8 Further topics

The main topic in this section is *Aschbacher's Theorem*, which describes the subgroups of the classical groups. First, there are two preliminaries: the *O'Nan–Scott Theorem*, which does a similar job for the symmetric and alternating groups; and the structure of *extraspecial p-groups*, which is an application of some of the earlier material and also comes up unexpectedly in Aschbacher's Theorem.

8.1 Extraspecial p-groups

An *extraspecial p-group* is a p-group (for some prime p) having the property that its centre, derived group, and Frattini subgroup all coincide and have order p. Otherwise said, it is a non-abelian p-group P with a normal subgroup Z such that $|Z| = p$ and P/Z is elementary abelian.

For example, of the five groups of order 8, two (the dihedral and quaternion groups) are extraspecial; the other three are abelian.

Exercise 8.1 Prove that the above conditions are equivalent.

Theorem 8.1 *An extraspecial p-group has order p^m, where m is odd and greater than 1. For any prime p and any odd $m > 1$, there are up to isomorphism exactly two extraspecial p-groups of order p^m.*

Proof We translate the classification of extraspecial p-groups into geometric algebra. First, note that such a group is nilpotent of class 2, and hence satisfies the following identities:

$$[xy,z] = [x,z][y,z], \tag{2}$$
$$(xy)^n = x^n y^n [y,x]^{n(n-1)/2}. \tag{3}$$

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

Exercise 8.2 Prove that these equations hold in any group which is nilpotent of class 2.

Let P be extraspecial with centre Z. Then Z is isomorphic to the additive group of $F = \mathrm{GF}(p)$; we identify Z with F. Also, P/Z, being elementary abelian, is isomorphic to the additive group of a vector space V over F; we identify P/Z with V.

Of course, we have to be prepared to switch between additive and multiplicative notation.

The structure of P is determined by two functions $B : V \times V \to F$ and $Q : V \to F$, defined as follows. Since P/Z is elementary abelian, the commutator of any two elements of P, or the pth power of any element of P, lie in Z. So commutation and pth power are maps from $P \times P$ to F and from P to F. Each is unaffected by changing its argument by an element of Z, since

$$[xz,y] = [x,y] = [x,yz] \text{ and } (xz)^p = x^p$$

for $z \in Z$. So we have induced maps $P/Z \times P/Z \to Z$ and $P/Z \to Z$, which (under the previous identifications) are our required B and Q.

Exercise 8.3 Show that the structure of P can be reconstructed uniquely from the field F, the vector space V, and the maps B and Q above.

Now Equation (2) shows that B is bilinear. Since $[x,x] = 1$ for all x, it is alternating. Elements of its radical lie in the centre of P, which is Z by assumption; so B is nondegenerate. Thus B is a symplectic form.

In particular, $n = \mathrm{rk}(V)$ is even; so $|P| = p^m$ where $m = 1+n$ is odd, proving the first part of the theorem.

Now the analysis splits into two cases, according as $p = 2$ or p is odd.

Case $p = 2$ Now consider the map Q. Since $|Z| = 2$, we have $[y,x] = [x,y]^{-1} = [x,y]$ for all x,y. Now Equation (3) for $n = 2$, in additive notation, asserts that

$$Q(x+y) = Q(x) + Q(y) + B(x,y),$$

In other words, Q is a quadratic form which polarises to B.

Since there are just two inequivalent quadratic forms, there are just two possible groups of each order up to isomorphism.

Case p **odd** The difference is caused by the behaviour of $p(p-1)/2 \bmod p$: for p odd, p divides $p(p-1)/2$. Hence Equation (3) asserts

$$Q(x+y) = Q(x) + Q(y).$$

In other words, Q is linear. Any linear function can be uniquely represented as $Q(x) = B(x,a)$ for some vector $a \in V$. Since the symplectic group has just two

orbits on V, namely $\{0\}$ and the set of all non-zero vectors, there are again just two different groups. Note that the choice $a = 0$ gives a group of exponent p, while $a \neq 0$ gives a group of exponent p^2. ■

Corollary 8.2 *(a) The outer automorphism groups of the extraspecial* 2*-groups of order* 2^{1+2r} *are the orthogonal groups* $\Omega^\varepsilon(2r,2)$*, for* $\varepsilon = \pm 1$.

