rangle$ is well defined.

Definition 0.5. Let G be a finite groups. Then M is a *maximal subgroup* of G if M is a proper subgroup of G which is contained in no other proper subgroups of G.

Proposition 0.6. *The following are true for a finite group G:*

(i) *M is maximal in G if and only if $G = \langle M, x \rangle$ for any $x \in G \setminus M$.*

(ii) *If G contains has a unique maximal subgroup then G is a cyclic p-group.*

Definition 0.7. Let G, H be finite groups. Then a map $\phi : G \to H$ is a *homomorphism* if for all $g, h \in G$ we have that $\phi(gh) = \phi(g)\phi(h)$. A group *isomorphism* between G and H is a bijective homomorphism, and we say G and H are isomorphic, written $G \cong H$, if there exists an isomorphism between them.

For a finite group G, an *automorphism* of G is any isomorphism from G to itself. We denote the set of all automorphisms of G by $\mathrm{Aut}(G)$.

Proposition 0.8. *Let G, H be a finite groups and $\phi : G \to H$ be a homomorphism. Then the following hold:*

(i) *If e is the identity element of G, then $\phi(e)$ is the identity element in H.*

(ii) *For all $x \in G$ we have that $\phi(x^{-1}) = \phi(x)^{-1}$.*

(iii) *For $K \leq G$, $\phi(K)$ is a subgroup of H.*

(iv) *The set $\mathrm{Aut}(G)$ forms a group under composition of maps.*

Definition 0.9. Let G be a finite group with H a subgroup. Define an equivalence relation on the elements of G as follows: $g_1 \sim g_2$ if $g_1 g_2^{-1} \in H$ for any $g_1, g_2 \in G$. Write Hg for the equivalence class of G containing the element $g \in G$. The set $\{Hg \mid g \in G\}$ is the set of *right cosets* of H in G. Of course, $H = He$.

There is an analogous notion of *left cosets* given by the symbols gH. For each $g \in G$, the map $Hg \to g^{-1}H$ is a bijective mapping from the set of right cosets to left cosets of H in G.

Define the *index* of H in G, denoted $[G : H]$, to be the number of (right) cosets of H in G.

Proposition 0.10. *Let G be a finite group and $H \leq G$. Then*

(i) $|gH| = |H| = |Hg|$ *for all* $g \in G$*;*

(ii) $Hg_1 = Hg_2$ *if and only if* $g_2 g_1^{-1} \in H$*; and*

(iii) *if* $G = HS = \{hs \mid h \in H, s \in S\}$ *for some* $S \leq G$ *and* $S \cap H = \{e\}$*, then* $\{Hs \mid s \in S\}$ *is a complete set of right cosets for* H *in* G*.*

Theorem 0.11 (Lagrange's Theorem)**.** *Let G be a finite group and $H \leq G$. Then $|G| = |H|[G : H]$. In particular, the order of every subgroup (and of every element) of G divides the order of G.*

Definition 0.12. Let G be a finite group and X a set. Then a *(right) group action* of G on X is a map $\phi : X \times G \to X$ such that

(i) $\phi(x, e) = x$ for all $x \in X$; and

(ii) $\phi(\phi(x, g), h) = \phi(x, gh)$ for all $g, h \in G$ and $x \in X$.

If X is a set admitting a group action of G, then call X a G-set. Given a group action, we will often suppress the ϕ notation and write $x \cdot g$ to mean $\phi(x, g)$. Note that each g defines a bijection $X \to X$ by $x \mapsto x \cdot g$. This gives an embedding of G into the symmetric group on $|X|$ elements $\mathrm{Sym}(|X|)$.

There is also a notion of a left group action.

Definition 0.13. Let G be a finite group and X a G-set. Then say that G is:

(i) *trivial* on X if for all $x \in X$ and $g \in G$, we have that $x \cdot g = x$;

(ii) *transitive* on X if for all $x, y \in X$ there is $g \in G$ such that $x \cdot g = y$;

(iii) *faithful* on X if whenever $g \in G$ is such that $x \cdot g = x$ for all $x \in X$, we have that $g = e$; and

(iv) *fixed point free* on X if for all $x \in X$ whenever $g \in G$ is such that $x \cdot g = x$, we have that $g = e$.

Definition 0.14. Let G be a finite group and X a G-set. Let $x \in X$. Then the *orbit* of x under G, denoted $x \cdot G$, is the set $\{x \cdot g \mid g \in G\}$. The set of G-orbits of X forms a set of equivalence classes, and so partitions X. We can then realize a transitive action of G on X as an action with exactly one orbit.

The *fixed points* of X under $g \in G$, written $\mathrm{Fix}_X(g)$, are the elements of X whose orbits under G are singleton sets. This may be extended to subgroups of G e,g, for $H \leq G$, $\mathrm{Fix}_X(H) = \bigcap_{h \in H} \mathrm{Fix}_X(h)$. Clearly, $\mathrm{Fix}_X(g) = \mathrm{Fix}_X(\langle g \rangle)$.

For $x \in X$, define the *stabilizer* of x in G to be the set $\{g \in G \mid x \cdot g = x\}$. You should check that for all $x \in X$, this forms a subgroup of G, denoted $\mathrm{Stab}_G(x)$. Then for $Y \subseteq X$ we have that $\mathrm{Stab}_G(Y) := \bigcap_{x \in Y} \mathrm{Stab}_G(x)$ is also a subgroup of G.

Theorem 0.15 (Orbit–Stabilizer Theorem)**.** *Let G be a finite group and X a G-set. Then for all $x \in X$ we have that*

$$[G : \mathrm{Stab}_G(x)] = |x \cdot G|.$$

Theorem 0.16 (Burnside's Lemma)**.** *Let G be a finite group and X a G-set. Then the number of orbits in X under the action of G is equal to*

$$\frac{1}{|G|} \sum_{g \in G} \mathrm{Fix}_X(g).$$

Definition 0.17. Let $H \leq G$ and $x, g \in G$. Define $x^g := g^{-1}xg$ to be the conjugate of x by g, and similarly define $H^g = \{g^{-1}hg \mid h \in H\}$. Then $H^g \leq G$.

This allows us to state one more basic result regarding group actions.

Proposition 0.18. *Let G be a finite group and X a G-set. Then $x \in y \cdot G$ if and only if there is $g \in G$ such that $\mathrm{Stab}_G(x) = \mathrm{Stab}_G(y)^g$.*

Definition 0.19. Let G be a group. Then N is a *normal subgroup* of G, written $N \trianglelefteq G$, if $N^g = N$ for all G. In other words, $gN = Ng$ for all $g \in G$ so that the left and right cosets of N in G coincide.

Say that G is a *simple group*, if the only normal subgroups of G are itself and the trivial group $\{e\}$.

Proposition 0.20. *The following hold:*

(i) *For $N \trianglelefteq G$ the map $c_g : N \to N$ given by $c_g(x) = x^g$ is an isomorphism of N.*

(ii) *For $N \trianglelefteq G$, conjugation defines a (right) group action of G on N.*

(iii) *For $N, K \trianglelefteq G$, we have that $N \cap K \trianglelefteq G$.*

(iv) *For $H \leq G$, we have that $\bigcap\limits_{g \in G} H^g$ is the largest subgroup of H which is normal in G.*

(v) *For $H \leq G$, we have that $\langle H^G \rangle = \langle H^g \mid g \in G \rangle$ is the smallest normal subgroup of G containing H (called the normal closure of H in G).*

(vi) *A non-trivial abelian simple group is cyclic of order p, for some prime number p.*

Definition 0.21. Let G be a group. The *center* of G is $Z(G) := \{z \in G \mid zg = gz \text{ for all } g \in G\}$. G is *abelian* (or *commutative*) if $G = Z(G)$.

The center of a group G may be defined as the fixed points of the conjugation action of G on itself. It is also an example of a *characteristic subgroup* of G.

Definition 0.22. Say that H is a characteristic subgroup of G if $\phi(K) = K$ for all $\phi \in \mathrm{Aut}(G)$.

Definition 0.23. Let G be a group and $N \trianglelefteq G$. Then the left and right cosets of N in G coincide. Define a multiplication of these cosets by $(Ng).(Nh) = Ngh$. This forms a group multiplication on the set of cosets of N in G. Call this group the *quotient* of G by N, written G/N. Then N plays the role of the identity of this group, and $(Ng)^{-1} = Ng^{-1}$.

Proposition 0.24. *The following hold:*

(i) *For a homomorphism $\phi : G \to H$, $\ker\phi \trianglelefteq G$.*

(ii) *For $N \trianglelefteq G$, there exists a homomorphism $\phi : G \to \phi(G)$ with $N = \ker\phi$.*

We will often use variants of the *bar* convention. Let G be a finite group with $H \leq G$ and $N \trianglelefteq G$. Let $\overline{G} := G/N$. Then, even if $N \ntrianglelefteq H$, we can define $\overline{H}$ as HN/N. We can then also talk about the image of H under the quotient of G by N.

Proposition 0.25 (Correspondence Theorem)**.** *Let G be a finite group and $N \trianglelefteq G$. Then the map $G \to G/N$ defines a bijection between subgroups of G containing N and subgroups of G/N. Moreover, this bijection send normal subgroups of G containing N to normal subgroups of G/N.*

Definition 0.26. Let G be a finite group. Then a chain of subgroups

$$G_0 = \{e\} \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

such that G_i/G_{i-1} is a non-trivial simple group for $i \in \{1, \ldots, n\}$ is called a *composition* series of G. Call the terms G_i/G_{i-1} the *composition factors* of the composition series.

Form a chain of subgroups

$$G_0 = \{e\} \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

with $G_{i-1} < G_i$ for all $i \in \{1, \ldots, n\}$. Suppose that whenever $G_{i-i} \leq H < G_i$ and $H \trianglelefteq G$, we have that $G_{i-1} = H$ for all $i \in \{1, \ldots, n\}$. Then this chain is called a *chief series* of G. Call the terms G_i/G_{i-1} the *chief factors* of the chief series.

Theorem 0.27 (Jordan–Hölder Theorem)**.** *Let G be a finite group. Then the following hold:*

(i) *G has a composition series;*

(ii) *any two composition series for G are the same length; and*

(iii) *the composition factors of G are uniquely determined. That is, if*

$$G_0 = \{e\} \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

and

$$H_0 = \{e\} \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

are two composition series for G, then there is a bijection $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ such that $G_i/G_{i-1} \cong H_{\sigma(i)}/H_{\sigma(i)-1}$.

Furthermore, all the above points hold replacing "composition" by "chief."

We now give the "isomorphism theorems" for finite groups.

Theorem 0.28 (First Isomorphism Theorem)**.** *Let G and H be a finite groups and $\phi : G \to H$ a homomorphism. Then $G/\ker\phi \cong \phi(G)$.*

Theorem 0.29 (Second Isomorphism Theorem)**.** *Let G be a finite group with $H \leq G$ and $K \trianglelefteq G$. Then $HK/K \cong H/H \cap K$.*

Theorem 0.30 (Third Isomorphism Theorem)**.** *Let G be a finite group and $H, K \trianglelefteq G$ with $K \leq H$. Then $(G/K)/(H/K) \cong G/H$.*

We give a short (and non-rigorous) overview of *group presentations.*

Definition 0.31. Let S be a set and suppose that for every symbol $s \in S$ there is a corresponding "inverse" symbol. Write S^{-1} for the set of "inverses" of S and form $T = S \cup S^{-1}$.

The *free group* on S, denoted F_S, is the group given by strings of elements of T. Multiplication is concatenation of strings (called *words*) and the *empty word*, that is the word composed of no elements of T which we occasionally write e, plays the role of the identity. For $s \in S$ there is $s^{-1} \in S^{-1} \subseteq T$ and we define $ss^{-1} = e$. Finally, we write $s^n = \underbrace{s \ldots s}_{n \text{ times}}$.

Let R be a subset of F_S and set $\langle\langle R \rangle\rangle$ be the normal closure of R in F_S (that is, the smallest normal subgroup of F_S containing R). Then the group $\langle S \mid R \rangle$ is the quotient $\mathrm{F}_S/\langle\langle R \rangle\rangle$. Call S the *generators* of $\langle S \mid R \rangle$ and R the *relators.*

Say that $\langle S \mid R \rangle$ is a *presentation* of a group G if $G \cong \langle S \mid R \rangle$. We will often identify S and R with subsets of G under this isomorphism. In this way, G is generated by S in the manner defined earlier.

For group presentations, we will often favor *relations* over relators. Suppose G has presentation $\langle S \mid R\rangle$. Given a word $r \in R$, the image of r in $\langle S \mid R\rangle$ is trivial and so r is equivalent to e in the quotient of F_S by $\langle\langle R\rangle\rangle$. That is r is equivalent to e in the group G, written $r =_G e$. This is an example of a *relation*.

Suppose that $r = ab \in R$. Then we may replace the statement $r =_G e$ by $a =_G b^{-1}$ or $b =_G a^{-1}$. These are all equivalent relations. A *relation* for us is then an expression $w_1 =_G w_2$ where $w_1, w_2 \in \mathrm{F}_S$ are equivalent in G.

Going the other way, we see that for any two words $w_1, w_2 \in \mathrm{F}_S$, we have that $w_1 =_G w_2$ if and only if $w_1 w_2^{-1} =_G e$ and so each relation corresponds to a relator. We will often write $G = \langle S \mid R^*\rangle$ where R^* is a collection of relations which give rise to the relators R, and we will often suppress $=_G$ to $=$.

Example 0.32. *Let G be a cyclic group of order n. Let $S = \{a\}$, $R = \{a^n\}$ and $R^* = \{a^n = e\}$. Then $G = \langle S \mid R\rangle = \langle S \mid R^*\rangle$.*

We return to the study of conjugation within a finite group G.

Definition 0.33. Let G be a finite group and $H \leq G$. Then the *normalizer* of H in G, written $N_G(H)$, is the subset $\{g \in G \mid H^g = H\}$. Then $N_G(H)$ is a subgroup of G containing H. In fact, $N_G(H)$ is the largest subgroup of G in which H is normal. Note that $x \in N_G(H)$ if and only if $\langle x\rangle \leq N_G(H)$.

Then *centralizer* of H in G, written $C_G(H)$, is the subset $\{g \in G \mid h^g = h \text{ for all } h \in H\}$. Then $C_G(H)$ is a subgroup of G and $H \cap C_G(H) = Z(H)$. Note that $x \in C_G(H)$ if and only if $\langle x\rangle \leq C_G(H)$. Define $C_G(x) = \{g \in G \mid x^g = x\}$ so that $C_G(x) = C_G(\langle x\rangle)$. Observe that for $H, K \leq G$, $H \leq C_G(K)$ if and only if $K \leq C_G(H)$.

Finally, for $H, K \in G$, we write $N_H(K) = N_G(K) \cap H$ and $C_H(K) = C_G(K) \cap H$.

Definition 0.34. Let G be a finite group and $H \leq G$. Then $N_G(H)$ acts on H by conjugation. This defines a map $\phi : N_G(H) \to \mathrm{Aut}(H)$ given by $g \mapsto c_g$ where $c_g(h) = h^g$ for $g \in N_G(H)$ and all $h \in H$. Write $\mathrm{Aut}_G(H)$ for the image of ϕ. We recognize $\ker(\phi) = C_G(H)$ so that, by the first isomorphism theorem, $N_G(H)/C_G(H) \cong \mathrm{Aut}_G(H) \leq \mathrm{Aut}(H)$.

Taking $G = H$ in the above definition we get that $G/Z(G) \cong \mathrm{Aut}_G(G) =: \mathrm{Inn}(G)$, the *inner automorphism group* of G. One can verify that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

The *outer automorphism group* of G, denoted $\mathrm{Out}(G)$, is the quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$. An element of $\mathrm{Aut}(G)$ which is not contained in $\mathrm{Inn}(G)$ is (rather confusingly) referred to as an *outer automorphism* of G.

Definition 0.35. Suppose that G is a finite group and $H, K \leq G$. Define $HK = \{hk \in G \mid h \in H, k \in K\}$ to be the product of H and K in G. Then $H, K \subseteq HK \subseteq G$. However, if $H \leq N_G(K)$ then HK is a subgroup of G.

Definition 0.36. Let G be a finite group and $H, K \leq G$. Then G is an *internal* direct product of H and K if $G = HK$, $H \leq C_G(K)$ and $H \cap K = \{e\}$.

Let H and K be finite groups. Then the *external direct product* of H and K, denoted $H \times K$, is the group with underlying set $\{(h,k) \mid h \in H, k \in K\}$ (the Cartesian product of H and K) with multiplication $(h_1,k_1)(h_2,k_2) = (h_1h_2, k_1k_2)$.

The external direct product and internal direct product of H and K give isomorphic groups and so we will often identify G with $H \times K$, where $H \leq G$ is identified with the subset $\{(h,e) \mid h \in H\}$ of $H \times K$ and $K \leq G$ is identified with $\{(e,k) \mid k \in K\}$.

Definition 0.37. Let G be a finite group and $H, K \leq G$. Then G is an *internal* semidirect product of H and K if $G = HK$, $H \leq N_G(K)$ (so that $K \trianglelefteq G$) and $H \cap K = \{e\}$.

Now let H and K be finite groups such that there is a homomorphism $\phi : H \to \mathrm{Aut}(K)$. Then the *external semidirect product* of H and K with respect to ϕ, denoted $K \rtimes_\phi H$, is the group with underlying set $\{(h,k) \mid h \in H, k \in K\}$ (the Cartesian product of H and K) with multiplication $(k_1,h_1)(k_2,h_2) = (k_1(\phi(h_1)(k_2)), h_1h_2)$. Taking ϕ to be the trivial map gives the external direct product of H and K.

Note that we may identify with external semidirect with an internal semidirect product taking the subgroups $K \times \{e\} \trianglelefteq K \rtimes_\phi H$ and $\{e\} \times H$, which are isomorphic to K and H respectively, in the definition. On the other hand, in the internal construction, since $H \leq N_G(K)$ we have a map $\theta : H \to \mathrm{Aut}(K)$ which allows us to define an external semidirect product $K \rtimes_\theta K$ which is isomorphic to G.

Proposition 0.38 (Dedekind Modular Law)**.** *Let G be a finite group, with $H \leq G$, $U \leq K \leq G$ and $U \leq N_G(H)$. Then $U(H \cap K) = K \cap UH$.*

We close the prerequisites with a short survey on *commutators* in finite groups.

Definition 0.39. Let G be a finite group and $x, y \in G$. Then the commutator of x and y is $[x,y] := x^{-1}y^{-1}xy \in G$. For $H, K \leq G$, we set $[H,K] := \langle [h,k] \mid h \in H, k \in K\rangle$. The group $G' := [G,G]$ will be referred to as the *derived subgroup* of G.

Proposition 0.40. *The following hold:*

(i) $G' \trianglelefteq G$.

(ii) *G/G' is abelian and for any $N \trianglelefteq G$ with G/N abelian, we have that $G' \leq N$. In particular, for any $G' < M \leq G$, we have that $M \trianglelefteq G$ and G/M is abelian.*

(iii) *For $H, K \leq G$ we have that $H \leq N_G(K)$ if and only if $[H,K] \leq K$. Moreover, $H \leq C_G(K)$ if and only if $[H,K] = \{e\}$.*

Proposition 0.41 (Commutator Identities)**.** *For all $x, y, z \in G$, the following hold:*

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

(ii) $[x,zy] = [x,y].[x,z]^y$ *and* $[xz,y] = [x,y]^z[z,y]$.

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

(iv) $[[x, y], z^x].[[z, x], y^z].[[y, z], z^y] = e$.

Let $H, K, L \leq G$ *and* $N \trianglelefteq G$. *If* $[[H, K], L] \leq N$ *and* $[[L, H], K] \leq G$, *then* $[[K, L], H] \leq N$.

In this course, we will omit certain brackets in commutators, reading them left to right i.e. $[H, K, L] = [[H, K], L]$. Moreover, for $n \in N$ and $x, y \in G$ the notation $[x, y; n]$ will mean $[x, \underbrace{y, \ldots, y}_{n \text{ times}}]$.

Chapter 1

Introduction to p-groups

Throughout this course, we will be interested in finite p-groups purely on their own merit. Of course, in analyzing their automorphisms some other finite groups will come into play, but in this course we will not even begin to do any kind of justice to the theory of finite p-groups' applicability and pervasiveness in mathematics. I'll take this space to list three directions in which the theory of finite p-groups plays a fundamental role which are of particular interest to me, but there is much more to discover.

Finite p-groups affect the structure of all finite groups. Indeed, most of the proof of the classification of the finite simple groups analyzed how finite p-groups embed in a target finite simple group to recover global information about the group. The following theorem is very classical (it dates back to at least 1911).

Theorem (Burnside's Theorem)**.** *Suppose that G is a finite group with a cyclic Sylow 2-subgroup. Write $|G| = 2^m q$ where $m \in \mathbb{N}_0$ and q is odd. Then G has a unique (so necessarily characteristic) subgroup of order q. In particular, no non-abelian finite simple group has a cyclic Sylow 2-subgroup.*

Not only do finite p-groups impact the internal structure of all finite groups, they also affect how groups act (via their representation theory).

Conjecture (McKay Conjecture (1972))**.** *Suppose that G is a finite group with a Sylow p-subgroup P. Write $\mathrm{Irr}_{p'}(G)$ for the set of complex characters of G of degree coprime to p. Then*

$$|\mathrm{Irr}_{p'}(G)| = |\mathrm{Irr}_{p'}(N_G(P))|.$$

The conjecture was proved in the case where $p = 2$ in 2015 by Malle and Späth.

As a final example, finite p-groups are pervasive in the mod p-cohomology of finite groups.

Theorem (Cartan–Eilenberg Stable Elements Method (1956))**.** *Suppose that G is a finite group with Sylow p-subgroup S. Then $H^*(G; \mathbb{F}_p)$ injects into $H^*(S; \mathbb{F}_p)$. Further-*

more, we may identify $H^*(G;\mathbb{F}_p)$ with $H^*(S;\mathbb{F}_p)^G$: the subring of $H^*(S;\mathbb{F}_p)$ invariant under the action of G.

1.1 Basic Definitions and Results

Definition 1.1. A p-group is a group in which all elements have order a power of p, where p is a prime number.

We port the various prefixes, or suffixes, attached to groups to p-groups e.g. a finite p-group is a group which is simultaneously a finite group and a p-group, and a normal p-subgroup of a group is a normal subgroup which is also a p-group.

You may have come across the following theorem in an earlier course on group theory. Indeed, this is a key ingredient in several approaches to the proof of Sylow's theorems.

