Chapter 3

Classical groups

3.1 Bilinear, sesquilinear and quadratic forms

There are a number of useful inner products on real and complex vector spaces, and these inner products give rise to various bilinear, sesquilinear and quadratic forms. The situation is similar for vector spaces over finite fields, although the classification of the forms is rather different. In characteristic 0, the three interesting types of forms are (i) skew-symmetric bilinear, (ii) conjugate-symmetric sesquilinear, and (iii) symmetric bilinear. Over finite fields of odd characteristic we can use the same definitions, using a field automorphism of order 2 in place of complex conjugation (thus the field order must be a square in this case). But in characteristic 2, these definitions do not capture the interesting geometrical (and group-theoretical) phenomena. To remedy this, we replace skew-symmetric bilinear forms by alternating bilinear forms, and symmetric bilinear forms by quadratic forms. In both cases, the two concepts are equivalent if the characteristic of the field is not 2.

3.1.1 Definitions

First, a *bilinear form* on a vector space V over a field F is a map $f : V \times V \to F$ satisfying the laws $f(\lambda u+v, w) = \lambda f(u, w)+f(v, w)$ and $f(u, \lambda v+w) = \lambda f(u, v)+f(u, w)$. It is

$$\begin{array}{rll} \textit{symmetric} & \text{if} & f(u,v) = f(v,u) \\ \textit{skew-symmetric} \text{ or } \textit{anti-symmetric} & \text{if} & f(u,v) = -f(v,u) \\ \text{and } \textit{alternating} & \text{if} & f(v,v) = 0. \end{array} \tag{3.1}$$

Now an alternating bilinear form is always skew-symmetric, since

$$\begin{aligned} 0 &= f(u+v, u+v) \\ &= f(u,u) + f(u,v) + f(v,u) + f(v,v) \\ &= f(u,v) + f(v,u). \end{aligned} \tag{3.2}$$

And if the characteristic is not 2, then a skew-symmetric bilinear form is alternating, since $f(v,v) = -f(v,v)$. But if the characteristic is 2, then a bilinear form can be skew-symmetric without being alternating.

A *quadratic form* is a map Q from V to F satisfying

$$Q(\lambda u + v) = \lambda^2 Q(u) + \lambda f(u,v) + Q(v), \tag{3.3}$$

where f is a symmetric bilinear form. Thus a quadratic form always determines a symmetric bilinear form, called its *associated bilinear form*. And if the characteristic is not 2, the quadratic form can be recovered from the symmetric bilinear form as $Q(v) = \frac{1}{2}f(v,v)$. If the characteristic is 2, then the associated bilinear form is actually alternating, since

$$0 = Q(2v) = Q(v+v) = 2Q(v) + f(v,v) = f(v,v). \tag{3.4}$$

Next we consider conjugate-symmetric sesquilinear forms. For this to make sense we need a field automorphism of order 2, to take the place of complex conjugation for $\mathbb{C}$. Thus we need a field of order q^2, for some $q = p^e$, and we write $\overline{x} = x^q$ for every element x of the field. Then a *conjugate-symmetric sesquilinear form* over a vector space V defined over $F = \mathbb{F}_{q^2}$ is a map $f : V \times V \to F$ satisfying

$$\begin{aligned} f(\lambda u + v, w) &= \overline{\lambda} f(u,w) + f(v,w) \\ \text{and } f(w,v) &= \overline{f(v,w)}. \end{aligned} \tag{3.5}$$

Note that this implies $f(u, \lambda v + w) = \overline{\lambda} f(u,v) + f(u,w)$.

Any of these forms f is determined by its values $f(e_i, e_j)$ on a basis $\{e_1, \ldots, e_n\}$. The matrix A whose (i,j)th entry is $f(e_i, e_j)$ is called the matrix of f (with respect to this ordered basis). It is easy to show that if $g : f_i \mapsto e_i$ is a base-change matrix then the matrix of the form with respect to the new basis $\{f_1, \ldots, f_n\}$ is $g^T A g$.

3.1.2 Vectors and subspaces

Many of the concepts, and much of the notation and nomenclature, are the same whichever type of bilinear or sesquilinear form f we have, although the quadratic forms are more complicated in characteristic 2. For example, we write $u \perp v$ to mean $f(u,v) = 0$ (which is equivalent to $f(v,u) = 0$ in each case), and say that u and v are *perpendicular* or *orthogonal* (with respect to the form f). We write $S^\perp = \{v \in V : v \perp s \text{ for all } s \in S\}$, for any subset S of V (and abbreviate $\{v\}^\perp$ to $v^\perp$). In many contexts $S^\perp$ is called the *orthogonal complement* of S, but I prefer the term *perpendicular space* as being more accurate and less liable to be misunderstood.

