

Subnormality and the Architectural Structure of Finite Groups

R. Lyons, Rutgers University

A.	Subnormality, $F^*(G)$, and Bender's Theorem	
1.	Introduction	1
2.	Subnormality in Theory	1
3.	Subnormality in Practice: Nilpotent Groups	3
4.	Fitting's Theorem	5
5.	The Frattini Subgroup	10
6.	Quasisimple and Semisimple Groups	13
7.	Subnormality in Practice: Components	17
8.	Bender's Theorem	18
B.	p -Locals in Simple Groups	
9.	Extra-special p -Groups	18
10.	Automorphisms of Extra-special p -Groups	22
11.	Groups of Characteristic p	27

1. Introduction

Helmut Wielandt (1910–2001) was the most important figure in the beautiful development of the notion of subnormality in the theory of finite groups. It is an idea that sheds important light on the “architectural” structure of finite groups, that is, the manner in which groups are “built” from their subgroups, particularly from their normal subgroups. In this theory, simple groups, having no normal subgroups, have no subnormal subgroups either, so the development below is trivial in most cases if G is a simple group. However, if G is a proper subgroup of a simple group, then its architectural structure can be heavily influenced by this theory of subnormality.

Expositions of this subject can be found in chapters of the beautiful books *Finite Group Theory: An Introduction* by Hans Kurzweil and Bernd Stellmacher, Springer-Verlag, 2004, and *Finite Group Theory* by I. Martin Isaacs, GTM, American Mathematical Society, 2008. Those expositions are the basis of these brief notes.

2. Subnormal Subgroups in Theory

All groups discussed throughout these notes are assumed to be finite, unless explicitly stated otherwise (or unless, like \mathbf{Z} , they are explicit infinite groups).

Let G be a group and H a subgroup of G . We say that H is **subnormal in** G and write $H \triangleleft\triangleleft G$ if and only if there exists a chain

$$(2A) \quad H = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

of subgroups of G .

We shall prove the following properties of this relation:

- (2.1) If $H \triangleleft\triangleleft K$ and $K \triangleleft\triangleleft G$, then $H \triangleleft\triangleleft G$.
- (2.2) If $H \triangleleft G$, then $H \triangleleft\triangleleft G$.
- (2.3) If $H \triangleleft\triangleleft K \leq G$, then $H^\alpha \triangleleft\triangleleft K^\alpha$ for all automorphisms α of G .
- (2.4) If $H \triangleleft\triangleleft G$ and $K \leq G$, then $H \cap K \triangleleft\triangleleft K$. If in addition $H \leq K$, then $H \triangleleft\triangleleft K$.
- (2.5) If $H \triangleleft\triangleleft G$ and $N \triangleleft G$, then $HN/N \triangleleft\triangleleft G/N$.
- (2.6) If $N \triangleleft G$ and $N \leq H \leq G$, then $H \triangleleft\triangleleft G$ if and only if $H/N \triangleleft\triangleleft G/N$.
- (2.7) If $H \triangleleft\triangleleft G$ and $K \triangleleft\triangleleft G$, then $H \cap K \triangleleft\triangleleft G$ and $\langle H, K \rangle \triangleleft\triangleleft G$.
- (2.8) If $H \triangleleft\triangleleft G$ and M is a minimal normal subgroup of G , then M normalizes H .
- (2.9) Suppose that $H \not\triangleleft G$ but $H \triangleleft\triangleleft G$. Let

$$N = N_G(H) \text{ and } V(H; N) = \langle H^x \mid x \in G, H^x \leq N \rangle.$$

Then $H < V(H; N) \triangleleft N_G(N)$.

- (2.10) (Wielandt's Zipper Lemma) Suppose that $H \leq G$, $H \triangleleft\triangleleft X$ for all $H \leq X < G$, but H is not subnormal in G . Then H is contained in exactly one maximal subgroup of G .
- (2.11) Let $H \leq G$. Then $H \triangleleft\triangleleft G$ if and only if for all $x \in G$, $H \triangleleft\triangleleft \langle H, H^x \rangle$.

Properties 2.1-2.3 are trivial. Property 2.4 follows by an easy induction from the well-known result that if $X \triangleleft G$ and $Y \leq G$, then $X \cap Y \triangleleft Y$. The first part of Property 2.5, and Property 2.6, follow easily by induction from the well-known corresponding statements for normality. The second part of Property 2.4 follows immediately from the first.

In Property 2.7, we have $H \cap K \triangleleft\triangleleft K$ by Property 2.4, and $K \triangleleft\triangleleft G$ by assumption, so $H \cap K \triangleleft\triangleleft G$ by Property 2.1. We skip the other part of Property 2.7 for the moment.

In Properties 2.8 and 2.9, since $H \triangleleft\triangleleft G$, there is a chain as in (2A), and we choose such a chain with n minimal. Notice that since $H \not\triangleleft G$, $n > 1$. Also by minimality of n , $G_{i-1} < G_i$ for each $i = 1, \dots, n$. Set $N = N_G(H)$; then certainly $G_1 \leq N$.

Let J be a minimal normal subgroup of G . By minimality either $J \leq G_{n-1}$ or $J \cap G_{n-1} = 1$. In the second case, $G_{n-1}J = G_{n-1} \times J$, so J actually centralizes H . In the first case, let J_0 be a minimal normal subgroup of G_{n-1} contained in J . Proving Property 2.8 by induction we conclude that J_0 normalizes H . Furthermore, for any $x \in G$, J_0^x is a minimal normal subgroup of $G_{n-1}^x = G_{n-1}$, so it similarly normalizes H . Therefore $\langle J_0^G \rangle$ normalizes H . But as J is minimal normal in G and contains $J_0 \neq 1$, $\langle J_0^G \rangle = J$. Thus, Property 2.8 is proved.

In Property 2.9, the minimality of n implies that $H \not\triangleleft G_2$. Choose $x \in G_2$ such that $H^x \neq H$. Then since $G_1 \triangleleft G_2$, $H^x \triangleleft G_1^x = G_1 \leq N$. Therefore H^x lies in the subgroup K as defined in Property 2.8. Since $H^x \neq H$, this proves that $H < K$. The fact that $K^y = K$ for all $y \in N_G(N)$ follows from the definition of K and the fact that $N^y = N$. Thus, Property 2.9 is proved.

Now using Property 2.8, we can prove the second part of Property 2.7. Let J be a minimal normal subgroup of G . Using Property 2.5 we get $HJ/J \triangleleft\triangleleft G/J$ and $KJ/J \triangleleft\triangleleft G/J$, so by induction $\langle HJ/J, KJ/J \rangle \triangleleft\triangleleft G/J$. Taking preimages and using Property 2.6, $\langle H, K \rangle J \triangleleft\triangleleft G$. By Property 2.8, J normalizes both H and K . Thus, $\langle H, K \rangle \triangleleft \langle H, K \rangle J \triangleleft\triangleleft G$ so $\langle H, K \rangle \triangleleft\triangleleft G$.

We now prove Property 2.10 by induction on $|G| + |G : H|$. Let $N = N_G(H)$ and let M be a maximal subgroup of G containing N . Suppose by way of contradiction that L is a maximal subgroup of G such that $H \leq L \neq M$.

Then $L \not\leq M$, so $L \not\leq N$, i.e., $H \not\triangleleft L$. However, by assumption, $H \triangleleft\triangleleft L$. We set $J = N_L(H)$ and are set up to apply Property 2.9 with L and J in the roles of G and N there. Set $V = V(H; J)$, the resulting subgroup. Thus, $H < V \leq J$, and in particular $H \triangleleft V$, so that $V \leq M$. Thus $V \leq M \cap L$.

We argue that $V \triangleleft\triangleleft X$ for all $V \leq X < G$. According to Property 2.9, V is generated by certain conjugates H^x of H . Since H is subnormal in any proper subgroup of G containing it, so is any G -conjugate of H , by Property 2.3. Therefore each such $H^x \triangleleft\triangleleft X$. Since $X < G$, Property 2.7 holds for X and any conjugate of H in place of G and H , and for any K , by induction. By repeated use of Property 2.7 we get $V \triangleleft\triangleleft X$, as claimed.

Since $H < V \leq M \cap L$, Property 2.10 holds for G and V by induction. Therefore $V \triangleleft\triangleleft G$. But $H \triangleleft V$, so $H \triangleleft\triangleleft G$ by Properties 2.1 and 2.2. This contradiction establishes Property 2.10.

The normality relation has the following obvious and important property: if $H \triangleleft A \leq G$ and $H \triangleleft B \leq G$, then $H \triangleleft \langle A, B \rangle$. However this property does not extend to the subnormality relation. The Wielandt Zipper Lemma can be used as a substitute tool when proving subnormality theorems by induction.

The proof of Property 2.11 is a case in point. One direction is of course immediate by Property 2.4. Conversely, suppose that $H \triangleleft\triangleleft \langle H, H^x \rangle$ for all $x \in G$. By induction on $|G|$, $H \triangleleft\triangleleft K$ whenever $H \leq K < G$. If the desired conclusion fails, then the Zipper Lemma implies that H lies in a unique maximal subgroup M of G . Furthermore, if the conclusion fails then of course $\langle H, H^x \rangle < G$ for all $x \in G$. Therefore, $\langle H, H^x \rangle \leq M$ for all such x , whence $\langle H^G \rangle \leq M$. Then $H \triangleleft\triangleleft \langle H^G \rangle$ by induction, and as $\langle H^G \rangle \triangleleft G$, we get $H \triangleleft\triangleleft G$, contrary to our assumption that the conclusion fails.

3. Subnormal Subgroups in Practice: Nilpotent Groups

By going on for more than two pages without an example the preceding development has broken an important rule. We turn attention to the question: what does subnormality have to do with the groups with which we are familiar?

In abelian groups, all subgroups are normal, hence subnormal. In solvable groups there are fewer subnormal subgroups in general, but always enough to build a composition series with abelian factors.

EXERCISES.

- 3.1 In the symmetric group S_3 , the subgroup of order 3 is the only nontrivially subnormal subgroup (i.e. besides 1 and S_3 itself).
- 3.2 In the symmetric group S_4 , the only nontrivially normal subgroups are A_4 and the Klein four-group V . The only subnormal subgroups that are not normal are the three subgroups of V of order 2.
- 3.3 A p -group (p prime) is a group G such that $|G| = p^n$ for some $n \geq 0$. Every subgroup of a p -group G is subnormal in G . (Hint. Use the next exercise.)
- 3.4 Let G be a p -group, $G \neq 1$, and M a maximal subgroup of G . Then $M \triangleleft G$. (Hint. From the action of G on itself by conjugation - and the resulting "class equation," it is well-known that the center $Z(G)$ of G is nontrivial. If $Z(G)$ lies in M , factor it out and use induction. If not, then $MZ(G) = G$.)

DEFINITION 3.5. A (finite) group G is **nilpotent** if and only if every subgroup of G is subnormal in G .

There are a number of definitions of nilpotence equivalent to this one for finite groups. Some of these, but not the one we have used, define the notion of nilpotence for arbitrary groups.

Nilpotence satisfies the following properties.

- (3.6) All abelian groups are nilpotent.
- (3.7) All p -groups are nilpotent.
- (3.8) All subgroups and quotient groups of nilpotent groups are nilpotent.
- (3.9) If G is nilpotent, then every maximal subgroup of G is normal in G and has prime index in G .
- (3.10) If G is nilpotent, then every minimal normal subgroup of G lies in $Z(G)$ and has prime order.
- (3.11) Let Z be a subgroup of $Z(G)$. Then G is nilpotent if and only if G/Z is nilpotent.
- (3.12) Direct products of nilpotent groups are nilpotent.
- (3.13) If G is nilpotent, then any Sylow p -subgroup of G (for any prime p) is normal in G .
- (3.14) G is nilpotent if and only if there are subgroups $G_i \leq G$ and primes p_i such that $G = G_1 \times \cdots \times G_n$ and each G_i is a p_i -group.

Property 3.6 is trivial since all subgroups of an abelian group are normal. Property 3.7 is Exercise 3.3. Property 3.8 follows without complication from Properties 2.4 and 2.6. Notice that in the series (2A), if H is maximal in G , then $H \triangleleft G$; and then the trivial subgroup is maximal in G/H , so G/H has prime order. This proves 3.9.