Theorem 1.2 (Cauchy's Theorem). *Let G be a finite group and p a prime. If p divides $|G|$, then G has an element of order p.*

Proof. Let $X = \{(x_1, \ldots, x_p) \in G^p \mid x_i \in G, x_1x_2\ldots x_p = e\}$. Then $x_p = (x_1 \ldots x_{p-1})^{-1}$ and so it follows that $|X| = |G|^{p-1}$. Furthermore, this also implies that every cyclic permutation of $(x_1, \ldots, x_p)$ belongs to X. This induces an action of C_p on the set X. By the Orbit-Stabilizer theorem, C_p has orbits of length 1 and p on X. The orbits of length 1 look like the tuples $(x, \ldots, x)$. If x is not the identity element, then we deduce that $x^p = e$ and x has order p.

Hence to prove the result, we may assume, aiming for a contradiction, that the orbits of C_p on X have length p, or is a singleton set consisting of the element $(e, \ldots, e)$. But now, X is a disjoint union of these orbits from which we conclude that $|X| = rp + 1$ for some $r \in \mathbb{N}$. But then $|X|$ is coprime to p, a contradiction since $|X| = |G|^{p-1}$ is divisible by p. This completes the proof. □

Proposition 1.3. *G is a finite p-group if and only if $|G| = p^a$ for some $a \in \mathbb{N}_0$.*

Proof. Assume first that G is a finite p-group. Aiming for a contradiction, assume that $|G| = p^a q$ where $q > 1$ is coprime to p. Then by Theorem 1.2, for some prime number $r \neq p$ with q divisible by r, G has an element of order r. Since G is a p-group, this is a contradiction.

Assume now that $|G| = p^a$ for some $a \in \mathbb{N}_0$. Let $x \in G$. Then $\langle x \rangle$ has order p^b for some $b \in \mathbb{N}_0$ with $b \leqslant a$ by Lagrange's theorem. Hence, x has p-power order, and the result holds. □

In this course, we will be primarily focused on finite p-groups. However, several of the results we prove will hold in a more general setting.

We first note that finite p-groups are *extension closed* in the following sense:

Proposition 1.4. *Let G be a finite group. If $N \trianglelefteq G$ such that both N and G/N are p-groups, then G is a p-group.*

Proof. Since $|G| = |G/N||N|$ and both G/N and N are p-groups, the result holds by Proposition 1.3. □

In the other direction, finite p-groups are also subgroup and quotient closed.

Proposition 1.5. *Let G be a finite p-group. Then every subgroup of G, and every quotient of G, is also a p-group.*

Proof. Let G be a finite p-group. Then by Proposition 1.3, $|G| = p^a$ for some $a \in \mathbb{N}_0$. Let $H \leq G$ so that by Lagrange's theorem, $|H| = p^b$ for some $b \in \mathbb{N}_0$ with $b \leqslant a$. Then another application of Proposition 1.3 implies that H is a p-group.

Let $N \trianglelefteq G$ so that $|N| = p^c$ for some c which divides a. Then

$$|G/N| = \frac{|G|}{|N|} = \frac{p^a}{p^c} = p^{a-c}$$

and as $a-c \in \mathbb{N}_0$, a final application of Proposition 1.3 implies that G/N is a p-group. □

This is actually the key idea we shall use in lots of the upcoming proofs, as it facilitates the use of induction arguments. A potentially interesting exercise is to go through some of the proofs in this course and replace finite p-groups with some other suitable family of groups which is subgroup and quotient closed e.g. *solvable groups.*

To exploit that finite p-groups are quotient closed in induction arguments, we need some normal subgroups to quotient G by.

Theorem 1.6. *Let G be a non-trivial finite p-group. Then $Z(G) \neq \{e\}$.*

Proof. Let G be a non-trivial finite p-group. Then G induces an action on its underlying set by conjugation. By the Orbit-Stabilizer theorem, the orbits of this action have length some power of p. Since the identity element is fixed under this action, there is some orbit of length 1. Since the set of non-identity elements of G has cardinality $p^a - 1$ for some $a \in \mathbb{N}$, and $p^a - 1$ is coprime to p, there must exist some $x \in G \setminus \{e\}$ that lies in an orbit of length 1, and so x is fixed by the action of G. In other words, $g^{-1}xg = x$ for all $g \in G$, from which we conclude that $x \in Z(G)$ and $Z(G) \neq \{e\}$. □

Exercise 1.7. Let G be a non-trivial finite p-group with $N \trianglelefteq G$. Then $N \cap Z(G) \neq \{e\}$.

Corollary 1.8. *All groups of order p^2 are abelian.*

Proof. Let G be a finite group with $|G| = p^2$. By Theorem 1.6 and Lagrange's theorem, we have that $|Z(G)| \in \{p, p^2\}$. If $|Z(G)| = p$, then for any $x \in G \setminus Z(G)$ and any $g \in G$, we have that $g = x^a z$ for some $0 \leqslant a < p$ and some $z \in Z(G)$. Then for $g_1, g_2 \in G$, we have that

$$g_1 g_2 = x^{a_1} z_1 x^{a_2} z_2 = z_2 x^{a_1+a_2} z_1 = z_2 x^{a_2} x^{a_1} z_1 = x^{a_2} z_2 x^{a_1} z_1 = g_2 g_1$$

for some $0 \leqslant a_1, a_2 < p$ and $z_1, z_2 \in Z(G)$, and G is abelian, a contradiction. Hence, $|Z(G)| = |G| = p^2$ so that $G = Z(G)$ is abelian, as desired. □

While the center is generally a good candidate to quotient by, p-groups tend to have lots of normal subgroups which lie in nice configurations.

Theorem 1.9. *Let G be a non-trivial finite p-group of order p^n. Then there is a chain of subgroups $\{e\} = G_0 < G_1 < \cdots < G_n = G$ such that $G_i \trianglelefteq G$ and $|G_i/G_{i-1}| = p$ for $1 \leqslant i \leqslant n$.*

Proof. The results clearly holds when G is a finite group of order p. So let G be a non-trivial finite p-group of order at least p^2, chosen such that G is a counterexample to the theorem with respect to order. Let $Z \leq Z(G)$ such that $|Z| = p$. Then $Z \trianglelefteq G$ and $p^{n-1} = |G/Z| < |G| = p^n$. By induction, there is $H_j \trianglelefteq G/Z$ with $H_0 = \{Z\}$, $H_{n-1} = G/Z$ and $|H_j/H_{j-1}| = p$ for $1 \leqslant j \leqslant n-1$.

Set $G_0 := \{e\}$ and G_i to be the preimage in G of H_{i-1}. Since there is a correspondence between the normal subgroups of G containing G_1 and the normal subgroups of G/G_1, we have that $G_i \trianglelefteq G$. Moreover, by the third isomorphism theorem

$$p = |H_{i-1}/H_{i-2}| = |(G_i/Z)/(G_{i-1}/Z)| = |G_i/G_{i-1}|$$

for $2 \leqslant i \leqslant n$, and we clearly have that $G_1/G_0 \cong G_1 = Z$ has order p. □

Exercise 1.10. Let G be a non-trivial finite p-group of order p^n with $N \trianglelefteq G$ of order p^a for some $a, n \in \mathbb{N}$ with $a \leqslant n$. Show the above chain of normal subgroups may be constructed so that $N = G_a$.

1.2 Central Series

For the following, it may help to have some familiarity with commutators and to recall the definition of the *derived subgroup* of G.

Lemma 1.11. *Let G be a non-trivial finite p-group and $\{e\} < H \trianglelefteq G$. Then $[G, H] < H$. In particular, $G' < G$.*

Proof. Let G be a non-trivial finite p-group and $H \trianglelefteq G$. Moreover, choose G such that G is a counterexample to the first statement of the lemma minimal with respect to order.

By Exercise 1.10 we can arrange that there is $K \trianglelefteq G$ with $|H/K| = p$. By minimality of G, we have that $[G/K, H/K] = \{K\}$. From this, it follows that $[G, H] \leq K < H$, a contradiction since G is a counterexample. Hence, no such counterexample exists and so the first statement holds. The second statement follows from the first taking $H = G$. □

By the above lemma, it is clear that taken repeated derived subgroups of a finite p-group G eventually terminates in the trivial group. This gives rise to a series of groups: the *derived series* of G.

Definition 1.12. Let G be a finite p-group. Set $G^{(0)} := G$ and $G^{(i)} := [G^{(i-1)}, G^{(i-1)}]$ for $i \in \mathbb{N}$. Set $n \in \mathbb{N}$ the smallest natural number such that $G^{(n)} = \{e\}$. Then the *derived series* of G is the chain of subgroups

$$\{e\} = G^{(n)} < G^{(n-1)} < \cdots < G' = G^{(1)} = G^{(0)} = G.$$

Of course, one need not restrict themselves to finite p-groups to make the above definition. Indeed, one can make such a definition for groups in which the series never terminates at the identity group. Groups in which taking repeated derived subgroups terminates in the trivial group in a finite number of steps are referred to as *solvable* (or soluble) groups. This class of groups is also subgroup and quotient closed, but is a much larger class of groups than finite p-groups.

There are other series to consider which narrow down the structure of a finite p-group among other finite groups. Namely, the various central series of a finite p-group.

Definition 1.13. Let G be a group. Then a central series of G is any chain of subgroups

$$\{e\} = G_0 < G_1 < \cdots < G_n = G$$

such that $[G, G_i] \leq G_{i-1}$ for $i \in \{1, \ldots, n\}$.

An arbitrary group need not have a central series. The groups which do have a central series are referred to as *nilpotent groups*. Comparing definitions, we see that every nilpotent group is also solvable. On the other hand, from the definition it is clear that a nilpotent group always has a non-trivial center, and this need not be true for even small examples of solvable group e.g. the symmetric group of degree 3.

We highlight two particular useful central series of a nilpotent group.

Definition 1.14. Let G be a non-trivial finite p-group. Set $\gamma_1(G) := G$ and $\gamma_i(G) := [G, \gamma_{i-1}(G)]$ for $i \in \mathbb{N}$. Let c be the smallest natural number such that $\gamma_{c+1}(G) = \{e\}$. Then the *lower central series* of G is the chain of subgroups

$$\{e\} = \gamma_{c+1}(G) < \gamma_c(G) < \cdots < G' = \gamma_2(G) < \gamma_1(G) = G.$$

That such a chain, and a natural number c, exists follows from Lemma 1.11 and observing that whenever $H \trianglelefteq G$, $[G, H] \trianglelefteq G$.

Definition 1.15. Let G be a non-trivial finite p-group. Set $Z_0(G) := \{e\}$, $Z_1(G) := Z(G)$ and $Z_i(G)$ to be the preimage in G of $Z(G/Z_{i-1}(G))$. Set c to be the smallest natural number such that $Z_c(G) = G$. Then the *upper central series* of G is the chain of subgroups

$$\{e\} = Z_0(G) < Z_1(G) = Z(G) < \cdots < Z_{c-1}(G) < Z_c(G) = G.$$

Of course, in making this definition we are heavily relying on Theorem 1.6. The upper and lower central series of G are the extremal central series of G in the following sense.

Proposition 1.16. *Let G be a non-trivial finite p-group. Suppose that*

$$\{e\} = G_0 < G_1 < \cdots < G_{n-1} < G_n$$

is a central series for G for some $n \in \mathbb{N}$. Then $G_i \leq Z_i(G)$ and $\gamma_{i+1}(G) \leq G_{n-i}$ for all $i \in \{0, \ldots, n\}$. In particular, the length of the upper central series and the lower central series is the same.

Proof. We will first show that $G_i \leq Z_i(G)$ for all $i \in \{0, \ldots, n\}$. The result is clearly true for $i \in \{0, 1\}$. Aiming for a contradiction, assume there is $i \in \mathbb{N}$ such that $G_i \not\leq Z_i(G)$ and choose i minimally with respect to this. Then $[G_i, G] \leq G_{i-1} \leq Z_{i-1}(G)$. In particular, $G_iZ_{i-1}(G)/Z_{i-1}(G) \leq Z(G/Z_{i-1}(G))$ from which we deduce that $G_i \leq Z_i(G)$, a contradiction. Hence, no such i exists and so $G_i \leq Z_i(G)$ for all $i \in \{0, \ldots, n\}$.

We will now show that $\gamma_{i+1}(G) \leq G_{n-i}$ for all $i \in \{0, \ldots, n\}$. We have that $\gamma_1(G) = G = G_n$ and $\gamma_2(G) = G' \leq G_1$ and so the result holds for $i \in \{0, 1\}$. As above, aiming for a contradiction, assume that there is $i \in \mathbb{N}$ such that $\gamma_{i+1}(G) \not\leq G_{n-i}$ and choose i minimal with respect to this. Then $\gamma_i(G) \leq G_{n-i+1}$. But then $\gamma_{i+1}(G) = [\gamma_i(G), G] \leq [G_{n-i+1}, G] \leq G_{n-i}$, a contradiction. Hence, no such i exists and so $\gamma_{i+1}(G) \leq G_{n-i}$ for all $i \in \{0, \ldots, n\}$.

Suppose that the lower central series of G has length $c + 1$ (so that $\gamma_{c+1}(G) = \{e\}$ but $\gamma_c(G) \neq \{e\}$) and that the upper central series of G has length $b + 1$ (so that $Z_{b-1}(G) < Z_b(G) = G$). We have shown that $\gamma_{c+1-i}(G) \leq Z_i(G)$ for all $i \in \{0, \ldots, b\}$ and that $\gamma_{i+1}(G) \leq Z_{b-i}(G)$ for all $i \in \{0, \ldots, b\}$. Assume that $b < c$. Then

$$\{e\} = \gamma_{c+1}(G) < \gamma_{b+1}(G) \leq Z_b(G) = \{e\},$$

absurd. Thus, we must have that $c \leqslant b$. If $c < b$ then

$$G = \gamma_1(G) = \gamma_{c+1-c}(G) \leq Z_c(G) < Z_b(G) = G,$$

yet another contradiction. Hence, we conclude that $b = c$ and the result holds. □

It follows from the above that the lower and upper central series have the fewest number of terms possible in a central series of G. Thus, we are motivated to make the following definition.

Definition 1.17. Let $c+1$ be the length of the upper or lower central series of G so that $\gamma_c(G) = \{e\}$ and $Z_c(G) = G$. Then c is the *nilpotency class* of G.

Everyone should be reasonably familiar with the finite groups of nilpotency class 1. These are abelian groups! Some effort has been expended to understand the finite p-groups of small nilpotency class. On the other hand, the effort to "classify" all finite groups made use of *coclass*, defined as $n-c$ for a p-group of order p^n and nilpotency class c. This is a deep theory, ultimately concluding in the proofs of the so called "coclass conjectures" in the setting of pro-p groups and using various techniques. We will not adopt this viewpoint in this course.

While not used in this course, it is a fun exercise to show that a finite nilpotent group is a direct product of finite groups, each of which is an r-group for some prime r. Hence, a nilpotent group has unique Sylow p-subgroups for every prime p dividing the order of the group, and the group may be completely understood by understanding each of these Sylow p-subgroups. Unlike p-groups, nilpotent groups are *not* extension closed.

Proposition 1.18. *Let G be a finite p-group and $H < G$. Then $H < N_G(H)$.*

Proof. Let G be a finite p-group and choose G to be a counterexample to the proposition minimal with respect to order. Let $H < G$ with $H = N_G(H)$. Since $Z(G)$ normalizes H, we have that $Z(G) \leq H$.

If there is M a maximal subgroup of G properly containing H, then by minimality of G, we have that $H < N_M(H) \leq N_G(H)$, a contradiction. Hence, H is a maximal subgroup of G.

Now, $H/Z(G)$ is a maximal subgroup of $G/Z(G)$ and so, by the minimality of G, $H/Z(G) \trianglelefteq G/Z(G)$. Since normal subgroups of G containing $Z(G)$ correspond to normal subgroups of $G/Z(G)$ and $Z(G) \leq H$, we see that $H \trianglelefteq G$, another contradiction. Hence no counterexample exists and the proposition holds. □

In other words, in finite p-groups "normalizers grow." The above proof can be adapted very slightly to prove that normalizers grow in all finite nilpotent groups.

1.3 Extra Bits

We shall end this chapter with some definition we will require later in the course (and which are fundamental in lots of aspects of group theory).

Definition 1.19. Let G be a finite p-group. Then G is *elementary* if G has exponent p. G is then *elementary abelian* if G is isomorphic to a direct product of cyclic groups of order p.

We note that if G is elementary abelian of order p^n, then we may identify G with an n-dimensional vector space over the field $\mathbb{F}_p$. Under these circumstances, we say that G has *rank* n.

Definition 1.20. Let G be a finite p-group. Then the *p-rank* of G, denoted $m_p(G)$, is the maximum rank among all elementary abelian subgroups of G.

We will see that groups of small p-rank behave rather differently than most p-groups. We observe that the abelian subgroups of p-rank 1 are cyclic groups. Later in the course, we will provide a full classification of p-groups of p-rank 1.

Chapter 2

Some Interesting Classes of p-groups

In this chapter, we will investigate some families of finite p-groups. This is absolutely not an exhaustive list of “interesting” p-groups, but will hopefully provide intuition for some of the theory we shall encounter later in the course. Moreover, the p-groups we examine in this chapter tend to appear frequently in other works and so you may come across them in lectures and seminars in the future.

2.1 Regular p-groups

We begin with a particularly friendly family of finite p-groups: the abelian ones. The following result is a particular case of a theorem you may have seen in an undergraduate group theory course.

Proposition 2.1. *Let G be a finite abelian p-group. Then G is a direct product of a finite number of finite cyclic p-groups. That is,*

$$G \cong C_{p^{r_1}} \times C_{p^{r_2}} \times \cdots \times C_{p^{r_l}}$$

where $r_i \in \mathbb{N}$ and $|G| = p^{r_1 + \cdots\cdots r_l}$.

Finite abelian p-groups satisfy many nice properties. To exhibit theses properties, we first define some important characteristic subgroups of a p-group:

Definition 2.2. Let G be a finite p-group and exponent p^t. Define

$$\Omega_i(G) := \langle x \in G \mid x^{p^i} = e \rangle$$

for $i \in \{0, \ldots, t\}$. Hence, $\Omega_i(G)$ is the subgroup of G generated by all elements of exponent at most p^i. Of course, $\Omega_0(G) = \{e\}$, $\Omega_t(G) = G$ and $\Omega_i(G) \leq \Omega_j(G)$ whenever $i \leqslant j$.

Definition 2.3. Let G be a finite p-group and exponent p^t. Define

$$\mho_i(G) := \langle x^{p^i} \in G \mid x \in G \rangle$$

for $i \in \{0, \dots, t\}$. Hence, $\mho_i(G)$ is the subgroup of G generated by all p^i-th powers of elements. This time, $\mho_0(G) = G$, $\mho_t(G) = \{e\}$ and $\mho_i(G) \geq \mho_j(G)$ whenever $i \leqslant j$.

Proposition 2.4. *Let G be a finite abelian p-group. The then following hold:*

(i) $\Omega_i(G) = \{x \in G \mid x^{p^i} = e\}$*;*

(ii) $\mho_i(G) = \{x^{p^i} \in G \mid x \in G\}$*;*

(iii) $|G/\Omega_i(G)| = |\mho_i(G)|$*; and*

(iv) $m_p(G) = \log_p(|\Omega_1(G)|)$*.*

Proof. For (i), (ii) and (iii), we observe that as G is abelian, the map $\phi_i : G \to G$ where $\phi_i(x) = x^{p^i}$ is a homomorphism. The result then follow from considering the kernel and image of this map, along with an application of the first isomorphism theorem. For (iv), applying (i) we observe that $\Omega_1(G)$ is the unique maximal elementary abelian subgroup of G. □

In the above proposition, outcomes (i), (ii) and (iii) are clearly useful properties to have in a finite p-group. Moreover, they all rely on the fact that for $x, y \in G$, where G is a finite abelian p-group, we have that $(xy)^i = x^i y^i$ for all $i \in \mathbb{N}$. This motivates the definition of the class of *regular* finite p-groups.

Definition 2.5. Let G be a finite p-group. Say that G is *regular* if for all $x, y \in G$ there is $z_i \in \langle x, y \rangle'$ such that $(xy)^p = x^p y^p z_1^p \dots z_l^p$.

Exercise 2.6. Let G be a regular finite p-group. Then every subgroup and every quotient of G is also regular.

Proposition 2.7. *Let G be a finite p-group. Then G is regular if and only if for all $x, y \in G$, $\langle x, y \rangle$ is regular.*

Proof. Note that regularity is defined in terms of pairs of elements. The proof comes quickly from Exercise 2.6. □

Regular groups are only a true generalization of abelian groups if p is an odd prime.

Exercise 2.8. A finite 2-group is regular if and only if it is abelian.

We note the following important theorem: the *Hall-Pertresco identity.* The proof of this theorem essentially comes as an application of Hall's *commutator collecting process* which we will not give here. We will not give a proof of the Hall-Petresco identity, but recommend that the reader familiarize themselves with it (it can be found in the standard texts or by some googling). While we have not defined $\gamma_i(G)$ for any arbitrary group, it is defined iteratively in the way one may expect (although it may not stabilize in finitely many steps).

Theorem 2.9 (Hall–Petresco Identity)**.** *Let* F_2 *be the free group on two generators* x *and* y*. Then for all* $m \in \mathbb{N}$ *there is* $c_i \in \gamma_i(\mathrm{F}_2)$ *such that*

$$x^m y^m = (xy)^m c_2^{\binom{m}{2}} \dots c_{m-1}^{\binom{m}{m-1}} c_m.$$

Theorem 2.10. *The following are true:*

(i) *Every finite* p*-group of nilpotency class strictly less than* p *is regular. In particular, every* p*-group of order strictly less than* p^{p+1} *is regular.*

(ii) *Every finite* p*-group of exponent* p *is regular.*

(iii) *If* $\gamma_{p-1}(G)$ *is cyclic, then* G *is regular. In particular, if* p *is an odd prime and* G' *is cyclic, then* G *is regular.*

Proof. Throughout, we let G be a finite p-group.

For (i) we apply the Hall–Petresco identity. Assume that G is of nilpotency class strictly less than p, so that $\gamma_p(G) = \{e\}$. Observe that $c_p \in \gamma_p(G)$ and as $\binom{p}{i}$ is divisible by p for $i \in \{2, \dots, p-1\}$, taking $z_i = c_{i-1}^{-1}$ in the definition of regularity, we see that G is regular. It is clear that groups of order p^m have nilpotency class at most $m-1$.

Part (ii) follows immediately from the definition.

For (iii), we note that if $p = 2$, then G is cyclic and so is regular. For the remainder of the proof, let p be an odd prime, $x, y \in G$ and set $H := \langle x, y \rangle$. We observe that if $\gamma_{p-1}(G)$ is cyclic then so to is $\gamma_{p-1}(H)$. By the Hall–Petresco identity, we need only show that for $c \in \gamma_p(H)$, we have that $c = z^p$ for some $z \in H'$. Indeed, we will actually show that $c \in \mho_1(\gamma_{p-1}(H))$, where we use that $\gamma_{p-1}(H)$ is regular. Trivially, we may assume that $\gamma_{p-1}(H) \neq \{e\}$. We observe that as $\mho_1(\gamma_{p-1}(H))$ is the unique maximal subgroup of $\gamma_{p-1}(H)$ and so $\gamma_p(H) = [H, \gamma_{p-1}(H)] \leq \mho^1(\gamma_{p-1})$, as desired. □

We now verify that regular groups capture the properties we desired from Proposition 2.4.