A non-zero vector which is perpendicular to itself is called *isotropic*. More generally $f(v, v)$ is called the *norm* of v. (This is not the same as the usual definition over $\mathbb{C}$, where we take the square root of $f(v, v)$. Over finite fields, however, there is no sensible analogue of this square root.) The *radical* of f, written $\mathrm{rad}\, f$, is $V^\perp$, and f is *non-singular* if the radical is 0, and *singular* otherwise. We are usually (but not always) only interested in forms which are non-singular. Similarly, the radical of a quadratic form Q is the subset of vectors v with $Q(v) = 0$ inside the radical of the associated bilinear form.

Given any subspace W of V, we can restrict the form f to W. In general this restriction, written $f|_W$, will be singular, and its radical is $W \cap W^\perp$. If $f|_W$ is non-singular, we say that W is *non-singular*, while if $f|_W$ is zero, we say W is *totally isotropic*. It is a straightforward exercise to show that if f is non-singular, and U is a subspace of V, then $(U^\perp)^\perp = U$ and $\dim(U) + \dim(U^\perp) = \dim(V)$, and hence if $U \cap U^\perp = 0$ then $V = U \oplus U^\perp$.

3.1.3 Isometries and similarities

If f is a form on a vector space V, an *isometry* of f (or of V, if f is understood) is a linear map $g : V \to V$ which preserves the form, in the sense that $f(u^g, v^g) = f(u, v)$ for all $u, v \in V$. Similarly, an isometry of a quadratic form Q is a linear map g such that $Q(v^g) = Q(v)$ for all $v \in V$. We think of an isometry as preserving inner products and norms, and therefore preserving 'distances' and 'angles'. If we allow also changes of scale we obtain *similarities*, that is linear maps g such that $f(u^g, v^g) = \lambda_g f(u, v)$ for a scalar λ_g which depends on g but not on u or v. A similarity of a quadratic form Q is a linear map g such that $Q(v^g) = \lambda_g Q(v)$. Similarities preserve 'angles' but not necessarily 'distances'.

We obtain the finite classical groups from the groups of isometries of non-singular forms. In order to classify these groups, we need to classify the forms, which we do by choosing a basis for the space in such a way that the matrix of the form takes one of a small number of possible shapes. We consider the different types separately. In each case, we say two forms on V are *equivalent* if they become equal after a change of basis.

3.1.4 Classification of alternating bilinear forms

Given an alternating bilinear form on a space V, we want to find a basis of V such that this form looks as nice as possible. Our argument in this section applies to arbitrary fields, finite or infinite, of any characteristic. If there are any vectors u and v with $f(u, v) = \lambda \neq 0$, then choose u and $v' = \lambda^{-1} v$ as the first two basis vectors e_1 and f_1, say. Then with respect to the basis $\{e_1, f_1\}$ the form f satisfies

$$\begin{aligned} f(e_1, e_1) = f(f_1, f_1) &= 0, \\ f(e_1, f_1) = -f(f_1, e_1) &= 1. \end{aligned} \tag{3.6}$$

Now restrict the form to $\{u, v\}^\perp$, and continue. Eventually we have chosen basis vectors $e_1, \ldots, e_m$ and $f_1, \ldots, f_m$, such that $f(u, v) = 0$ for all basis vectors u, v except $f(e_i, f_i) = -f(f_i, e_i) = 1$. Either we have a basis for the whole space, in which case f is non-singular and $\dim(V) = 2m$ is even, or else $f(u, v) = 0$ for all $u, v \in \{e_1, \ldots, f_m\}^\perp \neq 0$, in which case f is singular, and we can complete to a basis in any way we choose. Notice that in the latter case we have that $f(u, v) = 0$ for any $u \in \{e_1, \ldots, f_m\}^\perp$, and any $v \in V$. Usually (but not always) we shall be considering non-singular forms, in which case we have decomposed V as a perpendicular direct sum of m non-singular subspaces $\langle e_i, f_i \rangle$ of dimension 2, called *hyperbolic planes*. The basis $\{e_1, \ldots, f_m\}$ is called a *symplectic basis*.

3.1.5 Classification of sesquilinear forms

To classify conjugate-symmetric sesquilinear forms, we find a canonical basis for the space with the form. Recall that the underlying field is $\mathbb{F}_{q^2}$ which has an automorphism $x \mapsto \overline{x} = x^q$ of order 2. If there is a vector v with $f(v, v) \neq 0$, then $f(v, v) = \overline{f(v, v)}$ so $f(v, v)$ is in the fixed field $\mathbb{F}_q$ of the field automorphism $x \mapsto x^q$. Since the multiplicative group of the field is cyclic order $q^2 - 1 = (q+1)(q-1)$ there is a scalar $\lambda \in \mathbb{F}_{q^2}$ with $\lambda\overline{\lambda} = \lambda^{q+1} = f(v, v)$, so that $v' = \lambda^{-1}v$ satisfies $f(v', v') = 1$. Now restrict f to $v'^\perp$, and carry on. If we find that $f(v, v) = 0$ for all vectors v in the space remaining, then

$$\begin{aligned} 0 &= f(v + \lambda w, v + \lambda w) \\ &= f(v, v) + \overline{\lambda} f(v, w) + \lambda f(w, v) + \lambda\overline{\lambda} f(w, w) \\ &= \overline{\lambda} f(v, w) + \lambda f(w, v). \end{aligned} \tag{3.7}$$

Now we can choose two values of λ, say $\lambda_1 = 1$ and $\lambda_2 \neq \overline{\lambda_2}$, and solve the simultaneous equations to get $f(v, w) = f(w, v) = 0$, so that the form is identically 0. In particular, if the form is non-singular, then we have found an *orthonormal* basis for V, i.e. a basis of mutually perpendicular vectors each of norm 1.