Let G be nilpotent and let N be a minimal normal subgroup of G . If $N = G$ then N is simple by minimality; but as all subgroups are subnormal, N has no

proper subgroups so has prime order, and G is cyclic. Hence the conclusion of Property 3.10 holds in this case. Next, assume that $N < G$. It suffices to show that $N \leq Z(G)$ since all subgroups of $Z(G)$ are normal in G . Let M be any maximal subgroup of G ; we claim that M and N commute elementwise. If $M \cap N = 1$, then $G = M \times N$ and the claim holds. If $M \cap N \neq 1$, then $M \cap N = N$ so $N \leq M$. In this case reduce N to a minimal normal subgroup N_0 of M . Since M is nilpotent by Property 3.8, $N_0 \leq Z(M)$ by induction. But since $M \triangleleft G$, also $Z(M) \triangleleft G$. Then $N_0 \leq Z(M) \cap N \triangleleft G$, so $N \leq Z(M)$ by minimality of N . This proves the claim. Finally if G has two distinct maximal subgroups M, M^* , then N centralizes $\langle M, M^* \rangle = G$, as desired. If G has only one maximal subgroup M , then choosing any $g \in G - M$ we must have $\langle g \rangle \not\leq M$, so $\langle g \rangle = G$ is abelian. This establishes Property 3.10.

Property 3.11 makes sense since every subgroup of $Z(G)$ is normal in G . One direction follows from Property 3.8. Assume then that $Z \leq Z(G)$ and G/Z is nilpotent. Let H be any subgroup of G . Then $HZ/Z \triangleleft\triangleleft G/Z$, so $HZ \triangleleft\triangleleft G$. But it is easily checked that $H \triangleleft HZ$, since $Z \leq Z(G)$. Therefore $H \triangleleft\triangleleft G$. As H was arbitrary, G is nilpotent and Property 3.11 is verified.

Suppose that $G = G_1 \times G_2$ with G_1 and G_2 nilpotent. In proving Property 3.12 we may of course assume that the G_i are nontrivial. Let N be a minimal normal subgroup of G_1 , so that $N \leq Z(G_1)$ by Property 3.10. Then clearly $N \leq Z(G)$. Moreover, $G/N \cong (G_1/N) \times G_2$ so G/N is nilpotent by induction. Then G is nilpotent by Property 3.11. This proves Property 3.12.

To prove Property 3.13, let p be any prime divisor of $|G|$ and let P be a Sylow p -subgroup of G . Consider $N := N_G(P)$. Clearly $P \triangleleft N$, and so P is the unique Sylow p -subgroup of N .¹ Hence any automorphism of N must leave P invariant. Consequently $N_G(N) = N$. But G is nilpotent, so $N \triangleleft\triangleleft G$. These two conditions on N force $N = G$, proving Property 3.13.

We leave it to the reader to prove Property 3.12. The main point is to prove that a nilpotent group is the direct product of its Sylow subgroups (having established the useful fact that these subgroups are normal).

EXERCISE.

(3.15) G is nilpotent if and only if $xy = yx$ for all $x, y \in G$ such that the orders of x and y are relatively prime.

4. Subnormality in Practice: The Fitting Subgroup

Let's begin by examining some groups commonly encountered. Consider the group $G = GL_n(q)$ of all $n \times n$ nonsingular matrices over the finite field \mathbf{F}_q with q elements (we assume that $q = p^m$ for some prime p and natural number m). We assume that $n \geq 2$ in order to avoid trivial annoyances.

¹This is either by the conjugacy statement of Sylow's theorem, or by the fact that if P^* were another Sylow p -subgroup, then PP^* would be a subgroup of G whose order did not divide that of G .

We introduce several important subgroups of G . First, there is the *upper triangular group*

$$(4A) \quad B = \left\{ \begin{bmatrix} * & * & * & \cdots & * & * \\ 0 & * & * & \cdots & * & * \\ 0 & 0 & * & \cdots & * & * \\ & & & \cdots & & \\ 0 & 0 & 0 & \cdots & * & * \\ 0 & 0 & 0 & \cdots & 0 & * \end{bmatrix} \right\}.$$

Within B are three subgroups, the *unipotent upper triangular group* and the *diagonal group*

$$(4B) \quad U = \left\{ \begin{bmatrix} 1 & * & * & \cdots & * & * \\ 0 & 1 & * & \cdots & * & * \\ 0 & 0 & 1 & \cdots & * & * \\ & & & \cdots & & \\ 0 & 0 & 0 & \cdots & 1 & * \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \right\} \text{ and } T = \left\{ \begin{bmatrix} * & 0 & 0 & \cdots & 0 & 0 \\ 0 & * & 0 & \cdots & 0 & 0 \\ 0 & 0 & * & \cdots & 0 & 0 \\ & & & \cdots & & \\ 0 & 0 & 0 & \cdots & * & 0 \\ 0 & 0 & 0 & \cdots & 0 & * \end{bmatrix} \right\},$$

and the *scalar group* $Z = \{cI \mid c \in \mathbf{F}_q^\times\}$. Of course $Z \leq T$.

Then there is the *monomial group* N , consisting of all matrices with exactly one nonzero entry in each row and in each column.

What are the isomorphism types here? Bearing in mind that the multiplicative group of a finite field is cyclic, it is easy to see that

$$T \cong Z_{q-1} \times \cdots \times Z_{q-1} \text{ (} n \text{ factors), and } Z \cong Z_{q-1}.$$

The structure of U is more complicated in general.² However, as the above-diagonal entries of elements of U are arbitrary, $|U| = q^N$ where $N = n(n-1)/2$ is the number of above-diagonal places. Since $q = p^m$,

U is a p -group and is in particular nilpotent.

There is a homomorphism $\phi : B \rightarrow T$ which “forgets” the above-diagonal entries of a matrix by setting them all to zero. The kernel of ϕ is clearly U . Moreover, $\phi|_T$ is the identity mapping on T . Using these properties or equivalent ones, one sees that

$$B = UT, \quad U \cap T = 1, \quad U \triangleleft B.$$

Hence $|B| = |U||T| = q^N(q-1)^n$, so U is a Sylow p -subgroup of B . Since T is abelian it too is nilpotent.

Thus to understand B we need to understand the structure of U , and the action of T on U .

The reader should verify that

$$C_T(U) = Z.$$

²An important special case is the case $n = 2$. In that case $U \cong \mathbf{F}_q^+$, the additive group of \mathbf{F}_q , which is an elementary abelian p -group of order $q = p^m$. An isomorphism $\mathbf{F}_q^+ \rightarrow U$ is furnished by the mapping $a \mapsto \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$.

This is the only “missing piece” of B that is neither U itself nor embedded in $\text{Aut}(U)$, the automorphism group of U .

Let us set $F = UZ$. Since Z and U commute elementwise and since $|U|$ and $|Z|$ are relatively prime,

$$F = U \times Z.$$

Then

$$(4C) \quad F \text{ is nilpotent, } F \triangleleft B, \text{ and } C_B(F) \leq F, \text{ i.e., } C_B(F) = Z(F).$$

The reader should verify this final statement. For the moment what really counts, however, is simply that $C_T(F) = Z \leq F$. So if we look at F rather than B , there is no “missing piece,” just F and $T/C_T(F)$. In a sense F “controls” the structure of B .

As an illustration of this control, we prove:

(4D)

Let $\alpha \in \text{Aut}(B)$ and suppose that the order of α is relatively prime to $|F|$. If α acts trivially on F , then α acts trivially on B .

To see this, form the semidirect product $X = B \langle \alpha \rangle$. and assume that $\alpha \neq 1$. Replacing α by a power of itself we may assume that α has prime order r . By assumption $\alpha|_F = 1$, so $F \triangleleft X$ and $\alpha \in C_X(F) \triangleleft N_X(F) = X$. Therefore for any $g \in B$, $[\alpha, g] \in C_X(F) \cap B = C_B(F) = Z(F)$. From this one can show that $Z(F) \langle \alpha \rangle \triangleleft X$. But F and α commute and have relatively prime orders. Therefore $\langle \alpha \rangle$ is the only Sylow r -subgroup of $Z(F) \langle \alpha \rangle$. As $Z(F) \langle \alpha \rangle \triangleleft X$ it follows that $\langle \alpha \rangle \triangleleft X$. But then $[\alpha, g] \in \langle \alpha \rangle \cap B = 1$ for any $g \in B$ and so $\alpha = 1$, a contradiction.

The reader may have noticed that the only properties really used in the proof of (4D) were the last two properties in (4C).

Thus, it will be important when we presently prove Fitting’s theorem:

THEOREM 4.1 (HANS FITTING 1930’s). *Every finite solvable group G has a subgroup F such that F is nilpotent, $F \triangleleft G$, and $C_G(F) = Z(F)$.*

The importance will be that the kind of control demonstrated in (4D) has an analogue in any solvable group, for a suitable nilpotent normal subgroup F . Since nilpotent groups are “nicer” in some sense - “more commutative” - than solvable groups, this represents a bit of progress.

Before we prove Theorem 4.1, however, the reader should take a look at the monomial subgroup N introduced above. It will illustrate that the conclusion of Theorem 4.1 sometimes holds for nonsolvable groups, too. (Recall that the symmetric group S_n is solvable only for $n \leq 4$.)

EXERCISES.

- (4.2) Consider G to be acting by left multiplication on the vector space V of $n \times 1$ column vectors over \mathbf{F}_q . Let S be the basis of V consisting of the columns of the identity matrix I . Show that N leaves S invariant, yielding a surjective homomorphism $N \rightarrow S_n$ whose kernel is T . Show further that there is a

complement C to T in N , i.e. a subgroup $C \cong S_n$ such that $N = TC$ and $T \cap C = 1$.

- (4.3) Verify that $T \triangleleft N$, T is nilpotent (abelian!), and $C_N(T) = T$.
- (4.4) A *flag* in V is a chain of subspaces each properly included in the next; no restriction is made on the dimensions except that they obviously must increase strictly. Consider a flag

$$\mathcal{F}: \quad 0 = V_0 < V_1 < V_2 < \cdots < V_r = V, \quad \dim(V_i) = n_i, \quad i = 1, \dots, r.$$

Let $P = G_{\mathcal{F}}$ be the stabilizer of \mathcal{F} in $G = GL_n(q)$. Obtain a decomposition of P in the spirit of the above decompositions of B and N , and identify a subgroup F of P which is nilpotent and normal and contains its centralizer in P (in analogy to (4C)).

Now let us turn to Theorem 4.1. The first lemma is a key observation.

LEMMA 4.5. *Suppose that $G = G_1G_2$, where $G_2 \leq C_G(G_1)$, and G_1 and G_2 are both nilpotent. Then G is nilpotent.*

PROOF. First, a couple of remarks. Note that $G_1 \triangleleft G$ since G_1 normalizes itself, G_2 centralizes G_1 , and $G = G_1G_2$. Similarly $G_2 \triangleleft G$. We don't need these facts but it is worth noting them. The second remark is that if we make the additional assumption that $G_1 \cap G_2 = 1$, then we are in the situation of Property 3.12; and essentially the same proof works here. If $G_1 = 1$ there is nothing to prove; otherwise let $Z = Z(G_1)$. By nilpotence, $Z \neq 1$. Since $G_2 \leq C_G(G_1)$, G_2 centralizes Z , as of course does G_1 . But $G = G_1G_2$ so $Z \leq Z(G)$. Now set $\overline{G} = G/Z$, $\overline{G}_i = G_iZ/Z$, $i = 1, 2$, and use induction to see that \overline{G} is nilpotent. Hence G is nilpotent by Property 3.11.

Now we can prove Theorem 4.1. Let G be any solvable group. We take F to be any nilpotent normal subgroup of G of largest order. (The trivial subgroup is nilpotent; at the moment, perhaps $F = 1$, although we shall see that that is not the case.) We only need to prove that $C_G(F) \leq F$. Set $C = C_G(F)$ and suppose by way of contradiction that $C \not\leq F$. We will use C to construct a nilpotent normal subgroup F_1 of G such that $F < F_1$, which will contradict our choice of F and complete the proof.

Since $F \triangleleft G$, also $C \triangleleft G$. Clearly $F \cap C = Z(F) \leq Z(FC)$. Set $\overline{G} = G/F$ and write \overline{X} for the image of any element or subset X of G under the canonical homomorphism $G \rightarrow G/F$. We have $1 < \overline{C} \triangleleft \overline{G}$. Choose a subgroup Q of \overline{G} which is minimal subject to the conditions: $Q \triangleleft \overline{G}$, $Q \leq \overline{C}$. Then there is a normal subgroup D of G such that $D \leq C$ and $\overline{D} = Q$.³ Now the solvability comes into play. Since G is solvable, \overline{G} is solvable and so \overline{D} is solvable. Therefore $[\overline{D}, \overline{D}] < \overline{D}$. But $[\overline{D}, \overline{D}] \triangleleft \overline{G}$ since $\overline{D} \triangleleft G$. Therefore our minimal choice of \overline{D} forces $[\overline{D}, \overline{D}] = 1$, so that \overline{D} is abelian.

