Chapter 2

Linear groups

2.1 Finite fields

All the classical groups are defined in terms of groups of matrices over fields, so before we can define the finite classical groups we need to know what the finite fields are. A *field* is a set F with operations of addition, subtraction, multiplication and division satisfying the usual rules. That is, F has an element 0 such that $(F,+,-,0)$ is an abelian group, and $F \setminus \{0\}$ contains an element 1 such that $(F \setminus \{0\}, ., /, 1)$ is an abelian group, and $x(y+z) = xy + xz$. It is an easy exercise to show that the subfield F_0 generated by the element 1 in a finite field F is isomorphic to the integers modulo p, for some p, and therefore p is prime (called the *characteristic* of the field). Moreover, F is a vector space over F_0, as the vector space axioms are special cases of the field axioms. As every finite-dimensional vector space has a basis of n vectors, $v_1, \ldots, v_n$, say, and every vector has a unique expression $\sum_{i=1}^{n} a_i v_i$ with $a_i \in F_0$, it follows that the field F has p^n elements.

Conversely, for every prime p and every positive integer d there is a field of order p^d, which is unique up to isomorphism. [See below.]

The most important fact about finite fields which we need is that the multiplicative group of all non-zero elements is cyclic. For the polynomial ring $F[x]$ over any field F is a Euclidean domain and therefore a unique factorization domain. In particular a polynomial of degree n has at most n roots. If the multiplicative group $F^\times$ of a field of order q has exponent e strictly less than $q-1$, then $x^e - 1$ has $q-1$ roots, which is a contradiction. Therefore the exponent of $F^\times$ is $q-1$, so $F^\times$ contains elements of order $q-1$, since it is abelian, and therefore it is cyclic.

Note also that all elements x of F satisfy $x^q = x$, and so the polynomial $x^q - x$ factorizes in $F[x]$ as $\prod_{\alpha \in F}(x-\alpha)$. Moreover, the number of solutions to $x^n = 1$ in F is the greatest common divisor $(n, q-1)$ of n and $q-1$. A useful consequence of this for the field of order q^2 is that for every $\mu \in \mathbb{F}_q$ there are exactly $q+1$

elements $\lambda \in \mathbb{F}_{q^2}$ satisfying $\lambda\overline{\lambda} = \lambda^{1+q} = \mu$, where $\overline{\lambda} = \lambda^q$.

We now show that fields of order p^d exist and are unique up to isomorphism. Observe that if f is an irreducible polynomial of degree d over the field $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ of order p, then $\mathbb{F}_p[x]/(f)$ is a field of order p^d. Conversely, if F is a field of order p^d, let x be a generator for $F^\times$, so that the minimum polynomial for x over $\mathbb{F}_p$ is an irreducible polynomial f of degree d, and $F \cong \mathbb{F}_p[x]/(f)$. One way to see that such a field exists is to observe that any field of order $q = p^d$ is a splitting field for the polynomial $x^q - x$. Splitting fields always exist, by adjoining roots one at a time until the polynomial factorises into linear factors. But then the set of roots of $x^q - x$ is closed under addition and multiplication, since if $x^q = x$ and $y^q = y$ then $(xy)^q = x^q y^q = xy$ and $(x + y)^q = x^q + y^q = x + y$. Hence this set of roots is a subfield of order q, as required.

To show that the field of order $q = p^d$ does not depend on the particular irreducible polynomial we choose, suppose that f_1 and f_2 are two such, and $F_i = \mathbb{F}_p[x]/(f_i)$. Since $f_2(t)$ divides $t^q - t$, and $t^q - t$ factorizes into linear factors over F_1, it follows that F_1 contains an element y with $f_2(y) = 0$. Hence the map $x \mapsto y$ extends to a field homomorphism from F_2 to a subfield of F_1. Moreover, the kernel is trivial, since fields have no quotient fields, so this map is a field isomorphism, since the fields are finite.

If also $f_1 = f_2$ then any automorphism of $F = F_1 = F_2$ has this form, so is defined by the image of x, which must be one of the d roots of f_1. Hence the group of automorphisms of F has order d. On the other hand, the map $y \mapsto y^p$ (for all $y \in F$) is an automorphism of F, and has order d. Hence $\mathrm{Aut}(F)$ is cyclic of order d.