3.1.6 Classification of symmetric bilinear forms

Suppose f is a symmetric bilinear form on a vector space V over a field F of odd characteristic p. We first try to find a nice basis of V. If there are any vectors $u, v \in V$ with $f(u, v) \neq 0$ then there is a vector x (either u, or v or $u + v$) with $f(x, x) \neq 0$. If $f(x, x) = \lambda^2$, then writing $x' = \lambda^{-1}x$ we have $f(x', x') = 1$. Otherwise, we can choose our favourite non-square α in the field and scale so that $f(x', x') = \alpha$. (Here we use the finiteness of the field in an essential way.) Restricting the form now to $x'^\perp$ we continue until we find a perpendicular basis $x_1, \ldots, x_n$ such that for each i, $f(x_i, x_i) = 0, 1$ or α.

But if we have say $f(x_1, x_1) = f(x_2, x_2) = \alpha$, and $f(x_1, x_2) = 0$, then since the squares do not form a field we can choose λ and μ such that $\lambda^2 + \mu^2$ is a

non-square, and by scaling appropriately we can choose $\lambda^2 + \mu^2 = \alpha^{-1}$. Then we find that $x_1' = \lambda x_1 + \mu x_2$ and $x_2' = \mu x_1 - \lambda x_2$ form an orthonormal basis of the 2-space spanned by x_1 and x_2. In this way, we can ensure that our basis is either orthonormal, or the matrix of the form is diagonal with all entries except one being 1.

Thus we have shown that there are exactly two equivalence classes of non-singular symmetric bilinear forms under the action of the general linear group, in the case when F is a finite field of odd characteristic. Note that the finiteness of the field is essential: for example, over $\mathbb{Q}$ there are infinitely many equivalence classes of quadratic forms, even in dimension 1.

3.1.7 Classification of quadratic forms in characteristic 2

First we need to extend some of our earlier definitions. Suppose that Q is a quadratic form on V over a field $F = \mathbb{F}_q$ of characteristic 2, and that f is the associated bilinear form. The *radical of* Q, written $\operatorname{rad} Q$, is the subset of vectors $v \in \operatorname{rad} f$ such that $Q(v) = 0$. This is a subspace since $\operatorname{rad} f$ is a subspace and if $v, w \in \operatorname{rad} Q$ then $Q(v + \lambda w) = Q(v) + \lambda f(v, w) + \lambda^2 Q(w) = 0$. Indeed, if $v, w \in \operatorname{rad} f$ then $Q(v+\lambda w) = Q(v)+\lambda^2 Q(w)$, so Q is a semilinear map on $\operatorname{rad} f$, so $\operatorname{rad} Q$ has codimension 0 or 1 in $\operatorname{rad} f$.

Q is called *non-singular* if $\operatorname{rad} Q = 0$, and *non-degenerate* if $\operatorname{rad} f = 0$. Thus if Q is degenerate but non-singular then $\operatorname{rad} f$ has dimension 1, and $V/\operatorname{rad} f$ supports an alternating bilinear form induced by f. On the other hand, if $v_0 \in \operatorname{rad} f$ has $Q(v_0) = 1$, then $Q(v + \lambda v_0) = Q(v) + \lambda^2 Q(v_0)$, so every coset $v + \langle v_0 \rangle$ contains one vector of each possible norm.

It is not hard to show that every isometry of $V/\operatorname{rad} f$ can be lifted to a unique isometry of V, so the isometry groups of V (with the form Q) and $V/\operatorname{rad} f$ (with the form induced by f) are isomorphic. If we are only interested in the group theory rather than the geometry, therefore, we may, and do, restrict to the cases where $\operatorname{rad} f = 0$, so $\dim V$ is even.

We pick a basis for the space in the same way as for alternating bilinear forms, with the additional condition that we choose our basis vectors to be isotropic (i.e. $Q(v) = 0$) whenever possible. If $Q(e_i) = 0$, then $Q(f_i + \lambda e_i) = Q(f_i) + \lambda$, so replacing f_i by $f_i + Q(f_i)e_i$ we may assume $Q(f_i) = 0$. Moreover, if the dimension is at least 3 then there is always a pair of perpendicular vectors u, v say, and if u is not isotropic then set $\lambda = (Q(v)Q(u)^{-1})^{q/2}$ so that $\lambda^2 = Q(v)Q(u)^{-1}$ and therefore $Q(v + \lambda u) = 0$, so there is always a non-zero isotropic vector. To complete our basis, therefore, we only need to consider separately the case when the dimension is 2.