Proposition 2.11. *Let* G *be a finite regular* p*-group. Then the following hold:*

(i) $\Omega_i(G) = \{x \in G \mid x^{p^i} = e\}$;

(ii) $\mho_i(G) = \{x^{p^i} \in G \mid x \in G\}$;

(iii) $x^{p^i} = y^{p^i}$ *if and only if* $(xy^{-1})^{p^i} = e$*; and*

(iv) $|G/\Omega_i(G)| = |\mho_i(G)|$.

Proof. For part (i), we first prove this when $i = 1$. For this, we need to verify that if $x, y \in G$ with $x^p = y^p = e$, then $(xy)^p = e$. Let G be a finite regular p-group not satisfying (i) chosen with $|G|$ minimal. Then there is $x, y \in G$ such that $G = \langle x, y\rangle$, $x^p = y^p = e$ but $(xy)^p \neq e$. Then there is $M < G$ a maximal subgroup of G containing x. Then $M \trianglelefteq G$. We observe that x^y also has order p and $x^y \in M$. By induction, $[x, y]^p = (x^y x)^p = e$. Now, since G is generated by x and y, we see that G' is generated by conjugates of $[x, y]$ and so $G' = \Omega_1(G)$. Since subgroups of regular groups and regular, we deduce that G' has exponent p. But G is regular, and so by definition, $(xy)^p = x^p y^p = e$, a contradiction. Hence, no such counterexample exists and (i) holds in the case $i = 1$.

We now prove (i) for $i \in \mathbb{N}$ by induction. Again, it suffices to prove that if $x, y \in G$ with $x^{p^i} = y^{p^i} = e$, then $(xy)^{p^i} = e$ when $i > 1$. Note that if $x^{p^i} = e$ then $x^p \in \Omega_{i-1}(G)$. Set $\overline{G} := G/\Omega_{i-1}(G)$, a regular group. Then $\overline{x}^p = \overline{y}^p = e$ and by the proof of the $i = 1$ case, we have that $\overline{xy}^p = (\overline{xy})^p = e$ from which we deduce that $(xy)^p \in \Omega_{i-1}(G)$ and $(xy)^{p^i} = e$, as desired.

We leave the proof of (ii) to the reader. Treating the case where $i = 1$ and then using induction is again a good strategy.

For (iii), we again prove the case $i = 1$ and take G to be a minimal counterexample. Assume that $x^p = y^p$ for $x, y \in G$. Then $[x^p, y] = e$ so that $x^p = (y^{-1}xy)^p = (x[x, y])^p$. Let M be a maximal subgroup of G containing x. Then $G' \leq M$ and so $x, [x, y] \in M$. Since G is a minimal counterexample and M is regular, we deduce that $[x, y]^p = e$. We observe that $\langle x, y\rangle = \langle x, y^{-1}\rangle$ and $\langle x, y\rangle'$ is generated by conjugates of $[x, y]^p$. Since $\langle x, y\rangle'$ is regular, we deduce that $\langle x, y\rangle'$ has exponent p. But $\langle x, y\rangle$ is regular and so we conclude that $(xy^{-1})^p = x^p y^{-p} = e$, a contradiction. Hence, no counterexample exists and so $x^p = y^p$ implies that $(xy^{-1})^p = e$.

Assume now that $(xy^{-1})^p = e$ for $x, y \in G$. Conjugating by x, we have that $(y^{-1}x)^p = e$. By the previous paragraph. we have that $[x^{-1}, y]^p = (xy^{-1}x^{-1}y)^p = e$. Since $\langle x, y\rangle = \langle x^{-1}, y\rangle$ is regular and generated by conjugates of $[x^{-1}, y]$, we conclude that $\langle x, y\rangle'$ has exponent p. Finally, since G is regular, we see that $x^p = y^p$. Hence, (iii) holds when $i = 1$.

We prove (iii) when $i > 1$ using induction. Set $\overline{G} = G/\Omega_{i-1}(G)$. Then, by induction, $(x^p)^{p^{i-1}} = x^{p^i} = y^{p^i} = (y^p)^{p^{i-1}}$ if and only if $(x^p y^{-p})^{p^{i-1}} = e$ and by (i), $x^p y^{-p} \in \Omega_{i-1}(G)$. Hence, $\overline{x}^p = \overline{y}^p$. By the $i = 1$ case, $(xy^{-1})^p \in \Omega_{i-1}(G)$ and (i) implies that this happens if and only if $(xy^{-1})^{p^i} = e$, and the result holds.

For (iv), define $\phi : G/\Omega_i(G) \to \mho_i(G)$ by $\phi(\Omega_i(G)x) = x^{p^i}$. Note that $(xy^{-1})^{p^i} = e$ if and only if $xy^{-1} \in \Omega_i(G)$ by part (i). Then $\Omega_i(G)x = \Omega_i(G)y$ if and only if $xy^{-1} \in \Omega_i(G)$ if and only if $x^{p^i} = y^{p^i}$ by part (iii) and ϕ is well-defined and injective. Then part (ii) implies that ϕ is surjective and so (iv) holds. □

We observe that the equality in part (iv) is not induced by an isomorphism.

Exercise 2.12. Play around with the Small Groups package in MAGMA or GAP, and find some small finite regular p-groups in which $G/\Omega_1(G) \ncong \mho_1(G)$ and $G/\mho_1(G) \ncong \Omega_1(G)$.

Theorem 2.13. *Let G be a finite regular p-group with $M, N \trianglelefteq G$. Then the following hold:*

(i) $[\mho_i(M), \mho_j(N)] = \mho_{i+j}([M,N])$*;*

(ii) $\gamma_j(\mho_i(G)) = \mho_{ij}(\gamma_j(G))$ *for all $i, j \in \mathbb{N}$; and*

(iii) $\gamma_{j+1}(G) \leq \Omega_i(G)$ *if and only if* $\mho_i(G) \leq Z_j(G)$*.*

(iv) $[\Omega_i(G), \mho_j(G)] \leq \Omega_{i-j}(G)$ *where* $\Omega_k(G) = \{e\}$ *if* $k \leqslant 0$*.*

Proof. We have that $[\mho_i(M), \mho_j(N)] = \langle [x^{p^i}, y^{p^j}] \mid x \in M, y \in N \rangle$. Set $\overline{G} = G/\mho_{i+j}([M,N])$. Then, for $x \in M$ and $y \in N$, $[\overline{x}, \overline{y}]^{p^{i+j}} = e$ from which we conclude that $(\overline{x}^{-1}\overline{y}^{-1}\overline{xy})^{p^j} \in \Omega_i(\overline{G})$. Now, applying Proposition 2.11(iii), we have that $(\overline{x}^{-1}\overline{y}^{-1}\overline{x})^{p^j}\overline{y}^{p^j} \in \Omega_i(\overline{G})$ so that $\overline{x}^{-1}\overline{y}^{-p^j}\overline{xy}^{p^j} \in \Omega_i(\overline{G})$. Thus, we have shown that $(\overline{x}^{-1}\overline{y}^{-p^j}\overline{xy}^{p^j})^{p^i} = e$ and yet another application of Proposition 2.11(iii) yields that $\overline{x}^{-p^i}(\overline{y}^{-p^j}\overline{xy}^{p^j})^{p^i} = e$ so that $\overline{x}^{-p^i}\overline{y}^{-p^j}\overline{x}^{p^i}\overline{y}^{p^j} = e$. Finally, we deduce that $[\overline{x}^{p^i}, \overline{y}^{p^j}] = e$ so that $[x^{p^i}, y^{p^j}] \in \mho_{i+j}([M,N])$.

For the reverse inclusion, we now redefine $\overline{G} = G/[\mho_i(M), \mho_j(N)]$. Hence, for $x \in M$ and $y \in N$, $[\overline{x}^{p^i}, \overline{x}^{p^j}] = \{e\}$. Using Proposition 2.11 and some manipulation of commutators, we see that this yields that $[\overline{x}, \overline{y}]^{p^{i+j}} = \{e\}$ from which we conclude that $[x,y]^{p^{i+j}} \in [\mho_i(M), \mho_j(N)]$. Since $[M,N]$ is regular and generated by elements of the form $[x,y]$ for $x \in M$ and $y \in N$, we see that $\mho_{i+j}([M,N]) \leq [\mho_i(M), \mho_j(N)]$ and the proof of (i) is complete.

For part (ii), we fix i and apply induction on j. The case $j = 1$ follows from the definition $\gamma_1(G) = G$. Now, by induction and part (i), $\gamma_{j+1}(\mho_i(G)) = [\gamma_j(\mho_i(G)), \mho_i(G)] = [\mho_{ij}(\gamma_j(G)), \mho_i(G)] = \mho_{ij+i}([\gamma_j(G), G] = \mho_{i(j+1)}(\gamma_{j+1}(G))$, as desired.

For (iii), we note that $\gamma_{j+1}(G) \leq \Omega_i(G)$ if and only if $\mho_i(\gamma_{j+1}(G)) = \{e\}$. But by (i), we have that $\mho_i(\gamma_{j+1}(G)) = \mho_{i+0)}([G, \gamma_j(G)]) = [\mho_i(G), \gamma_j(G)]$ and so we conclude that $\gamma_{j+1}(G) \leq \Omega_i(G)$ if and only if $[\mho_i(G), \gamma_j(G)]$. This is equivalent to $\mho_i(G) \leq Z_j(G)$ (examine the proof of Proposition 1.16).

We leave the proof of (iv) as an exercise. □

Exercise 2.14. Reprove part (i) of Theorem 2.13 assuming that every proper subgroup of G is regular, but G itself is not necessarily regular.

Theorem 2.15 (Hall's Criterion for Regularity)**.** *Let G be a finite p-group. Then G is regular provided any one of the following hold:*

(i) $|G/\mho_1(G)| < p^p$*;*

(ii) $|G'/\mho_1(G')| < p^{p-1}$*;*

(iii) $|\Omega_1(G)| < p^{p-1}$.

Proof. We will only prove part (i). (ii) and (iii) are left as an exercise. We first start with an observation.

Claim:. If $|G/\mho_1(G)| < p^p$ then $|H/\mho_1(H)| < p^p$ for all $H \leq G$.

Proof of claim. Suppose first that $p = 2$. Since groups of order p^2 are abelian, provided $|G| > 2$, $|G/G'| \geqslant 4$. If $|G/\mho_1(G)| < 4$, then $\mho_1(G)$ is a maximal subgroup of G and so properly contains G', from which we deduce that G/G' is cyclic. Hence, G has a unique maximal subgroup and by another exercise, we conclude that G itself is cyclic. Hence, $|H/\mho_1(H)| = 2$ for all $H \leq G$.

Suppose now that p is an odd prime, and choose G a counterexample to the claim of minimal order. We may as well choose H maximal in G, for otherwise there is $H < M < G$ and as G is a minimal counterexample, H satisfies the property since M does. Hence, H is a maximal subgroup of G with $|H/\mho_1(H)| \geqslant p^p$. Since $\mho_1(H)$ is characteristic in H, and H is normal in G, we have that $\mho_1(H) \trianglelefteq G$. By considering the quotient $G/\mho_1(G)$, and by an exercise, we see that there is $N \trianglelefteq G$ such that $\mho_1(H) \leq N \leq H$ and $|H/N| = p^p$. Hence, G/N is a group of order p^{p+1} and H/N has exponent p. If N is nontrivial, then as $\mho_1(G) \geq \mho_1(H)$, we have that $\mho_1(G/N) = \mho_1(G)N/N$ has index at most p^{p-1} in G, a contradiction since $\mho_1(H/N)$ has index p^p in H and G is a minimal counterexample. Hence, $N = \{e\}$ and so $|G| = p^{p+1}$.

Now, every proper subgroup of G has order at most p^p and so by Theorem 2.10(i), every proper subgroup of G is regular. Hence, by the previous exercise, $[G, \mho_1(G)] = \mho_1(G') \leq \mho_1(H) = \{e\}$ from which we conclude that $\mho_1(G) \leq Z(G)$. Moreover, since $\mho_1(G)$ has index at most p^{p-1} in G we see that $\gamma_{p-1}(G) \leq \mho_1(G)$ and so $[G, \gamma_{p-1}(G)] = \{e\}$ so that G has nilpotency class strictly less than p. Hence, G is regular and so $|\Omega_1(G)| = |G/\mho_1(G)| < p^p$ by Proposition 2.11(iv). But $H \leq \Omega_1(G)$ and as H has order p^p, we have reached a contradiction. Hence, no minimal counterexample to the claim exists and so the claim holds.

We now prove part (i). As in the proof of the claim, we let G be a counterexample to (i) of minimal order. By the claim, $|H/\mho_1(H)| < p^p$ for all $H < G$ and by minimality of G, every proper subgroup of G is regular. As in the proof of the claim, since $|G/\mho_1(G)| < p^p$, we ascertain that $\gamma_p(G) = [G, \gamma_{p-1}(G)] \leq [G, \mho_1(G)] = \mho_1(G')$. By Proposition 2.7, since G is a minimal counterexample, we need to verify regularity for all $x, y \in G$ with $G = \langle x, y \rangle$. But an application of the Hall–Petresco identity implies that G is regular in this case, a contradiction since G is a counterexample. Hence, no counterexample exists and the proof of (i) is complete. □

2.2 Dihedral and Semidihedral Groups

Recall that the *Dihedral group* of order $2n$, which we write as $\mathrm{Dih}(2n)$, arises as the groups of symmetries of a n-sided polygon. In this course, we will work with a more abstract definition:

Definition 2.16. The dihedral group of order $2n$ is given by the following presentation:

$$\mathrm{Dih}(2n) := \langle x, y \mid x^n = y^2 = e, x^y = x^{-1}\rangle.$$

You should verify that $\mathrm{Dih}(2n)$ truly does have order $2n$. (Hint: Show that every element can be written as $x^i y$ for some $i \in \{0, \dots, n-1\}$.)

We will focus on the particular case where n is a power of 2. We note the following elementary properties:

Proposition 2.17. *The following hold when $n > 1$:*

(i) *The group $\mathrm{Dih}(4)$ is isomorphic to the elementary abelian group $C_2 \times C_2$.*

(ii) *If $n > 2$ then $Z(\mathrm{Dih}(2^n)) = \{e, x^{2^{n-2}}\}$ has order 2.*

(iii) *We have that $\mathrm{Dih}(2^n)' = \langle x^2\rangle$ has index 4 in $\mathrm{Dih}(2^n)$.*

(iv) *$\mathrm{Dih}(2^n)$ has nilpotency class $n-1$.*

Proof. Part (i) is clear from the presentation of $\mathrm{Dih}(4)$. The result clearly holds when $n = 2$ and so for the remainder, we set $G := \mathrm{Dih}(2^n)$ for $n > 2$. We observe that G is non-abelian whenever $n > 2$. Since $\langle x\rangle$ is abelian subgroup of index 2 in G, we deduce that $Z(G) \leq \langle x\rangle$. Since $(x^i)^y = x^{-i}$ for all $i \in \{0, \dots, n-1\}$ we conclude $(x^i)^y = x^i$ if and only if $i \in \{0, 2^{n-2}\}$. Hence, (ii) is proved.

Now, G has an abelian subgroup of index 2, namely $\langle x\rangle$. Since $|Z(G)| = 2$, it follows from an exercise that G' has index 4 in G. Now, $[y, x] = (x^{-1})^y x = x^2$ and so $x^2 \in G'$. Then $\langle x^2\rangle$ has index 4 in G and is contained in G' and so (iii) holds.

In a similar fashion, we see that $[y, x^2] = (x^{-2})^y x^2 = x^4$ and we deduce that $[y, G'] = \langle x^4\rangle$. Since $\gamma_3(G) = [G, G']$ is generated by $[x, G'] \leq \langle x\rangle' = \{e\}$ and $[y, G'] = \langle x^4\rangle$, we conclude that $\gamma_3(G) = \langle x^4\rangle$. Applying a similar reasoning, we see that $\gamma_i(G) = \langle x^{2^{i-1}}\rangle$ from which we deduce that $\gamma_{n-1}(G) = Z(G)$ and $\gamma_n(G) = \{e\}$. Hence, G has nilpotency class $n-1$. □

The normal subgroups of $\mathrm{Dih}(2^n)$ have a very simple structure.

Proposition 2.18. *The following hold:*

(i) *Every subgroup of $\mathrm{Dih}(2^n)'$ is normal in $\mathrm{Dih}(2^n)$.*

(ii) *Every proper normal subgroup of* $\mathrm{Dih}(2^n)$ *is either a maximal subgroup or some subgroup of* $\mathrm{Dih}(2^n)'$.

(iii) $\mathrm{Dih}(2^n)$ *has three maximal subgroups: one cyclic maximal subgroup and two maximal dihedral groups.*

Proof. Set $G = \mathrm{Dih}(2^n)$ for $n > 2$ (the result is clear when $n = 2$). Clearly, every maximal subgroup of G is normal in G. Note that subgroups of G' are of the form $\langle x^{2^i} \rangle$ for $i \in \{1, \ldots, n-1\}$. Now, x centralizes x^{2^i} and $(x^{2^i})^y = x^{-2^i} \in \langle x^{2^i} \rangle$ and since $G = \langle x, y \rangle$, all subgroups of G' are normal in G. Alternatively, we note that G' is characteristic in G and abelian, and $\langle x^{2^i} \rangle = \mho_{i-1}(G')$ is characteristic in G for each $i \in \{1, \ldots, n-1\}$, and so each subgroup of G' is normal in G.

Let $N \trianglelefteq G$. If $N \leq \langle x \rangle$, then N is either equal to $\langle x \rangle$ so maximal; or N is proper in $\langle x \rangle$. Since $\langle x \rangle$ is cyclic, it has a unique maximal subgroup, namely G' from which we conclude that $N \leq G'$. Hence, $N \not\leq \langle x \rangle$, $G = N\langle x \rangle$ and we infer that $G' = N'[N, \langle x \rangle] \leq N$. Since $|G/G'| = 4$ and $N \neq G'$, we must have that $|G/N| \leqslant 2$ and the proof of (ii) is complete.

Finally, we observe that every maximal subgroup properly contains G' and as $|G/G'| = 4$ and G/G' is not cyclic, G has exactly three maximal subgroups. We immediately account for one: the subgroup $\langle x \rangle$. Another is given by $\langle y, G' \rangle$. We verify that $xy \notin \langle y, G' \rangle$. Otherwise $xy = x^{2^i} y$ for some $i \in \{1, \ldots, n-1\}$. But then $e = x^{2^{i-1}}$, a contradiction since $i - 1 \leqslant n - 2$. Hence, the final maximal subgroup is $\langle xy, G' \rangle$. Now, $\langle y, G' \rangle = \langle y, x^2 \rangle$ with the condition $(x^2)^y = x^{-2} = (x^2)^{-1}$ and $(x^2)^{2^{n-1}} = e$ from which we conclude that $\langle y, G' \rangle$ is isomorphic to a quotient of $\mathrm{Dih}(2^{n-1})$ and of equal order from which we conclude that $\langle y, G' \rangle \cong \mathrm{Dih}(2^{n-1})$. □

In fact, we can say something about all subgroups of $\mathrm{Dih}(2^n)$ from this.

Proposition 2.19. *Every subgroup of* $\mathrm{Dih}(2^n)$ *is either cyclic or dihedral.*

Proof. The result is clearly true when $n = 2$. We prove the result using induction on n. Let H be a proper subgroup of $G := \mathrm{Dih}(2^{n+1})$. By Proposition 2.18, the result holds if H is maximal and so we may assume that H is properly contained in a maximal subgroup of G. But every maximal subgroup of G is dihedral or cyclic, and since subgroups of cyclic groups are cyclic and applying induction if the maximal subgroup in question is dihedral, we have that H is cyclic or dihedral, as desired. □

We now showcase the "universal property" of dihedral groups.

Theorem 2.20. *Let G be a finite 2-group generated by two distinct involutions. Then G is a dihedral group.*

Proof. Let $G := \langle a, b \rangle$ where $a^2 = b^2 = e$. Since G is finite, there is $m \in \mathbb{N}$ minimal such that $(ab)^{2^m} = e$. Now, $(ab)^a = a^{-1}aba = ba$ and $(ab)^{-1} = b^{-1}a^{-1} = ba$ and so the conjugation action of a inverts ab.

We may also enumerate the elements of G. Since $a^2 = e = b^2$, every element is either of the form $abab\dots$ or of the form $baba\dots$. Since $(ab)^{2^m}$ there are exactly $2^m - 1$ ways to write elements beginning a. For each element beginning b, we may multiply on the left by b^{-1} to either get a element beginning a or the trivial element, and so this provides 2^m ways to write elements beginning b. Along with the identity element, we see that this implies that $|G| \leqslant 2^{m+1}$. Now, $\langle ab\rangle$ has order 2^m and so to show that $|G| = 2^{m+1}$, it suffices to show that either $a \neq (ab)^{2^i}$ or $b \neq (ab)^{2^i}$ for any $i \in \{0, \dots, m-1\}$. Assume that $a = (ab)^{2^i}$ for some $i \in \{0, \dots, m-1\}$. Then $e = a^2 = (ab)^{2^{i+1}}$ and by minimality of m, we get that $i = m - 1$. Then, if $b = (ab)^{2^j}$ for some $j \in \{0, \dots, m-1\}$, a similar argument implies that $e = b^2 = (ab)^{2^{j+1}}$ and $j = m-1$. But then $a = b$, a contradiction since a and b are distinct. Hence, $|G| = 2^{m+1}$.

Let $f : \mathrm{Dih}(2^{m+1}) \to G$ be a homomorphism defined by $x \mapsto ab$ and $y \mapsto a$ (you should verify that this information suffices to determine a homomorphism). Let $g \in \ker(f)$. Clearly, $f(y) = a \neq e$. Then $e = f(g) = f(x^{2^i}y) = f(x)^{2^i}f(y) = (ab)^{2^i}a$ for some $i \in \{0, \dots, m-1\}$. Since $a^2 = e$, we see that $(ab)^{2^i} = a$ so that $(ab)^{2^{i+1}}$ from which we deduce that $i = m-1$. In particular, $(ab)^{2^{m-1}}a = e$. But $(ab)^{2^m} = e$ from which we deduce that $b = e$, an obvious contradiction. Hence, f is injective and since $|\mathrm{Dih}(2^{m+1})| = |G|$, we see that $\mathrm{Dih}(2^{m+1}) \cong G$. □

We note that this holds in a greater generality, and can be extended to (not necessarily finite) groups.

This yields the following easy corollary concerning the quotients of dihedral groups.