2.2 General linear groups

Let V be a vector space of dimension n over the finite field $\mathbb{F}_q$ of order q. The *general linear group* $\mathrm{GL}(V)$ is the set of invertible linear maps from V to itself. Without much loss of generality, we may take V as the vector space $\mathbb{F}_q^n$ of n-tuples of elements of $\mathbb{F}_q$, and identify $\mathrm{GL}(V)$ with the group (denoted $\mathrm{GL}_n(q)$) of invertible $n \times n$ matrices over $\mathbb{F}_q$.

There are certain obvious normal subgroups of $G = \mathrm{GL}_n(q)$. For example, the centre, Z say, consists of all the scalar matrices λI_n, where $0 \neq \lambda \in \mathbb{F}_q$ and I_n is the $n \times n$ identity matrix. Thus Z is a cyclic normal subgroup of order $q-1$. The quotient G/Z is called the *projective general linear group*, and denoted $\mathrm{PGL}_n(q)$.

Also, since $\det(AB) = \det(A)\det(B)$, the determinant map is a group homomorphism from $\mathrm{GL}_n(q)$ onto the multiplicative group of the field, so its kernel is a normal subgroup of index $q - 1$. This kernel is called the *special linear group* $\mathrm{SL}_n(q)$, and consists of all the matrices of determinant 1. Similarly, we can quotient $\mathrm{SL}_n(q)$ by the subgroup of scalars it contains, to obtain the *projective special linear group* $\mathrm{PSL}_n(q)$, sometimes abbreviated to $\mathrm{L}_n(q)$. [The alert reader will have noticed that as defined here, $\mathrm{PSL}_n(q)$ is not a necessarily a subgroup of $\mathrm{PGL}_n(q)$. However, there is an obvious isomorphism between $\mathrm{PSL}_n(q)$ and a normal subgroup of $\mathrm{PGL}_n(q)$, so we shall ignore the subtle distinction.]

2.3 The orders of the linear groups

Now an invertible matrix takes a basis to a basis, and is determined by the image of an ordered basis. The only condition on this image is that the ith vector is linearly independent of the previous ones—but these span a space of dimension $i-1$, which has q^{i-1} vectors in it, so the order of $\mathrm{GL}_n(q)$ is

$$\begin{aligned}|\mathrm{GL}_n(q)| &= (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})\\ &= q^{n(n-1)/2}(q-1)(q^2-1)\cdots(q^n-1). \qquad (2.1)\end{aligned}$$

The orders of $\mathrm{SL}_n(q)$ and $\mathrm{PGL}_n(q)$ are equal, being $|\mathrm{GL}_n(q)|$ divided by $q-1$. To obtain the order of $\mathrm{PSL}_n(q)$, we need to know which scalars λI_n have determinant 1. But $\det(\lambda I_n)=\lambda^n$, and the number of solutions to $x^n=1$ in the field $\mathbb{F}_q$ is the greatest common divisor $(n,q-1)$ of n and $q-1$. Thus the order of $\mathrm{PSL}_n(q)$ is

$$|\mathrm{PSL}_n(q)| = \frac{1}{(n,q-1)}q^{n(n-1)/2}\prod_{i=2}^{n}(q^i-1). \qquad (2.2)$$

The groups $\mathrm{PSL}_n(q)$ are all simple except for the small cases $\mathrm{PSL}_2(2)\cong S_3$ and $\mathrm{PSL}_2(3)\cong A_4$. We shall prove the simplicity of these groups below. First we note that these exceptions are genuine. For $\mathrm{PSL}_2(2)\cong \mathrm{GL}_2(2)$, and $\mathrm{GL}_2(2)$ permutes the three non-zero vectors of $\mathbb{F}_2^2$; moreover, any two of these vectors form a basis for the space, so the action of $\mathrm{GL}_2(2)$ is 2-transitive, and faithful, so $\mathrm{GL}_2(2)\cong S_3$.