In this case, we may choose basis vectors v, w with $Q(v) = f(v, w) = 1$, and then for all λ we have $f(v, w + \lambda v) = 1$ and $Q(w + \lambda v) = Q(w) + \lambda^2 + \lambda$. Now for each μ the equation $\lambda^2 + \lambda = \mu$ has at most two solutions, so there are at least $q/2$ distinct values for $\lambda^2 + \lambda$ as λ ranges over $\mathbb{F}_q$. So replacing w by $w + \lambda v$

we see that there are at most two possible quadratic forms, up to equivalence. Indeed, the equation $\lambda^2 + \lambda = 0$ has two solutions $\lambda = 0, 1$, so there are exactly two possible quadratic forms, up to equivalence. This argument also shows that there is a value of μ such that $x^2 + x + \mu = 0$ has no solutions, so $x^2 + x + \mu$ is an irreducible polynomial. Moreover, the two types of quadratic forms are represented by $Q(x, y) = xy$ and $Q(x, y) = x^2 + xy + \mu y^2$ where $x^2 + x + \mu$ is irreducible.

The first of these is called of *plus type*, as there are isotropic vectors, while the second is of *minus type* as there are not. More generally, in $2m$ dimensions, there is one form (called the *plus type*) which has isotropic m-spaces, and another (called the *minus type*) which does not.

3.1.8 Witt's Lemma

A key result which plays an important role in the study of the geometry of these spaces, and hence in the study of the subgroups of the classical groups, is Witt's Lemma (also known as Witt's Theorem). Essentially this says that the isometry groups of nonsingular forms are transitive on subspaces of any given isometry type. We prove here the cases where the forms are alternating bilinear, or conjugate-symmetric sesquilinear, or symmetric bilinear in odd characteristic. More formally:

THEOREM 1. *If (V, f) and (W, g) are isometric spaces, with f and g non-singular, and either alternating bilinear, or conjugate-symmetric sesquilinear, or symmetric bilinear in odd characteristic, then any isometry α between subspaces X of V and Y of W extends to an isometry of V with W.*

Proof. Suppose for a contradiction that Witt's Lemma is false, and pick a counterexample such that $\dim V$ is minimal, and X is as large as possible in V. We divide into two cases, according as X contains a non-trivial non-singular subspace U, or X is totally isotropic. In the first case $V = U \oplus U^\perp$, and the classification of non-singular forms in the previous sections shows that $U^\perp$ and $(U^\alpha)^\perp$ are isometric. Therefore, by induction, the restriction of α to $U^\perp \cap X$ extends to an isometry from $U^\perp$ to $(U^\alpha)^\perp$. Combining this with α on U gives the required isometry between V and W, extending α.

In the second case, pick $0 \neq x \in X$ and a complement Z to $\langle x \rangle$ in X, so that $X = \langle x \rangle \oplus Z$, and pick $x_1 \in Z^\perp \setminus X^\perp$. Scaling x_1 if necessary, we may assume $f(x, x_1) = 1$, and then replacing x_1 by $x_1 + \lambda x$ for suitable λ we may assume x_1 is isotropic. Similarly, $Y = \langle x_1^\alpha \rangle \oplus Z^\alpha$ and we pick an isotropic vector $y_1 \in (Z^\alpha)^\perp \setminus Y^\perp$ with $g(y, y_1) = 1$. Then we extend α to an isometry from $\langle X, x_1 \rangle$ to $\langle Y, y_1 \rangle$ by mapping x_1 to y_1. By induction, this map extends to an isometry from V to W, as required. □

Witt's Lemma for orthogonal groups in characteristic 2 states that if (V, Q) and (W, R) are isometric spaces, where Q and R are non-degenerate quadratic forms, then any isometry between subspaces X of V and Y of W extends to an isometry of V and W. We leave the proof as an exercise.

3.2 Symplectic groups

The *symplectic group* $\mathrm{Sp}_{2m}(q)$ is the isometry group of a non-singular alternating bilinear form f on $V \cong \mathbb{F}_q^{2m}$, i.e. the subgroup of $\mathrm{GL}_{2m}(q)$ consisting of those elements g such that $f(u^g, v^g) = f(u, v)$ for all $u, v \in V$. Recall from Section 3.1.4 that V has a symplectic basis $\{e_1, \ldots, e_m, f_1, \ldots, f_m\}$ such that all basis vectors are perpendicular to each other except that $f(e_i, f_i) = 1$. To calculate the order of the symplectic group, we simply need to count the number of ways of choosing an (ordered) symplectic basis $e_1, \ldots, f_m$. Now e_1 can be any non-zero vector, so can be chosen in $q^{2m} - 1$ ways. Then $e_1^\perp$ has dimension $2m - 1$, so contains q^{2m-1} vectors. Thus there are $q^{2m} - q^{2m-1} = (q-1)q^{2m-1}$ vectors v with $f(u, v) \neq 0$. These come in sets of $q - 1$ scalar multiples, one with each possible value of $f(u, v)$, so there are just q^{2m-1} choices for f_1. Hence by induction the order of $\mathrm{Sp}_{2m}(q)$ is

$$|\mathrm{Sp}_{2m}(q)| \;=\; \prod_{i=1}^{m}(q^{2i}-1)q^{2i-1} = q^{m^2}\prod_{i=1}^{m}(q^{2i}-1). \tag{3.8}$$