(b) Let p be odd. The outer automorphism group of the extraspecial p-group of order p^{1+2r} *and exponent p is the* general symplectic group $\mathrm{GSp}(2r,p)$ *consisting of linear maps preserving the symplectic form up to a scalar factor. The automorphism group of the extraspecial p-group of order* p^{1+2r} *and exponent* p^2 *is the stabiliser of a non-zero vector in the general symplectic group.*

Exercise 8.4 (a) Let P_1 and P_2 be groups and θ an isomorphism between central subgroups Z_1 and Z_2 of P_1 and P_2. The *central product* $P_1 \circ P_2$ of P_1 and P_2 with respect to θ is the factor group

$$(P_1 \times P_2)/\{(z^{-1}, z\theta) : z \in Z_1\}.$$

Prove that the central product of extraspecial p-groups is extraspecial, and corresponds to taking the orthogonal direct sum of the corresponding vector spaces with forms.

(b) Hence prove that any extraspecial p-group of order p^{1+2r} is a central product of r extraspecial groups of order p^3 where

- if $p = 2$, all or all but one of the factors is dihedral;
- if p is odd, all or all but one of the factors has exponent p.

We conclude with one more piece of information about extraspecial groups. Let p be extraspecial of order p^{1+2r}. The p elements of the centre lie in conjugacy classes of size 1; all other conjugacy classes have size p, so there are $p^{2r} + p - 1$ conjugacy classes. Hence there are the same number of irreducible characters. But P/P' has order p^{2r}, so there are p^{2r} characters of degree 1. It is easy to see that the remaining $p-1$ characters each have degree p^r; they are distinguished by the values they take on the centre of P.

For $p = 2$, there is only one non-linear character, which is fixed by outer automorphisms of P. Thus the representation of P lifts to the extension $P.\Omega^\varepsilon(2r,2)$.

For $p = 2$, suppose that P has exponent p. The subgroup $\mathrm{Sp}(2r, p)$ of the outer automorphism group acts trivially on the centre, so fixes the $p-1$ non-linear representations; again, these representations lift to $P.\mathrm{Sp}(2r, p)$.

In the case of the last remark, the representation of $P.\mathrm{Sp}(2r, p)$ can be written over $\mathrm{GF}(l)$ (l a prime power) provided that this field contains primitive pth roots of unity, that is, $l \equiv 1 \pmod{p}$. For the corresponding case with $p = 2$, we require primitive 4th roots of unity, that is, $l \equiv 1 \pmod{4}$.

Thus, if these conditions hold, then $\mathrm{GL}(p^r, l)$ contains a subgroup isomorphic to $P.\mathrm{Sp}(2r, p)$ or $P.\Omega^{\varepsilon}(2r, 2)$ (for $p = 2$).

8.2 The O'Nan–Scott Theorem

The O'Nan–Scott Theorem for subgroups of symmetric and alternating groups is a slightly simpler prototype for Aschbacher's Theorem

A group G is called *almost simple* if $S \leq G \leq \mathrm{Aut}(S)$ for some non-abelian finite simple group S.

We define five classes of subgroups of the symmetric group S_n as follows:

$\mathcal{C}_1$	$\{S_k \times S_l : k+l = n, k, l > 1\}$	intransitive
$\mathcal{C}_2$	$\{S_k \wr S_l : kl = n, k, l \geq 2\}$	imprimitive
$\mathcal{C}_3$	$\{S_k \wr S_l : k^l = n, k, l \geq 2\}$	product action
$\mathcal{C}_4$	$\{\mathrm{AGL}(d, p) : p^d = n\}$	affine
$\mathcal{C}_5$	$\{(T^k).(\mathrm{Out}(T) \times S_k) : k \geq 2\}$	diagonal

In the last row of the table, T is a non-abelian simple group, and the group in question has its *diagonal action*: the stabiliser of a point is $\mathrm{Aut}(T) \times S_k = (T_d).(\mathrm{Out}(T) \times S_k)$, where the embedding of T_d in T^k is the diagonal one, as

$$T_d = \{(t, t, \ldots, t) : t \in T\},$$

and the action of $T = T_d$ is by inner automorphisms.

Now we can state the O'Nan–Scott Theorem.

Theorem 8.3 *Let G be a subgroup of S_n or A_n, not equal to S_n or A_n. Then either*

(a) G is contained in a subgroup belonging to one of the classes $\mathcal{C}_i$, $i = 1, \ldots, 5$; or

(b) G is primitive and almost simple.