Similarly, $\mathrm{GL}_2(3)$ permutes the four 1-dimensional subspaces of $\mathbb{F}_3^2$, spanned by the vectors $(1,0)$, $(0,1)$, $(1,1)$ and $(1,-1)$. The action is 2-transitive since the group acts transitively on ordered bases. Moreover, fixing the standard basis, up to scalars, the matrix $\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ interchanges the other two 1-spaces, so the action of $\mathrm{GL}_2(3)$ is S_4. The kernel of the action is just the group of scalar matrices, and the matrices of determinant 1 act as even permutations, so $\mathrm{PSL}_2(3)\cong A_4$.

We use the term *linear group* loosely to refer to any of the groups $\mathrm{GL}_n(q)$, $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$ or $\mathrm{PSL}_n(q)$.

2.4 Simplicity of $\mathrm{PSL}_n(q)$

The key to proving simplicity of the finite classical groups is Iwasawa's Lemma:

Theorem 1. *If G is a finite perfect group, acting faithfully and primitively on a set Ω, such that the point stabilizer H has a normal abelian subgroup A whose conjugates generate G, then G is simple.*

Proof. For otherwise, there is a normal subgroup K with $1 < K < G$, which does not fix all the points of Ω, so we may choose a point stabilizer H with $K \not\leq H$, and therefore $G = HK$ since H is a maximal subgroup of G. So any $g \in G$ can be written $g = hk$ with $h \in H$ and $k \in K$, and therefore every conjugate of A is of the form $g^{-1}Ag = k^{-1}h^{-1}Ahk = k^{-1}Ak \leq AK$. Therefore $G = AK$ and $G/K = AK/K \cong A/A \cap K$ is abelian, contradicting the assumption that G is perfect. □

For $n \geq 2$ we let $\mathrm{SL}_n(q)$ act on the set Ω of 1-dimensional subspaces of $\mathbb{F}_q^n$, so that the kernel of the action is just the set of scalar matrices, and we obtain an action of $\mathrm{PSL}_n(q)$ on Ω. Moreover, this action is 2-transitive, and therefore primitive.

To study the stabiliser of a point, we might as well take this point to be the 1-space $\langle(1, 0, \ldots, 0)\rangle$. The stabiliser then consists of all matrices whose first row is $(\lambda, 0, \ldots, 0)$. It is easy to check that the subgroup of matrices of the shape $\begin{pmatrix} 1 & 0_{n-1} \\ v_{n-1} & I_{n-1} \end{pmatrix}$, where v_{n-1} is an arbitrary column vector of length $n-1$, is a normal abelian subgroup A. Moreover, all non-trivial elements of A are *transvections*, that is, matrices (or linear maps) t such that $t - I_n$ has rank 1 and $(t - I_n)^2 = 0$. By suitable choice of basis (but remember that the base change matrix must have determinant 1) it is easy to see that every transvection is contained in some conjugate of A.

We have two more things to verify: first, that $\mathrm{SL}_n(q)$ is generated by transvections, and second, that $\mathrm{SL}_n(q)$ is perfect, except for the cases $\mathrm{SL}_2(2)$ and $\mathrm{SL}_2(3)$. The first fact is a restatement of the elementary result that every matrix of determinant 1 can be reduced to the identity matrix by a finite sequence of elementary row operations of the form $r_i \mapsto r_i + \lambda r_j$. To prove the second it suffices to verify that every transvection is a commutator of elements of $\mathrm{SL}_n(q)$. An easy calculation shows that the commutator

$$\left[\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & x & 1 \end{pmatrix}\right] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -x & 0 & 1 \end{pmatrix}, \tag{2.3}$$

so by suitable choice of basis we see that if $n > 2$ then every transvection is a commutator in $\mathrm{SL}_n(q)$. If $n = 2$ and $q > 3$, then $\mathbb{F}_q$ contains a non-zero element x with $x^2 \neq 1$, and then the commutator

$$\left[\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}, \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}\right] = \begin{pmatrix} 1 & 0 \\ y(x^2-1) & 1 \end{pmatrix}, \tag{2.4}$$

which is an arbitrary element of A.

We can now apply Iwasawa's Lemma, and deduce that $\mathrm{PSL}_n(q)$ is simple provided $n > 2$ or $q > 3$.