However, $D/D \cap F \cong \overline{D}$ and $D \cap F \leq C \cap F \leq Z(CF)$, so in particular $D \cap F \leq Z(D)$. By Property 3.11, D is therefore nilpotent. By construction,

³Take $D = C \cap R$, where R is the full preimage of Q in G .

$D \leq C$, $D \triangleleft G$ and $D \not\leq F$. Set $F_1 = DF$. Then $F_1 > F$, $F_1 \triangleleft G$, and by Lemma 4.5, F_1 is nilpotent. This completes the proof of Theorem 4.1.

Although our proof took “any” normal nilpotent subgroup of largest order⁴, there is really only one such subgroup. It is called the Fitting subgroup of G in his honor.

DEFINITION 4.6. *Let G be a group. The Fitting subgroup $F(G)$ of G is the unique maximal element among all normal nilpotent subgroups of G .*

The uniqueness - and hence the validity of the definition - depends on the following lemma.

LEMMA 4.7. *Let N_1 and N_2 be normal nilpotent subgroups of the group G . Then N_1N_2 is nilpotent (and of course normal in G).*

PROOF. Although we are not assuming that $N_2 \leq C_G(N_1)$, the proof is really no harder than that of Lemma 4.5.

If $N_1 \cap N_2 = 1$, then $N_1N_2 = N_1 \times N_2$, which is nilpotent by Property 3.12. So we may assume that $K := N_1 \cap N_2 \neq 1$. Now $K \triangleleft N_1$ and we take a minimal normal subgroup Z_1 of N_1 contained in K . By Property 3.10 and the nilpotence of N_1 , $Z_1 \leq Z(N_1)$. But $Z_1 \leq K$, and so $K \cap Z(N_1) \neq 1$. In a similar way, $K \cap Z(N_1)$ is a nontrivial normal subgroup of N_2 , so reducing it to a minimal normal subgroup of N_2 and again using Property 3.10, we conclude that $K \cap Z(N_1) \cap Z(N_2) \neq 1$. Call this intersection Z . It is then immediate that $1 \neq Z \leq Z(N_1N_2)$. The rest of the proof is routine: use induction to obtain that N_1N_2/Z is nilpotent, and use Property 3.11 to get that N_1N_2 is nilpotent.

From the definition it is clear that $F(G)$ is invariant under all automorphisms of G .⁵

There is a neat characterization of the elements of $F(G)$, based on the Zipper Lemma. The result is originally due to Reinhold Baer, and several proofs existed before Wielandt’s Zipper Lemma was discovered - it provides the optimal proof.

THEOREM 4.8. *Let G be a group and $g \in G$. Then the following conditions are equivalent:*

- (a) $g \in F(G)$.
- (b) $\langle g^G \rangle$ is nilpotent.
- (c) For any $x \in G$, $\langle g, g^x \rangle$ is nilpotent.

⁴Any normal nilpotent subgroup maximal with respect to inclusion would have done just as well.

⁵Such subgroups are said to be *characteristic subgroups of G* . Characteristic subgroups of G are of course normal in G , since they are invariant under all inner automorphisms of G . An easy but useful lemma states that if $N \triangleleft G$, then any characteristic subgroup of N is normal in G .

PROOF. The equivalence of (a) and (b) is left to the reader. Obviously (b) implies (c) as well. We prove that (c) implies (b). By induction, for any proper subgroup X of G containing g , $g \in F(X)$. Set $H = \langle g \rangle$. By (c) and the definition of nilpotence, $H \triangleleft \triangleleft \langle H, H^x \rangle$ for all $x \in G$. Thus by Property 2.11, an immediate consequence of the Zipper Lemma, $H \triangleleft \triangleleft G$. Choose a chain (2A). Then as noted at the start, $g \in F(G_{n-1})$. But $G_{n-1} \triangleleft G$, so $F(G_{n-1})$ is a normal nilpotent subgroup of G . Thus, $F(G_{n-1}) \leq F(G)$ and so $g \in F(G)$, completing the proof.

EXERCISES.

- (4.9) Show that if $H \triangleleft \triangleleft G$, then $F(H) \leq F(G)$. Show by example that without the assumption $H \triangleleft \triangleleft G$, this is false.
- (4.10) Show that for any group G and prime p there is a unique largest normal p -subgroup of G . It is traditionally called $O_p(G)$. Show that an element $g \in G$ lies in $O_p(G)$ if and only if for every $x \in G$, $\langle g, g^x \rangle$ is a p -group.
- (4.11) Suppose that G is a simple group of even order and $z \in G$ is an involution (element of order 2). Show that unless $G = \langle z \rangle$, there exists an element $1 \neq w \in G$ of odd order such that $w^z = w^{-1}$. (Hint. For any involution $z' \in G$, show that $\langle z, z' \rangle = \langle v \rangle \langle z \rangle$ where $v = zz'$ and $v^z = v^{-1}$.)
- (4.12) Show that if $N \triangleleft G$, then any characteristic subgroup of N is normal in G .

5. The Frattini Subgroup

Closely related to the Fitting subgroup of G is the Frattini subgroup, whose basic properties we derive in this section. Among other things they shed some light on the action of any group G on $F(G)$.

DEFINITION 5.1. The Frattini subgroup $\Phi(G)$ of a group G is the intersection of all maximal subgroups of G . The Frattini quotient of G is the quotient $G/\Phi(G)$.

The Frattini subgroup is the group-theoretic analogue of many algebraic “radicals”, for instance the Jacobson radical for rings. It satisfies the following properties, of which (5.2), (5.5) and (5.10) are the most important.

- (5.2) If X is any subset of G and $G = \langle X, \Phi(G) \rangle$, then $G = \langle X \rangle$.
- (5.3) Property 5.2 fails if we replace $\Phi(G)$ by any subset of G not contained in $\Phi(G)$.
- (5.4) $\Phi(G) \triangleleft G$, indeed $\Phi(G)$ is characteristic in G .
- (5.5) $\Phi(G) \leq F(G)$, i.e., $\Phi(G)$ is nilpotent.
- (5.6) If $N \triangleleft \triangleleft G$, then $\Phi(N) \leq \Phi(G)$.
- (5.7) $\Phi(G_1 \times G_2) = \Phi(G_1) \times \Phi(G_2)$.
- (5.8) If $N \triangleleft G$ and $N \leq \Phi(G)$, then $\Phi(G/N) = \Phi(G)/N$.
- (5.9) G is nilpotent if and only if $G/\Phi(G)$ is nilpotent.

(5.10) If G is nilpotent and $G \neq 1$, then $\Phi(G)$ is the unique smallest subgroup of G such that $G/\Phi(G)$ is abelian of square-free exponent⁶.

To prove Property 5.2, if $G > \langle X \rangle$ then $\langle X \rangle \leq M$ for some maximal subgroup M of G . Hence $\langle X, \Phi(G) \rangle \leq M < G$, contradiction. For Property 5.3, suppose that $Y \subseteq G$ and $Y \not\leq \Phi(G)$. Then there is a maximal subgroup M of G such that $Y \not\leq M$. Hence $G = \langle M, Y \rangle$ whereas $G > M$. Property 5.4 is clear since automorphisms of G map the set of maximal subgroups of G to itself. To prove Property 5.6, we may assume inductively that $N \triangleleft G$. Let M be any maximal subgroup of G . We argue that $\Phi(N) \leq M$. Indeed if $\Phi(N) \not\leq M$, then $G = \Phi(N)M$. The Dedekind law⁷ yields $N = \Phi(N)(M \cap N)$. By Property 5.2, $N = M \cap N \leq M$, contradicting $\Phi(N) \not\leq M$. Therefore $\Phi(N) \leq M$, and as M was arbitrary, $\Phi(N) \leq \Phi(G)$.

The proof of Property 5.5 depends on the following result, one of the most useful applications of Sylow's Theorem.

THEOREM 5.11 (THE FRATTINI ARGUMENT). *Let $N \triangleleft G$ and let P be a Sylow p -subgroup of N for some prime p . Then $G = N_G(P)N$.*

PROOF. Let $g \in G$. Then $P^g \leq N^g = N$, so P^g is a Sylow p -subgroup of N . By Sylow's Theorem there is $n \in N$ such that $P^g = P^n$. Then $P^{gn^{-1}} = P$. Hence $g = (gn^{-1})n$ with $gn^{-1} \in N_G(P)$ and $n \in N$.

Now for any group G , let P be any Sylow p -subgroup of $\Phi(G)$. By the Frattini Argument, $G = N_G(P)\Phi(G)$, so $G = N_G(P)$ by Property 5.2. *A fortiori*, $P \triangleleft \Phi(G)$ so $P \leq F(\Phi(G))$. As P was arbitrary, $\Phi(G) = F(\Phi(G))$, i.e., N is nilpotent.

The proof of Property 5.9 is not much different. Suppose that $G/\Phi(G)$ is nilpotent. Let $P \in \text{Syl}_p(G)$. Then $P\Phi(G)/\Phi(G)$ is a Sylow p -subgroup of $G/\Phi(G)$. Since $G/\Phi(G)$ is nilpotent, $P\Phi(G)/\Phi(G) \triangleleft G/\Phi(G)$ by Property 3.13. Therefore $P\Phi(G) \triangleleft G$. Naturally P is a Sylow p -subgroup of $P\Phi(G)$, so $G = N_G(P)P\Phi(G)$ by the Frattini Argument. But then $G = N_G(P)\Phi(G) = N_G(P)$, using Property 5.2. As above, as P was arbitrary, G is nilpotent.

The proofs of Properties 5.7 and 5.8 are left to the reader.

Now let us prove Property 5.10. Suppose that G is nilpotent. Let M be any maximal subgroup of G . By Property 3.9, $M \triangleleft G$ and G/M has prime order. Let \mathcal{M} be the set of all maximal subgroups of G . Then the projection mappings $G/\Phi(G) \rightarrow G/M$, $M \in \mathcal{M}$, induce an injection

$$G/\Phi(G) = G / \bigcap_{M \in \mathcal{M}} M \longrightarrow \prod_{M \in \mathcal{M}} G/M$$

into an abelian group of square-free exponent. Hence $G/\Phi(G)$ is abelian of square-free exponent.

⁶The *exponent* of a finite group G is the least positive integer e such that $g^e = 1$ for all $g \in G$. It is the least common multiple of the orders of the elements of G , and divides $|G|$. The exponent of a group is always divisible by the exponent of any subgroup.

⁷Also known as the "modular law", this law states that if A , B and C are subgroups of G such that $C \leq A$, then $BC \cap A = (B \cap A)C$.

Conversely, suppose that $N \triangleleft G$ and G/N is abelian of square-free exponent. We must prove $N \geq \Phi(G)$. Now $G/(N \cap \Phi(G))$ embeds in $G/N \times G/\Phi(G)$, which is abelian of square-free exponent. Hence $G/N \cap \Phi(G)$ is as well. Replacing N by $N \cap \Phi(G)$, we may assume that $N \leq \Phi(G)$ and must prove that $N = \Phi(G)$. Now $\Phi(G/N) = \Phi(G)/N$ so it is enough to show that $\Phi(G/N) = 1$. But $G/N = A_1 \times \cdots \times A_m$ with all A_i of prime order. For each i , the product $A^i = \langle A_j \mid j \neq i \rangle$ is a maximal subgroup of G/N . There may well be other maximal subgroups, but in any case $\Phi(G/N) \leq \bigcap_{i=1}^m A^i = 1$, completing the proof of Property 5.10.

When a group G acts on a nilpotent normal subgroup N (such as $F(G)$, for example), it also acts on $N/\Phi(N)$, which, by Property 5.10 and the fundamental structure theorems for finite abelian groups, is the direct product of elementary abelian p -groups for various primes p . Letting p_1, p_2, \dots be these *distinct* primes, we have

$$N/\Phi(N) \cong (Z_{p_1})^{n_1} \times (Z_{p_2})^{n_2} \times \cdots .$$

for certain natural numbers n_1, n_2, \dots . Then we get a homomorphism

$$\phi : G \longrightarrow \text{Aut}(N) \longrightarrow \text{Aut}(N/\Phi(N)) \cong X_N := GL_{n_1}(p_1) \times GL_{n_2}(p_2) \times \cdots$$

so that the action of G on N , which is *internal to the structure of G* , is related to the *representation theory of G over fields of prime order*⁸.