3.2.1 Symplectic transvections

Notice that $\mathrm{Sp}_2(q) = \mathrm{SL}_2(q)$. For if we write elements of $\mathrm{Sp}_2(q)$ with respect to a symplectic basis, then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_2(q)$ if and only if $f((a, b), (c, d)) = 1$, that is $ad - bc = 1$. In particular, every element of $\mathrm{Sp}_2(q)$ has determinant 1, and $\mathrm{Sp}_2(q)$ is generated by transvections, which are maps of the form $T_v(\lambda) : x \mapsto x + \lambda f(x, v)v$.

More generally, a *symplectic transvection* is a linear map

$$T_v(\lambda) \;:\; x \mapsto x + \lambda f(x, v)v, \tag{3.9}$$

where f is a fixed alternating bilinear form on the space V, and $v \neq 0$ and $\lambda \neq 0$. We aim to show that the group S generated by symplectic transvections is the whole of $\mathrm{Sp}_{2m}(q)$. As well as feeding in to Iwasawa's Lemma, to prove simplicity of $\mathrm{PSp}_{2m}(q)$, this implies that every element of $\mathrm{Sp}_{2m}(q)$ has determinant 1, so that $\mathrm{Sp}_{2m}(q) \leq \mathrm{SL}_{2m}(q)$. Our method is to prove that S acts transitively on the set of ordered symplectic bases. Since the stabilizer of an ordered basis is (obviously!) trivial, it will then follow immediately that $S = \mathrm{Sp}_{2m}(q)$.

So let v, w be two distinct non-zero vectors. If $f(v, w) = \lambda \neq 0$, then $T_{v-w}(\lambda^{-1}) : v \mapsto w$. Otherwise, pick x such that $f(v, x) \neq 0 \neq f(w, x)$: such an

x exists because if not then by non-singularity there exist y and z with $f(v,y) = f(w,z) = 0$ and $f(v,z) \neq 0$ and $f(w,y) \neq 0$, whence a suitable linear combination of y and z has the required properties. Now we can map v to x and x to w, and deduce that S is transitive on non-zero vectors.

Similarly, suppose u is a fixed vector, and $f(u,v) = f(u,w) = 1$. If $f(v,w) = \lambda \neq 0$, then $T_{v-w}(\lambda^{-1}) : v \mapsto w$ and fixes u. Otherwise, let $x = u + v$, so that $f(u,x) = 1$ and $f(v,x) = f(w,x) = -1$, so we can map v to x and x to w while fixing u. Thus by induction S is transitive on ordered symplectic bases, as required.

Observe that the only scalars in $\mathrm{Sp}_{2m}(q)$ are ± 1, since $f(\lambda u, \lambda v) = \lambda^2 f(u,v)$, which equals $f(u,v)$ only if $\lambda = \pm 1$. The group $\mathrm{PSp}_{2m}(q)$ is defined to be the quotient of $\mathrm{Sp}_{2m}(q)$ by the subgroup (of order 1 or 2) of scalar matrices. It is usually simple, as we are about to see.

3.2.2 Simplicity of $\mathrm{PSp}_{2m}(q)$

We usually disregard the case $m = 1$, because $\mathrm{Sp}_2(q) = \mathrm{SL}_2(q)$, as we saw in Section 3.2.1. The only other non-simple case is $\mathrm{Sp}_4(2) \cong S_6$. To see this isomorphism, let S_6 act on the 6-space $\mathbb{F}_2^6$ over $\mathbb{F}_2$ by permuting the coordinates. The subspace $U = \langle (1,1,1,1,1,1) \rangle$ of dimension 1 is fixed by S_6, as is the subspace W of dimension 5 consisting of vectors $x = (x_1, \ldots, x_6)$ satisfying $\sum_{i=1}^6 x_i = 0$. There is a natural alternating bilinear form on W given by $f(x,y) = \sum_{i=1}^6 x_i y_i$, under which U is the radical of f.

Since $U < W$ we obtain (as in Section 3.1.7) an induced alternating bilinear form on the 4-space W/U and an induced action of S_6 on W/U preserving this form. Therefore there is a homomorphism from S_6 to $\mathrm{Sp}_4(2)$, and the image is certainly bigger than C_2, so the kernel of the homomorphism is trivial, and since the two groups have the same order they are isomorphic.