2.5 Some subgroups of the linear groups

Here we introduce some of the more important subgroups of the linear groups, including the subgroups B, N, T and W, and the parabolic subgroups. We use this notation and terminology since it is standard in the theory of groups of Lie type. A fuller discussion of the subgroup structure, incorporating Aschbacher's theorem on maximal subgroups, will be found later, in Section 2.7. We work in $\mathrm{GL}_n(q)$ for simplicity, but it is easy to modify the constructions for $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$ and $\mathrm{PSL}_n(q)$.

The subgroup B of $\mathrm{GL}_n(q)$ consisting of all lower-triangular matrices is the *Borel subgroup*, and N is the subgroup of all *monomial* matrices, i.e. matrices with exactly one non-zero entry in each row and column. Then $T = B \cap N$, called the *maximal split torus*, consists of the diagonal matrices, which form a normal subgroup of N. (Indeed, N is the normalizer of T, except when $q = 2$, in which case T is trivial.) The quotient group $W = N/T$ is called the *Weyl group*. It is clear that the torus T is isomorphic to the direct product of n copies of the cyclic group C_{q-1} (or $n-1$ copies in $\mathrm{SL}_n(q)$), and that the Weyl group is isomorphic to the symmetric group S_n of all coordinate permutations.

The subgroup U of all lower unitriangular matrices (i.e. matrices having all diagonal entries 1, and all above-diagonal entries 0) is easily seen to be a group of order $q^{n(n-1)/2}$, so it is a Sylow p-subgroup of $\mathrm{GL}_n(q)$, where p is the characteristic of $\mathbb{F}_q$. Moreover, B is the semidirect product of U with T, the group of diagonal matrices, so B has order $q^{n(n-1)/2}(q-1)^n$. This group B may also be defined as the stabilizer of the chain of subspaces

$$0 = V_0 < V_1 < V_2 < \cdots < V_n = V \tag{2.5}$$

defined by $V_i = \{(x_1, \ldots, x_i, 0, \ldots, 0)\}$, so that $\dim(V_i) = i$. A chain of subspaces ordered by inclusion is called a *flag*, and if such a chain has a subspace of each possible dimension it is called a *maximal flag*. Thus B is the stabilizer of a maximal flag.

The *parabolic subgroups* are the stabilizers of flags, and the maximal parabolic subgroups are the stabilizers of minimal flags $0 < W < V$, i.e. the stabilizers of subspaces W. If W has dimension k, say, we may choose a basis $\{e_1, \ldots, e_k\}$ for W and extend it to a basis $\{e_1, \ldots, e_n\}$ for V. Then the matrices for elements of the subspace stabilizer have the shape $\begin{pmatrix} A & 0 \\ C & D \end{pmatrix}$, where A and D are non-singular $k \times k$ and $(n-k) \times (n-k)$ matrices and C is an arbitrary $k \times (n-k)$

matrix. The subset U of matrices of the shape $\begin{pmatrix} I_k & 0 \\ C & I_{n-k} \end{pmatrix}$ is easily checked to be an elementary abelian normal subgroup of order $q^{k(n-k)}$. (An abelian group is called *elementary* if it is a direct product of cyclic groups of order p, for some fixed prime p.) The subset L of matrices of the shape $\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}$ is a subgroup isomorphic to $\mathrm{GL}_k(q) \times \mathrm{GL}_{n-k}(q)$. Moreover, $L \cap U = 1$ and LU is the full stabilizer of W, so this has the structure of a semidirect product $U{:}L$. In the language of Lie theory, U is the *unipotent radical* and L is a *Levi complement* . We leave it as an exercise to show that the maximal parabolic subgroups are indeed maximal subgroups.

2.6 Some more subgroups

For each family of classical groups we aim eventually to prove a theorem analogous to the O'Nan–Scott theorem for the alternating and symmetric groups. Just as in that case we had to construct various subgroups as stabilizers of certain structures on the underlying set, so here we have various structures on the underlying vector space V.

We have already seen the stabilizers in $\mathrm{GL}_n(q)$ of subspaces (also known as the maximal parabolic subgroups): if the subspace has dimension k, then the stabilizer is a group of shape $q^{km}{:}(\mathrm{GL}_k(q) \times \mathrm{GL}_m(q))$, where $k + m = n = \dim V$. These are analogous to the intransitive subgroups of S_n.