The smaller the kernel of the homomorphism $\phi : G \rightarrow X_N$ above, the more information can be translated from representation theory to structure theory of G . So it is useful to know something about the kernel of the component function

$$\psi_N : \text{Aut}(N) \longrightarrow \text{Aut}(N/\Phi(N))$$

of ϕ .

When N is a p -group, an important special case, this question has a pretty answer.

THEOREM 5.12 (COPRIME ACTION). *Let N be a p -group for some prime p , and let $\psi := \psi_N$ be the natural homomorphism from $\text{Aut}(N)$ to $\text{Aut}(N/\Phi(N))$. Then the kernel of ψ is a p -group.*

Put somewhat differently: if an automorphism α of the p -group N has order (in $\text{Aut}(N)$) that is relatively prime to p , and α induces the trivial automorphism on $N/\Phi(N)$, then α is the trivial automorphism of N .

PROOF. We prove the statement in this second form. Form the semidirect product $G := N \langle \alpha \rangle$. Assume that α induces the trivial automorphism on $N/\Phi(N)$. Then in $G/\Phi(N)$, the abelian subgroup $N/\Phi(N)$ lies in the center. In particular $G/\Phi(N)$ is nilpotent. By Property 5.9, G is nilpotent. Then by Exercise 3.15, α is the trivial automorphism of N , as required.

⁸A vast amount of information about modular representations of interesting particular finite groups can be found in the *Atlas of Group Representations* maintained by Rob Wilson of Queen Mary College. See <http://brauer.maths.qmul.ac.uk/Atlas/v3/>.

Combining this theorem with Fitting’s Theorem 4.1 we get the following picture of a solvable group G when $F(G)$ is a p -group:

THEOREM 5.13. *Let G be a solvable group and suppose that $F := F(G)$ is a p -group. Set $\overline{G} = G/\Phi(F(G))$. Then $C_{\overline{G}}(\overline{F}) = \overline{F}$. Moreover, G/F embeds in $\text{Aut}(\overline{F}) \cong GL_n(p)$ where $|\overline{F}| = p^n$.*

PROOF. By Theorem 4.1, $C_G(F) = Z(F)$. The normal subgroup $C_{\overline{G}}(\overline{F})$ of \overline{G} has the form \overline{D} for some subgroup $D \triangleleft G$ such that $F \leq D$. Then $D/Z(F)$ acts faithfully on F , so embeds in $\text{Aut}(F)$. But because D acts trivially on \overline{F} , the image of $D/Z(F)$ in $\text{Aut}(F)$ is in the kernel of the homomorphism ψ_F , in the notation of Theorem 5.12. This kernel is a p -group, according to that theorem. Therefore $|D/Z(F)|$ is a power of p . But F is a p -group, so D is a p -group as well. As $D \triangleleft G$, $D \leq F(G) = F$. Therefore $D = F$, which proves the first assertion of the theorem. The rest is clear since $G/F \cong \overline{G}/\overline{F}$ embeds in $\text{Aut}(\overline{F})$.

The solvability assumption was used only in the first line of the proof. The rest of the proof then demonstrates the following more general result:

THEOREM 5.14. *Let G be a group such that $F := F(G)$ is a p -group. Assume that $C_G(F) \leq F$. Set $\overline{G} = G/\Phi(F(G))$. Then $C_{\overline{G}}(\overline{F}) = \overline{F}$. Moreover, G/F embeds in $\text{Aut}(\overline{F}) \cong GL_n(p)$ where $|\overline{F}| = p^n$.*

6. Quasisimple and Semisimple Groups

A group G is *simple* if and only if G has precisely two normal subgroups, namely 1 and G . Abelian simple groups are cyclic of prime order. Nonabelian simple groups G satisfy $G = [G, G]$. According to the classification of finite simple groups, the list of finite simple groups consists of the alternating groups A_n , $n \geq 5$; nineteen families of “simple groups of Lie type,” and twenty-six “sporadic” simple groups, ranging in size from M_{11} , the smallest, to F_1 , the largest.

Let us call a group *dsimple* if and only if

$$(6A) \quad G = G_1 \times \cdots \times G_n, \text{ where } G_1, \dots, G_n \text{ are simple and nonabelian.}$$

If all the G_i are isomorphic to one another, call G *hsimple*.

We have the following properties:

- (6.1) Let G be dsimple as in (6A). Then G has precisely 2^n normal subgroups, namely: for any subset of $\{G_1, \dots, G_n\}$, the product of those in the subset is a normal subgroup containing no other G_j .
- (6.2) Suppose that G is generated by distinct normal nonabelian simple subgroups G_1, \dots, G_n . Then G is their direct product (and so is dsimple).
- (6.3) Let M be a minimal normal subgroup of the group G . If M is solvable, then M is an elementary abelian p -group for some p . If M is not solvable, then M is hsimple.

- (6.4) Suppose that $G = G_1 \times \cdots \times G_n$ is hsimple with the G_i simple. Then $\text{Aut}(G)$ permutes the G_i , indeed

$$\text{Aut}(G) = [\text{Aut}(G_1) \times \cdots \times \text{Aut}(G_n)]S \cong \text{Aut}(G_1) \wr S_n$$

where $S \cong S_n$ permutes by conjugation the isomorphic factors $\text{Aut}(G_1), \dots, \text{Aut}(G_n)$.

To prove Property 6.1, clearly the G_i are minimal normal subgroups of G . Let M be any normal subgroup. If $G_i \leq M$ for some i , then set $G^i = \langle G_j \mid j \neq i \rangle$. We have $M = G_i \times (G^i \cap M)$, and by induction, M is the product of some G_i 's. If $G_i \not\leq M$ for any i , then $G_i \cap M = 1$ by minimality of G_i , and so $[G_i, M] = 1$ for each i . But then $M \leq Z(G)$. Since the G_i are nonabelian simple, $M = 1$, completing the proof.

To prove Property 6.2, observe that since all $G_i \triangleleft G$, $G = G_1 \cdots G_n$. By normality, $[G_i, G_j] \leq G_i \cap G_j = 1$ for all $i \neq j$. Inductively, we argue that $G^i := G_1 \cdots G_i = G_1 \times \cdots \times G_i$ for all $i = 1, \dots, n$. Indeed if this holds for some i , then by Property 6.1, the only normal simple subgroups of G^i are G_1, \dots, G_i themselves. As $G_{i+1} \triangleleft G$ but G_{i+1} is different from all of G_1, \dots, G_i , it follows that $G_{i+1} \not\leq G^i$. But then $G_{i+1} \cap G^i = 1$ by simplicity of G_{i+1} , completing the induction.

Now we prove Property 6.3. Any minimal subnormal subgroup of M is subnormal in G , hence normal in M by Property 2.8. Choose a minimal subnormal subgroup $M_1 \leq M$. By minimality, M_1 is simple. The subgroup $M^* := \langle M_0 \triangleleft M \mid M_0 \cong M_1 \rangle$ is clearly characteristic in M , so equals M by minimality of M . Therefore M is generated by mutually isomorphic normal simple subgroups. Property 6.2 applied to M shows that M is hsimple if M_1 is not abelian. Otherwise $M_1 \cong Z_p$. In any case any two generating subgroups M_0 commute elementwise as they are distinct, simple, and normal. Therefore M is abelian, indeed, elementary abelian in this case, completing the proof.

DEFINITION 6.5. A group G is quasisimple if and only if $G/Z(G)$ is simple and $[G, G] = G$. A group G is semisimple if and only if $G/Z(G)$ is dsimple and $[G, G] = G$.

A classic example of a quasisimple group is $G = SL_n(q)$, $n \geq 2$, q a prime power, except for $SL_2(2)$ and $SL_2(3)$. The reader can check that $Z(G)$ is the scalar subgroup of G , $Z(G) \cong Z_{(n, q-1)}$, and $G/Z(G) = PSL_n(q)$, well known to be simple with the two noted exceptions for n and q .

- (6.6) Let G be semisimple. Then there exist uniquely determined (up to order) quasisimple normal subgroups G_1, \dots, G_n of G mapping onto to the simple direct factors of $G/Z(G)$. Moreover, $[G_i, G_j] = 1$ for all $i \neq j$; and $Z(G)$ contains $G_1 \cap G_2 \cdots G_n$ and the other $n - 1$ intersections of G_i with the product of the other G_j 's.
- (6.7) Suppose that G is any group such that $G/Z(G)$ is dsimple (resp. simple). Then $[G, G]$ is semisimple (resp. quasisimple).
- (6.8) Let $G = G_1 \cdots G_n$ be semisimple, as in 6.6. Let $N \triangleleft G$. Then $N = (N \cap Z(G)) \prod_{i \in I} G_i$ for some subset $I \subseteq \{1, \dots, n\}$.
- (6.9) Let G be semisimple. Then $\Phi(G) = F(G) = Z(G)$, and the canonical mapping $\text{Aut}(G) \longrightarrow \text{Aut}(G/Z(G))$ is injective.

The following easy lemma is useful for these purposes⁹:

LEMMA 6.10. *Suppose that $H \subseteq G$ and $K \subseteq G$ and $Z \subseteq Z(G)$. Then $[HZ, KZ] = [H, K]$.*

Indeed, for elements h, k, y, z of H, K, Z and Z , one quickly sees that $[hy, kz] = [h, k]$.

The lemma can be rephrased as follows: given H and K , the subgroup $[H, K]$ depends only on the images of H and K in $G/Z(G)$.

In Property 6.6, let $\overline{G} = G/Z(G)$. Write the dsimple group \overline{G} as $\overline{G} = \overline{G}_1 \times \cdots \times \overline{G}_n$, with each \overline{G}_i simple. For all groups $H \leq G$ such that $\overline{H} = \overline{G}_i$, Lemma 6.10 implies that the group $[H, H]$ is independent of H . This commutator group, which we call G_i , is then the unique minimal subgroup of G mapping onto \overline{G}_i . In particular it is normal in G , and perfect¹⁰, and indeed the unique perfect subgroup of G mapping onto \overline{G}_i . Clearly G_i is quasisimple. For any $i \neq j$, $[\overline{G}_i, \overline{G}_j] = 1$, so $[G_i, G_j] \leq Z(G)$. Therefore $[[G_i, G_j], G_j] = 1$. It then follows from the Three Subgroups Lemma¹¹ that $[[G_j, G_j], G_i] = 1$, i.e., $[G_j, G_i] = 1$. The rest of Property 6.6 is immediate from the fact that $\overline{G} = \overline{G}_1 \times \cdots \times \overline{G}_n$.

For Property 6.7, again let $\overline{G} = G/Z(G)$, a dsimple group. Set $H = [G, G]$. By the lemma, $H = [H, H]$. Hence H is semisimple.

For Property 6.8, we first pass to $G/Z(G)$ and conclude by Property 6.1 that $NZ(G) = KZ(G)$, where $K = \prod_{i \in I} G_i$ for some $I \subseteq \{1, \dots, n\}$. It follows that $[N, N] = [K, K] = K$, and then $N = (N \cap Z(G))K$ by the Dedekind law.

For Property 6.9, suppose first that G is semisimple and M is a maximal subgroup of G not containing $Z(G)$. Then $G = MZ(G)$. Therefore $G = [G, G] = [M, M] \leq M$, a contradiction. So $Z(G) \leq M$, whence $Z(G) \leq \Phi(G) \leq F(G)$. But $F(G) < G$ and $G/Z(G)$ is dsimple, so $F(G) \leq Z(G)$ and all three subgroups coincide. To show the final statement, we choose any $\alpha \in \text{Aut}(G)$ such that α induces the trivial automorphism on $G/Z(G)$ and show that α is itself trivial. Namely, for any $g \in G$ there is $\zeta(g) \in Z(G)$ such that $\alpha(g) = g\zeta(g)$. The facts that α preserves multiplication and $\zeta(g) \in Z(G)$ imply that ζ is a homomorphism from G to $Z(G)$ (Check!). Hence the kernel of ζ contains $[G, G] = G$, whence $\alpha(g) = g$ for all $g \in G$ as claimed.

Quasisimple and semisimple normal subgroups are an important focus of analysis of the structure of an arbitrary group, for reasons to be seen in the next section.

⁹Note that if H and K are subgroups of G , then $[H, K]$ is defined to be the subgroup *generated* by all commutators $[h, k]$ such that $h \in H$ and $k \in K$. The set of all commutators itself may not be a subgroup.