Note that the action of G in case (b) is not specified.

We sketch a proof of the theorem. If G is intransitive, then it is contained in a maximal intransitive subgroup, which belongs to $\mathcal{C}_1$. If G is transitive but imprimitive, then it is contained in a maximal imprimitive subgroup, which belongs to $\mathcal{C}_2$. So we may suppose that G is primitive.

Let N be the *socle* of G, the product of its minimal normal subgroups. It is well known and easy to prove that a primitive group has at most two minimal normal subgroups; if there are two, then they are abelian. So N is a product of isomorphic simple groups.

Now the steps required to complete the proof are as follows:

- If N is abelian, then it is elementary abelian of order p^d for some prime p, and N is regular, so $n = p^d$. Then $G \leq \mathrm{AGL}(d,p) = p^d : \mathrm{GL}(d,p)$, so G is contained in a group in $\mathcal{C}_4$.

- If N is non-abelian but not simple, then it can be shown that G is contained in a group in $\mathcal{C}_3 \cup \mathcal{C}_5$.

- Of course, if N is simple, then G is almost simple.

In order to understand the maximal subgroups of S_n and A_n, there are two things to do now. The theorem shows that the maximal subgroups are either in the classes $\mathcal{C}_1$–$\mathcal{C}_5$ or almost simple. First, we must resolve the question of which of these groups contains another; this has been done by Liebeck, Praeger and Saxl. Second, we must understand how almost simple groups act as primitive permutation groups; equivalently, we must understand their maximal subgroups (since a primitive action of a group is isomorphic to the action on the right cosets of a maximal subgroup).

According to the Classification of Finite Simple Groups, most of the finite simple groups are classical groups. So this leads us naturally to the question of proving a similar result for classical groups.

8.3 Aschbacher's Theorem

Aschbacher's Theorem is the required result. After a preliminary definition, we give the eight classes of subgroups, and then state the theorem.

A subgroup H of $\mathrm{GL}(n,F)$ is said to be *irreducible* if no subspace of F^n is invariant under H. We say that H is *absolutely irreducible* if, regarding elements

of H as $n \times n$ matrices over F, the group they generate is an irreducible subgroup of $\mathrm{GL}(n,K)$ for any algebraic extension field K of F.

For example, the group

$$\mathrm{SO}(2,\mathbb{R}) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbb{R} \right\}$$

is irreducible but not absolutely irreducible since, if we write it relative to the basis $(e_1 + \mathrm{i}e_2, e_1 - \mathrm{i}e_2)$, the group would be

$$\left\{ \begin{pmatrix} \mathrm{e}^{\mathrm{i}\theta} & 0 \\ 0 & \mathrm{e}^{-\mathrm{i}\theta} \end{pmatrix} \right\}.$$

Now we describe the Aschbacher classes. The examples of groups in these classes will refer particularly to the general linear groups, but the definitions apply to all the classical groups. We let V be the natural module for the classical group G.

$\mathcal{C}_1$ consists of reducible groups, those which stabilise a subspace W of V. In $\mathrm{GL}(V)$, the stabiliser of W consists of matrices which, in block form (the basis of W coming first), have shape

$$\begin{pmatrix} A & O \\ X & B \end{pmatrix},$$

where $A \in \mathrm{GL}(k,F)$, $B \in \mathrm{GL}(l,F)$ (with $k+l=n$), and X an arbitrary $l \times k$ matrix; its structure is $F^{kl} : (\mathrm{GL}(k,F) \times \mathrm{GL}(l,F))$.

Note that, in a classical group with a sesquilinear form B, if the subspace W is fixed, then so is $W \cap W^\perp$. So we may assume that either $W \cap W^\perp = \{0\}$ (so that W is non-degenerate) or $W \leq W^\perp$ (so that W is flat).

$\mathcal{C}_2$ consists of irreducible but imprimitive subgroups, those which preserve a direct sum decomposition

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_t,$$

where $\mathrm{rk}(V_i) = m$ and $n = mt$; elements of the group permute these subspaces among themselves. The stabiliser of the decomposition in $\mathrm{GL}(n,F)$ is $\mathrm{GL}(m,F) \wr S_t$.