Corresponding to the imprimitive subgroups of S_n we have the stabilizers of direct sum decompositions of the space. Thus if $V = V_1 \oplus V_2 \oplus \cdots \oplus V_m$, with $\dim V_i = k$, then we have a group $\mathrm{GL}_k(q) \wr S_m$ stabilizing this decomposition. These groups are also called *imprimitive* linear groups.

There are a number of other types of subgroups which we shall construct later, namely tensor product subgroups (somewhat analogous to the primitive wreath products), subgroups of extraspecial type (somewhat analogous to the affine groups), and various types of almost simple subgroups. See Section 2.7.

2.7 Maximal subgroups of linear groups

We wish to classify maximal subgroups of classical groups along the lines of the O'Nan–Scott theorem for symmetric and alternating groups. For classical groups over $\mathbb{C}$, such a result was obtained by Dynkin in 1952. The first part of his argument works also for finite fields, and a more detailed version of the theorem in the finite case was published by Aschbacher in 1984. Nevertheless, Aschbacher's Theorem falls far short of the degree of explicitness of the O'Nan–Scott Theorem. It was not until 1990 that Kleidman and Liebeck provided (for all classical groups) the level of detail which is required to write doen explicit lists of maximal subgroups in particular cases.

First we describe the types of subgroups which arise in this classification. The maximal reducible subgroups are obviously the stabilizers of subspaces, and if there is a form on the space we may assume the subspace is either non-singular or totally isotropic. Any imprimitive subgroup preserves a decomposition of the space as a direct sum of subspaces of the same dimension. If there is a form then either the subspaces are non-singular or there are precisely two of them. The other groups either arise from tensor products or extraspecial groups, or are almost simple (modulo scalars).

2.8 Tensor products

We first need to define the concept of a *tensor product* of vector spaces. If U is a vector space with basis $\{u_1,\ldots,u_k\}$ and W is a vector space with basis $\{w_1,\ldots,w_m\}$, over the same field F, we define the *tensor product space* $V = U\otimes W$ to be the vector space of dimension $n = km$ with basis $\{v_1,\ldots,v_{km}\}$, where we write $v_{i+kj} = u_i\otimes w_j$ to exhibit the connection with U and W. If A is a $k\times k$ matrix acting on U, and B is an $m\times m$ matrix acting on W, then we get an action on $U\otimes W$ by sending $u_i\otimes w_j$ to $u_iA\otimes w_jB$, interpreted as

$$u_iA\otimes w_jB = \sum_{r=1}^{k}\sum_{s=1}^{m} a_{ir}b_{js}(u_r\otimes w_s).$$

The corresponding $n\times n$ matrix with entries $a_{ir}b_{js}$ (with rows indexed by $i+kj$ and columns indexed by $r+ks$) is called the *Kronecker product* of A and B, and written $A\otimes B$.

If we take all possibilities for A and B, we get an action of $\mathrm{GL}_k(q)\times\mathrm{GL}_m(q)$ on $U\otimes W$. However, this is not a faithful action. For the scalar matrices in both $\mathrm{GL}_k(q)$ and $\mathrm{GL}_m(q)$ act as scalars on $U\otimes W$ (more precisely, $(\lambda I_k)\otimes I_m = \lambda I_{km} = I_k\otimes(\lambda I_m)$), so that the kernel of the action consists of the elements $(\lambda I_k, \lambda^{-1}I_m)$ of $\mathrm{GL}_k(q)\times\mathrm{GL}_m(q)$. The quotient of $\mathrm{GL}_k(q)\times\mathrm{GL}_m(q)$ by this kernel of order $q-1$ is an example of a central product. In general a *central product* $G\circ H$ of two groups G and H is a quotient of $G\times H$ by a subgroup of the centre. Usually the subgroup we quotient by is, as in this case, a diagonal subgroup of $Z(G)\times Z(H)$.