Corollary 2.21. *Any proper quotient of* $\mathrm{Dih}(2^n)$ *of order strictly larger than* 2 *is dihedral.*

Proof. Let $G := \mathrm{Dih}(2^n)$ and $N \trianglelefteq G$ with $|G/N| \geqslant 4$. Then $N = \langle x^{2^i}$ for some $i \in \{1, \dots, n-1\}$. Now, $(yx)^2 = y^{-1}xyx = x^y x = e$ and so yx is an involution. Clearly, $G = \langle yx, y\rangle$, neither yx nor y are contained in N, and $G/N = \langle Nyx, Ny\rangle$. Moreover, $Nyx \neq Ny$ for otherwise $N = Nx$, $\langle x\rangle \leq N$ and N has index at most 2 in G. Hence by Theorem 2.20, we have that G/N is a dihedral group. □

Less well known than dihedral groups are the *semidihedral* (sometimes called *quasidihedral*) groups.

Definition 2.22. The semidihedral group of order 2^n is given by the following presentation:

$$\mathrm{SDih}(2^n) := \langle x, y \mid x^{2^{n-1}} = y^2 = e, x^y = x^{2^{n-2}-1}\rangle.$$

Of course, $\mathrm{SDih}(4) = \mathrm{Dih}(4) \cong C_2 \times C_2$ and $\mathrm{SDih}(8) \cong C_4 \times C_2$. We mention some properties of semidihedral groups. We omit the proofs of the following proposition, but encourage the reader to prove them using the proofs in the dihedral case as inspiration.

Proposition 2.23. *The following hold when* $n > 3$*:*

(i) $Z(\mathrm{SDih}(2^n)) = \{e, x^{2^{n-2}}\}$ *has order* 2.

(ii) *We have that* $\mathrm{SDih}(2^n)' = \langle x^2 \rangle$ *has index* 4 *in* $\mathrm{SDih}(2^n)$.

(iii) $\mathrm{SDih}(2^n)$ *has nilpotency class* $n-1$.

(iv) *Every proper normal subgroup of* $\mathrm{SDih}(2^n)$ *is either a subgroup of* $\mathrm{SDih}(2^n)'$ *or is a maximal subgroup properly containing* $\mathrm{SDih}(2^n)'$.

(v) *We have that* $G/Z(G) \cong \mathrm{Dih}(2^{n-1})$.

(vi) *We have that* $\Omega_1(G) = \langle x^2, y \rangle$ *is isomorphic to* $\mathrm{Dih}(2^{n-1})$.

We mention also the *modular* (maximal-by-cyclic) groups $\mathrm{Mod}(p^n)$, defined for all prime p. These groups are given by the presentation

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

These groups appear a lot less in the literature than the previously mentioned groups but will appear later in the course.

2.3 Quaternion and Generalized Quaternion Groups

Another important class of 2-groups are the *generalized quaternion* groups.

Definition 2.24. The generalized quaternion group of order 2^n, for $n > 2$, is given by the following presentation:

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

The group Q_8 is referred to as the *quaternion group*.

The following proposition provides a shortcut for proving structural results about generalized quaternion groups by utilizing our earlier work on dihedral groups.

Proposition 2.25. *We have that* $Z(Q_{2^n}) = \{e, x^{2^{n-2}}\} = \{e, y^2\}$ *has order* 2 *and* $Q_{2^n}/Z(Q_{2^n}) \cong \mathrm{Dih}(2^{n-1})$.

Proof. Since $\langle x \rangle$ has order 2^{n-1} is abelian of index 2 and Q_{2^n} is non-abelian, we deduce that $Z(Q_{2^n}) \leq \langle x \rangle$. Then $Z(Q_{2^n}) = \langle x^{2^k} \rangle$ for some $0 \leqslant k < n-1$. But $x^y = x^{-1}$ and so we conclude that $x^{2^k} = (x^{2^k})^y = x^{-2^k}$ so that $x^{2^{k+1}} = e$. Hence, we deduce that $n-1$ divides $k+1$ and as $k < n-1$, we see that $n-1 = k+1$, $k = n-2$ and $Z(Q_{2^n}) = \langle x^{2^{n-2}} \rangle$ has order 2. Since $y^2 = x^{2^{n-2}}$, first statement of the proposition holds.

We observe that $Q_{2^n}/Z(Q_{2^n})$ has order 2^{n-1} and that $Z(Q_{2^n})y$ is an involution. Now, $(xy)^2 = xyxy = xy^{-1}y^2xy = xx^yy^2 = y^2$ from which we conclude that $Z(Q_{2^n})xy$ is an involution. Clearly, Q_{2^n} is generated by $Z(Q_{2^n})y$ and $Z(Q_{2^n})xy$ and the result now follows from Theorem 2.20. □

The following facts then follow quickly from the structure of $Q_{2^n}/Z(Q_{2^n})$ and knowledge of the dihedral groups. We leave the proofs to the reader.

Proposition 2.26. *The following hold for $n > 2$:*

(i) *Every subgroup of Q'_{2^n} is normal in Q_{2^n}.*

(ii) *We have that $Q'_{2n} = \langle x^2 \rangle$ has index 4 in Q_{2^n}.*

(iii) *Every proper normal subgroup of Q_{2^n} is either a maximal subgroup or some subgroup of Q'_{2^n}.*

(iv) *Q_{2^n} has nilpotency class $n-1$.*

We now record some key differences in structure of generalized quaternion groups when compared to dihedral and semidihedral groups.

Proposition 2.27. *The following hold:*

(i) *Every subgroup of Q_{2^n} is either cyclic or generalized quaternion.*

(ii) *Every element of Q_{2^n} lying outside of $\langle x \rangle$ has order 4.*

(iii) $\Omega_1(Q_{2^n}) = Z(Q_{2^n})$.

Proof. For part (i), we will prove the every maximal subgroup of Q_{2^n} is either cyclic or generalized quaternion. The result will then follow by induction. We observe that as Q'_{2^n} has index 4 in Q_{2^n}, Q_{2^n} has exactly three maximal subgroups. If $n = 3$, then the subgroups $\langle x \rangle$, $\langle y \rangle$ and $\langle xy \rangle$ are all cyclic of order 4 and pairwise distinct. So assume that $n > 3$. The subgroup $\langle x \rangle$ is a cyclic maximal subgroup of Q_{2^n}. Since $y \notin \langle x \rangle$, we see that the subgroups $\langle x^2, y \rangle$ and $\langle x^2, xy \rangle$ are distinct maximal subgroups. Label $a := x^2$ and $b = y$. Then $a^{2^{n-3}} = x^{2^{n-2}} = y^2 = b^2$, $a^b = (x^2)^y = x^{-2} = a^{-1}$ and $a^{2^{n-2}} = x^{2^{n-1}} = e = y^4 = b^4$. These are the relations satisfied by the group $Q_{2^{n-1}}$ and since $\langle x^2, y \rangle$ has order 2^{n-1}, $\langle x^2, y \rangle \cong Q_{2^{n-1}}$. The proof that $\langle x^2, xy \rangle \cong Q_{2^{n-1}}$ is left as an exercise.

We will prove the result first for Q_8. Note that every maximal subgroup of Q_8 is cyclic. Since they are all normal, they all contain $Z(Q_8) = \langle x^2 \rangle = \langle y^2 \rangle = \langle (xy)^2 \rangle$ and the non-trivial element of $Z(Q_8)$ is the unique involution in each of these maximal subgroups. Since Q_8 is not cyclic, every element is contained in some maximal subgroup from which we conclude that x^2 is the unique involution in Q_8. Since Q_8 is non-cyclic, no element has order 8 and so every element of Q_8 lying outside of $Z(Q_8)$ has order 4.

We now prove the result for $n > 3$ by induction. Let $g \in Q_{2^n}$ such that $g \notin \langle x \rangle$. Then g lies in a maximal subgroup of Q_{2^n}, and as $g \notin \langle x \rangle$, we see that $g \in M$ where $M \cong Q_{2^{n-1}}$. If $n = 4$, then $g \notin Z(M) = Z(Q_{16}) = \langle x^{2^{n-2}} \rangle$ and so g has order 4. If $n > 4$, then M has exactly three maximal subgroups: two which are generalized quaternion and the subgroup $\langle x^2\rangle$. Since $g \notin \langle x^2\rangle \leq \langle x\rangle$, the inductive hypothesis implies that g has order 4, completing the proof of (ii).

By part (ii), every involution is contained in $\langle x\rangle$. But $\langle x\rangle$ is cyclic and so has a unique involution, namely $x^{2^{n-2}}$. Hence, $\Omega_1(Q_{2^n}) = Z(Q_{2^n})$ as desired. □

2.4 Extraspecial and Special Groups

Another important class of finite p-groups are (the somewhat appropriately named *special groups.*

Definition 2.28. Let G be a finite p-group. Say that G is *special* if (G is elementary abelian or) $G' = Z(G)$ and $G/Z(G)$ has exponent p.

Proposition 2.29. *Let G be a non-abelian finite special p-group. Then $Z(G)$ has exponent p.*

Proof. Since $Z(G) = G'$, we need only show that $[x, y]^p = e$ for all $x, y \in G$. Now, $G/Z(G)$ has exponent p and so $x^p \in Z(G)$ from which we deduce that $[x^p, y] = e$. Note that $[x^p, y] = [xx^{p-1}, y] = [x, y]^{x^{p-1}}[x^{p-1}, y] = [x, y][x^{p-1}, y]$ since x^{p-1} centralizes $[x, y] \in Z(G)$. Repeating this process we get that $[x^p, y] = [x, y]^p$, as desired. □

A case of particular interest is when $|Z(G)| = p$:

Definition 2.30. Let G be a finite p-group. Say that G is *extraspecial* if G is non-abelian, special, and $|Z(G)| = p$.

We have already bumped into two distinct extraspecial groups. Namely, $\mathrm{Dih}(8)$ and Q_8. Since groups of order p^2 are abelian, these are clearly some the smallest extraspecial groups one can encounter. However, $\mathrm{Dih}(8)$ and Q_8 arise specifically for the prime 2. We require some minimal extraspecial groups when p is an odd prime.

Definition 2.31. For p an odd prime, we set

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

We set

$$p_-^{1+2} := \langle x, y \mid x^{p^2} = y^p = e, x^y = x^{p+1}\rangle.$$

You should compare p_-^{1+2} with $\mathrm{Mod}(p^3)$ from earlier.

Proposition 2.32. *The following hold for p an odd prime:*

(i) *Both p_+^{1+2} and p_-^{1+2} are extraspecial groups of order p^3.*

(ii) *If G is extraspecial of order p^3, then G has no complement to $Z(G)$.*

(iii) *p_+^{1+2} is of exponent p, has exactly $p+1$ subgroups of order p^2, and has exactly one proper non-trivial characteristic subgroup.*

(iv) *p_-^{1+2} is of exponent p^2, $|\Omega_1(p_-^{1+2})| = p^2$ and p_-^{1+2} has exactly p cyclic subgroups of order p^2.*

Proof. For part (i), we note from the presentations that the groups p_+^{1+2} and p_-^{1+2} are non-abelian. If both groups are of order p^3, since the center of a p-group is never a maximal subgroup and every normal subgroup of a finite p-group intersects the center non-trivially, we must have that the derived subgroup and the center coincide and have order p. Then every maximal subgroup contains the derived subgroup and since the groups are non-cyclic, there exists at least two maximal subgroup from which we deduce that the groups are extraspecial. It follows from the presentation of p_+^{1+2} that every element may be written as $x^a y^x z^c$ for some $a, b, c \in \mathbb{N}_0$. Since x, y, x have order p, we have that p_+^{1+2} has order p^3. For p_-^{1+2}, since $x^y = x^{p+1}$ we see that $xy = yx^{p+1}$ and so every element may be written in the form $x^a y^b$ for some $a, b \in \mathbb{N}_0$. Since x has order p^2 and y has order p, it follows that $|p_-^{1+2}| = p^3$.

For part (ii), if there is $H \leq G$ such that $G = HZ(G)$ and $H \cap Z(G)$ then H has order p^2, so is abelian, from which we deduce that G is abelian.

For (iii), let $G = p_+^{1+2}$. Since x, y and z has exponent p, we immediately have that $G = \Omega_1(G)$. Since p is odd and G has nilpotency class 2, it follows from Theorem 2.10(i) that G is regular. Then Proposition 2.11)i) reveals that G has exponent p. We note that $G' = Z(G)$ is contained in every maximal subgroup of G, and since G/G' is elementary abelian of order p^2, one can calculate that G/G' has exactly $p+1$ subgroups of order p. It follows that G has exactly $p+1$ maximal subgroups. We leave it as an exercise that $\langle x, Z(G)\rangle$ and $\langle x^i y, Z(G)\rangle$ for $i \in \{0, \ldots, p-1\}$ constitutes a complete set of maximal subgroups of G.

Clearly, $Z(G) = G'$ is a proper non-trivial subgroup of G. Every characteristic subgroup of G is normal in G and so contains $Z(G)$ and so a proper non-trivial subgroup of G is elementary abelian of order p^2. We define $\alpha : G \to G$ an automorphism such that $\alpha(x) = x$, $\alpha(y) = xy$ and $\alpha(z) = z$. We leave it to the reader to verify that this is indeed an automorphism. Then α fixes $\langle x, z\rangle$ and has $\alpha(x^i y) = x^{i+1} y$. Since the maximal subgroups of G are of the form $\langle x, Z(G)\rangle$ or $\langle x^k y, Z(G)\rangle$ for $k \in \{0 \ldots, p-1\}$, we deduce that α permutes the p distinct elementary abelian subgroups of G which are not equal to $\langle x\rangle$. Hence, the only candidate for a proper, non-trivial subgroup of G is $\langle x\rangle$. We leave the reader to verify that the map $\beta : G \to G$ where $\beta(y) = y$, $\beta(x) = xy$, $\beta(z) = z$ may be extended to an automorphism of G which fixes $\langle y\rangle$ and permutes the remaining the elementary abelian subgroup of G of order p^2.

For (iv), let $G = p_-^{1+2}$. Since G is not cyclic and x has exponent p^2, it follows that G has exponent p^2. As above, G is a regular p-group and as $\langle y, Z(G)\rangle$ has exponent p, we must have that $\Omega_1(G) = \langle y, Z(G)\rangle$, and every element outside of $\Omega_1(G)$ has exponent

p^2. In a similar manner to the proof of (iii), we see that G has exactly $p+1$ maximal subgroups. Since $\Omega_1(G)$ is maximal and groups of order p^2 are abelian, we have that the remaining p maximal subgroups of G are cyclic of order p^2. □

Exercise 2.33. Show that every non-abelian p-group of order p^3 is isomorphic to $\mathrm{Dih}(8)$, Q_8, p_+^{1+2} or p_-^{1+2}.

We shall use these minimal extraspecial groups to construct larger extraspecial groups via *central products*. We recall the definition of a central product for those who may not have encountered it before. Similar to a direct product, there is an *internal* version and an *external* version. You should verify that these conditions give rise to the same structures.

Definition 2.34. Let G, H be groups with central subgroups $Z_1 \leq G$ and $Z_2 \leq H$ such that $Z_1 \cong Z_2$. Choose an isomorphism $\alpha : Z_1 \to Z_2$. Define the (external) central product of G and H with respect to α, denoted by $G \circ_\alpha H$, as the quotient of $G \times H$ by the normal subgroup $N := \{(g,h) \in Z_1 \times Z_2 \mid \alpha(g)h = e\}$.

Let G be a group with subgroups H, K such that $G = HK$ and $[H,K] = \{e\}$. Then G is the (internal) central product of H and K.

It should be clear that considering $H \circ_{\alpha^{-1}} G$ results in an isomorphic group. We can extend the above definition iteratively to take a central product of multiple groups. That this procedure is well-defined is worth checking. We also note that the construction naturally does depend on both the choice of Z_1 and Z_2, and the map α. For the purposes of this course (and in particular for the groups we shall consider), the condition may be remedied by the following theorem.

Theorem 2.35. *Let $\{G_i \mid 1 \leqslant i \leqslant r\}$ be a family of subgroups such that $Z(G_i) = Z(G_j)$, and such that $\mathrm{Aut}(Z(G_i)) = \mathrm{Aut}_{\mathrm{Aut}(G_i)}(Z(G_i))$ 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 $Z(H_i) = Z(H_j)$ for all i and j.*

Finally, we can get our hands on some larger extraspecial groups.

Proposition 2.36. *Let G be a central product of n (not necessarily isomorphic) extraspecial groups of order p^3 for some $n \in \mathbb{N}$. Then G is extraspecial.*

Proof. Let $G = G_1 \circ \cdots \circ G_n$, which is uniquely determined by $G_1, \ldots, G_n$ by Theorem 2.35. By construction, we have that $Z(G_i) = Z(G_j)$ has order p for all $1 \leqslant i, j \leqslant n$ and so $Z(G_i) \leq Z(G)$. Note that if $|Z(G)| > p$ then there must exist i such that $Z(G) \not\leq G_1 \ldots G_{i-1}G_{i+1} \ldots G_n$. Indeed, $Z(G)G_1 \ldots G_{i-1}G_{i+1} \ldots G_n$ has index at most p in G and is centralized by G_i. But $Z(G) \cap G_i \leq Z(G_i)$ and $Z(G_i)$ has index p^2 in G_i. Hence, we deduce that $|Z(G)| = p$ and $Z(G) = Z(G_i)$ for all $0 \leqslant i \leqslant n$. Note that by the commutator laws, $G' = \prod_{0 \leqslant i,j \leqslant n}[G_i, G_j] = \prod_{0 \leqslant i \leqslant n} G_i' = Z(G)$. Now, $G/Z(G) = G_1/Z(G) \times \ldots G_n/Z(G)$ is abelian, and as $G_i/Z(G)$ has exponent p, we deduce that $G/Z(G)$ has exponent p. Therefore, G is extraspecial. □

We will now set about answering the natural next question to answer: can we classify all finite extraspecial groups?

We must first recognize some isomorphisms, which we leave as an exercise.

Exercise 2.37. Show that $Q_8 \circ Q_8 \cong \mathrm{Dih}(8) \circ \mathrm{Dih}(8) \not\cong Q_8 \circ \mathrm{Dih}(8)$ and $p_+^{1+2} \circ p_-^{1+2} \cong p_-^{1+2} \circ p_-^{1+2} \not\cong p_+^{1+2} \circ p_+^{1+2}$.

Definition 2.38. Let $p = 2$. For $n > 1$ define

$$2_+^{1+2n} := \underbrace{\mathrm{Dih}(8) \circ \cdots \circ \mathrm{Dih}(8)}_{n \text{ times}}$$

and

$$2_-^{1+2n} := Q_8 \circ \underbrace{\mathrm{Dih}(8) \circ \times \circ \mathrm{Dih}(8)}_{n-1 \text{ times}}.$$

We have the convention that $2_+^{1+2} \cong \mathrm{Dih}(8)$ and $2_-^{1+2} \cong Q_8$.

Let p be an odd prime. For $n > 1$ define

$$p_+^{1+2n} := \underbrace{p_+^{1+2} \circ \cdots \circ p_+^{1+2}}_{n \text{ times}}$$

and

$$p_-^{1+2n} := p_-^{1+2} \circ \underbrace{p_+^{1+2} \circ \times \circ p_+^{1+2}}_{n-1 \text{ times}}.$$

Proposition 2.39. *For p a prime and $n > 1$, the following are true:*

(i) *p_-^{1+2n} and p_+^{1+2n} are extraspecial groups of order p^{1+2n};*

(ii) *2_+^{1+2n} has maximal elementary abelian subgroups of order 2^{n+1} while the maximal elementary abelian subgroups of 2_-^{1+2n} have order 2^n; and*

(iii) *if p is odd, then p_+^{1+2n} has exponent p while p_-^{1+2} has exponent p^2.*

Proof. Part (i) follows from Proposition 2.36.

For part (ii), we first let $G \cong 2_+^{1+2n}$ and set $G_i \cong \mathrm{Dih}(8)$ such that $G = G_1 \circ \cdots \circ G_n$. Let A_i be an elementary abelian subgroup of G_i order 4. Then the group $\prod_{1 \leqslant i \leqslant n} A_i$ is elementary abelian of order 2^{n+1}. We prove that this is maximal by induction. This is clearly true when $n = 1$. Note that if there is $A \leq G$ elementary abelian of order 2^{n+2} then $A \cap G_1 \circ \cdots \circ G_{n-1}$ is elementary abelian of order at least 2^n and as $G_1 \circ \cdots \circ G_{n-1} \cong 2^{1+2(n-1)}$ by definition, we see that $B := A \cap G_1 \circ \cdots \circ G_{n-1}$ has order exactly 2^n. Moreover, $C_G(B) \cap G_1 \circ \cdots \circ G_{n-1} = B$ and so $|C_G(B)| \leqslant 2^{n+2}$ from which we conclude that $C_G(B) = A$ is abelian. But $G_n \leq C_G(B)$, a contradiction. Hence, no subgroup exists and since elementary abelian subgroups of order 2^{n+1} do exist, they are maximal with respect to this.

Let $G \cong 2_-^{1+2n}$ with $G_1 \cong Q_8$ and $G_i \cong \mathrm{Dih}(8)$ for $2 \leqslant i \leqslant n$. Replaying the above, we see that the maximal abelian subgroups of 2_-^{1+2n} have order 2^{n+1}. We have that $G_2 \circ \cdots \circ G_n \cong 2_+^{1+2n}$ has an elementary abelian subgroup of order 2^n. The result is clearly true when $n = 1$ so that $G \cong Q_8$. So assume that $n > 1$. Aiming for a contradiction, assume that $A \leq G$ is elementary abelian of order 2^{n+1}. Then $G_2 \circ \cdots \circ G_n \cong 2_+^{1+2(n-1)}$ and so $B := A \cap (G_2 \circ \cdots \circ G_n)$ has order at most 2^n. Now, similarly to above, we conclude that $A \leq C_G(B) = BG_1$. Hence, $A = A \cap BG_1 = B(A \cap G_1)$ by the Dedekind modular law. Since $B < A$, we conclude that $A \cap G_1 \not\leq B$ and as $Z(G_1) \leq B$, we deduce that $A \cap G_1$ is elementary abelian of order 4. But $G_1 \cong Q_8$ and we have a contradiction. This completes the proof of (ii).

For part (iii), we observe that both p_+^{1+2n} and p_-^{1+2} has nilpotency class 2 and so are regular by Theorem 2.10(i). Since p_+^{1+2} is generated by elements of order p, it follows that p_+^{1+2n} has exponent p. On the other hand, p_-^{1+2} is generated by element of order p^2 and has an element of order p^2 (visible in the p_-^{1+2} subgroup), and so has exponent p^2. □

The "usual" treatment of finite extraspecial groups generally continues by observing that for G a finite extraspecial p-group with center $Z(G) = \langle z \rangle$, G (or more precisely $G/Z(G)$) supports a non-degenerate, bilinear, alternating form (also called a *symplectic form*):

$$f : G/Z(G) \times G/Z(G) \to \mathbb{F}_p$$
$$f(\overline{x}, \overline{y}) = c$$

where $x, y \in G$, $\overline{x}$ and $\overline{y}$ are their images in $G/Z(G)$, and $[x, y] = z^c$.