$\mathcal{C}_3$ consists of *superfield groups*. That is, a group in this class is a classical group acting on $\mathrm{GF}(q^r)^m$, where $rm = n$, and it is embedded in $\mathrm{GL}(n,q)$ by restricting scalars on the vector space from $\mathrm{GF}(q^r)$ to $\mathrm{GF}(q)$. Elements of the Galois group of $\mathrm{GF}(q^r)$ over $\mathrm{GF}(q)$ are also linear. So in $\mathrm{GL}(n,q)$, a subgroup of this form has shape $\mathrm{GL}(m,q^r):C_r$. For maximality, we may take r to be prime.

In the case of the classical group, we must sometimes modify the form (by taking its trace from $\mathrm{GF}(q^r)$ to $\mathrm{GF}(q)$); this may change the type of the form.

$\mathcal{C}_4$ consists of groups which preserve a tensor product structure $V = F^{n_1} \otimes F^{n_2}$, with $n_1 n_2 = n$. The appropriate subgroup of $\mathrm{GL}(n,F)$ is the central product $\mathrm{GL}(n_1,F) \circ \mathrm{GL}(n_2,F)$. We can visualise this example most easily by taking V to be the vector space of all $n_1 \times n_2$ matrices, and letting the pair $(A,B) \in \mathrm{GL}(n_1,F) \times \mathrm{GL}(n_2,F)$ act by the rule

$$(A,B) : X \mapsto A^{-1}XB.$$

The kernel of the action is the appropriate subgroup which has to be factored out to form the central product.

$\mathcal{C}_5$ consists of *subfield groups*, that is, subgroups obtained by restricting the matrix entries to a subfield $\mathrm{GF}(q_0)$ of $\mathrm{GF}(q)$, where $q = q_0^r$ (and we may take r to be prime).

$\mathcal{C}_6$ consists of groups with extraspecial normal subgroups. We saw in the section on extraspecial groups that the group $P.\mathrm{Sp}(2r,p)$ or (if $p = 2$) $P.\Omega^\varepsilon(2r,2)$ can be embedded in $\mathrm{GL}(p^r,l)$ if p (or 4) divides $l-1$. These, together with the scalars in $\mathrm{GF}(l)$, form the groups in this class.

$\mathcal{C}_7$ consists of groups preserving tensor decompositions of the form

$$V = V_1 \otimes V_2 \otimes \cdots \otimes V_t,$$

with $\mathrm{rk}(V_i) = m$ and $n = m^t$. These are somewhat difficult to visualise!

$\mathcal{C}_8$ consists of classical subgroups. Thus, any classical group acting on F^n can occur here as a subgroup of $\mathrm{GL}(n,F)$ provided that it is not obviously non-maximal (e.g. we exclude $\Omega^\varepsilon(2r,q)$ for q even, since these groups are contained in $\mathrm{Sp}(2r,q)$. However, these groups would occur as class $\mathcal{C}_8$ subgroups of the symplectic group.

Now some notation for Aschbacher's Theorem. We let $X(q)$ denote a classical group over $\mathrm{GF}(q)$, and $V = \mathrm{GF}(q)^n$ its natural module. Also, $\Omega(q)$ is the normal subgroup of $X(q)$ such that $\Omega(q)$ modulo scalars is simple; and $A(q)$ is the normaliser of $X(q)$ in the group of all invertible semilinear transformations of $\mathrm{GF}(q)^n$. A bar over the name of a group denotes that we have factored out scalars. Note that $\overline{A}(q)$ is the automorphism group of $\overline{\Omega}(q)$ except in the cases $X(q) = \mathrm{GL}(n,q)$ (where there is an outer automorphism induced by duality), $X(q) = O^+(8,q)$ (where there is an outer automorphism induced by triality), and $X(q) = \mathrm{Sp}(4,q)$ with q even (where there is an outer automorphism induced by the exceptional duality of the polar space).

Theorem 8.4 *With the above notation, let $\Omega(q) \leq G \leq A(q)$, and suppose that H is a subgroup of G not containing $\Omega(q)$. Then either*

(a) H is contained in a subgroup in one of the classes $\mathcal{C}_1, \ldots, \mathcal{C}_8$; or

(b) H is absolutely irreducible and almost simple modulo scalars.

Kleidman and Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Mathematical Society Lecture Note Series **129**, Cambridge University Press, 1990, gives further details, including an investigation of which of the groups in the Aschbacher classes are actually maximal.