Thus we have $\mathrm{GL}_k(q)\circ\mathrm{GL}_m(q)$ as a subgroup of $\mathrm{GL}_{km}(q)$. In this case it is clearer to work modulo scalars, in the sense that $\mathrm{PGL}_k(q)\times\mathrm{PGL}_m(q) < \mathrm{PGL}_{km}(q)$. This subgroup is usually maximal, unless $k = m$ in which case we can identify U with W, and there is a map taking $u_i\otimes u_j$ to $u_j\otimes u_i$ which acts on $U\otimes U$ and extends the group to $\mathrm{PGL}_k(q)\wr S_2$.

Since we can take the tensor product of two spaces, we can take the tensor product of several, say $V = V_1\otimes V_2\otimes\cdots\otimes V_m$. If all the V_i are isomorphic, say

$\dim V = k$, then $n = \dim V = k^m$, and we have an embedding of $\mathrm{PGL}_k(q) \wr S_m$ in $\mathrm{PGL}_n(q)$. These groups correspond to the primitive wreath products in the symmetric groups.

2.9 Extraspecial groups

A p-group G is called *special* if $Z(G) = G' = \Phi(G)$, and is called *extraspecial* if also $|Z(G)| = p$. For any group G, the commutator map from $G/Z(G) \times G/Z(G)$ to G' satisfies $[h, g] = [g, h]^{-1}$, and if G is special then $G/Z(G) = G/\Phi(G)$ is a vector space over $\mathbb{F}_p$. Moreover, in this case $[g, hk] = [g, k][g, h]^k = [g, h][g, k]$, so if G is extraspecial then this commutator map is a skew-symmetric bilinear form (written multiplicatively). Indeed, it is alternating since $[g, g] = 1$. Moreover, by the assumption $Z(G) = \Phi(G)$, no non-zero vector in $G/\Phi(G)$ is central, so for every $g \notin \Phi(G)$ there is an $h \in G$ with $[g, h] \neq 1$, so this alternating bilinear form is non-singular.

For every g in an extraspecial p-group G, we have that $g^p \in Z(G)$, and therefore

$$\begin{aligned}(gh)^p &= g^p[h^{-1}, g^{-1}]^{g^{p-1}}[h^{-2}, g^{-1}]^{g^{p-2}} \cdots [h^{-p+1}, g^{-1}]h^p \\ &= g^p h^p [g, h]^{-1} \cdots [g, h]^{-p+1} \\ &= g^p h^p [h, g]^{p(p-1)/2}. \qquad (2.6)\end{aligned}$$

Now if $p = 2$ this reduces to $(gh)^2 = g^2h^2[h, g]$, which is just the multiplicative version of the definition of a quadratic form, so the squaring map $G/Z(G) \to Z(G)$ is a quadratic form. On the other hand if p is odd it reduces to $(gh)^p = g^p h^p$, so either all elements have order p, or the elements of order 1 or p form a characteristic subgroup of index p.

Our classification of non-singular (quadratic or alternating bilinear) forms in the next lecture implies that there are exactly two isomorphism types of extraspecial p-groups of each order. We write 2_ε^{1+2m} for the extraspecial group of order 2^{1+2m} whose associated quadratic form is of type ε. For p odd we write p_+^{1+2m} for the extraspecial group of exponent p, and p_-^{1+2m} for the one of exponent p^2.

It is easy to see that $D_8 \cong 2_+^{1+2}$ and $Q_8 \cong 2_-^{1+2}$. Taking central products of these in such a way that all the central involutions are identified gives us constructions of $2_+^{1+2m} = D_8 \circ \cdots \circ D_8$ and $2_-^{1+2m} = D_8 \circ \cdots \circ D_8 \circ Q_8$. The 2-dimensional representations of D_8 and Q_8 (which exist over any field of odd characteristic) can therefore be tensored together to get representations of 2_ε^{1+2m} of dimension 2^m.

Similarly for p odd we obtain a p-dimensional representation of p_+^{1+2} by taking an element cycling the p coordinates, and a diagonal element $\mathrm{diag}(1, \alpha, \ldots, \alpha^{p-1})$, where α is an element of order p in the field. (This can be modified for p_-^{1+2} by multiplying the diagonal element by a pth root of α, if one exists, but we shall not be using this case.) A representation of degree p^m of p_+^{1+2m} is then obtained by tensoring together m copies of these matrices. (Note that in this case we need elements of order p in the field, since there are scalars of order p. In other words, the order of the field is congruent to 1 modulo p.)