This provides a lot of information about an extraspecial group. We present the following theorem regarding symplectic vector spaces over finite fields. We will not prove this here, although all the material can be extracted from Chapter II, Section 9 of Huppert's "Eindliche Gruppen I.

Theorem 2.40. *Let (V, f) be a non-degenerate symplectic vector space over a finite field $\mathbb{F}$. Then the following hold:*

(i) *V has dimension $2n$ for some $n \in N$.*

(ii) *(V, f) is the unique non-degenerate symplectic vector space over $\mathbf{F}$ of dimension $2n$.*

(iii) *There is a decomposition $V = H_1 \times \cdots \times H_n$ with $H_i = \langle x_i, y_i \rangle$ a two dimensional subspace. Moreover, $x_i y_i \in V$ may be chosen such that $f(x_i, y_i) = 1$ and $f(x_i, x_j) = 0 = f(y_i, y_j)$ for all $1 \leqslant i, j \leqslant n$.*

(iv) *For $1 \leqslant r \leqslant n$ and $x_1, \ldots, x_n$ a linear independent set of vectors in V, there are $y_1, \ldots, y_n \in V$ with $f(x_i, y_i) = 1$ and $f(x_i, x_j) = 0 = f(y_i, y_j)$ for all $1 \leqslant i, j \leqslant n$. In particular, writing $H_i := \langle x_i, y_i \rangle$, we have that $V = H_1 \times \cdots \times H_n$.*

(v) *If U is an isotropic subspace of V then U is contained in a maximal isotropic subspace of V of dimension n. In particular,* $\dim U \leqslant n$.

Proposition 2.41. *Let G be a finite extraspecial p-group. Then the following hold:*

(i) $|G| = p^{1+2m}$ *for some $m \in \mathbb{N}$;*

(ii) *for $x \in G \setminus Z(G)$, $|C_G(x)| = p^{2m}$;*

(iii) *the maximal abelian subgroups of G have order p^{1+m}; and*

(iv) *for every maximal abelian subgroup A of G, there is B a maximal abelian subgroup such that $G = AB$ and $[A, B] = A \cap B = Z(G)$.*

Proof. We have that $G/Z(G)$ is a non-degenerate symplectic vector space over $\mathrm{GF}(p)$. Then $|G/Z(G)| = p^{2m}$ for some $m \in \mathbb{N}$ from which we deduce that $|G| = p^{1+2m}$ and (i) holds.

For part (ii), we choose $x \in G \setminus Z(G)$ and form $P := \langle x, Z(G)\rangle$ abelian of order p^2. Then $P/Z(G)$ is a dimension 1 subspace of $G/Z(G)$. Then $(P/Z(G))^{\perp}$ has codimension 1. For C_x the preimage in G of $(P/Z(G))^{\perp}$, the element of C_x are precisely the elements y of G for which $[x, y] = z^0 = e$. Since $(P/Z(G))^{\perp}$ has codimension 1, $|C_x| = p^{2m}$ and (ii) holds.

For part (iii), we observe that for A a maximal abelian subgroup of G, $[x, y] = e = z^0$ for all $x, y \in A$. Hence, $A/Z(G)$ is an isotropic subspace of $G/Z(G)$ and so is contained in a maximal isotropic subspace P of dimension m. But for B the preimage in G of P, we have that $[x, y] = z^{f(\overline{x}, \overline{y})} = e$ and so B is abelian. Since A was maximal, $A = B$ and $|A| = p^{1+m}$.

For part (iv), we have that $A/Z(G)$ is elementary abelian of order p^m and so there are m elements $x_1, \ldots, x_m \in G$ such that $A = \langle x_1, \ldots, x_m, Z(G)\rangle$ and $[x_1, x_m] = e$. In particular, $Z(G)x_1, \ldots, Z(G)x_m$ are linear independent in $G/Z(G)$. Hence, there are $y_1, \ldots, y_n \in G$ such that $f(Z(G)x_i, Z(G)y_j) = \delta_{ij}$ and $f(y_i, y_j) = 0$ for all $1 \leqslant i, j \leqslant m$. Moreover, writing $B = \langle y_1, \ldots, y_m, Z(G)\rangle$, we have that $G = AB$, B is abelian of order p^{1+m} and $[A, B] = Z(G)$. □

Finally, putting a form on extraspecial groups allows us a path to classify them.

Theorem 2.42. *Let G be a finite p-group. If G is extraspecial and $|G| > p^3$ then $G \cong p_+^{1+2n}$ or $G \cong p_-^{1+2n}$ for some $n > 1$.*

Proof. We have that $G/Z(G)$ is a non-degenerate symplectic vector space over $\mathrm{GF}(p)$. Let $G/Z(G) = H_1 \times \cdots \times H_n$ be a decomposition for $G/Z(G)$ as in Theorem 2.40(iii). Then for R_i the preimage in G of H_i, we have that R_i is non-abelian of order p^3 and that $[H_i, H_j] = \{e\}$ whenever $i \neq j$. By an exercise, R_i is an extraspecial group and so G is a central product of extraspecial groups of order p^3. If $p = 2$, rearranging terms we may assume that $G \cong Q_8 \circ \cdots \circ Q_8 \circ \mathrm{Dih}(8) \circ \cdots \circ \mathrm{Dih}(8)$. By an earlier exercise, $Q_8 \circ Q_8 \cong \mathrm{Dih}(8) \circ \mathrm{Dih}(8)$ and so we can arrange that $G \cong 2_-^{1+2n}$ or 2_-^{1+2n}. The proof for p odd is similar, using the observation that $p_+^{1+2} \circ p_-^{1+2} \cong p_-^{1+2} \circ p_-^{1+2}$. $\square$

Chapter 3

Characteristic Subgroups of p-groups

We will list some basic results about characteristic subgroups. The proofs are all elementary and so we will not provide them, although the reader is encouraged to prove a selection of them in their own time.

Lemma 3.1. *Let G be a finite group with M, N characteristic subgroups of G. Then the following are true:*

(i) *MN is characteristic in G;*

(ii) *$[M, N]$ is characteristic in G;*

(iii) *$M \cap N$ is characteristic in G;*

(iv) *$C_G(M)$ is characteristic in G;*

(v) *if K is characteristic in M, then K is also characteristic in G; and*

(vi) *$\mathrm{Aut}(G)$ has an induced action on M and G/M.*

3.1 Examples of Characteristic Subgroups of p-groups

In this section, we will give some characteristic subgroups of a finite p-group G. We will often not prove that these groups are characteristic, and the reader is encouraged to prove these claims themselves.

We have already encountered lots of characteristic subgroups of G. All the terms of the derived series, the upper central series, the lower series, the “Omega” subgroups $\Omega_i(G)$ and the “Agemo” subgroups $\mho_i(G)$ are all characteristic in G. We now introduce a particularly interesting characteristic subgroup that would have came in handy in previous parts of this course: the *Frattini subgroup*.

Definition 3.2. Let G be a finite group. Then the Frattini subgroup of G, denoted $\Phi(G)$, is the intersection of all maximal subgroups of G.

We begin with some basic results which hold for all finite groups.

Lemma 3.3. *Let G be a finite group. Then $\Phi(G)$ consists of the elements $x \in G$ such that for every $K \subseteq G$ with $G = \langle x, K\rangle$ we have that $G = \langle K\rangle$. In particular, if $G = \langle M, \Phi(G)\rangle$ for some $M \leq G$, then $G = M$.*

Proof. Let $x \in \Phi(G)$ and assume that $G = \langle x, K\rangle$ for some $K \subseteq G$. Aiming for a contradiction, assume that $\langle K\rangle < G$. Then $\langle K\rangle$ lies in a maximal subgroup of G, H say. But $x \in \Phi(G) \leq H$ by definition and so $G = \langle K, x\rangle \leq H < G$, absurd. Hence, $G = \langle K\rangle$. On the other hand, assume that $x \in G$ is such that for every $K \subseteq G$ with $G = \langle x, K\rangle$ we have that $G = \langle K\rangle$. Let M be a maximal subgroup of G. Then $M = \langle M\rangle < G$. By the assumption on x, we have that $M \leq \langle M, x\rangle < G$ and by maximality of M, we deduce that $M = \langle M, x\rangle$ so that $x \in M$. This holds for all maximal subgroups of G and so $x \in \Phi(G)$.

Assume that $G = \langle M, \Phi(G)\rangle$ for some $M < G$. Then there is H, a maximal subgroup of G, such that $M \leq H$. But $\Phi(G) \leq H$ by definition and so $G = \langle M, \Phi(G)\rangle \leq H < G$, absurd. Thus, so such M exists and the result holds. □

In the case of finite p-groups we may provide an alternate characterization of the Frattini subgroup.

Lemma 3.4. *Suppose that G is a finite p-group. Then $G/\Phi(G)$ is elementary abelian. Moreover, for any $H \trianglelefteq G$ such that G/H is elementary abelian, $\Phi(G) \leq H$.*

Proof. We observe for each maximal subgroup $M < G$, we have that G/M is abelian of order p and so $G' \leq M$. Hence, $G' \leq \Phi(G)$ and $G/\Phi(G)$ is abelian. Let $M < G$ be a maximal subgroup and choose $x \in G \setminus M$. Since $|G/M| = p$, we must have that $x^p \in M$. Hence, we conclude that $x^p \in \Phi(G)$ for all $x \in G$. Thus, $(\Phi(G)x)^p = \Phi(G)x^p = \Phi(G)$ for all $x \in G$ and we conclude that $G/\Phi(G)$ has exponent p. Thus, $G/\Phi(G)$ is elementary abelian.

Assume that $H \trianglelefteq G$ and G/H is elementary abelian. By correspondence, there are $M_i \trianglelefteq G$ containing H such that $G/H = M_1/H \times \cdots \times M_r/H$ where $|G/H| = p^r$. Then $M_i^* := M_1 \dots M_{i-1}M_{i+1} \dots M_r$ is maximal subgroup of G for $i \in \{1, \dots, r\}$ (with the convention $M_0 = M_{r+1} = \{e\}$). Moreover, $\bigcap_{i\in\{1,\dots,r\}} M_i^* = H$ and since M_i^* is maximal in G, we deduce that $\Phi(G) \leq \bigcap_{i\in\{1,\dots,r\}} M_i^* = H$, as desired. □

Proposition 3.5. *Suppose that G is a finite p-group. Then $\Phi(G) = G'\mho_1(G)$.*

Proof. Since $\Phi(G)$ is abelian, $G' \leq \Phi(G)$. Furthermore, by Lemma 3.4, we see that $x^p \in \Phi(G)$ for all $x \in G$ so that $\mho_1(G) \leq \Phi(G)$. Set $Y := G'\mho_1(G)$ so that $Y \leq \Phi(G)$. We claim that G/Y is elementary abelian from which we shall deduce by Lemma 3.4 that $\Phi(G) = Y$. Note that $G' \leq Y$ and so G/Y is abelian. Moreover, for all $x \in G$, $x^p \in \mho_1(G) \leq Y$ and so $(Yx)^p = Yx^p = Y$ and so each element of G/Y has order p. Hence, G/Y is elementary abelian and we conclude that $Y = \Phi(G)$. □

We give some more elementary lemmas regarding the Frattini subgroup.

Lemma 3.6. *Let G be a finite p-group. Then the following hold:*

(i) *if $H \leq G$, then $\Phi(H) \leq \Phi(G)$;*

(ii) *if $H \trianglelefteq G$, then $\Phi(G)H/H = \Phi(G/H)$;*

(iii) *if $G = H \times K$, then $\Phi(G) = \Phi(H) \times \Phi(K)$; and*

(iv) *if $p = 2$ then $\Phi(G) = \mho_1(G)$.*

Proof. For part (i), we observe that $H\Phi(G)/\Phi(G)$ is a subgroup of an elementary abelian group, and so itself is elementary abelian. Then $H\Phi(G)/\Phi(G) \cong H/H \cap \Phi(G)$ by the second isomorphism theorem and so $H/H \cap \Phi(G)$ is elementary abelian. By Lemma 3.4, we deduce that $\Phi(H) \leq H \cap \Phi(G) \leq \Phi(G)$, as desired.

We observe that $G/\Phi(G)H \cong (G/H)/(\Phi(G)H/H)$ by the third isomorphism theorem. Since $\Phi(G) \leq \Phi(G)H$, we have that $(G/H)/(\Phi(G)H/H)$ is elementary abelian and so by Lemma 3.4, $\Phi(G/H) \leq \Phi(G)H/H$. For the reverse inclusion, set P to be the preimage in G is $\Phi(G/H)$. Then $G/P \cong (G/H)/(P/H) = (G/H)/\Phi(G/H)$ is elementary abelian by the third isomorphism theorem and by Lemma 3.4 we deduce that $\Phi(G) \leq P$. Hence, $\Phi(G)H \leq P$ and we conclude that $\Phi(G)H/H \leq \Phi(G/H)$ by correspondence. Hence $\Phi(G)H/H = \Phi(G/H)$ and (ii) holds.

Assume that $G = H \times K$. Then We identify $H, K \trianglelefteq G$ and by (i), $\Phi(H)\Phi(K) \leq \Phi(G)$. Since $H, K \trianglelefteq G$ and $\Phi(H), \Phi(K)$ are respective characteristic subgroups, we see that $\Phi(H), \Phi(K) \trianglelefteq G$. Since $H \cap K = \{e\}$, we conclude that $\Phi(H)\Phi(K) = \Phi(H) \times \Phi(K) \leq \Phi(G)$. Now, let A be a maximal subgroup of H. Then $A \times K$ is a maximal subgroup of G and so $\Phi(H) \times K$ is equal to an intersection of some of the maximal subgroups of G. Hence, $\Phi(G) \leq \Phi(H) \times K$. Similarly, we observe that $\Phi(G) \leq H \times \Phi(K)$. Hence, $\Phi(G) \leq H\Phi(K) \cap \Phi(H)K$. But $H\Phi(K) \cap \Phi(H)K = \Phi(H)(K \cap H\Phi(K)) = \Phi(H)\Phi(K)(H \cap K) = \Phi(H)\Phi(K)$ be repeated by application of the Dedekind modular law. Hence, $\Phi(G) = \Phi(H) \times \Phi(K)$, proving (iii).

For (iv), we need only show that $G' \leq \mho_1(G)$. Note that $(\mho_1(G)x)^2 = \mho_1(G)x^2 = \mho_1(G)$ and so $G/\mho_1(G)$ has exponent 2. But then $G/\mho_1(G)$ is abelian by an exercise and so $G' \leq \mho_1(G)$. □

We close with one of the many theorems which exemplify the importance of the Frattini subgroup in understanding finite p-groups.

We first make a short definition. Let $K \subseteq G$ with the property $G = \langle K \rangle$. Say that K is a *minimal generating set* for G if for all $k \in K$, setting $K^* = K \setminus \{k\}$ we have that $\langle K^* \rangle < G$.

Theorem 3.7 (Burnside Basis Theorem)**.** *Let G be a finite p-group and suppose that $|G/\Phi(G)| = p^d$ for some $d \in \mathbb{N}$. Then every minimal generating set of G is of size d.*

Proof. We claim first that there is a generating set for G of size d. By correspondence, there is $x_1, \ldots, x_d \in G$ such that $G/\Phi(G) = \langle \Phi(G)x_1, \ldots, \Phi(G)x_d \rangle$. Set $M := \langle x_1, \ldots, x_d \rangle$ and assume that $M < G$. Then $\langle x_i, \Phi(G) \rangle \leq \langle M, \Phi(G) \rangle$ for $i \in \{1, \ldots, d\}$ and we deduce that $G \leq \langle M, \Phi(G) \rangle$ and we conclude that $G = M$, a contradiction. Hence, $G = \langle x_1, \ldots, x_d \rangle$.

Suppose now that $Y := \langle y_1, \ldots, y_r \rangle$ is generating set for G where $r < d$. Then $G/\Phi(G) = \langle \Phi(G)y_1, \ldots, \Phi(G)y_r \rangle$. Since $G/\Phi(G)$ is elementary abelian, we have that $G/\Phi(G)$ is isomorphic to additive group of the vector space $\mathrm{GF}(p)^d$. Then a generating set for $G/\Phi(G)$ coincides with a basis for $\mathrm{GF}(p)^d$. Since $\mathrm{GF}(p)^d$ has dimension d, a basis contains precisely d elements, which forces a contradiction. □

Remark. Following the above proof through again, we can prove that for any $x \in G \backslash \Phi(G)$ there is a minimal generating set K for G such that $x \in K$ (using the fact that every vector in a finite dimensional vector space lies in a basis).

We now move onto analyzing abelian subgroups of some finite p-groups and characteristic subgroups arising from this.

Definition 3.8. Let G be a finite p-group and define the following three sets:

$\mathcal{A}_a(G)$ is the set of abelian subgroups of maximal possible order in G;

$\mathcal{A}_r(G)$ is the set of abelian subgroups of maximal possible p-rank in G; and

$\mathcal{A}_e(G)$ is the set of elementary abelian subgroups of maximal possible order(/rank) in G.

Then the *Thompson subgroup* of G may refer to any of three groups $J(G) = \langle \mathcal{A}(G) \rangle$, $J_r(G) = \langle \mathcal{A}_r(G) \rangle$ or $J_e(G) := \langle \mathcal{A}_e(G) \rangle$.

The group $J_r(G)$ was the original subgroup conceived by Thompson, but the groups $J_a(G)$ and especially $J_e(G)$ seem to be more popular currently.

We will prove some results about the above sets and characteristic subgroup. The results and proofs can be adapted to each of the three cases and so in this course we will focus only on the set $\mathcal{A}(G)$ and the group $J_a(G)$.

Lemma 3.9. *Let G be a finite p-group and let $A \in \mathcal{A}_a(G)$. Then the following hold:*

(i) *$A = C_G(A)$; and*

(ii) *if $A \leq H \leq G$, then $A \in \mathcal{A}_a(H) \subseteq \mathcal{A}_a(G)$.*

Proof. Let $A \in \mathcal{A}_a(G)$. Then clearly we have that $A \leq C_G(A)$. Assume that there is $g \in C_G(A) \setminus A$. Then $\langle g, A\rangle$ is abelian of order strictly larger than A, a contradiction. Hence $C_G(A) = A$ and (i) holds.

Suppose that there is $B \in \mathcal{A}_a(H)$ with $B \notin \mathcal{A}_a(G)$. Since $A \leq H$ we have that $|A| \leqslant |B|$, and since $B \leq H \leq G$, we have that $|A| = |B|$. But then clearly $B \leq \mathcal{A}_a(G)$. Hence, no such B exists and $\mathcal{A}_a(H) \subseteq \mathcal{A}_a(G)$. Since $A \leq H$, we immediately see that $A \in \mathcal{A}_a(H)$. □

We pause to prove a slight generalization of the above result.

Proposition 3.10. *Let G be a finite p-group and let A be a normal, abelian subgroup of G which is not properly contained in any other abelian subgroup which is normal in G. Then $A = C_G(A)$.*

Proof. Since A is abelian $A \leq C_G(A)$. Aiming for a contradiction, assume that $A < C_G(A)$. Note that as $A \trianglelefteq G$, we have that $C_G(A) \trianglelefteq G$. In particular, there is a chain of subgroups $\{1\} = G_0 \leq G_1 \cdots \leq C_G(A) = G_i \leq \ldots G_n = G$ such that $G_i \trianglelefteq G$ for all $i \in \{0\ldots, n\}$. Let $t \in \{0, \ldots, i\}$ be minimal such that $G_t \not\leq A$. Then $|G_tA/A| = p$ and since A is central and index p in G_tA, we have that G_tA is abelian. But $G_t, A \trianglelefteq G$ so that $G_tA \trianglelefteq A$, contradicting the maximality of A. Hence, $A = C_G(A)$, as desired. □

Proposition 3.11. *Let G be a finite p-group. Then the following hold:*

(i) *$C_G(J_a(G)) = Z(J_a(G)) \leq J_a(G)$;*

(ii) *$\bigcap_{A\in\mathcal{A}_a(G)} A = Z(J_a(G))$; and*

(iii) *if $J_a(G) \leq H \leq G$, then $J_a(G) = J_a(H)$.*

Proof. Note that $Z(J_a(G)) \leq C_G(J_a(G)) \cap J_a(G)$ and $C_G(J_a(G)) \cap J_a(G)$ is contained in $J_a(G)$ and centralizes $J_a(G)$. Hence, to prove (i) it suffices to show that $C_G(J_a(G)) \leq J_a(G)$. But $C_G(J_a(G)) \leq C_G(A) = A \leq J_a(G)$ for all $A \in \mathcal{A}_a(G)$ and so (i) is proved.

Since $J_a(G) = \langle \mathcal{A}_a(G)\rangle$, it is clear that $\bigcap_{A\in\mathcal{A}_a(G)} A \leq Z(J_a(G))$. It remains to show that $Z(J_a(G)) \leq A$ for all $A \in \mathcal{A}_a(G)$. But $Z(J_a(G)) = C_G(J_a(G)) \leq C_G(A) = A$, and so (ii) is proved.

Finally, if $J_a(G) \leq H \leq G$ then for all $A \in \mathcal{A}_a(G)$, $A \leq H \leq G$. Then $\mathcal{A}_a(H) = \mathcal{A}_a(G)$ so that $J_a(H) = J_a(G)$, as desired. □

We close this slew of subgroups with a slightly more complex characteristic subgroup of a finite p-group. First we need some definitions.

Definition 3.12. Let G be a finite p-group with N a normal p-subgroup. Say that N admits a *Q-series* in G if there is a chain of subgroups

$$\{1\} = Q_0 \leq Q_1 \leq \cdots \leq Q_{l-1} \leq Q_l = N$$

such that $Q_i \trianglelefteq G$ and

$$[\Omega_1(C_G(Q_{i-1})), \underbrace{Q_i, \ldots, Q_i}_{p-1 \text{ times}}] = \{e\}$$

for each $1 \leqslant i \leqslant l$.

Exercise 3.13. Suppose that G is a finite p-group with $N, K \trianglelefteq G$. If N admits a Q-series in G

$$\{e\} = Q_0 \leq \cdots \leq Q_l = N$$

and K admits a Q-series in G

$$\{e\} = R_0 \leq \cdots \leq R_t = K$$

then the series

$$\{e\} = Q_0 \leq \cdots \leq Q_l \leq Q_l R_1 \leq \cdots \leq Q_l R_t$$

is a Q-series in G for NK. In particular, there is a unique largest subgroup of G admitting a Q-series.

Definition 3.14. For G a finite p-group, we set $\mathfrak{X}(G)$, called *Oliver's p-subgroup*, to be the largest subgroup of G admitting a Q-series.