To prove simplicity of the symplectic groups $\mathrm{PSp}_{2m}(q)$, for all $m > 2$, or $m = 2$ and $q > 2$, we just need to verify the hypotheses of Iwasawa's Lemma. We have already seen in Section 3.2.1 that the group $\mathrm{Sp}_{2m}(q)$ is generated by its symplectic tranvections. In the action of $\mathrm{Sp}_{2m}(q)$ on 1-dimensional subspaces, we proved that the stabilizer of a point is transitive on the q^{2m-1} points which are not orthogonal to the fixed point. It is also transitive on the $(q^{2m-1}-1)/(q-1)-1$ points which are orthogonal but not equal to it: for if v and w are both orthogonal to u, then either $f(v,w) = \lambda \neq 0$, in which case $T_{v-w}(\lambda^{-1}) : v \mapsto w$ while fixing u, or there exists a vector x with $f(v,x) \neq 0 \neq f(w,x)$ and we can map v via x to w while fixing u. Therefore the action is primitive, since the only possibilities for block sizes are now $1 + q^{2m-1}$ and $1 + (q^{2m-1} - 1)/(q-1)$, neither of which divides number of points, $(q^{2m} - 1)/(q-1)$.

It is obvious that the symplectic transvections $T_v(\lambda)$ for a fixed vector v form a normal abelian subgroup of stabiliser of the point $\langle v \rangle$, so the only remaining thing to check is that $\mathrm{Sp}_{2m}(q)$ is perfect. It is enough to check that the symplectic

transvections are commutators. If $q > 3$, this is already true in $\mathrm{Sp}_2(q) \cong \mathrm{SL}_2(q)$, so we only need to check the two cases $\mathrm{Sp}_4(3)$ and $\mathrm{Sp}_6(2)$. This is left as an exercise.

3.2.3 Subgroups of symplectic groups

To construct groups B, N, T, U and W by analogy with the general linear groups, we take B to be the stabilizer of a maximal flag of the shape $0 < W_1 < W_2 < \cdots < W_m = (W_m)^\perp < (W_{m-1})^\perp < \cdots < (W_1)^\perp < V$. We may as well take $W_k = \langle e_1, \ldots, e_k \rangle$, for simplicity, and order the basis $e_1, \ldots, e_m, f_m, \ldots, f_1$ to show the structure of the flag. For all $i < j \leq m$ and all $\lambda \in \mathbb{F}_q$, define the maps $x_{ij}(\lambda)$ and $y_{ij}(\lambda)$ to fix all basis vectors e_k and f_k except

$$\begin{aligned} x_{ij}(\lambda) \;&:\; f_i \mapsto f_i + \lambda f_j \\ &\quad\; e_j \mapsto e_j - \lambda e_i \\ \text{and } y_{ij}(\lambda) \;&:\; f_i \mapsto f_i + \lambda e_j \\ &\quad\; f_j \mapsto f_j + \lambda e_i. \end{aligned} \tag{3.10}$$

We then see that the unitriangular subgroup U is generated by the maps $x_{ij}(\lambda)$ and $y_{ij}(\lambda)$, together with the symplectic transvections $T_{e_i}(-\lambda) : f_i \mapsto f_i + \lambda e_i$, so that U has order q^{m^2} and is a Sylow p-subgroup.

The torus T is generated by diagonal elements $f_i \mapsto \lambda f_i, e_i \mapsto \lambda^{-1} e_i$, so is a direct product of m cyclic groups of order $q-1$, and $B = UT$ as before. The normalizer N of this torus is generated modulo the torus by permutations of the subscripts $1, \ldots, m$, together with the element $e_1 \mapsto f_1 \mapsto -e_1$, and therefore the Weyl group N/T is isomorphic to the wreath product $C_2 \wr S_m$. As before, N is represented by monomial matrices, and the Weyl group is the quotient group of 'allowable' permutations of the coordinate 1-spaces $\langle e_i \rangle$ and $\langle f_i \rangle$.

3.2.4 Subspaces of a symplectic space

Since the stabilizer of any subspace W of V must stabilize $W^\perp$ and $W \cap W^\perp$, we are generally only interested in the cases where $W \cap W^\perp = 0$ or $W \cap W^\perp = W$, so either W is a non-singular subspace, or W is totally isotropic.

The stabilizer of a non-singular subspace of dimension $2k$ preserves the decomposition $V = W \oplus W^\perp$, so is just $\mathrm{Sp}_{2k}(q) \times \mathrm{Sp}_{2m-2k}(q)$. This is usually a maximal subgroup of $\mathrm{Sp}_{2m}(q)$, unless $m = 2k$, in which case there is an element exchanging W and $W^\perp$, and extending the group to $\mathrm{Sp}_{2k}(q) \wr S_2$.

More generally, if $m = kl$ there is a subgroup $\mathrm{Sp}_{2k}(q) \wr S_l$ preserving a decomposition of V as a direct sum of mutually prependicular non-singular spaces of dimension $2k$.

The stabilizer of an isotropic subspace W of dimension k preserves the flag $0 < W < W^\perp < V$, and there is an induced non-singular form on $W^\perp/W$.