¹⁰By definition, a group X is perfect if and only if $X = [X, X]$.

¹¹The Three Subgroups Lemma states that if H_1, H_2 , and H_3 are subgroups of G such that $[[H_1, H_2], H_3] = [[H_2, H_3], H_1] = 1$, then $[[H_3, H_1], H_2] = 1$. It is based on *Philip Hall's identity* for all $x_1, x_2, x_3 \in G$:

$$[[x_1, x_2^{-1}], x_3]^{x_2} [[x_2, x_3^{-1}], x_1]^{x_3} [[x_3, x_1^{-1}], x_2]^{x_1} = 1.$$

One cannot quite get away with thinking only about simple or dsimple groups. This is in a way unfortunate since the classification of finite simple groups, and Property 6.1, give a complete classification of dsimple groups.

The preceding development also suggests the question: given a nonabelian simple (resp. dsimple) group H , what are all the different quasisimple (resp. semisimple) groups G such that $G/Z(G) \cong H$? This question was first investigated by Issai Schur¹², who showed that there are only finitely many such quasisimple or semisimple groups, for a given H . The determination of this finite set of groups leads one through some quite complicated technicalities¹³, which fortunately have been worked through as of the 1980's. We state the results without proof¹⁴.

THEOREM 6.11 (SCHUR). *Let H be a finite group such that $H = [H, H]$. Define a covering of H to be a pair (G, f) such that $f : G \rightarrow H$ is a surjective group homomorphism, $G = [G, G]$, and the kernel of f lies in $Z(G)$. Then the kernel of any covering of H is a finite (abelian) group. Moreover, there exists a covering $\hat{u} : \hat{H} \rightarrow H$ that is “universal” in the following sense. For any covering $f : G \rightarrow H$ of H there is a covering $v : \hat{H} \rightarrow G$ of G such that $v \circ f = \hat{u}$. We write $M(H)$ for the kernel of \hat{u} . In particular for any covering $f : G \rightarrow H$, G is isomorphic to a quotient of \hat{H} by a subgroup of the finite group $M(H)$. Finally, if $H = H_1 \times H_2$, then $M(H) \cong M(H_1) \times M(H_2)$.*

As an example, if $H = A_5$, the alternating group, it was known to Schur (but is by no means trivial) that for $\hat{H} = SL_2(5)$, there is a universal covering $\hat{H} \rightarrow H$. We have $|Z(\hat{H})| = 2$ and so $|\hat{H}| = 120$.

The kernel of \hat{u} is called the *Schur multiplier* $M(H)$ of H .¹⁵ Thus $M(A_5) = Z_2$, for example.

The work of many authors, most notably Schur himself, Robert Steinberg, and Robert Griess, has determined the Schur multipliers of all the finite simple groups (as determined in the classification).¹⁶ This work is unusually delicate.

The Schur multipliers of all the dsimple groups are determined by the Schur multipliers of all the simple groups and the final sentence of Schur's theorem.

¹²Schur actually investigated the more general question: given any finite group G , what are all the groups G and subgroups $Z \leq G$ such that $G/Z \cong H$ and $Z \leq Z(G) \cap [G, G]$? These questions are equivalent when H is semisimple.

¹³Some incorrect answers to these questions have from time to time been accepted and not noticed to be wrong for years! For example, a universal covering of the Mathieu group M_{22} was thought for at least 20 years to have a kernel of order 2, until Griess discovered in 1979 that the kernel is cyclic of order 4.

¹⁴An exposition of this theorem may be found, for example, in Chapter IV of *Endliche Gruppen I* by B. Huppert, Springer-Verlag 1968.

¹⁵The Schur multiplier of H can be shown to be isomorphic to the cohomology group $H^2(H, \mathbf{Q}/\mathbf{Z})$ where the additive group \mathbf{Q}/\mathbf{Z} is considered to be a trivial H -module. The isomorphism is natural with the dual of this cohomology group.

¹⁶For details, see section 6.1 of vol. 3 of *The Classification of the Finite Simple Groups* by D. Gorenstein, R. Lyons and R. Solomon, Surveys and Monographs **40**, Amer. Math. Soc., 1998.

7. Subnormality in Practice: Components of Groups

If one re-examines the proof of Fitting's theorem 4.1, one sees that the solvability assumption is used only in one place: in the analysis of the subgroup $D \triangleleft G$, when $C_G(F) \not\leq F$. In that proof, D was chosen so that $D \leq C_G(F)$ and DF/F is minimal normal in G . Thus $D \cap F \leq Z(D)$, and the solvability forces $D/D \cap F \cong DF/F$ to be abelian, whence D is nilpotent and has no business being outside F . Without this assumption there would be the additional possibility that DF/F is hsimple, implying that $D/Z(D)$ is hsimple, and so $[D, D]$ is semisimple.

Therefore in order to generalize Fitting's theorem beyond the solvable case, it seems reasonable to use an expanded version of the Fitting subgroup that also includes by definition the normal semisimple subgroups of G . This is precisely what Helmut Bender did in the 1960's, defining the *generalized Fitting subgroup* $F^*(G)$ of an arbitrary finite group and proving the analogue of Fitting's theorem in full generality.

DEFINITION 7.1. A *component* of a group G is a subnormal quasisimple subgroup of G .

DEFINITION 7.2. The *layer* $E(G)$ of a group G is the largest normal semisimple subgroup of G .

Of course, this definition of $E(G)$ requires some preparation, to justify the phrase "the largest."

(7.3) If N_1 and N_2 are normal semisimple subgroups of G , then N_1N_2 is again semisimple.

(7.4) In any group G , the components of $E(G)$ are exactly the components of G . In particular distinct components of G commute elementwise.

To prove the first of these, note that $[N_1N_2, N_1N_2]$ contains $[N_i, N_i] = N_i$ for both $i = 1$ and 2 , so N_1N_2 is perfect. Therefore we need only show that $N_1N_2/Z(N_1N_2)$ is dsimple. Now $Z(N_i) \triangleleft G$ since $N_i \triangleleft G$, for each $i = 1, 2$. In particular, $[N_1, Z(N_2)] \leq Z(N_2) \cap N_1$. But $Z(N_2) \cap N_1$ is a normal abelian subgroup of N_2 . $N_2/Z(N_2)$ has no nontrivial normal abelian subgroup, so $Z(N_2) \cap N_1 \leq Z(N_1)$. Thus $[[N_1, Z(N_2)], N_1] = 1$. Another use of the Three Subgroups Lemma gives $[N_1, Z(N_2)] = 1$. Thus, $Z(N_2) \leq Z(N_1N_2)$. Indeed, $Z(N_1N_2) \cap N_2 \leq Z(N_2)$, so equality holds. Now passing to $\bar{G} := G/Z(N_1N_2)$, we have that $\bar{N}_i \cong N_i/Z(N_i)$ is dsimple for $i = 1$ and 2 . We have therefore reduced to the case that N_i is dsimple for $i = 1$ and 2 .

If $N_1 \cap N_2 = 1$, then $N_1N_2 = N_1 \times N_2$ is obviously dsimple. Otherwise for each i , $N_i = (N_1 \cap N_2) \times H_i$ with each factor the product of some of the simple direct factors of N_i (see Property 6.1). Hence $N_1N_2 \leq (N_1 \cap N_2)C_G(N_1 \cap N_2) = (N_1 \cap N_2) \times C_G(N_1 \cap N_2)$. But H_1 and H_2 are normal dsimple subgroups of $C_G(N_1 \cap N_2)$ so by induction H_1H_2 is semisimple, whence $N_1N_2 = (N_1 \cap N_2) \times H_1H_2$ is as well. Thus Property 7.3 holds.

In Property 7.4, components of $E(G)$ are normal in $E(G)$, hence subnormal in G . Suppose conversely that H is a component of G . We may of course assume

that $H < G$. As $H \triangleleft\triangleleft G$, we have $H \triangleleft\triangleleft K \triangleleft G$ for some $K < G$. By induction $H \leq E(K)$. Clearly $E(K)$ is characteristic in K so $E(K) \triangleleft G$. But $E(K)$ is semisimple so $E(K) \leq E(G)$ by definition. Thus, $H \leq E(G)$. As H is quasisimple, the image of H in $\overline{E(G)}/Z(E(G))$ is subnormal in that dsimple group, so is one of its simple direct factors. As seen in the proof of Property 6.6, $[H, H]$ is then a component of $E(G)$. But H is perfect, so is itself a component of $E(G)$.

8. Bender's Theorem

DEFINITION 8.1 (HELMUT BENDER). $F^*(G) = F(G)E(G)$.

THEOREM 8.2 (BENDER). *Let G be a group. Then $C_G(F^*(G)) \leq F^*(G)$.*

EXERCISES.

- (8.3) If $G \neq 1$, then $F^*(G) \neq 1$. (Prove this without using Bender's Theorem, and use it in the next exercise.)
- (8.4) Imitate and adapt the proof of Fitting's Theorem to prove Bender's Theorem.
- (8.5) Show that if $N \triangleleft\triangleleft G$, then $F^*(N) \triangleleft\triangleleft F^*(G)$. Also, $F^*(F^*(G)) = F^*(G)$.
- (8.6) Show that if $Z \leq Z(G)$, then $F^*(G/Z) = F^*(G)/Z$. Show however that in general $F^*(G/F(G))$ and $F^*(G)/F(G)$ do not coincide. What is the "biggest subgroup" $Q(G)$ of $F^*(G)$ that you can name in general such that it is always true that $F^*(G/Q(G)) = F^*(G)/Q(G)$?
- (8.7) Suppose that X is a group such that $X = F^*(X)$. Describe all subnormal subgroups of X .
- (8.8) Suppose that G is a finite group of order $2^a \cdot 3^b \cdot 5^c \cdot 7$ with $a < 5$, $b \leq 5$ and $c \leq 5$. Suppose that there is a subgroup $A_5 \cong H \triangleleft G$, and no other subnormal quasisimple subgroup of G . (A_5 is the alternating group). Show that a Sylow 7-subgroup of G is normal in G . (Hint. Show that a Sylow 7-subgroup centralizes $F^*(G)$. This may require you to analyze the automorphism groups of some particular groups, like A_5 .) Show that the conclusion need not hold if $a = 5$.
- (8.9) Suppose that $F^*(G)$ has order p^a and $\Phi(F^*(G))$ has order p^b . Show that $|G|$ divides $p^c m$, where $2c = a^2 - 2ab + b^2 - a + 2b$ and $m = \prod_{i=1}^{a-b} (p^i - 1)$. For any p and a , construct such a group G of order $p^c m$ (you may choose the value of b).

9. p -Locals in Sporadic Groups I: Extra-special p -Groups

A p -local¹⁷ subgroup of a group G is a subgroup $N_G(Q)$ such that Q is some p -subgroup of G with $Q \neq 1$. The p -local "structure" of a group G (a loosely defined term) can be thought of as the lattice of those p -local subgroups $N_G(Q)$ arising from all the non-identity subgroups Q of a fixed Sylow p -subgroup of G .

¹⁷The terminology is due to J. L. Alperin, I believe.

An important theme of finite group theory is that the p -local structures in a finite group G (for all primes p , sometimes just for one prime or for certain primes) strongly influence the structure of G . Furthermore, the 2-local structure of a finite simple group, it turns out, determines the isomorphism type of the simple group! The latter statement was central to the philosophy of the classification of the finite simple groups, not as a theorem (indeed, its only proof uses the classification), but as a plan of action: determine all possible 2-local structures for simple groups; then for each one, show that there is exactly one simple group up to isomorphism with that 2-local structure.

Many of the *sporadic* simple groups, as well as some of the simple groups of Lie type, possess a p -local subgroup N such that $F^*(N)$ is an “extra-special” p -group.¹⁸ We study extra-special p -groups in this section, and their automorphisms groups – in order to get a handle on the structure of N – in the next section.

DEFINITION 9.1. *Let P be a p -group. Then P is said to be extra-special¹⁹ if and only if $Z(P)$, $[P, P]$, and $\Phi(P)$ all coincide and have order p .*

Somewhat more simply, extra-special groups can be recognized as follows:

LEMMA 9.2. *Let P be a p -group with $|P| > p$. Then P is extra-special if and only if $|Z(P)| = p$ and $P/Z(P)$ is elementary abelian.*

PROOF. Since $|Z(P)| < |P|$, P is not abelian, so $[P, P] \neq 1$. Since $P/Z(P)$ is elementary abelian, but P is not, Property 5.10 implies that $1 < \Phi(P) \leq Z(P)$, so $\Phi(P) = Z(P)$. Similarly $1 < [P, P] \leq Z(P)$ and so $[P, P] = Z(P)$.