Proposition 3.15. *Let G be a finite p-group. Then the following hold:*

(i) *If $p = 2$, then $\mathfrak{X}(G) = C_G(\Omega_1(G))$.*

(ii) *If p is odd and A is an abelian normal subgroup of G, then $A \leq \mathfrak{X}(G)$. In particular, $C_G(\mathfrak{X}(G)) = Z(\mathfrak{X}(G))$.*

(iii) *If $R \trianglelefteq G$ with $[\Omega_1(Z(\mathfrak{X}(G))), \underbrace{R, \ldots, R}_{p-1 \text{ times}}] = \{e\}$, then $R \leq \mathfrak{X}(G)$.*

(iv) *If $\mathfrak{X}(G) \leq H \leq G$, then $\mathfrak{X}(G) \leq \mathfrak{X}(H)$.*

Proof. For (i), we have that $p = 2$. Then the definition of a Q-series becomes $[\Omega_1(C_G(Q_{i-1})), Q_i] = \{e\}$. Note that $[\Omega_1(C_G(\{e\})), C_G(\Omega_1(G))] = [\Omega_1(G), C_G(\Omega_1(G))] = \{e\}$ and so $\{e\} \leq C_G(\Omega_1(G))$ is a Q-series in G. Hence, $C_G(\Omega_1(G)) \leq \mathfrak{X}(G)$. Conversely, for any other subgroup N which admits a Q-series in G, by an exercise we can form the Q-series

$$\{e\} = Q_0 \leq \cdots \leq C_G(\Omega_1(G)) \leq Q_l \leq \cdots \leq C_G(\Omega_1(G))N.$$

Assume that $C_G(\Omega_1(G)) < Q_l$. Then $[\Omega_1(C_G(C_G(\Omega_1(G)))), Q_l] = \{e\}$ by definition. But $\Omega_1(G) \leq \Omega_1(C_G(C_G(\Omega_1(G))))$ and so $Q_l \leq C_G(\Omega(G))$, a contradiction. Hence, $\mathfrak{X}(G) = C_G(\Omega_1(G))$.

Since A is an abelian normal subgroup of G and $p > 2$, we have that

$$\{e\} = [A, A] = [\Omega_1(G), A, A] \geq [\Omega_1(G), \underbrace{A, \dots, A}_{p-1 \text{ times}}] = [\Omega_1(C_G(\{e\})), \underbrace{A, \dots, A}_{p-1 \text{ times}}]$$

and so $\{e\} \leq A$ is a Q-series for A is G. That $C_G(\mathfrak{X}(G)) = Z(\mathfrak{X}(G))$ follows quickly from Proposition 3.10, completing the proof of (ii).

For (iii) we observe that there is a Q-series $\{e\} \leq Q_1 \leq \cdots \leq Q_n = \mathfrak{X}(G)$. Set $Q_{n+1} = \mathfrak{X}(G)R$. We observe that $\mathfrak{X}(G)$ centralizes $Z(\mathfrak{X}(G)) = C_G(\mathfrak{X}(G))$. Then

$$\{e\} = [\Omega_1(Z(\mathfrak{X}(G))), \underbrace{Q_{n+1}, \dots, Q_{n+1}}_{p-1 \text{ times}}] = [\Omega_1(C_G(\mathfrak{X}(G))), \underbrace{Q_{n+1}, \dots, Q_{n+1}}_{p-1 \text{ times}}].$$

Hence, $\{e\} \leq Q_1 \leq \cdots \leq Q_n \leq Q_{n+1}$ is a Q-series for Q_{n+1} in G and by definition of $\mathfrak{X}(G)$, we see that $Q_{n+1} = \mathfrak{X}(G)$ so that $R \leq \mathfrak{X}(G)$.

Suppose that there is $H \leq G$ with $\mathfrak{X}(G) \leq H$. Let $\{e\} = Q_0 \leq Q_1 \leq \cdots \leq Q_n = \mathfrak{X}(G)$ be a Q-series for $\mathfrak{X}(G)$ in G. Note that each Q_i is normal in G and contained in H so that $Q_i \trianglelefteq H$ for all $i \in \{0, \dots, n\}$. Moreover, for each i we have that $C_H(Q_{i-1}) \leq C_G(Q_{i-1})$ so that

$$[\Omega_1(C_H(Q_{i-1})), \underbrace{Q_i, \dots, Q_i}_{p-1 \text{ times}}] \leq [\Omega_1(C_G(Q_{i-1})), \underbrace{Q_i, \dots, Q_i}_{p-1 \text{ times}}] = \{e\}$$

and so $\mathfrak{X}(G)$ admits a Q-series in G. Hence, $\mathfrak{X}(G) \leq \mathfrak{X}(H)$ completing the proof of (iv). □

The interaction between $J_e(G)$ and $\mathfrak{X}(G)$ was the original motivation for the study of $\mathfrak{X}(G)$. The following conjecture has been verified in some cases but (at the time of writing) is very much still open.

Conjecture 1 (Oliver's p-group Conjecture)**.** *For p an odd prime and G a finite p-group, we have that $J_e(G) \leq \mathfrak{X}(G)$.*

3.2 Characterization Theorems

In this section, we will use the knowledge we've garnered previously in this chapter to prove some classification theorems for finite p-groups. This, in some way, might justify our selection of "interesting" p-groups from this previous chapter.

Theorem 3.16. *Suppose that G is a finite p-group of order p^{n+1} with a cyclic maximal subgroup. Then one of the following holds:*

(i) $G = C_{p^{n+1}}$;

(ii) $G = C_{p^n} \times C_p$;

(iii) *$p = 2$ and G is either dihedral, semidihedral, generalized quaternion or a modular group; or*

(iv) *p is odd and $G = \mathrm{Mod}(p^n)$ for some $n \in N$.*

Proof. Suppose that G is a finite p-group with a maximal subgroup M such that M is cyclic. Set $|M| = p^n$ so that $|G| = p^{n+1}$. Since groups of order p^2 are abelian, and we have determined all groups of order p^3, we may as well assume throughout that $n > 2$. Then $\Phi(M)$ has index p in M, and is contained in $\Phi(G)$. If $\Phi(G)$ is maximal in G, then $\Phi(G) = M$ is the unique maximal subgroup of G and so G is cyclic.

Thus, from this point, we may assume that $\Phi(G) = \Phi(M)$ has index p^2 in G. By Burnside's Basis Theorem, there are $a, b \in G$ such that $M = \langle a \rangle$ and $G = \langle a, b \rangle$. Since $b^p \leq \mho_1(G)\Phi(G) \leq M$, we can choose b such that $b^p = a^{p^l}$ for some l. We further make the choice of b such that $l \leqslant n$ is as large as possible. We observe that b^p is centralized by $G = \langle a, b \rangle$.

Now, $M \trianglelefteq G$ and so $a^b = a^r$ for some $1 \leqslant r < p^n$. If $r = 1$, then b centralizes a from which we deduce that G is abelian, and outcome (ii) holds. Hence, we assume that $r > 1$. Now, $a^{r-1} = a^{-1}a^b = [a, b] \in G'$. But G' has index at least p in M and so $a^{r-1} = a^{sp}$ for some $s \in \mathbb{N}$, from which we conclude that p divides $r - 1$. Since $b^p \in Z(G)$ we see that $a = b^{-p}ab^p = a^{r^p}$ and we conclude that $a^{r^p-1} = e$ so that p^n divides $r^p - 1$.

Case 1:

Suppose that p is odd. Write $t = r - 1$ and consider $d := \frac{r^p-1}{r-1} = \frac{(t+1)^p-1}{t}$. Since $r < p^n$, we have that p^n does not divide $r - 1$. But p^n does divide $r^p - 1$ and so we conclude that p divides d. Now,

$$d = \frac{t^p + \binom{p}{1}t^{p-1} + \cdots + \binom{p}{p-1}t + 1 - 1}{t} = t^{p-1} + \binom{p}{1}t^{p-2} + \cdots + \binom{p}{p-2}t + p$$

and as p divides $t = r - 1$ and $p > 2$, we deduce that p^2 divides $d - p$. If p^2 divides d, then p^2 divides p, absurd. Hence, p^{n-1} divides $r - 1$ and $r = kp^{n-1} + 1$. Then $(a^p)^b = a^{pr} = a^{kp^n+p} = a^p$ and so $a^p \in Z(G)$. Hence, $Z(G) = \Phi(G)$ has index p^2 in G and G has nilpotency class two.

Set i minimal such that $ik \equiv 1 \mod p$ so that $ik = 1 + pl$ for some $l \in N$. Then $b^i \notin M$ and $a^{b^i} = a^{(kp^{n-1}+1)^i}$. If $i = 1$ then as a has order p^n, we see that $a^b = a^{(1+pl)p^{n-1}+1} = a^{p^{n-1}+1}$. If $i > 1$ then

$$(kp^{n-1} + 1)^i = (kp^{n-1})^i + \binom{i}{2}(kp^{n-1})^{i-1} + \cdots + ikp^{n-1} + 1$$

where every summand except the final two is divisible by p^n. Again, since a has order p^n, we conclude that $a^{b^i} = a^{ikp^{n-1}+1} = a^{(1+pl)p^{n-1}+1} = a^{p^{n-1}+1}$.

Now, $(b^i)^p \in \mho_1(G) \leq \Phi(G) = \Phi(M)$ and so there is $j \in \mathbb{N}$ such that $(b^i)^p = (a^p)^j = (a^j)^p$. Set $x := a$ and $y := b^i a^{-j}$. Since $b \notin M$, we have that $y \notin M$ and $G = \langle x, y \rangle$.

Then $x^y = a^{ba^{-j}} = a^{-j}a^{b^i}a^j = a^{p^{n-1}+1}$. Since G is of nilpotency class two, G is regular and as $(b^i)^p = (a^j)^p$, Proposition 2.11(iii) yields that $y^p = e$. Hence, G is quotient of the group described in (iv). We leave it to the reader to verify the group described in (iv) has order p^{n+1}.

Case 2:

We have that 2^n divides $r^2 - 1 = (r+1)(r-1)$ and that r is odd. Note that 4 cannot simultaneously divide $r-1$ and $r+1$ and so, as $n > 2$, 2^{n-1} divides one of $r-1$ or $r+1$.

Case 2a:

Suppose that 2^{n-1} divides $r-1$. Since $r < 2^n$ we have that $r = 2^{n-1}+1$. Hence, $a^b = a^{2^{n-1}+1}$. If $b^2 = e$ then setting $a = x$ and $b = y$, we have that G is a quotient of $\mathrm{Mod}(2^{n+1})$ of the same order as $\mathrm{Mod}(2^{n+1})$ and so $G = \mathrm{Mod}(2^{n+1})$. Assume now that $b^2 \neq e$ and set $b_* = b^{-1}a^{2^{l-1}}$. Then $b^* \notin M$ and so $G = \langle a, b^* \rangle$. Moreover,

$$(b^*)^2 = b^{-1}a^{2^{l-1}}b^{-1}a^{2^{l-1}} = (a^{2^{l-1}})^b b^{-2}a^{2^{l-1}} = a^{2^{l-1}r}a^{-2^l}a^{2^{l-1}} = a^{2^{n+l-2}}.$$

Since l was chosen as large as possible, we have that $l \geqslant n+l-2$ so that $n \leqslant 2$, a contradiction since we assumed that $n > 2$.

Case 2b:

Suppose that 2^{n-1} divides $r+1$. Then as $r < 2^n$, either $r = 2^{n-1}-1$ or $r = 2^n - 1$. In the latter case, we have that $a^b = a^{2^n-1} = a^{-1}$. If $b^2 = e$ then taking $a = x$ and $b = y$, G is a quotient of the dihedral group of order 2^{n+1} of order 2^{n+1}. Hence, $G = \mathrm{Dih}(2^{n+1})$. If $b^2 = a^{2^l} \neq e$, then we consider $(a^{2^l})^b = b^2$ from which we deduce that b centralizes a^{2^l}. Since $a^b = a^{-1}$, we get that $a^{2^l} = (a^{2^l})^b = a^{-2^l}$ from which we conclude that $a^{2^{l+1}} = e$. It follows that $l+1 = n$ and so $b^2 = a^{2^{n-1}}$ so that $b^4 = e$. Taking $x = a$ and $y = b$, we have that G is a quotient of $Q_{2^{n+1}}$ of order 2^{n+1} and so $G = Q_{2^{n+1}}$.

In the former case, we have that $r = 2^{n-1}-1$ and so $a^b = a^{2^{n-1}-1}$. If $b^2 = e$, then taking $x = a$ and $b = y$, we have that G is a quotient of $\mathrm{SDih}(2^{n+1})$ of order 2^{n+1} and so $G = \mathrm{SDih}(2^{n+1})$. Hence, we assume, aiming for a contradiction, that $b^2 \neq e$. Since $b^2 = a^{2^l}$, we have that $a^{2^l} = (a^{2^l})^b$. On the other hand, $a^b = a2^{n-1} - 1$ implies that $a^{2^l} = a^{2^l(2^{n-1}-1)}$ so that $a^{2^l(2^{n-1}-2)} = e$. Hence, 2^n divides $2^l(2^{n-1}-2) = 2^{l+1}(2^{n-2}-1)$. Since $2^{n-2}-1$ is odd, we conclude that $n = l+1$ and so $b^2 = a^{2^{n-1}}$. But now $ab \notin M$ and $(ab)^2 = ab^2a^b = aa^{2^{n-1}}a^{2^{n-1}-1} = a^{2^n}$, a contradiction since b was chosen with l as large as possible. □

From this theorem, we can prove a slew of other recognition results. These theorems end up being extremely important for certain “small” configurations in finite group theory.

Theorem 3.17. *Suppose that G is a finite p-group with $N \trianglelefteq G$. Then either:*

(i) *there is $K \leq N$ with $K \trianglelefteq G$ and K elementary abelian of order p^2; or*

(ii) *N is cyclic, dihedral, semidihedral or generalized quaternion.*

Moreover, in (ii) if $N \leq \Phi(G)$ then N is cyclic.

Proof. Choose $N \trianglelefteq G$ a counterexample minimal with respect to order. Since $N \trianglelefteq G$, we have that $Y := N \cap Z(G) \neq \{e\}$. If $|\Omega_1(Y)| > p$, then any subgroup of $\Omega_1(Y)$ of order p^2 is elementary abelian, normal in G and contained in N and so outcome (i) would hold in this case. Hence, $|\Omega_1(Y)| = p$ so that Y is cyclic.

Suppose first that N is abelian, but not cyclic and let $X = \Omega_1(N)$. Since N is non-cyclic, $|X| \geqslant p^2$ and since since X is characteristic in N, $X \trianglelefteq G$. In particular, $Y = X \cap Z(G) \neq \{e\}$. By an exercise, there is a chain $\{e\} = G_0 \leq G_1 \leq \cdots \leq G_k = \Omega_1(N) \leq \cdots \leq G_n = G$ such that $G_i \trianglelefteq G$ and $|G_i/G_{i-1}| = p$ for $i \in \{1, \dots, n\}$. Then for K the preimage in G of G_1, we have that $K \leq \Omega_1(N)$ and so is elementary abelian, $K \trianglelefteq G$ and $|K| = p^2$, and so (i) holds.

Hence, we may assume for the remainder of the proof that N is non-abelian. In particular, $|G| \geqslant p^4$. Let A be the largest abelian subgroup of N which is normal in G. Clearly, $Y \leq A < N$ and $C_N(A) \trianglelefteq G$. By considering the quotient G/A and using correspondence, we must have that $C_N(A) = A$. Moreover, since any subgroup of A which is normal in G and elementary abelian of order p^2 satisfies the requirements of K in outcome (i), and as N is a counterexample, we must have that A is abelian and satisfies (ii) so that A is cyclic.

Suppose that $|N/A| \geqslant p^2$ and let R be the unique subgroup of A of order p^2. Since $|\mathrm{Aut}(R)|$ is not divisible by p^2, it follows that $A < C_N(R)$. Since R is characteristic in A, R is normal in G from which we deduce that $R < C_N(R) \trianglelefteq G$. Again by correspondence, this time considering the quotient G/A, we deduce that there is $W \trianglelefteq G$ with $|W/A| = p$, W non-abelian and $W \leq C_N(R)$. By minimality of N, we have that W satisfies the conclusion of the theorem. Any subgroup of W which is normal in G and elementary abelian of order p^2 satisfies the requirements for part (i) and so we may assume that W satisfies part (ii). Since W is non-abelian and $R \leq Z(W)$ where $|R| \geqslant p^2$, we have a contradiction.

Hence, $|N/A| = p$ and N has a maximal subgroup which is cyclic. By Theorem 3.16 it remains to show that N is not isomorphic to $\mathrm{Mod}(p^n)$. So assume that $N \cong \mathrm{Mod}(p^n)$ is generated by elements $x, y \in N$ satisfying the presentation given in the previous chapter. Suppose that $n = 3$. Then either N satisfies (ii), or p is odd and $N \cong p_-^{1+2}$. But then $\Omega_1(N)$ is elementary abelian of order p^2 and since $\Omega_1(N)$ is characteristic in N, we may take $K = \Omega_1(N)$ satisfying (i). Hence, we assume that $n > 3$.

Observe that, by an exercise, $|N'| = p$ and $|N/Z(N)| = p^2$. Let $T = \langle x \rangle$ be the cyclic subgroup of index p in N. Note that $\Omega_1(N)$ is contained in the preimage in N of $\Omega_1(N/N')$ and since N/N' has a cyclic subgroup of index p, we conclude that $|\Omega_1(N)| \leqslant p^3$. Moreover, $|Z(N)| \geqslant p^2$ and $Z(N) \leq T$ so that $\Omega_1(N) \cap T \leq Z(N)$ from which we conclude that $\Omega_1(N)$ is abelian. But then $\Omega_1(N)$ has exponent p and so $\Omega_1(N) \cap T = \Omega_1(N)$ has order p. Hence, $|\Omega_1(N)| \leqslant p^2$. Since $y^p = e$ we see that $\langle \Omega_1(T), y \rangle$ is elementary abelian and contained in $\Omega_1(N)$ from which we deduce that $\Omega_1(N)$ is elementary abelian of order p^2. Taking $K = \Omega_1(N)$, we satisfy part (i).

Suppose that N is as described in (ii) and is not cyclic. Then N has a unique cyclic maximal subgroup T. Then T is characteristic in N, and so is $\Omega_2(T)$. Hence, $\Omega_2(T)$ is a cyclic normal subgroup of G of order 4. Moreover, since $|Z(N)| = 2$, $\Omega_2(T)$ is not central in N. But now, $|\mathrm{Aut}(\Omega_2(T))| = 2$ from which we deduce that $|G/C_G(\Omega_2(T))| \leqslant 2$ so that $N \leq \Phi(G) \leq C_G(\Omega_2(T))$, a contradiction. □

Theorem 3.18. *Suppose that G is a finite p-group with $m_p(G) = 1$. Then G is cyclic, or $p = 2$ and G is generalized quaternion.*

Proof. Since $m_p(G) = 1$, G has no subgroup which is elementary abelian of order p^2. Therefore, by Theorem 3.17, G is either cyclic, generalized quaternion, dihedral or semidihedral. In the latter two cases, the subgroup $\langle x^{2^{n-2}}, y \rangle$ is elementary abelian of order 4. □

Theorem 3.19. *Suppose that G is a non-abelian finite 2-group such that $|G/G'| = 4$. Then G is dihedral, semidihedral or generalized quaternion.*

Proof. Suppose that G is counterexample to the theorem chosen minimally with respect to order and set $|G| = 2^n$. The result is true when $|G| = 2^3$ and so we may assume that $|G| \geqslant 2^4$. Let $R \leq Z(G) \cap G'$ with $|R| = 2$ so that $(G/R)' = G'/R$ has index 4 in G/R. Since $G \geqslant 2^4$, we have that G/R is non-abelian. By minimality of G, G/R is dihedral, semidihedral or generalized quaternion. Let $x \in G$ be such that $\langle x \rangle R/R$ is a cyclic of index 2 in G/R. Set $X := \langle x \rangle$ so that X is a cyclic subgroup of index at most 4 in G.

If X is maximal in G then G is determined by Theorem 3.16. In particular, since G is counterexample to the theorem we have that $G = \mathrm{Mod}(2^n)$ for $n > 3$. But then $|G/G'| > 4$, a contradiction. Hence, X has index 4 in G so has order at least 4, and $X \cap R = \{e\}$. Then $N := XR \cong C_{2^{n-2}} \times C_2$ is abelian. Then, by an exercise, $Z(G) = |A/G'| = 2$ so that $Z(G) = R$. But $\mho_1(N)$ is normal in G, index 2 in X and intersects R trivially, a contradiction. □

We finish with a corollary, classifying the *maximal class* 2-groups. If G is a p-group of order p^n, say that G has *maximal class* if G has nilpotency class $n - 1$.

Corollary 3.20. *Suppose that G is a non-abelian 2-group of maximal class. Then G is dihedral, semidihedral or generalized quaternion.*

Proof. Since G has maximal class, we have that $|G/G'| = 4$ and so G is determined by Theorem 3.19. □

Chapter 4

Actions and Automorphisms of p-groups

In this chapter, we focus on what can be said about actions on p-groups (most in the form of automorphisms), and what happens to these actions when restricted to certain characteristic subgroups or quotients. We first make precise what mean mean by *actions* on groups.

Definition 4.1. Let G and K be finite groups. Say that K acts on G if K acts on the underlying set of G and satisfies $(gh) \cdot k = (g \cdot k)(h \cdot k)$ for all $k \in K$ and $g, h \in G$.

It may be parsed from the definition, that if the action of K on G is faithful, then there is an embedding of K into $\mathrm{Aut}(G)$.

We have already seen an example of a group acting on group. Let G be a finite group and $N \trianglelefteq G$. Then conjugation defines an action of G on N. This motivates the following notations/definitions.

Definition 4.2. Let G be a finite group and A a finite group acting on G. Then write

(i) $C_G(A) := \{g \in G \mid g \cdot a = g \text{ for all } a \in A\}$;

(ii) $C_A(G) := \{a \in A \mid g \cdot a = g \text{ for all } g \in G\}$;

(iii) $[G, a] := \langle g^{-1}(g \cdot a) \mid g \in G\rangle \leq G$; and

(iv) $[G, A] := \langle [G, a] \mid a \in A\rangle \leq G$.

We wish to highlight that $C_G(A)$ is the set of fixed points of G under the action of A. Moreover, the induced action of $A/C_A(G)$ is faithful on G. Finally if $G \trianglelefteq A$ and A acts on G by conjugation, then $[G, A]$ is the standard commutator as defined earlier.