By Witt's lemma, we may choose our symplectic basis so that W is spanned by $e_1, \ldots, e_k$, and $W^\perp$ is spanned by $e_1, \ldots, e_m, f_{k+1}, \ldots, f_m$. We therefore see a basis of $W^\perp/W$ consisting of the images of e_{k+1}, ..., e_m, f_{k+1},...,f_m, and a quotient group $\mathrm{Sp}_{2m-2k}(q)$ acting on $W^\perp/W$. We also see a group $\mathrm{GL}_k(q)$ acting on W (and inducing the dual action on $V/W^\perp$), and a p-group of lower triangular matrices generated by elements

$$\begin{aligned} x_{ij}(\lambda) \;&:\; f_i \mapsto f_i + \lambda f_j \\ &\quad\; e_j \mapsto e_j - \lambda e_i \\ \text{and } y_{ij}(\lambda) \;&:\; f_i \mapsto f_i + \lambda e_j \\ &\quad\; f_j \mapsto f_j + \lambda e_i \end{aligned} \tag{3.11}$$

for all $i \le k < j \le m$. It can be shown that these elements generate a non-abelian group Q, such that $Z(Q) = \Phi(Q) = Q'$ is an elementary abelian group of order $q^{k(k+1)/2}$, and Q/Q' is an elementary abelian group of order $q^{2k(m-k)}$. (Here $\Phi(G)$ denotes the *Frattini subgroup*, i.e. the intersection of all the maximal subgroups of G. A p-group with the property that the centre, derived group and Frattini subgroup are equal is called a *special* group. We shall have more to say about them later.) The full stabilizer is therefore a group of shape $q^{k(k+1)/2}.q^{2k(m-k)}{:}(\mathrm{Sp}_{2m-2k}(q) \times \mathrm{GL}_k(q))$. In the case when $k = m$, the corresponding group has shape $q^{m(m+1)/2}{:}\mathrm{GL}_m(q)$. These stabilizers are the *maximal parabolic subgroups*.

Given a maximal isotropic subspace $W = W^\perp$, of dimension m, we can choose a complement U which is also totally isotropic. For example, if $W = \langle e_1, \ldots, e_m \rangle$ we may take $U = \langle f_1, \ldots, f_m \rangle$. The stabilizer of the direct sum decomposition $V = W \oplus U$ is $\mathrm{GL}_m(q).2$, in which the elements swapping W and U induce the duality automorphism on $\mathrm{GL}_m(q)$.

3.3 Unitary groups

We obtain the unitary groups in much the same way, starting from a non-singular conjugate-symmetric sesquilinear form instead of a non-singular alternating bilinear form. The *unitary group* $\mathrm{U}_n(q)$ (sometimes called the general unitary group and, as here, written $\mathrm{GU}_n(q)$, to distinguish it from the special unitary group defined below) is defined as the isometry group of a non-singular conjugate-symmetric sesquilinear form f, i.e. the subgroup of $\mathrm{GL}_n(q^2)$ consisting of the elements g which preserve the form, in the sense that $f(u^g, v^g) = f(u, v)$ for all $u, v \in V$. To calculate its order, we need to count the number of vectors of norm 1, and use induction. Let z_n denote the number of vectors of norm 0, and y_n denote the number of vectors of norm 1. Then the total number of vectors in the space is $q^{2n} = 1 + z_n + (q-1)y_n$, and we calculate $z_{n+1} = z_n + (q^2-1)y_n$ so $z_{n+1} = (q^{2n}-1)(q+1) - qz_n$. Since $z_0 = z_1 = 0$ we may solve the recurrence relation to get $z_n = (q^n - (-1)^n)(q^{n-1} + (-1)^n)$, and therefore $y_n = q^{n-1}(q^n - (-1)^n)$.

Now an arbitrary element of $\mathrm{GU}_n(q)$ may be specified by picking an orthonormal basis one vector at a time, so the order of $\mathrm{GU}_n(q)$ is

$$\begin{aligned} |\mathrm{GU}_n(q)| &= \prod_{i=1}^{n} q^{i-1}(q^i - (-1)^i) \\ &= q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - (-1)^i). \end{aligned} \tag{3.12}$$

Writing elements M of $\mathrm{GU}_n(q)$ with respect to an orthononormal basis, we have that the rows of M are orthonormal vectors, which can be expressed by the equation $M\overline{M}^T = I_n$. In particular if $\det(M) = \lambda$ then $\lambda\overline{\lambda} = \lambda^{q+1} = 1$. Now as λ is in a cyclic group of order $q^2 - 1 = (q+1)(q-1)$ this equation says that λ is in the unique subgroup of order $q+1$. In particular, $\mathrm{GU}_n(q)$ has a subgroup $\mathrm{SU}_n(q)$ of index $q+1$ consisting of all the elements with determinant 1.

Similarly, the scalars in $\mathrm{GU}_n(q)$ are those λ for which $\lambda\overline{\lambda} = \lambda^{q+1} = 1$. There are exactly $q+1$ such λ in $\mathbb{F}_{q^2}$. In particular, $\mathrm{GU}_n(q)$ has a central subgroup Z of order $q+1$. The quotient $\mathrm{PGU}_n(q) = \mathrm{GU}_n(q)/Z$ is called the projective unitary group. .