Here are some examples of extraspecial groups:

- (9.3) The group E_{p^3} with generators x, y, z and defining relations $x^p = y^p = z^p = 1$, $[x, y] = z$, $[x, z] = [y, z] = 1$. Moreover, $|E_{p^3}| = p^3$ and $Z(E_{p^3}) = \langle z \rangle$.
- (9.4) The group F_{p^3} with generators x, y, z and defining relations $x^p = z$, $y^p = z^p = 1$, $[x, y] = z$, $[y, z] = 1$. Moreover, $|F_{p^3}| = p^3$ and $Z(F_{p^3}) = \langle z \rangle$.
- (9.5) In the subgroup U of $GL_n(p)$ (see (4B), the “border” group Q_n of order p^{2n-1} , namely

$$Q_n = \left\{ \begin{bmatrix} 1 & * & * & \cdots & * & * \\ 0 & 1 & 0 & \cdots & 0 & * \\ 0 & 0 & 1 & \cdots & 0 & * \\ & & & \cdots & & \\ 0 & 0 & 0 & \cdots & 1 & * \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \right\}.$$

Further examples are so-called “central products” of extra-special groups. The term “central product” is not commonly well-defined. A group G is said to be a central product of subgroups H and K if and only if $G = HK$ and $[H, K] = 1$. The structure of G is not determined uniquely by that of H and K in general. One

¹⁸For readers familiar with Heisenberg groups, extra-special groups are their finite analogues.

¹⁹If the order p condition is dropped, then P is said to be special.

only knows that there is a surjection $H \times K \rightarrow G$ which restricts to the identity mapping on both H and K . Put differently, the direct product of H and K is a central product of its direct factors, but there may be others in which $H \cap K \neq 1$. (The definition does force $H \cap K \leq Z(H) \cap Z(K)$.)

In the particular situation that H and K are extra-special p -groups for the same prime p , however, we write $G = H * K$ to mean $G = HK$, $[H, K] = 1$, and $Z(H) = Z(K)$.²⁰ Note that in this situation $H \cap K$ centralizes both H and K , so $H \cap K \leq Z(H) \cap Z(K)$, and then $H \cap K = Z(H) = Z(K)$. Thus if $|H| = p^a$ and $|K| = p^b$, then $|H * K| = p^{a+b-1}$. By analogy with direct products, one can consider $G = H * K$ to define the “internal” central product of H and K . One can also define the “external” central product to be $H * K = (H \times K) / \langle z_H z_K^{-1} \rangle$, where $Z(H) = \langle z_H \rangle$ and $Z(K) = \langle z_K \rangle$. Informally one says that $H * K$ is “the central product of H and K with central generators z_H and z_K identified.”

Here are important properties of extra-special groups:

- (9.6) If H and K are extra-special p -groups for the same prime p , then $H * K$ is extra-special.
- (9.7) Let H , K , and L all be extra-special p -groups for the same prime p . Then the groups $(H * K) * L$ and $H * (K * L)$ are naturally isomorphic.
- (9.8) Let P be an extra-special p -group. Fix an isomorphism $Z(P) \cong \mathbf{F}_p^+$ and use it to identify $Z(P)$ with \mathbf{F}_p . Set $\overline{P} = P/Z(P)$, fix an isomorphism $\overline{P} \cong (\mathbf{F}_p^+)^N$, where $|\overline{P}| = p^N$, and use it to consider \overline{P} an N -dimensional vector space over \mathbf{F}_p . Then the mapping

$$\begin{aligned} \overline{P} \times \overline{P} &\longrightarrow \mathbf{F}_p \\ (\overline{x}, \overline{y}) &\mapsto [x, y] \end{aligned}$$

is an alternating nondegenerate \mathbf{F}_p -bilinear form on \overline{P} .

- (9.9) Let P be an extra-special p -group. Then there exist extra-special subgroups H_1, \dots, H_n of P , all of order p^3 , such that $P = H_1 * H_2 * \dots * H_n$.
- (9.10) Any extra-special p -group of order p^3 is isomorphic to either E_{p^3} or F_{p^3} . Moreover, $E_{p^3} \not\cong F_{p^3}$.
- (9.11) If $p > 2$, then E_{p^3} and F_{p^3} have exponent p and p^2 , respectively. If $p = 2$, then E_{2^3} and F_{2^3} are isomorphic respectively to the dihedral group and the quaternion group of order 8.
- (9.12) If $p > 2$, then $E_{p^3} * E_{p^3} \not\cong F_{p^3} * F_{p^3} \cong E_{p^3} * F_{p^3}$. If $p = 2$, then $D_8 * D_8 \cong Q_8 * Q_8 \not\cong D_8 * Q_8$.
- (9.13) Every extra-special p -group has order p^{2n+1} for some $n > 0$, sometimes called the *width* of the extra-special group. There are exactly two isomorphism classes of extra-special groups of order p^{2n+1} , represented by²¹

²⁰The older notation $G = H \circ K$ is still sometimes used since it avoids confusion with the notation for free products.

²¹*Warning on notation:* This is not commonly used notation. In the group-theoretic literature, there is no common notation for $F_{p^{2n+1}}$ when $p > 2$, perhaps because this group arises quite infrequently. The group $E_{p^{2n+1}}$ for $p > 2$, which does arise frequently, is most commonly and most efficiently denoted p^{1+2n} , e.g. p^{1+2} , p^{1+4} , etc. For $p = 2$, both types occur frequently enough to deserve brief notation, and one commonly writes 2_+^{1+2n} for $E_{2^{2n+1}}$ and 2_-^{1+2n} for $F_{2^{2n+1}}$.

$E_{p^{2n+1}} := (E_{p^3})^{*n} := E_{p^3} * \cdots * E_{p^3}$ (n times) and $F_{p^{2n+1}} := (E_{p^3})^{*(n-1)} * F_{p^3}$.

(9.14) If $p > 2$, then $E_{p^{2n+1}}$ has exponent p , but $F_{p^{2n+1}}$ has exponent p^2 . For $p = 2$, 2_{\pm}^{1+2n} has $2^{2n} \pm 2^n - 2$ noncentral involutions. That is, $(D_8)^{*n}$ has $2^{2n} + 2^n - 2$ noncentral involutions and $(D_8)^{*(n-1)} * Q_8$ has $2^{2n} - 2^n - 2$ noncentral involutions.

(9.15) Every maximal abelian subgroup of $E_{p^{2n+1}}$ or $F_{p^{2n+1}}$ has order p^{n+1} , and is either of rank $n + 1$ (in $E_{p^{2n+1}}$) or of rank at least n (in $F_{p^{2n+1}}$).

To see Property 9.6, set $Z = Z(H) = Z(K)$. Notice that since $[H, K] = 1$, $K \leq C_G(H)$ and so by the Dedekind law, $C_G(H) = K(C_G(H) \cap H) = KZ = K$. Hence $Z(G) \leq K$, whence $Z(G) \leq Z(K) = Z$. As $G/Z = HKZ/Z = H/Z \times K/Z$, G is extra-special by Lemma 9.2. The proof of Property 9.7 is straightforward and left to the reader.

In Property 9.8, if $x_1, y_1 \in P$ and $\bar{x} = \bar{x}_1, \bar{y} = \bar{y}_1$, then $x_1 = xz$ and $y_1 = yw$ for some $z, w \in Z$, and $[x_1, y_1] = [x, y]$ as $z, w \in Z(P)$. So the (allegedly) bilinear form is well-defined. When $P/Z(P)$ and $Z(P)$ are identified with a vector space and \mathbf{F}_p , respectively, the operation of addition is derived from the multiplication in P . Moreover, scalar multiplication by $n \in \mathbf{F}_p$ comes from the n^{th} power map on P . So bilinearity simply means the following conditions for all $t, u, v \in P$:

$$(9A) \quad [tu, v] = [t, v][u, v]; \quad [t, uv] = [t, u][t, v]; \quad [t^n, u] = [t, u]^n = [t, u^b].$$

These identities hold in any group X such that $[X, X] \leq Z(X)$. Indeed in any group²² $[t, uv] = [t, v][t, u]^v$, which implies the second identity. Also $[a, b] = [b, a]^{-1}$ in any group, so the first identity holds, and the final ones follow immediately. Hence, the form is bilinear.

Since $[t, t] = 1$ for all $t \in P$, the bilinear form is alternating. Nonsingularity means that if $x \in P$ and $[x, y] = 1$ for all $y \in P$, then $x \in Z$. But this is obvious.

It is well-known²³ that a finite-dimensional vector space equipped with a non-degenerate alternating form is the orthogonal sum of hyperbolic planes, which are two-dimensional nonsingular subspaces. Property 9.9 amounts to exactly this fact applied to \bar{P} . In group-theoretic language, choose any $x \in P - Z$ and then any $y \in P$ such that $[x, y] \neq 1$. Set $H_1 = \langle x, y \rangle$. Then $Z = \langle [x, y] \rangle \leq H_1$ and $\bar{H}_1 = \langle \bar{x}, \bar{y} \rangle \cong Z_p \times Z_p$. Moreover $[x^i y^j, y] = [x, y]^i = 1$ if and only if p divides i , so $Z(H_1) \leq \langle y \rangle$ and then $Z(H_1) = Z(P)$ as $[x, y] = 1$. Thus H_1 is extra-special. Note that since $x^g = x[x, g] \in xZ$ for all $g \in P$, x has at most p conjugates and so $|P : C_P(x)| = p$. Similarly $|P : C_P(y)| = p$, so $|P : C_P(H_1)| = |P : C_P(x) \cap C_P(y)| \leq p^2$. Because $|H_1 : Z(H_1)| = p^2$, we conclude that $|P : C_P(H_1)| = p^2$ and $P = H_1 C_P(H_1)$. Now $Z(C_P(H_1))$ centralizes $C_P(H_1)$ and H_1 , so lies in $Z(P)$ and has order p . Lemma 9.2 applies to $C_P(H_1)$ and yields that it is extra-special. Now $P = H_1 * C_P(H_1)$ and induction completes the proof of Property 9.9.

²²The identity $t[t, u] = t^u$ “conceptualizes” this identity a bit, as follows. $t[t, uv] = t^{uv} = (t^u)^v = (t[t, u])^v = t^v[t, u]^v = t[t, v][t, u]^v$.

²³See for example the classic *Geometric Algebra* by Emil Artin. (Even if you know this result, read the masters.)

Let P be extra-special of order p^3 . If $p = 2$, then P has exponent 4 (groups of exponent 2 are abelian!). Choose $x \in P$ of order 4 and $y \in P - \langle x \rangle$. Then y has order 2 or 4, and since $x \notin Z(P)$, $x^y = x^{-1}$. According as y has order 2 or 4, therefore, $P \cong D_8 \cong E_{2^3}$ or $Q_8 \cong F_{2^3}$. Now suppose that $p > 2$. In this case we need the following fact, which depends on the facts that p is odd, $[P, P] \leq Z(P)$ and $[P, P]$ has exponent p :

$$(9B) \quad \text{For all } g, h \in P, (gh)^p = g^p h^p.$$

To see this, imagine rearranging the $2p$ terms in $(gh)^p$, moving g 's to the left past h 's. Each such move introduces a term $[h, g]$, which belongs to $[P, P] \leq Z(P)$. Therefore these terms can immediately be pulled out to the right without effect. Continuing to pull all the g 's to the front, we find that the number of interchanges has created the triangular number $p(p-1)/2$ of terms $[h, g]$ at the right. Thus,

$$(gh)^p = g^p h^p [h, g]^{p(p-1)/2}.$$

Since p is odd and $[P, P]$ has exponent p , $[h, g]^{p(p-1)/2} = 1$, establishing (9B).

Returning to our generators x, y of P in the case $p > 2$, if $x^p \neq 1$, then $\langle x^p \rangle = Z(P)$ contains y^p . Hence $y^p = x^{ip}$ for some i . Set $y' = x^{-i}y$. Then $(y')^p = 1$ and still, x and y' generate P . So we can assume that one of our original generators, say x , has order p . Set $z = [x, y]$. According as y has order p or p^2 , we have the defining relations for E_{p^3} or F_{p^3} . Note that by (9B), E_{p^3} has exponent p , but of course F_{p^3} does not, so these two groups are not isomorphic. We have proved Properties 9.10 and 9.11.

We leave the proof of 9.12 to the reader with the hint to look for elements of order p .