Lemma 4.3. *Let G be a finite group and A a finite group acting on G. Then*

(i) *$C_G(A) \leq G$ and $C_A(G) \leq A$;*

(ii) *$C_G(\langle a \rangle) = \{g \in G \mid g \cdot a = g\} =: C_G(a)$ for $a \in A$;*

(iii) *if $B \leq A$, then $[g, B] \cdot a = [g \cdot a, B^a]$; and*

(iv) *$[G, A] = [A, G] := \langle (g^{-1} \cdot a)g \mid g \in G, a \in A\}$.*

Proof. Part (i) follows quickly from definitions and we leave it as an exercise for the reader. For part (ii), we clearly have that $C_G(\langle a \rangle) \subseteq C_G(a)$ by definition. Let $g \in C_G(a)$. Then $g \cdot a^i = (g \cdot a) \cdot a^{i-1} = g \cdot a^{i-1}$ for all $i \in \mathbb{N}$ and it follows that $g \cdot a^i = g$ from which we conclude that $g \in C_G(\langle a \rangle)$, completing the proof of (ii).

Let $B \leq A$, $a \in A$ and $b \in B$. Then

$$[g, b] \cdot a = (g^{-1}(g \cdot b)) \cdot a = (g^{-1} \cdot a)(g \cdot ba) = (g \cdot a)^{-1}(g \cdot aa^{-1}ba) = (g \cdot a)^{-1}(g \cdot a) \cdot b^a = [g \cdot a, b^a].$$

Hence, (iii) holds.

Finally, for (iv) let $g \in G$ and $a \in A$. Then $[a, g] = (g^{-1} \cdot a)g = (g^{-1}(g \cdot a^{-1})) \cdot a = [g, a^{-1}] \cdot a = [g \cdot a, a^{-1}]$ by part (iii). Hence, $[A, G] \subseteq [G, A]$. We leave the other inclusion as an exercise. □

Letting $N \leq G$, we say that N is A-invariant if the restriction of the action of A on G to N preserves N i.e. $N \ldots A \leq N$.

Moreover, if $N \trianglelefteq G$, then we can form the quotient G/N which inherits a well-defined A-action where $gN \cdot a = (g \cdots a)N$.

We also remark that the three subgroups lemma also holds: for X, Y, Z a mix of subgroups of G and A, whenever $[X, Y, Z] = [Y, Z, X] = \{e\}$ we have that $[Z, X, Y] = \{e\}$.

Proposition 4.4. *Let G be a finite group, A a finite group acting on G and N be an A-invariant subgroup of G. Then*

(i) *every characteristic subgroup of G is an A-invariant normal subgroup of G;*

(ii) *$[G, A]$ is an A-invariant subgroup of G;*

(iii) *if $N \trianglelefteq G$ then $[G, A] \leq N$ if and only if the induced action of A on G/N is trivial;*

(iv) *if $N \trianglelefteq G$ and A acts trivially on N, then $[G, A] \leq C_G(N)$; and*

(v) *if $N \trianglelefteq G$ and A acts trivially on N and G/N, then $[A, G] \leq Z(N)$ and $A' \leq C_A(G)$.*

Proof. We observe that $A/C_A(G)$ embeds in $\mathrm{Aut}(G)$. Hence, the induced action of $A/C_A(G)$ on G leaves every characteristic subgroup invariant, and since $C_A(G)$ leaves every invariant every subgroup of G, (i) holds.

Part (ii) comes from Lemma 4.3 (ii) taking $B = A$.

Suppose that $[G, A] \leq N \trianglelefteq G$. Let $g \in G$ and $a \in A$. Then $g^{-1}(g \cdot a) = n \in N$ so that $g \cdot a = gn$ from which we deduce that $(gN) \cdot a = (g \cdot a)N = gN$ and A acts trivially on G/N. On the other hand, if $(gN) \cdot a = gN$ then $gn \cdot a = gn'$ for $n \in N$ and some $n' \in N$. Since N is A-invariant, $n \cdot a = n'' \in N$ so that $(g \cdot a)n'' = (g \cdot a)(n \cdot a) = gn \cdot a = gn'$. Finally, we have that $[g, a] = g^{-1}(g \cdot a) = n'(n'')^{-1} \in N$ from which we conclude that $[G, A] \leq N$, and (iii) is proved.

Suppose that A acts trivially on $N \trianglelefteq G$ so that $[N, A] = \{e\}$. Then $[N, A, G] = \{e\}$ and as $N \trianglelefteq G$, $[G, N, A] \leq [N, A] = \{e\}$. By the three subgroups lemma, we deduce that $[A, G, N] = [G, A, N] = \{e\}$ from which we conclude that $[G, A] \leq C_G(N)$, which is (iv). (In particular, $C_G(N)$ is A-invariant.)

Finally, suppose that A acts trivially on $N \trianglelefteq G$ and G/N. By parts (iii) and (iv), we have that $[A, G] = [G, A] \leq N \cap C_G(N) \leq Z(N)$. Since A acts trivially on N, we have that $[G, A, A] \leq [Z(N), A] = \{e\}$. Also, $[A, G, A] = [G, A, A] = \{e\}$ and so the three subgroups lemma implies that $[A, A, G] = \{e\}$ so that $A' \leq C_A(G)$, completing the proof of (v) and the proposition. □

4.1 Coprime Action Results

We now specialize to the situation where G is a finite p-group.

Proposition 4.5. *Suppose that G is a finite p-group and A is a finite p-group which acts on G. Then $C_G(A) \neq \{1\}$ and $[G, A] < G$.*

Proof. Form the semidirect product $G \rtimes A$, where the action of A on G defines the conjugation action of A on G in the semidirect product. Since G and A are p-groups, $G \rtimes A$ is a p-group. Since $G \trianglelefteq G \rtimes A$, we have that $G \cap Z(G \rtimes A) \neq \{e\}$. But $Z(G \rtimes A)$ is fixed by the action of A and so $\{e\} \neq G \cap Z(G \rtimes A) \leq C_G(A)$. That $[G, A] < G$ follows from Lemma 1.11. □

In particular, finite p-groups act *unipotently* on other finite p-groups. One can then ask how elements of order prime to p act on finite p-groups. The study of these types of actions fall under the umbrella term *coprime action.*

Definition 4.6. Let G be a finite group and A be a finite group which acts on G. Say that A acts *coprimely* on G if $(|G|, |A|) = 1$ and one of A or G is a solvable.

By the Feit–Thompson theorem, every group of odd order is solvable and so the second condition in coprime action is superfluous. For us, the group G will primarily be a finite p-group. In particular, G is a solvable group and so we will not require the Feit–Thompson theorem. All we require is that $(|A|, p) = 1$.

In the following lemma, we will make use of the Schur–Zassenhaus theorem which we state without proof.

Theorem 4.7. *Let G be a finite group with a normal subgroup N. Suppose that $(|N|, |G/N|) = 1$. Then there is $H \leq G$ a* complement *to N such that $G = N \rtimes H$. Moreover, provided one of G/N or N is solvable, all complements to N in G are conjugate.*

As intimated earlier, we will always have one of G/N or N a finite p-group and so the solvability condition comes for free.

Lemma 4.8. *Let G be a finite p-group and A be a finite group acting coprimely on G. Suppose that U is an A-invariant subgroup of G and there is $g \in G$ with Ug an A-invariant subset of G. Then there is $c \in C_G(A)$ such that $Ug = Uc$.*

Proof. Since U and Ug are A-invariant, for all $a \in A$ and $u \in U$ there is $u', u'' \in U$ such that $u'(g \cdot a) = (u \cdot a)(g \cdot a) = ug \cdot a = u''g$. Hence, $[a, g^{-1}] = (g \cdot a)g^{-1} = (u')^{-1}u'' \in U$ so that $[G, A] = [A, G] \leq U$. Form the semidirect product $G \rtimes A$, where the action of A on G defines the conjugation action of A on G in the semidirect product. Since U is A-invariant, we recognize $U \trianglelefteq G \rtimes A$. That $[A, G] \leq U$ implies that $a^{-1}a^{g^{-1}} \in U$. Hence, for all $a \in A$ we have that $a^{g^{-1}} \in aU$ so that $A^{g^{-1}} \leq AU = UA$.

Since $A \cap G = \{e\}$, we have that $A \cap U = \{e\}$ and as $U^{g^{-1}} = U$, we deduce that that $A^{g^{-1}} \cap U = \{e\}$. Moreover, $|A| = |A^{g^{-1}}|$ and we deduce that $UA = UA^{g^{-1}}$ and so A and $A^{g^{-1}}$ are complements to U in $U \rtimes A$. By the Schur–Zassenhaus theorem, there is $u \in U$ such $A^u = A^{g^{-1}}$. Then $A = A^{ug}$ so that $ug \in C_G(A)$. Since $Ug = Uug$, the lemma is proved. □

Proposition 4.9. *Let G be a finite p-group and A be a finite group acting coprimely on G. Let N be an A-invariant normal subgroup of G. Then the following hold:*

(i) *$C_{G/N}(A) = C_G(A)N/N$;*

(ii) *$G = [G, A]C_G(A)$;*

(iii) *$[G, A] = [G, A, A]$; and*

(iv) *if A acts trivially on G/N and N then A acts trivially on G.*

Proof. For part (i), since $[C_G(A), A] = \{e\} \leq N$, we have that $C_G(A)N/N \leq C_{G/N}(A)$. For the other inclusion, we let $Ng \in C_{G/N}(A)$. Then Ng is A-invariant and so by Lemma 4.8, there is $c \in C_G(A)$ such that $Ng = Nc$ so that $Ng \in C_G(a)N/N$.

For part (ii), let $U = [G, A]$ so that U is A-invariant. Moreover, for $g \in G$ we have that $g \cdot a = (g \cdot a)g^{-1}g = [a, g^{-1}]g$ and since $[A, G] = [G, A]$ we ascertain that $(Ug) \cdot a = Ug$ for all $g \in G$. Hence, by Lemma 4.8 we have that $Ug = Uc$ for some $c \in C_G(A)$. Since this holds for all $g \in G$ and G is a union of the cosets Ug for $g \in G$, we see that $G = UC_G(A)$ and (ii) holds.

For (iii), we apply (ii) with the appropriate commutator laws so that $[G, A] = [G, A, A][C_G(A), A] = [G, A, A]$, as desired. Finally, for (iv), since A acts trivially on G/N we have that $[G, A] \leq N$. Since, as A acts trivially on N, by part (iii) we see that $[G, A] = [G, A, A] \leq [N, A] = \{e\}$ and A acts trivially on G. □

The following proposition is yet another classical result of Burnside.

Proposition 4.10. *Let G be a finite p-group and A be a finite group acting faithfully on G. Suppose that A acts trivially on $G/\Phi(G)$. Then the image of A in* $\mathrm{Aut}(G)$ *is contained in a normal p-subgroup of* $\mathrm{Aut}(G)$*. In particular, any finite group which acts coprimely and faithfully on G, acts faithfully on $G/\Phi(G)$.*

Proof. Since A acts faithfully on G, we identify A with its image in $\mathrm{Aut}(G)$. We leave it to the reader to verify that $C_{\mathrm{Aut}(G)}(G/\Phi(G)) \trianglelefteq G$. It remains to prove that $C := C_{\mathrm{Aut}(G)}(G/\Phi(G))$ is a p-group. Aiming for a contradiction, assume not so that, by Cauchy's theorem, there is $R \leq C$ of order r where r is a prime not equal to p. Since R acts trivially on $G/\Phi(G)$, we have that $[G, R] \leq \Phi(G)$. But then $G = [G, R]C_G(R) = \Phi(G)C_G(R)$ and by properties of the Frattini subgroup, $G = C_G(R)$. Since R is non-trivial, we have a contradiction from which we conclude that C is a p-group. □

In a similar direction, we can describe what happens when a a group acts coprimely and trivially on a chain of subgroups.

Proposition 4.11. *Let G be a finite p-group and A be a finite group acting faithfully on G. Let $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$ be a chain of A-invariant subgroups of G. Suppose that $[G_i, B] \leq G_{i-1}$ for all $i \in \{1, \ldots, n\}$ for some $B \leq A$. Then B is contained in a normal p-subgroup of A.*

Proof. Since A acts faithfully on G, we identify G with a subgroup of $\mathrm{Aut}(G)$. Let C be the largest subgroup of A satisfying the properties of B. As in Proposition 4.10, we leave it to the reader to verify that C is a normal subgroup of A. Once again, it remains to prove that C is a p-group. We shall induct on n, the length of the chain. If $n = 1$, then $[C, G] = \{e\}$ and as A acts faithfully on G, we have that $C = \{1\}$.

Aiming for a contradiction, we assume that there is $R \leq C$ with $|R| = r$ where p is a prime number distinct from p. Then there is an induced action of R on the chain $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_{n-1}$ and so, by induction, $[G_{n-1}, R] = \{e\}$. By hypothesis, $[G, R] \leq G_{n-1}$ so that R acts trivially on G/G_{n-1}. Hence, R centralizes G, a contradiction since the action of A (and so R) is faithful on G. Thus, C is a p-group and the proposition holds. □

We have have seen that finite p-groups act unipotently on finite p-groups, and have analyzed the case of a group of order coprime to p acting on a finite p-group. Through the following theorem, we realize one way in which these viewpoints interact.

Theorem 4.12 (A×B-lemma)**.** *Let G be a finite p-group and let A be a finite group acting on G. Assume that $A = PQ$ where P is a finite p-group, $(|Q|, p) = 1$ and $[P, Q] = \{e\}$ (so that $A = P \times Q$). If Q acts trivially on $C_G(P)$ then Q acts trivially on G.*

Proof. Suppose that Q acts trivially on $C_G(P)$. We first observe that $C_G(P)$ is acted on trivially by A, and so is A-invariant. Let X be a subgroup of G containing $C_G(P)$ such X is A-invariant and Q acts trivially on X, and X has maximal order with respect to adhering to these conditions. If $X = G$, then Q acts trivially on G and the theorem holds. Hence, aiming for a contradiction, we may assume that $X < G$.

Since G is a p-group, we have that $X < N_G(X)$. Since G and X are A-invariant, we deduce that $N_G(X)$ is also A-invariant (you should check this). Let Y an A-invariant subgroup of $N_G(X)$ properly containing X, and choose Y of minimal order with respect to adhering to these conditions. Then $\overline{Y} = Y/X$ is a p-group which is acted upon by A. In particular, $C_{\overline{Y}}(P)$ is non-trivial. Since $[P, Q]$, Q normalizes P and so $C_{\overline{Y}}(P)$ is a Q-invariant subgroup of $\overline{Y}$ from which we conclude that $C_{\overline{Y}}(P)$ is A-invariant. In particular, the preimage in Y of $C_{\overline{Y}}(P)$ is A-invariant and by minimality of Y, we deduce that $[Y, P] \leq X$. Then $[Y, P, Q] = \{e\}$ and $[P, Q, Y] = \{e\}$ from which we deduce, by the three subgroups lemma, that $[Y, Q, P] = \{e\}$ so that $[Y, Q] \leq C_G(P)$. But then $[Y, Q] = [Y, Q, Q] \leq [C_G(P), Q] = \{e\}$ and so Q acts trivially on Y. Since X was maximally chosen and Y properly contains X, we have the required contradiction. □

Let us now specialize to the case where G is a finite abelian p-group, where we can say a little more regarding coprime action.

Proposition 4.13. *Let G be a finite abelian p-group and assume that A is a finite group acting coprimely on G. Then the following hold:*

(i) *$G = [G, A] \times C_G(A)$; and*

(ii) *if A acts trivially on $\Omega_1(G)$, then A acts trivially on G.*

Proof. Let $\phi : G \to G$ be the mapping such that $\phi(g) = \prod_{a\in A} g \cdot a$. Then, for $g, h \in G$, $\phi(gh) = \prod_{a\in A} gh \cdot a = \prod_{a\in A}(g \cdot a)(h \cdot a) = \prod_{a\in A} g \cdot a \prod_{a\in A} h \cdot a$ and so ϕ is a homomorphism.

Now, for $g \in G$ and $x \in A$, we have that $\phi([g, x]) = \phi(g^{-1}(g \cdot x)) = \phi(g^{-1})\phi(g \cdot x) = \prod_{a\in A}(g \cdot a)^{-1} \prod_{b\in A}(g \cdot xb)$. Since $x \in A$, for all $a \in A$ there is b such that $x^{-1}a = b$ so that $a = xb$ from which we such that $\phi([g, x]) = \{e\}$ and $[G, A] \leq \ker(\phi)$.

Now, let $g \in C_G(A)$. Then $\phi(g) = \prod_{a\in A} g \cdot a = \prod_{a \in A} g^{|a|}$. Since $(|A|, p) = 1$, $g^{|a|} = e$ if and only if $g = e$ and so $C_G(A) \cap [G, A] \leq C_G(A) \cap \ker(\phi) = \{e\}$. Since $G = [G, A]C_G(A)$ we conclude that $G = [G, A] \times C_G(A)$ and (i) holds.

Now, if A acts trivially on $\Omega_1(G)$, then $\Omega_1(G) \leq C_G(A)$. Since $[G, A] \cap C_G(A) = \{e\}$, it follows that $[G, A]$ has no elements of order p and so $[G, A] = \{e\}$ so that $G = C_G(A)$, so (ii) holds. □

Part (ii) of the above proposition, and extension to the case where G is non-abelian, allows us to understand faithful actions on G by restricting to $\Omega_1(G)$. However, in the general case where G is not necessarily abelian, the structure of $\Omega_1(G)$ may be no simpler than G itself e.g. in the case where $G = \Omega_1(G)$. We conclude this section with Thompson's critical subgroup theorem which delivers a "small" subgroup of G which witnesses all the faithful coprime action on G.

Theorem 4.14 (Critical Subgroup Theorem). *Let G be a finite p-group. Then G has a* critical subgroup X. *That is, $X \leq G$ satisfies the following properties:*

(i) *X is a characteristic subgroup of G.*

(ii) *$[G, X] \leq Z(X)$ and $\Phi(X) \leq Z(X)$. In particular, X has nilpotency class two.*

(iii) *$C_G(X) = Z(X)$.*

(iv) *if R is a group acting faithfully and coprimely on G, then the restriction of the action of R to X is faithful.*

Proof. We first observe that (iv) follows from (i) and (iii) in the statement of the theorem. Assume that R acts coprimely on G and acts trivially on X. Then $[X, R] = \{e\}$ and by Proposition 4.4 (iv), we have that $[G, R] \leq C_X(R) \leq X$. Then by coprime action, $[G, R] = [G, R, R] \leq [X, R] = \{e\}$ and R acts trivially on G. Hence, any faithful coprime action on G restricts to a faithful action on X. We now set about showing such an X exists.

Let A be a normal, abelian subgroup of G which is not contained in any other normal, abelian subgroup of G. Assume that A is characteristic in G. We will show that we may take $X = A$. (i) holds by assumption. Then $[G, A] \leq A = Z(A)$ and $\Phi(A) \leq A = Z(A)$ and so (ii) holds. (iii) holds by Proposition 3.10 and so A satisfies the required properties. Thus, to complete the proof we assume that every characteristic abelian subgroup is properly contained in some normal, abelian subgroup of G.

Let Y be a abelian, characteristic subgroup of G and chosen Y maximally by inclusion with respect to adhering to these conditions. Since Y is properly contained in some normal, abelian subgroup, we have that $Y < C_G(Y)$. Write $\overline{G} = G/Y$ and set $\overline{X} = \overline{C_G(Y)} \cap \Omega_1(Z(\overline{G}))$. Let X be the preimage in G of $\overline{C}$. We claim that X is a critical subgroup.

Since Y is characteristic in G, so too is $C_G(Y)$. Moreover, every automorphism of G induces a (possibly trivial) automorphism of $\overline{G}$ which leaves invariant $\overline{C_G(Y)}$ and $\Omega_1(Z(\overline{G}))$ and we ascertain that X is fixed by every automorphism of G, and so is characteristic in G. Hence (i) holds. As a consequence, we have that $Z(X)$ is characteristic in G, and since Y was chosen maximally and $X \leq C_G(Y)$, we have that $Z(X) = Y$.

Since $\overline{X} \leq \Omega_1(Z(\overline{G}))$, we have that $[X, G] \leq Z(X)$. In particular, $X' \leq Z(X)$. Since $\overline{X}$ has exponent p, we see that $\mho_1(X) \leq Z(X)$ so that $\Phi(X) \leq Z(X)$. Hence (ii) holds.

Set $C := C_G(X)$ so that $Y = C \cap X$. Moreover, $C \leq C_G(Y)$ and so $\overline{C} \leq \overline{C_G(Y)}$ such that $\overline{C} \cap \overline{X} = \{e\}$. But $\overline{C} \trianglelefteq \overline{G}$, and so if $\overline{C}$ is non-trivial, we have that $\{e\} \neq \overline{C} \cap \Omega_1(Z(\overline{G})) \leq \overline{C_G(Y)} \cap \Omega_1(Z(\overline{G})) = \overline{X}$, a contradiction. Hence, $\overline{C} = \{e\}$ so that $C \leq Y$ and we conclude that $C = Y = Z(X)$ so that (iii) holds. This completes the proof of the theorem. □

Over the course of this chapter, we have amassed a toolkit for dealing with actions *on* finite p-groups. These results are still at the heart of lots of mathematics involving finite groups to this day. In this final section, we flip this on its head and ask whether we can say anything meaningful about finite p-groups acting on other finite groups.

We first present an elementary result in finite group theory which will easily enable us to prove a further lemma.

Proposition 4.15 (Frattini Argument). *Let G be a finite group with $R \trianglelefteq G$. Let P be a Sylow p-subgroup of R. Then $G = RN_G(P)$.*

Proof. Let $g \in G$. Then $|P| = |P^g|$ and since $R \trianglelefteq G$, $P^g \leq R$. Hence, R^g is a Sylow p-subgroup of R. Then, by Sylow's theorems, there is $r \in R$ such that $P^g r = P$. Then $gr \in N_G(P)$ so that $g = nr^{-1}$ for some $n \in N_G(P)$. Since $g \in G$ was arbitrary, $G = N_G(P)R = RN_G(P)$, as desired. □

Lemma 4.16. *Let A be a finite p-group acting on a finite group G such that $(|G|, p) = 1$. For $r \neq p$ a prime dividing $|G|$, there is a Sylow r-subgroup of G which is A-invariant.*

Proof. Let $H = G \rtimes A$ be the semidirect product defined by the action of A on G. Then $G \trianglelefteq H$ and so, by the Frattini argument, $H = GN_H(P)$ for some $P \in \mathrm{Syl}_r(G)$. Since $(G, p) = 1$, A is a Sylow p-subgroup of H and P is a Sylow r-subgroup of H. By consider group orders, we see that $N_G(P)$ contains a Sylow p-subgroup of H. By Sylow's theorem, there is $h \in H$ such that $A^{h^{-1}} \leq N_H(P)$ from which we conclude that $A \leq N_H(P^h)$. Since $|P| = |P^h|$ and $G^h = G$, we see that P^h is a Sylow r-subgroup of G which is A-invariant. □

We finish with the following theorem.