What has all this got to do with maximal subgroups of classical groups? A faithful representation of G of degree n over F is nothing more than an embedding of G into $\mathrm{GL}_n(F)$. Thus we have constructed subgroups of $\mathrm{GL}_n(F)$ isomorphic to p_ε^{1+2m}, where $n = p^m$. The subgroups we are after are the normalisers in $\mathrm{GL}_n(F)$ (or in other classical groups) of these extraspecial groups. In the rest of this section we consider in more detail the structure of these normalisers.

These representations extend to representations of $2_\varepsilon^{1+2m}\mathrm{O}_{2m}^\varepsilon(2)$ for $p = 2$, or $p_+^{1+2m}{:}\mathrm{Sp}_{2m}(p)$ for p odd. To see this we need a little representation theory, specifically the fact that the extraspecial group G has a unique representation of degree p^m such that a given generator for its centre acts as a given scalar. It follows that any automorphism of $G \cong p^{1+2m}$ which centralizes the centre $Z(G)$ can be realised inside the general linear group in dimension p^m over any field of order $q \equiv 1 \bmod p$. But every isometry of the form on $G/Z(G)$ lifts to p^{2m} automorphisms of G, so we obtain in this way an extension of G by the isometry group of the form. If p is odd this extension splits since the involution centralizer is $C_p \times \mathrm{Sp}_{2m}(p)$, while if $p = 2$ it is almost always non-split. (A *split extension* $A{:}B$ is the same thing as a semidirect product.) Thus it is a group G with a normal subgroup A and a subgroup B such that $G = AB$ and $A \cap B = 1$. A *non-split extension* $A{}^{\cdot}B$ is a group G with a normal subgroup A and $G/A \cong B$, but with no subgroup B satisfying $G = AB$ and $A \cap B = 1$.) Similarly, if our field F contains 4th roots of 1, i.e. square roots of -1, then there is a representation of $4 \circ 2^{1+2m}$ in 2^m dimensions, and working modulo $\{\pm 1\}$ we get a quadratic form on a space of dimension $2m + 1$ over $\mathbb{F}_2$, with isometry group $\mathrm{O}_{2m+1}(2) \cong \mathrm{Sp}_{2m}(2)$. Thus we get a representation of $4 \circ 2^{1+2m}\mathrm{Sp}_{2m}(2)$ in 2^m dimensions over F.

All these groups of extraspecial type are in $\mathrm{SL}_{p^m}(r)$, where r is a prime congruent to 1 modulo p (or modulo 4, in the last case). In some cases, they also fix forms and so are in smaller classical groups. Thus D_8 fixes a quadratic form (of + type if and only if $r \equiv 1 \bmod 4$) and Q_8 fixes a symplectic form, so 2_+^{1+2m} fixes a quadratic form and 2_-^{1+2m} fixes a symplectic form. Therefore, for r odd and $n \geq 2$, $2_+^{1+2m}\Omega_{2m}^+(2) < \mathrm{SO}_{2^m}^+(r)$ and $2_-^{1+2m}\Omega_{2m}^-(2) < \mathrm{Sp}_{2^m}(r)$. Similarly, p_+^{1+2} fixes a unitary form over $\mathbb{F}_{r^2}$ if and only if p divides $r + 1$, and so the same is true of p_+^{1+2m}. This gives $p_+^{1+2m}{:}\mathrm{Sp}_{2m}(p) < \mathrm{SU}_{p^m}(r)$ provided $p|(r+1)$. Similarly, the groups $4 \circ 2^{1+2m}$ are unitary whenever $4|(r + 1)$.

2.10 The Aschbacher–Dynkin theorem

It is relatively easy to show that every subgroup of $\mathrm{PGL}_n(q)$ which does not contain $\mathrm{PSL}_n(q)$ is either contained in a maximal subgroup of one of the types we have seen above (namely the stabilizers of subspaces, the imprimitive groups, the groups constructed from tensor product decompositions of the underlying vector space, and the groups of extraspecial type) or is of *almost simple type*, which means that its intersection with $\mathrm{PSL}_n(q)$ is almost simple (i.e. a group G with $S \leq G \leq \mathrm{Aut}S$ for some non-abelian simple group G). This is a special case of Aschbacher's theorem, but the proof we sketch is essentially due to Dynkin. The proof requires a little (modular) representation theory but is otherwise elementary.