EXERCISES.

- 9.16 Show that if H is an extra-special 2-group of width n with exactly r noncentral involutions, then $D_8 * H$ has width $n+1$ and has exactly $2^{2n+1} + 2r + 2$ noncentral involutions. Deduce Property (9.14).
- 9.17 Prove Property (9.13).
- 9.18 Let G be extra-special of width n . Suppose that $x \in G - Z(G)$ be an element of order p . Show that $C_G(x) = \langle x \rangle \times G_0$, where G_0 is extra-special of width $n-1$ and the same "type" (E or F) as G . Deduce Property (9.15).

10. Automorphisms of Extra-special p -Groups

We turn to the analysis of groups G such that $F^*(G) =: P$ is an extra-special p -group. By Bender's Theorem, $C_G(P) = Z(P)$, and so $G/Z(P)$ embeds in $\text{Aut}(P)$, with $P/Z(P)$ mapping onto the group $\text{Inn}(P)$ of inner automorphisms of P . Therefore G/P embeds into $\text{Out}(P) := P/\text{Inn}(P)$. One may understand the desired structure by a series of three questions: a) What is the structure of $\text{Out}(P)$? b) What is the structure of $\text{Aut}(P)$, which is an extension the elementary abelian p -group $\text{Inn}(P)$ by $\text{Out}(P)$? and c) Given the structure of $G/Z(P) \leq \text{Aut}(P)$, how do we understand the structure of G , a central extension of $G/Z(P)$ by the group $Z(P) \cong Z_p$? In this section we address the first two of these questions.

Again write $\overline{P} = P/Z(P)$. Then $\text{Inn}(P) \cong \overline{P}$. This isomorphism transports the action of $\text{Aut}(P)$ by conjugation on its normal subgroup $\text{Inn}(P)$ to the action of $\text{Aut}(P)$ on $\overline{P} = P/Z(P)$.

$$(10A) \quad \phi : \text{Aut}(P) \rightarrow \text{Aut}(\text{Inn}(P)).$$

The following properties are important:

(10.1) For any $\alpha \in \text{Aut}(P)$ and $x \in P$, $\phi(\alpha)(\overline{x}) = \overline{\alpha(x)}$. That is, the mapping ϕ takes α to the automorphism of \overline{P} induced by α .

(10.2) $\ker(\phi) = \text{Inn}(P)$.

The reader should make the straightforward calculation establishing Property 10.1. In view of that property, Property 10.2 asserts that an automorphism of P is inner if and only if it acts trivially on \overline{P} . Since \overline{P} is abelian, one implication is trivial. Suppose conversely that $\alpha \in \text{Aut}(P)$ and $\overline{\alpha(x)} = \overline{x}$ for all $x \in P$. Then $\alpha(x) = x\zeta(x)$ with $\zeta(x) \in Z(P)$. Then $xy\zeta(xy) = \alpha(xy) = \alpha(x)\alpha(y) = x\zeta(x)y\zeta(y) = xy\zeta(x)\zeta(y)$, so $\zeta : P \rightarrow Z(P)$ is a homomorphism.

Since α and ζ determine each other, $|\ker(\phi)| \leq |\text{Hom}(\overline{P}, Z(P))| = |\overline{P}| = |\text{Inn}(P)|$, which completes the proof of Property 10.2.

The answers are different for $p > 2$ and for $p = 2$.

Recall that

$$B(\overline{x}, \overline{y}) = [x, y]$$

is a nondegenerate alternating bilinear form on \overline{P} (Property (9.8)). We define

$$(10B) \quad \begin{aligned} Sp(\overline{P}, B) &:= \{g \in GL(\overline{P}) \mid B(g\overline{x}, g\overline{y}) = B(\overline{x}, \overline{y}) \text{ for all } \overline{x}, \overline{y} \in \overline{P}\} \\ CSp(\overline{P}, B) &:= \{g \in GL(\overline{P}) \mid (\exists c \in \mathbf{F}_p) B(g\overline{x}, g\overline{y}) = cB(\overline{x}, \overline{y}) \text{ for all } \overline{x}, \overline{y} \in \overline{P}\} \end{aligned}$$

LEMMA 10.3. *The image of ϕ lies in $CSp(\overline{P}, B)$. Moreover for any $\alpha \in \text{Aut}(P)$, $\phi(\alpha) \in Sp(\overline{P})$ if and only if $\alpha|_{Z(P)} = id_{Z(P)}$.*

PROOF. The proof is left to the reader. The $c \in \mathbf{F}_p$ corresponding to α is specified by $\alpha(z) = z^c$, $z \in Z(P)$. Note that it makes sense here to have an exponent in the field of p elements. \square

In order to prove that the image of ϕ is large, we need to construct automorphisms of P , and for that we devise a presentation of P . First, choose a basis $\{\overline{x}_1, \dots, \overline{x}_n\}$ for \overline{P} as a \mathbf{F}_p -vector space. Here of course n is defined by $p^n = |\overline{P}|$. Take any preimages $x_1, \dots, x_n \in P$ of $\overline{x}_1, \dots, \overline{x}_n$. Also choose a generator z of $Z(P) \cong Z_p$. (There is nothing canonical about our presentation.) It is obvious that x_1, \dots, x_n, z generate P (and indeed z can be omitted). Then $x_i^p \in Z(P)$ and $[x_i, x_j] \in Z(P)$ for all $i, j = 1, \dots, n$. Thus there exist (unique) $a_i, b_{ij} \in \mathbf{F}_p$ such that

$$(10C) \quad \begin{aligned} (1) \quad &x_i^p = z^{a_i} \text{ for all } i = 1, \dots, p, \text{ and } z^p = 1; \\ (2) \quad &[x_i, x_j] = z^{b_{ij}} \text{ and } [x_i, z] = 1 \text{ for all } i, j = 1, \dots, p. \end{aligned}$$

LEMMA 10.4. *The generators x_1, \dots, x_n, z and relations (10C) comprise a presentation of P .*

PROOF. Let F be the free group on x_1, \dots, x_n, z , and N the smallest normal subgroup of F containing the elements asserted to equal 1 in (10C) ($x_i^p z^{-a_i}$, z^p , $[x_i, x_j] z^{-b_{ij}}$, and $[x_i, z]$). The unique homomorphism $F \rightarrow P$ taking each x_i to x_i and taking z to z then has N in its kernel, so we get a homomorphism

$$\psi : F/N \rightarrow P.$$

Since P is generated by the x_i 's and z , ψ is surjective.

The assertion of the lemma is just that ψ is an isomorphism. To demonstrate that, we show that $|F/N| \leq |P| = p^{n+1}$. Write \hat{x}_i and \hat{z} for the images of the free generators $x_i, z \in F$ in F/N . Set

$$\hat{S} = \{\hat{x}_1^{c_1} \cdots \hat{x}_n^{c_n} \hat{z}^c \mid c_1, \dots, c_n, c \text{ running from } 1 \text{ to } p\}.$$

Now in F/N , we have $\hat{x}_i = \hat{z}^{a_i}$, $\hat{z}^p = 1$, $[\hat{x}_i, \hat{x}_j] = \hat{z}^{b_{ij}}$, and $[\hat{x}_i, \hat{z}] = 1$. The reader should check that this implies that

$$\hat{x}_i \hat{S} \subseteq \hat{S} \text{ and } \hat{z} \hat{S} \subseteq \hat{S} \text{ for all } i = 1, \dots, p.$$

This implies that $\hat{S} = F/N$ by the next lemma; so $|F/N| = |\hat{S}| \leq p^{n+1}$, the inequality immediate from the definition of \hat{S} . \square

LEMMA 10.5. *Suppose that $T \subset G$ and T generates G (as a monoid). Let S be any nonempty subset of G . If $xS \subseteq S$ for every $x \in T$, then $S = G$.*

PROOF. Every $g \in G$ is represented by a product of elements of T . By induction on the length of that product, $gS \subset S$. Thus $GS \subset S$. Fix any $s \in S$. Then S contains $Gs = G$. \square

REMARK. For a finite group there is no difference between generating it as a monoid or as a group. For infinite groups there is a big difference.

The structure of P is thus not determined solely by the bilinear form B (which carries the information about the b_{ij} , but by B together with the a_i 's, which come from the p^{th} power mapping $x \mapsto x^p$).

If we assume that the p^{th} power mapping is trivial, then the structure of P is determined by B alone. This remark has a drawback however: it is of no use for $p = 2$, because a group of exponent 2 is abelian and cannot be extraspecial.

PROPOSITION 10.6. *Let p be an odd prime. Then for every positive integer n there exists a unique extra-special group P of order p^{2n+1} and exponent p , up to isomorphism. This group is usually denoted just p^{1+2n} . Moreover, there are split exact sequences*

$$(10D) \quad \begin{array}{ccccccc} 1 & \longrightarrow & \text{Inn}(p^{1+2n}) & \longrightarrow & \text{Aut}(p^{1+2n}) & \longrightarrow & \text{CSp}(\overline{P}, B) \longrightarrow 1 \\ & & & & & & \\ 1 & \longrightarrow & \text{Inn}(p^{1+2n}) & \longrightarrow & \text{Aut}_0(p^{1+2n}) & \longrightarrow & \text{Sp}(\overline{P}, B) \longrightarrow 1, \end{array}$$

where $\text{Aut}_0(P) := \{\alpha \in \text{Aut}(P) \mid \alpha|_{Z(P)} = \text{id}_{Z(P)}\}$.

PROOF. The central product of n copies of p^{1+2} (called E_{p^3} above) is extraspecial of order p^{1+2n} and exponent p . For any such extraspecial group P , apply the well-known theory of alternating forms to the \mathbf{F}_p -space $\overline{P} = P/Z(P)$ with the nondegenerate alternating bilinear form B . We conclude (e.g., see Artin, *Geometric Algebra*) that \overline{P} is the orthogonal sum of n hyperbolic planes. The preimages of these planes in P are then copies of p^{1+2} and the orthogonality implies that P is their central product.

In view of Lemmas 10.1 and 10.3, we need only prove the surjectivity and splitting of

$$(10E) \quad \text{Aut}(p^{1+2n}) \longrightarrow \text{CSp}(\overline{P}, B).$$

We choose generators x_1, \dots, x_{2n}, z of P , as in Lemma 10.4. Let $\beta \in \text{CSp}(\overline{P}, B)$. Thus there are integers a_{ij} such that for each $i = 1, \dots, 2n$, we have

$$\beta(\overline{x}_i) = \prod_{j=1}^{2n} \overline{x}_j^{a_{ij}}.$$

Moreover, there is an integer c such that $B(\beta(\overline{x}), \beta(\overline{y})) = cB(\overline{x}, \overline{y})$, for all $\overline{x}, \overline{y} \in \overline{P}$. Now define

$$\alpha(z) = z^c, \quad \alpha(x_i) = \prod_{j=1}^{2n} x_j^{a_{ij}}, \quad i, j = 1, \dots, 2n.$$

It is tedious but routine to check that α preserves the defining relations in Lemma 10.4. Note that as P has exponent p , all the a_i may be taken as 0. What needs to be checked is:

- (1) $\alpha(x_i)^p = 1$ for all $i = 1, \dots, p$, and $\alpha(z)^p = 1$;
- (2) $[\alpha(x_i), \alpha(x_j)] = \alpha(z)^{b_{ij}}$ and $[\alpha(x_i), \alpha(z)] = 1$ for all $i, j = 1, \dots, p$.

As a result, by Lemma 10.4, α extends to a homomorphism $\alpha : P \rightarrow P$ which is clearly surjective (β was a bijection). Thus $\alpha \in \text{Aut}(P)$ and α maps to β under (10E). This proves the surjectivity.

As for the splitting, notice that $\text{CSp}(\overline{P}, B)$ has an involution u in its center, namely the scalar mapping -1 (or inversion, in multiplicative notation). Since u inverts $\overline{P} \cong \text{Inn}(P)$, $C_{\text{CSp}(\overline{P}, B)}(u)$ is a complement to $\text{Inn}(P)$ in $\text{Aut}(P)$, proving that the first sequence in (10D) splits. The splitting of the second is left as an exercise. \square

For the case $p = 2$, we cannot avoid nontrivial squares in (10C). Again let $Z(P) = \langle z \rangle$. For any $x \in P$, observe that $(xz)^2 = x^2$ and so the mapping $x \mapsto x^2$ lifts to a mapping

$$Q : \overline{P} \rightarrow Z(P), \quad Q(\overline{x}) = x^2.$$

This mapping is a *quadratic form* over \mathbf{F}_2 .