Theorem 4.17. *Let A be an abelian finite p-group acting on a finite group G such that $m_p(A) \geqslant 2$ and $(|G|, p) = 1$. Then the following hold:*

(i) $G = \langle C_G(B) \mid [A : B] = p\rangle$*;*

(ii) $G = \langle C_G(a) \mid e \neq a \in A\rangle$*; and*

(iii) $[G, A] = \langle [C_G(B), A] \mid [A : B] = p\rangle$.

Proof. For part (i), we note that if the result holds true for some Sylow r-subgroup, for all primes r dividing $|G|$, then it holds for G. So we may assume that G is an r-group for some prime r distinct from p. Let the pair (G, A) be a counterexample chosen such that $|G| + |A|$ is minimal. If $C_A(G) \neq \{e\}$, the applying induction we have that $G = \langle C_G(B/C_A(G)) \mid [A : BC_A(G)] = p\rangle$ and since $C_G(BC_A(G)) = C_G(BC_A(G)/C_A(G))$ and $[A : BC_A(G)] = p$, the result holds. Hence, we may assume that A acts faithfully on G.

Suppose that $\Phi(G) \neq \{1\}$ so that the result holds true for the pair $(G/\Phi(G), A)$. Then

$$\begin{aligned} G/\Phi(G) = \langle C_{G/\Phi(G)}(B) \mid [A : B] = p\rangle &= \langle C_G(B)\Phi(G)/\Phi(G) \mid [A : B] = p\rangle \\ &= \langle C_G(B) \mid [A : B] = p\rangle\Phi(G)/\Phi(G) \end{aligned}$$

and by properties of the Frattini subgroup, we deduce that $G = \langle C_G(B) \mid [A : B] = p\rangle$ and the result holds. Hence, it remains to prove the result when G is an elementary abelian r-group.

Suppose that W is a proper non-trivial A-invariant subgroup of G. Since G is abelian, $W \trianglelefteq G$. Then, by induction applied to the pairs $(G/W, A)$ and (W, A), we may assume that $G/W = \langle C_{G/W}(B) \mid [A : B] = p\rangle$ and $W = \langle C_W(B) \mid [A : B] = p\rangle$. But $C_{G/W}(B) = C_G(B)W/W$ from which we deduce that $G = \langle C_G(B)W \mid [A : B] = p\rangle$ so that $G = \langle C_G(B) \mid [A : B] = p\rangle$, and the result holds.

Now, for all $a, x \in A$ we have that $C_G(a)^x = C_G(a^x) = C_G(a)$ since A is abelian and so $C_G(a)$ is an A-invariant subgroup of G and since A acts faithfully on G, we have that $C_G(a) = \{e\}$ for all $a \in A \setminus \{e\}$.

Since $m_p(A) \geqslant 2$ there is $R \leq A$ with R elementary abelian of order p^2. We observe that $C_G(r) = \{e\}$ for all $r \in R \setminus \{e\}$. By induction, we must have that $A = R$. We observe that A has $p+1$ subgroups of order p. Let $B \leq A$. For $g \in G$ and $\{e\} \neq B \leq A$, define $g_B = \prod_{a \in B} g \cdot a$. Then for $b \in B$ we have that $g_B \cdot b = \prod_{a \in B} g \cdot ab = \prod_{a \in B} g \cdot a$ and so $g_B \in C_G(b) = \{e\}$. Now, $g_A = g \prod_{a \in A \setminus \{e\}} g \cdot a$. If $B_1, B_2 \leq A$ have order p, then $B_1 \cap B_2 = \{e\}$ and so $g_A = g \prod_{B \leq A \mid [A:B] = p} g_B g^{-1}$ and as $g_A = g_B = e$, we have that $e = g^{-p}$ from which we deduce that $g^p = e$, a contradiction since $(|G|, p) = 1$. Hence, no counterexample exists, which completes the proof of (i).

Part (ii) follows from repeatedly applying part (i) to chains of subgroups of A. It remains to prove (iii). We observe that for $B \leq A$ with $[A : B] = p$, we have that $C_G(A) \leq C_G(B)$. Moreover, since A is abelian, A normalizes B so that $C_G(B)$ is an A-invariant subgroup of G. Then $C_G(B) = [C_G(B), A]C_{C_G(B)}(A) = [C_G(B), A]C_G(A)$.

Now, $G = \langle C_G(B) \mid [A : B] = p\rangle = \langle [C_G(B), A]C_G(A) \mid [A : B] = p\rangle = \langle [C_G(B), A] \mid [A : B] = p\rangle C_G(A)$ from which we conclude that $[G, A] = \langle [C_G(B), A] \mid [A : B] = p\rangle$, completing the proof of (iii). □

4.2 Some More Characterization Results

Given the theory we have built up in the previous section, we can now provide some more identification theorems for finite p-groups. We start first with finite p-groups admitting *fixed point free actions.*

Definition 4.18. Let G be a finite p-group and let A be a finite group acting on G. Say that $a \in A$ acts fixed point freely on G if $g \cdot a \neq g$ for all $g \in G \setminus \{e\}$.

Lemma 4.19. *Let G be a finite group and A be a finite group acting on G. Suppose that $a \in A$ acts fixed point freely on G. Then the map $[\cdot, a] : G \to G$ given by $g \mapsto [g, a]$ is a bijective map.*

Proof. Let $g, h \in G$ and assume that $[g, a] = [h, a]$. Then $g^{-1}(g \cdot a) = h^{-1}(h \cdot a)$ so that $hg^{-1} = (h \cdot a)(g \cdot a)^{-1} = (h \cdot a)(g^{-1} \cdot a) = (hg^{-1} \cdot a)$. Since $a \in A$ acts fixed point freely, we deduce that $hg^{-1} = e$ so that $h = g$. Hence, $[\cdot, a]$ is injective. But $|G|$ is finite, so $[\cdot, a]$ is bijective. □

Lemma 4.20. *Let G be a finite group, A a finite group acting on G, and N an A-invariant normal subgroup of G. If $a \in A$ acts fixed point freely on G, then a acts fixed point freely on N and on G/N.*

Proof. Since a acts fixed point freely on G, we have that the map $[\cdot, a] : G \to G$ is bijective. Since N is A-invariant, it follows that $[\cdot, a]|_N : N \to N$ is also bijective, as is the map $[\cdot, a] : G/N \to G/N$ such that $[gN, a] = g^{-1}N((gN \cdot a)$. Then bijectivity (or more accurately, injectivity) implies that a acts fixed point freely on both N and G/N. □

Proposition 4.21. *Let G be a finite group and A be a finite group acting on G. Suppose that $a \in A$ acts fixed point freely on G and has order n. Then $g(g \cdot a) \ldots (g \cdot a^{n-1}) = e$ for all $g \in G$.*

Proof. Let $g \in G$. By Lemma 4.19, there is $h \in G$ such that $g = h^{-1}(h \cdot a)$. Then

$$g(g \cdot a) \ldots (g \cdot a^{n-1}) = h^{-1}(h \cdot a)(h^{-1} \cdot a)(hcdota^2) \ldots (h^{-1} \cdot a^{n-1})(h \cdot a^n)$$

and as $a^n = e$, we conclude that $g(g \cdot a) \ldots (g \cdot a^{n-1}) = e$. □

The following result of Burnside (who proved it for G an arbitrary finite group) emphasizes how limiting it is for a group to act fixed point freely on another group.

Theorem 4.22. *Let G be a non-trivial finite p-group and let A be a finite group acting on G. If every non-trivial element of A acts fixed point freely on G, then $(|G|, |A|) = 1$ and every Sylow r-subgroup of A has r-rank 1.*

Proof. Since G is a finite p-group, p-elements of A acts unipotently on G and so have fixed points on G. Hence, $(|G|, |A|) = 1$. Now, let R be a Sylow r-subgroup of A for some prime r dividing $|A|$.

Assume that $m_r(R) \geqslant 2$ and choose $B \leq R$ such that B is elementary abelian of order r^2. Then $G = \langle C_G(r) \mid r \in B \setminus \{e\}\rangle$ by Theorem 4.17. But $r \in B \setminus \{e\}$ acts fixed point freely on G from which we conclude that $G = \langle C_G(r) \mid r \in B \setminus \{e\}\rangle = \langle \{e\}\rangle = \{e\}$. Hence, no such B exists and we conclude that $m_r(R) = 1$, as desired. □

On the other hand, a group which is acted *on* fixed point freely also has a restricted structure, as evidenced by the following result.

Proposition 4.23. *Let G be a non-trivial finite p-group and a be an involution acting on G fixed point freely. Then for all $g \in G$, we have that $g \cdot a = g^{-1}$, p is odd and G is abelian.*

Proof. Let $g \in G$. Then by Lemma 4.19 there is $h \in G$ such that $g = [h, a] = h^{-1}(h \cdot a)$. Hence, $h \cdot a = hg$. Since a is an involution

$$h = h \cdot a^2 = (h \cdot a) \cdot a = (hg \cdot a) = (h \cdot a)(g \cdot a) = hg(g \cdot a)$$

from which we conclude that $g(g \cdot a) = e$ so that $g \cdot a = g^{-1}$. Now, if $p = 2$ then there is $e \neq g \in G$ such that $g^2 = e$. But then $g = g^{-1}$ so that $g \cdot a = g^{-1} = a$, a contradiction since a acts fixed freely on G. Hence, p is odd. Finally, for $g, h \in G$ we have that $gh = (g^{-1} \cdot a)(h^{-1} \cdot a) = g^{-1}h^{-1} \cdot a = hg$ and we conclude that G is abelian. □

It is not too hard to see that the above result is true for any finite group G with a fixed point free involutary automorphism. The following theorems complete the picture for finite groups admitting fixed point free actions by elements of order p.

Theorem 4.24. *Let G be a finite group and let A be a finite group acting on G. Suppose that $a \in A$ has order p for some prime p and acts fixed point freely on G. Then G is nilpotent.*

In his thesis, Thompson proved that any finite group which has a fixed point free action by an element of order p is nilpotent. The following result of Higman (which was shown to be "tight" by Kreknin and Kostrikin) restricts the structure of G further.

Theorem 4.25. *Let G be a finite nilpotent group and let A be a finite group acting on G. Suppose that $a \in A$ has order p for some prime p and acts fixed point freely on G. Then the nilpotency class of G is bounded by some function of p, denoted $h(p)$, and*

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

We now present two theorems for recognizing special p-groups.

Theorem 4.26 (Hall–Higman Reduction)**.** *Let G be a finite p-group and A be a finite group acting on G with $(|A|, p) = 1$. Let $B \trianglelefteq A$ with $B \not\leq C_A(G)$. Set*

$$\mathcal{P} := \{P \leq G \mid \ P \text{ is } A\text{-invariant, } B \not\leq C_A(P)\}.$$

If $Q \in \mathcal{P}$ does not properly contain any other element of $\mathcal{P}$, termed minimal*, then*

(i) *if $\Phi(Q) < R \leq Q$ and R is A-invariant, then $R = Q$;*

(ii) *$Q = [Q, B]$; and*

(iii) *Q is a special group.*

Proof. Let Q be a minimal element of $\mathcal{Q}$. Then $Q = [Q, B]C_Q(B)$. Since $B \trianglelefteq A$, we have that $[Q, B]$ is A-invariant. Moreover, $[Q, B] = [Q, B, B]$ and so if $B \leq C_A([Q, B])$ then $[Q, B] = \{e\}$ and $B \leq C_A(Q)$, a contradiction. Hence, $Q = [Q, B]$ and (ii) is prove. Let R be a critical subgroup of Q. Then R is characteristic in Q and as Q is A-invariant, R is A-invariant. Moreover, the restriction of B to R is faithful and so $B \not\leq C_A(R)$ and so $R \in \mathcal{P}$. Since Q is minimal, we have that $Q = R$. Hence, $Q' \leq \Phi(Q) \leq Z(Q)$. By minimality of Q and as $\Phi(Q)$ is characteristic in Q (so is A-invariant), we must have that $B \leq C_A(\Phi(Q))$ so that $\Phi(Q) \leq C_Q(B)$.

Set $\overline{Q} := Q/Q'$. Then $\overline{Q} = [\overline{Q}, B] \times C_{\overline{Q}}(B)$. Set X to be the preimage of $[\overline{Q}, B]$ in Q. Since Q is A-invariant and $B \trianglelefteq A$, it follows that X is A-invariant. Moreover, B acts non-trivially on $[\overline{Q}, B]$, for otherwise $[Q, B] \leq Q'$ and as $Q' \leq C_Q(B)$, $[Q, B] = [Q, B, B] = \{e\}$ from which we deduce that $B \leq C_A(Q)$, a contradiction. Hence, B acts non-trivially on X and by minimality of Q, we conclude that $Q = X$. Since $\Phi(Q) \leq C_G(B)$, $\overline{\Phi(Q)} \leq C_{\overline{Q}}(B) = \{e\}$ so that $\Phi(Q) = Q'$.

Suppose that there is $\Phi(Q) < R < Q$ with R A-invariant, so that $\overline{R} \neq \{e\}$. By minimality of Q, we must have that $[R, B] = \{e\}$. Then $\overline{R} \leq C_{\overline{Q}}(B) = \{e\}$, a contradiction. Hence, no such R exists and (i) holds. Finally, $Z(Q)$ is an A-invariant subgroup of Q which contains $\Phi(Q)$ and so either $\Phi(Q) = Z(Q)$ and Q is a special group; or $Q = Z(Q)$ is abelian. In the latter case, we have that $\Omega_1(Q)$ is a non-trivial characteristic (so A-invariant) subgroup of Q which admits B faithfully, and as Q is minimal we have that $Q = \Omega_1(Q)$ and Q is elementary abelian. This completes the proof of (iii). □

Theorem 4.27 (Thompson)**.** *Let G be a finite p-group and A be a finite group acting on G with $(|A|, p) = 1$. Suppose that $G = [G, A]$ and $[B, A] = \{e\}$ for all $B \leq G$ with B abelian and characteristic in G. Then G is (non-abelian) special.*

Proof. Suppose that G has nilpotency class c of at least 3. By an exercise, $[\gamma_2(G), \gamma_{c-1}(G)] \leq \gamma_{c+1}(G) = \{e\}$ and since $c > 2$, $\gamma_{c-1}(G) \leq \gamma_2(G)$ and so $\gamma_{c-1}(G)$ is a abelian and non-central in G. Then $[\gamma_{c-1}(G), A] = \{e\}$ by assumption so that $G = [G, A] \leq C_G(\gamma_{c-1}(G))$, a contradiction since $\gamma_{c-1}(G)$ is non-central. Hence, G has nilpotency class exactly 2.

Now, $G' \le Z(G)$ and by assumption we have that $Z(G) \le C_G(A)$. Set $\overline{G} = G/G'$. Then $\overline{G} = [\overline{G}, A] \times C_{\overline{G}}(A)$ and as $G = [G, A]$, we have that $C_{\overline{G}}(A) = \{e\}$ and $G' = Z(G)$.

It remains to show that G/G' has exponent p. Let $m \in \mathbb{N}$ be such that G/G' has exponent p^m. Then for all $x, y \in G$ we have that $[x, y]^{p^m} = [x^{p^m}, y] = e$. Since $G'$is abelian, we have that G' has exponent at most p^m. Now, $[x^{p^{m-1}}, y^{p^{m-1}}] = [x, y^{p^{m-1}}]^{p^{m-1}} = [x, y]^{p^{2(m-1)}}$. If $m > 1$, then $2(m-1) \geqslant m$ and we deduce that $[x^{p^{m-1}}, y^{p^{m-1}}] = e$. Hence, we have that $\mho_{m-1}(G)$ is abelian from which we conclude that that $[\mho_{m-1}(G), A] = \{e\}$. Hence, $\mho_{m-1}(G) \le C_G(A) = G'$ from which we conclude that G/G' has exponent $p^{m-1} < p^m$, a contradiction. Hence, $m = 1$ and G/G' has exponent p so that G is a special group. □

Finally, we conclude this section (and this final chapter) with a theorem of Hall.

Theorem 4.28. *Suppose that G is a finite p-group such that every characteristic abelian subgroup of N is cyclic. Then $G = E \circ R$ is central product where E is extraspecial and R is cyclic, dihedral, semidihedral or generalized quaternion.*

Proof. Let C be a critical subgroup of G. Then $Z(C)$ is a cyclic group and $Z(G) \le Z(C)$. Set $Z := \Omega_1(Z(C)) = \Omega_1(Z(G))$ and $\overline{G} := G/Z$. Let $x, y \in C$ and so that $x^p \in Z(C)$. Hence, $e = [x^p, y] = [x, y]^p$. Since $C' \le Z(C)$ is generated by $[x, y]$ for $x, y \in C$, we see that $C' \le \Omega_1(Z(C)) = Z$. Hence, $\overline{C}$ is abelian. Let R to be the preimage in C of $\Omega_1(\overline{C})$. Then $\overline{R}$ is elementary abelian and $Z(R)$ is cyclic so that $Z \le Z(R)$ and $|Z(R)| \leqslant p^2$. Write $\overline{R} = \overline{Z(R)} \times \overline{E}$ for some $E \le R$.

Suppose that $R = Z(R)$ so that R is cyclic of order at most p^2. Hence $m_p(\overline{C}) = 1$ so that $\overline{C}$ is cyclic. Now, $|C| > p$ so that $\Phi(C)$ is non-trivial and $Z \le \Phi(C)$. Hence, $|C/\Phi(C)| = p$ and we conclude that C is cyclic. We may assume that $G > C$ else the theorem holds. Since C is self-centralizing, G/C embeds in $\mathrm{Aut}(C)$. If $|G/C| = p$, then G has a cyclic subgroup of index p and since $\Omega_1(\mathrm{Mod}_n(p))$ is elementary abelian of order p^2, we deduce by Theorem 3.16 that G is dihedral, semidihedral or generalized quaternion and the result is proved. We continue assuming that $R = Z(R)$ and $|G/C| \geqslant p^2$. By an exercise, if p is odd then G/C is cyclic, while if $p = 2$ then G/C is isomorphic to a subgroup of $C_{2^{n-2}} \times C_2$ where $|C| = 2^n$. In particular, $|C| \geqslant p^3$. If $p = 2$, then by an exercise we see that $C_G(\Omega_2(C))/C$ is a cyclic group and $C_G(\Omega_2(C))$ has index at most 2 in G. If p is odd then again $C_G(\Omega_2(C))/C$ is a cyclic group and $C_G(\Omega_2(C))$ has index at most p in G.

Let $X \le C_G(\Omega_2(C))$ such that $X/C = \Omega_1(C_G(\Omega_2(C))/C)$ so that X is characteristic in G and $|X/C| = p$. Since C is is self-centralizing, X is not cyclic. Moreover, since $\Omega_2(X)$ has order p^2, we see by Theorem 3.16 that X is a modular group. But then $\Omega_1(X)$ is a characteristic subgroup of G which is elementary abelian of order p^2, a contradiction.

Thus, to prove the theorem we may now assume that $R \neq Z(R)$. Since $Z(E)$ is centralized by E and $Z(R)$, we conclude that $Z(E) = Z$ and E is an extraspecial group. Now, $[G, C] \le Z(C)$ and we deduce that $[G, R] \le Z(C) \cap R$. Thus, for $f \in E$, we have that $f^g = fk$ for some $k \in Z(C) \cap R$. Then $f^p \in Z$ so that $f^p = (f^p)^g = (f^g)^p = (fk)^p = f^p k^p$

from which we deduce that $k^p = e$. Hence, $k \in Z$ and we deduce that $[G, E] \leq Z$ so that $E \trianglelefteq G$. Since $[G, E] \leq Z(E)$ we have, by an exercise, that $G = EC_G(E)$. Hence, $Z(C_G(E)) = Z(G)$ and $C = EC_C(E)$. Then $\overline{C} = \overline{E} \times \overline{C_C(E)}$. It follows that either $C = E$; or $m_p(\overline{C_C(E)}) = 1$ and since $\overline{C}$ is abelian, $\overline{C_C(E)}$ is cyclic. In the former case, we have that $C_G(E) \leq E$ so that $G = E$ is extraspecial and the theorem holds.

In the latter case, we that $\Phi(C_C(E))$ has index p in $C_C(E)$ so that $C_C(E)$ is cyclic and $C_C(E) = Z(C)$. Then $C_{C_G(E)}(Z(C)) = C_{C_G(E)}(C) = Z(C)$. We may assume that $Z(C) < C_G(E)$ else $G = EZ(C)$, and G satisfies the properties of the theorem. In particular, we have that $|Z(C)| > p$ and $C_G(E)/Z(C)$ is isomorphic to a subgroup of $\mathrm{Aut}(Z(C))$. If $|C_G(E)/Z(C)| = p$ then by Theorem 3.16, we conclude that $C_G(E)$ is modular, dihedral, semidihedral or generalized quaternion. The conclusion of the theorem holds unless $C_G(E)$ is modular and $\Omega_2(Z(C)) \leq Z(C_G(E))$. But then $E \leq \Omega_1(C) \leq E\Omega_2(Z(C))$ is characteristic in G and so too is $C_G(E) = C_G(\Omega_1(C))$. Then $\Omega_1(C_G(E))$ is characteristic in G and elementary abelian of order p^2, a contradiction.

We assume now that $|C_G(E)/Z(C)| \geqslant p^2$. In particular, $|Z(C)| \geqslant p^3$. Note that $E \leq \Omega_1(C) \leq E\Omega_2(Z(C))$ is characteristic in G. Then $Y := C_G(\Omega_1(C))$ is a subgroup of $C_G(E)$ of index at most p, and is characteristic in G.

Assume that $E = \Omega_1(C)$ so that $Y = C_G(E)$ is a characteristic subgroup of G. Then $C_{C_G(E)}(\Omega_2(Z(C)))$ is a characteristic subgroup of G and $C_{C_G(E)}(\Omega_2(Z(C)))/Z(C)$ is cyclic. Let $X \leq C_{C_G(E)}(\Omega_2(Z(C)))$ be such that $X/Z(C) = \Omega_1(C_{C_G(E)}(\Omega_2(Z(C)))/Z(C))$ so that X is characteristic in G and $|X/Z(C)| = p$. As above, we quickly deduce by Theorem 3.16 that X is a modular group and $\Omega_1(X)$ is a characteristic subgroup of G which is elementary of order p^2, a contradiction.

Assume that $\Omega_1(C) = E\Omega_2(Z(C))$ (so that $p = 2$). Then Y has index p in $C_G(E)$ and so $Y = C_{C_G(E)}(\Omega_2(Z(C)))$. In particular, $Y/Z(C)$ is cyclic. Let $X \leq Y$ be such that $X/Z(C) = \Omega_1(Y/Z(C))$ so that X is characteristic in G and $|X/Z(C)| = p$. Using that $Z(C)$ is self-centralizing in $C_G(R)$ and that $\Omega_2(Z(C)) \leq Z(X)$, we conclude that X is a modular group and the same contradiction as above (that $\Omega_1(X)$ is elementary abelian of order p^2) gives the final contradiction. This completes the proof. □