THEOREM 2. *Any subgroup of* $\mathrm{GL}_n(q)$ *not containing* $\mathrm{SL}_n(q)$ *is contained in one of the following subgroups:*

1. *a reducible group* $q^{km}{:}(\mathrm{GL}_k(q) \times \mathrm{GL}_m(q))$*, the stabilizer of a* k*-space, where* $k + m = n$*;*
2. *an imprimitive group* $\mathrm{GL}_k(q) \wr S_m$*, the stabilizer of a direct sum decomposition, where* $km = n$*;*
3. *a simple tensor product* $\mathrm{GL}_k(q) \circ \mathrm{GL}_m(q)$*, the stabilizer of a tensor product decomposition* $F^k \otimes F^m$*, where* $km = n$ *and* $F = \mathbb{F}_q$*;*
4. *a wreathed tensor product, the preimage of* $\mathrm{PGL}_k(q) \wr S_m$*, the stabilizer of a tensor product decomposition* $F^k \otimes \cdots \otimes F^k$*, where* $k^m = n$*;*
5. *the preimage of* $p^{2k}{:}\mathrm{Sp}_{2k}(p)$*, where* $n = p^k$ *(or* $2^{2k}{\cdot}\mathrm{O}_{2k}^{\varepsilon}(2)$ *if* $p = 2$*);*
6. *the preimage of an almost simple group, acting irreducibly.*

Proof. Given any subgroup H of $G = \mathrm{PGL}_n(q)$ not containing $\mathrm{PSL}_n(q)$, let $\tilde{H}$ denote its preimage in $\tilde{G} = \mathrm{GL}_n(q)$. The *socle* of H, written $\operatorname{soc} H$, is the product of all the minimal normal subgroups of H. Writing $N = \operatorname{soc} H$, we are interested in the representation ρ of $\tilde{N}$ on the underlying n-dimensional vector space V. If ρ is not completely reducible (a representation is *completely reducible* if it is a direct sum of irreducibles), then there is a unique largest subspace W of V such that $\rho|_W$ is completely reducible. Therefore $\tilde{H}$ fixes W (case 1).

If ρ is completely reducible but not homogeneous (a representation is *homogeneous* if it is a direct sum of isomorphic irreducibles) then $\tilde{H}$ preserves the decomposition of V as a direct sum of its homogeneous components, so $\tilde{H}$ is either reducible (case 1 again) or imprimitive (case 2).

If ρ is completely reducible and homogeneous, but not irreducible, then $\tilde{N} \circ C_{\tilde{G}}(\tilde{N})$ acts as a tensor product (case 3). Similarly, if H has more than one minimal normal subgroup, then $\tilde{N}$ acts as a tensor product (case 3 again).

So we have reduced to the case that N is the unique minimal normal subgroup of H. This may be either abelian, in which case it lifts to an extraspecial group (case 5), or non-abelian simple (case 6), or non-abelian non-simple, in which case the representation of $\tilde{N}$ is again a tensor product (case 4). This completes the proof of this easy version of the Aschbacher–Dynkin Theorem. □

It is possible then to look more closely at the subgroups of almost simple type. Some are 'really' written over a smaller field, so are contained in a subgroup $\mathrm{PGL}_n(q_0)$ of $\mathrm{PGL}_n(q)$, where $q = q_0^e$ and e is prime. Some are 'really' of smaller dimension over some extension field, so are contained in a subgroup $\mathrm{P\Gamma L}_{n/k}(q^k)$ for some prime k. Some are other classical groups in their natural representations. And the more one knows about the representations of the quasisimple groups, the more one can extend or refine this list.

Aschbacher's 1984 version of the list of maximal subgroups comprises nine types, as follows:

1. subspace stabilizers,
2. imprimitive wreath products,
3. simple tensors,
4. wreathed tensors,
5. extraspecial type,
6. subfield groups,
7. extension field groups,
8. classical type,
9. other almost simple groups.

There is a version of this theorem for each of the classical groups, in which case more details can be given of many of these subgroups.