DEFINITION 10.7. Let V be a vector space over a field \mathbf{F} . A quadratic form on V is a mapping $Q : V \rightarrow \mathbf{F}$ such that

- (a) $Q(cv) = c^2Q(v)$ for all $c \in \mathbf{F}$ and $v \in V$; and
- (b) The binary form $B(v, w) := Q(v + w) - Q(v) - Q(w)$ on V is \mathbf{F} -bilinear.

Since our field is \mathbf{F}_2 , condition (a) is trivial. Condition (b) holds since $(xy)^2 = xyxy = x^2x^{-1}y^2y^{-1}xy = x^2y^2[x, y]$ (note: $y^2 \in Z(P)$). The binary form in (b) is our old friend $B(\bar{x}, \bar{y}) = [x, y]$.

PROPOSITION 10.8. For every positive integer n there exist two extra-special groups P of order 2^{2n+1} , up to isomorphism. The central product of n copies of D_8 is denoted 2_+^{1+2n} and the central product of $n-1$ copies of D_8 and one copy of Q_8 is denoted 2_-^{1+2n} . In each case there is an exact sequence

$$(10F) \quad 1 \longrightarrow \text{Inn}(P) \longrightarrow \text{Aut}(P) \longrightarrow O(\bar{P}, Q) \longrightarrow 1.$$

where $O(\bar{P}, Q)$ is the subgroup of $GL(\bar{P})$ preserving the quadratic form Q .

Previous exercises have shown that every P is isomorphic to either 2_+^{1+2n} or 2_-^{1+2n} . The fact that they are themselves not isomorphic can be shown by counting the number of elements of order 2 in each group, for instance. The proof of the exact sequence is quite similar to that of Proposition 10.6.

In general, the above sequences do *not* split, as shown by R. L. Griess. The orthogonal groups corresponding to the two different Q 's arising from the two different P 's are also distinguished by a \pm sign. Thus, one writes

$$\begin{aligned} 1 &\longrightarrow \text{Inn}(2_+^{1+2n}) \longrightarrow \text{Aut}(2_+^{1+2n}) \longrightarrow O^+(2n, 2) \longrightarrow 1 && \text{and} \\ 1 &\longrightarrow \text{Inn}(2_-^{1+2n}) \longrightarrow \text{Aut}(2_-^{1+2n}) \longrightarrow O^-(2n, 2) \longrightarrow 1 \end{aligned}$$

EXERCISES.

- (10.9) Show that $O^+(2, 2) \cong Z_2$, $O^-(2, 2) \cong S_3$, $O^+(4, 2) \cong S_3 \wr Z_2$, and $O^-(4, 2) \cong S_5$.
- (10.10) Suppose that V is a finite-dimensional vector space over \mathbf{F}_p and the group X acts linearly and absolutely irreducibly on V . Show that up to scalars, there is at most one nonsingular \mathbf{F}_p -bilinear form on V that is preserved by X . If $p = 2$ then show that there is at most one nonsingular quadratic form preserved by X . (Hints. Use Schur's Lemma. Also show that the difference between two quadratic forms with the same associated bilinear form is a linear function.)
- (10.11) Let $G = PSL(V)$ where V is an n -dimensional vector space over \mathbf{F}_p . Let V_1 and V_{n-1} be fixed subspaces of dimension 1 and codimension 1 in V , respectively. Let P_1 and P_{n-1} be the stabilizers in G of V_1 and V_{n-1} , respectively.
 - (1) Establish isomorphisms $F^*(P_1) \cong (V/V_1)^+$ and $P_1/F^*(P_1) \cong GL(V/V_1)$.
 - (2) Prove similar statements about P_{n-1} .
 - (3) Assuming that $V_1 \subseteq V_{n-1}$, show that $F^*(P_1 \cap P_{n-1}) \cong p^{1+2(n-1)}$ if p is odd and $F^*(P_1 \cap P_{n-1}) \cong 2_{\pm}^{1+2(n-1)}$ if $p = 2$, for some choice of the sign (which you have to decide).

- (4) Show that $GL_n(p)$ embeds in $Sp_{2n}(p)$ if p is odd, and in $O_{2n}^\pm(2)$ if $p = 2$, for some choice of the sign.
- (10.12) In the previous exercise, is it true that $P_1 \cong P_{n-1}$? Prove your answer.
- (10.13) Let V be a finite-(even!)-dimensional vector space over \mathbf{F}_p equipped with a nonsingular alternating bilinear form ϕ . Let $G = Sp(V) = Sp(V, \phi)$. Let V_1 be a 1-dimensional subspace of V and $V_{n-1} = V_1^\perp := \{v \in V \mid \phi(v, w) = 0 \text{ for all } w \in V_1\}$. Let P_1 and P_{n-1} be the stabilizers in G of V_1 and V_{n-1} , respectively. Formulate and prove statements analogous to those of the previous exercise, if possible.
- (10.14) Describe how the previous exercises must be altered if the field is not assumed to be the prime field, i.e. if V is a vector space over \mathbf{F}_q for some prime power q .
- (10.15) Suppose that α is an automorphism of the extra-special p -group P . Suppose that α has order r , where r and p are distinct primes. Suppose further that $p^n \equiv 1 \pmod{r}$ for some *odd* integer n . Show that there exists an α -invariant abelian subgroup A of P containing $Z(P)$ and of order p^m for some even integer m .

11. Groups of Characteristic p

DEFINITION 11.1. *Let p be a prime and X a finite group. Then $O_p(X)$ is the largest normal subgroup of X whose order is a power of p . Moreover, X is said to be of characteristic p if and only if any (all) of the following equivalent conditions hold:*

- (a) $F^*(X) = O_p(X)$;
- (b) $C_X(O_p(X)) \leq O_p(X)$;
- (c) $C_X(O_p(X))$ is a p -group.

Note that (a) implies (b) by the F^* -Theorem, and (b) trivially implies (c). If (c) holds, then $E(X) = 1$ and $O_r(X) = 1$ for all primes $r \neq p$, since $E(X)$ and $O_r(X)$ lie in $C_X(O_p(X))$ but are not p -groups unless they are trivial. Thus $F^*(X) = F(X) = O_p(X)$, i.e., (a) follows, and the conditions are indeed equivalent.

In a group X of characteristic p , p' -elements (elements whose order is relatively prime to p) act faithfully on $O_p(X)$. The faithful action carries over to various pieces of $O_p(X)$ as well, in the following senses. In the following properties, X is assumed to be of characteristic p , and we set $Q = O_p(X)$. Thus, $C_X(Q) \leq Q$.

$$(11.2) \quad C_X(Q/\Phi(Q)) = Q.$$

- (11.3) If $1 = Q_0 \leq Q_1 \leq \cdots \leq Q_m = Q$ is a chain of subgroups with $Q_i \triangleleft X$ for each $i = 0, \dots, m$, then

$$\bigcap_{i=1}^m C_X(Q_i/Q_{i-1}) \leq Q.$$

- (11.4) If $R \leq Q$, $R \triangleleft X$, and $C_Q(R) \leq R$, then $C_X(R) \leq Q$.

(11.5) If Q is abelian or if $p > 2$, then $C_X(\Omega_1(Q)) \leq Q$. Here for any p -group P , we use the notation

$$\Omega_1(P) = \langle x \in P \mid x^p = 1 \rangle.$$

Property 11.2 is part of Theorem 5.14, restated. In Property 11.3, the notation by definition means

$$C_X(Q_i/Q_{i-1}) := \{x \in X \mid [x, Q_i] \leq Q_{i-1}\}.$$

We give two different proofs of Property 11.3. In the first, we make a routine reduction. Set $\overline{X} = X/\Phi(Q)$. Thus by Property 11.2, $F^*(\overline{X}) = \overline{Q}$.²⁴ Note that the images $\overline{Q}_0 \leq \overline{Q}_1 \leq \dots \leq \overline{Q}_m$ form a chain of normal subgroups of \overline{X} with $\overline{Q}_m = \overline{Q}$. Furthermore $\overline{Q}_i/\overline{Q}_{i-1} \cong Q_i/Q_{i-1}(Q_i \cap \Phi(Q))$ is a quotient of Q_i/Q_{i-1} , and as a consequence, $\overline{C}_X(Q_i/Q_{i-1}) \leq C_{\overline{X}}(\overline{Q}_i/\overline{Q}_{i-1})$. Therefore if we set $C = \bigcap_{i=1}^m C_X(Q_i/Q_{i-1})$, we conclude that $\overline{C} \leq \bigcap_{i=1}^m C_{\overline{X}}(\overline{Q}_i/\overline{Q}_{i-1})$. If Property 11.3 holds for \overline{X} , then it follows that $\overline{C} \leq \overline{Q}$. But this immediately implies that $C \leq Q$. We have thus reduced the proof to the case of \overline{X} , i.e., to the case that

Q is elementary abelian.

Now suppose that Property 11.3 fails in this case and choose $x \in \bigcap_{i=1}^m C_X(Q_i/Q_{i-1})$ such that the order of x is not a power of p . Replacing x by x^{p^s} for suitable s , we may assume that the order of x is relatively prime to p , but $x \neq 1$. We consider Q as an $F_p[\langle x \rangle]$ -module and apply Maschke's Theorem, which applies as the order of the group $\langle x \rangle$ is relatively prime to the characteristic p . Maschke's Theorem asserts that Q is a completely reducible $F_p[\langle x \rangle]$ -module. Consequently each Q_{i-1} has an x -invariant complement in Q_i , $i = 1, \dots, m$. Since x acts trivially on Q_i/Q_{i-1} , it acts trivially on each of these complements. But Q is the direct product of all these complements so x acts trivially on Q . Therefore $x \in C_X(Q) = Q$, which is absurd as the order of x is relatively prime to p .

This completes the first verification of Property 11.3.

The second verification uses Sylow theory instead. Again assume that the property fails, and choose an element $x \in \bigcap C_X(Q_i/Q_{i-1})$ such that $|x|$ is not a power of p , and subject to this, so that $m + |x|$ is minimal (here $|x|$ is the order of x). As in the first verification, we can replace x by a suitable power of itself and so the minimality implies that $|x|$ is relatively prime to p . Replacing x by a further power of itself, we see by minimality that $|x|$ is a prime $r \neq p$.

Consider the group $Y = Q_{m-1} \langle x \rangle$, of order $p^a \cdot r$ for some a . Of course $Q_{m-1} \triangleleft Y$. If Y is not nilpotent, then $F^*(Y) = Q_{m-1}$, and then Y is a counterexample with a smaller value of $m + |x|$, contrary to our minimal choice. Therefore Y is nilpotent, so x centralizes Q_{m-1} . Therefore the hypotheses are satisfied for the chain $1 = Q_0 \leq Q_{m-1} \leq Q_m = Q$, and so by minimality $m = 2$.

²⁴Here we use the ‘‘bar convention’’: having defined \overline{X} as a certain quotient of X , we define \overline{Y} , for any element Y or subset Y of X , to be the image of Y in \overline{X} , under the natural projection mapping $X \rightarrow \overline{X}$.

This time set $\overline{X} = X/Q_1$. By assumption \overline{x} and \overline{Q} centralize each other. Therefore $\overline{X} = \overline{Q} \times \langle \overline{x} \rangle$. In particular $\langle \overline{x} \rangle \triangleleft \overline{X}$. Returning to X , this means that $Q_1 \langle x \rangle \triangleleft X$. Since $\langle x \rangle$ is a Sylow r -subgroup of X , it is also one of $Q_1 \langle x \rangle$. Now the Frattini Argument (Theorem 5.11) implies that $X = Q_1 \langle x \rangle N_X(\langle x \rangle)$. But $Q_1 \leq C_X(\langle x \rangle) \leq N_X(\langle x \rangle)$ by assumption, and so $X = N_X(\langle x \rangle)$, i.e., $\langle x \rangle \triangleleft X$. But then $X = Q \times \langle x \rangle$ and x centralizes Q , a final contradiction.

Property 11.4 follows quickly as well. Since $R \triangleleft X$, we have $C_X(R) \triangleleft N_X(R) = X$. Therefore $[C_X(R), Q] \leq C_X(R) \cap Q = C_Q(R) \leq R$. It follows that $C_X(R) \leq C_X(R) \cap C_X(Q/R)$. By Property 11.3, $C_X(R) \leq Q$, as desired.

THEOREM 11.6. *Suppose that the group X is of characteristic p . Then for any p -subgroup $P \leq X$, $N_X(P)$ is also of characteristic p .*

... To Be Continued ...