The scalars of determinant 1 are those λ for which both $\lambda^n = 1$ and $\lambda^{q+1} = 1$. The number of such scalars is precisely the greatest common divisor $d = (n, q+1)$. The quotient $\mathrm{PSU}_n(q)$ of $\mathrm{SU}_n(q)$ by the scalars it contains is usually a simple group. The exceptions are those explained by the isomorphisms $\mathrm{PSU}_2(q) \cong \mathrm{PSL}_2(q)$, together with the group $\mathrm{PSU}_3(2)$, which is a soluble group of order 72.

To see that $\mathrm{SU}_2(q) \cong \mathrm{SL}_2(q)$ we take the natural module for $\mathrm{SU}_2(q)$ over $\mathbb{F}_{q^2}$, and find a 2-dimensional $\mathbb{F}_q$-subspace which is invariant under the action of the group. We first pick an element $\mu \in \mathbb{F}_{q^2}$ with $\mu\overline{\mu} = \mu^{1+q} = -1 \in \mathbb{F}_q$, and then take all vectors of the form $(\lambda, \mu\overline{\lambda})$ where $\lambda \in \mathbb{F}_{q^2}$. This is clearly a 2-dimensional $\mathbb{F}_q$-subspace, and we can check it is invariant under an arbitrary element $\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$ of $\mathrm{SU}_2(q)$. [For this matrix maps $(\lambda, \mu\overline{\lambda})$ to $(\alpha\lambda - \mu\overline{\beta\lambda}, \beta\lambda + \mu\overline{\alpha\lambda})$ and $\mu(\overline{\alpha\lambda - \mu\overline{\beta\lambda}}) = \mu\overline{\alpha\lambda} - \mu\overline{\mu}\beta\lambda = \beta\lambda + \mu\overline{\alpha\lambda}$ since $\mu\overline{\mu} = -1$.] The kernel of this action is obviously trivial, and $|\mathrm{SU}_2(q)| = |\mathrm{SL}_2(q)|$, so the groups are isomorphic.

3.4 Orthogonal groups in odd characteristic

Recall from Section 3.1.6 that, up to equivalence, there are exactly two non-singular symmetric bilinear forms f on a vector space V over a finite field F of odd order. The orthogonal group $\mathrm{O}(V, f)$ is defined as the group of linear maps g satisfying $f(u^g, v^g) = f(u, v)$ for all $u, v \in V$. If n is odd, and $\alpha \in F$ is a non-square, then f and αf are in different classes, but the groups $\mathrm{O}(V, f)$ and $\mathrm{O}(V, \alpha f)$ are obviously equal, so there is only one orthogonal group (up to

isomorphism) in this case, and we write it as $\mathrm{O}_n(q)$ without ambiguity. If n is even, however, we have two thoroughly different orthogonal groups (they do not even have the same order, as we shall see).

For example, if $n = 2$, the two forms may be taken as f_1 and f_2 given with respect to an orthogonal basis $\{x, y\}$ by $f_1(x, x) = f_1(y, y) = 1$, and $f_2(x, x) = 1, f_2(y, y) = \alpha \notin F^2$. Now, if -1 is a square in F, say $-1 = i^2$, then $f_1(x + iy, x + iy) = 0$, while $f_2(x + \lambda y, x + \lambda y) = 1 + \lambda^2\alpha$, which cannot be 0 (otherwise $\alpha = -\lambda^{-2}$, which is a contradiction). On the other hand, if -1 is not a square, then $-\alpha = \lambda^{-2}$ for some λ, so $f_2(x + \lambda y, x + \lambda y) = 0$, while $f_1(x + \lambda y, x + \lambda y)$ can never be 0. Thus there is a non-zero isotropic vector for f_1 if and only if $q \equiv 1 \bmod 4$, and there is a non-zero isotropic vector for f_2 if and only if $q \equiv 3 \bmod 4$. We prefer the geometric distinction to the number-theoretic one, so we say the form is of *plus type* if there is an isotropic vector, and of *minus type* if there is not. Thus f_1 is of plus type and f_2 is of minus type if $q \equiv 1 \bmod 4$, and vice versa if $q \equiv 3 \bmod 4$.

More generally, a form in $2m$ dimensions is of *plus type* if there is a totally isotropic subspace of dimension m, and of *minus type* otherwise. The form which has an orthonormal basis is of minus type just if $q \equiv 3 \bmod 4$ and m is odd. If f is of plus type we write $\mathrm{O}^+_{2m}(q)$ for $\mathrm{O}(V, f)$, while if f is of minus type we write $\mathrm{O}^-_{2m}(q)$. The maximal dimension of a totally isotropic subspace is often called the *Witt index* of the form. Thus the forms of plus type have Witt index m while those of minus type have Witt index $m - 1$.

3.4.1 Determinants and spinor norms

Now in any of these orthogonal groups G the elements have determinant ± 1. For if M is the matrix of the form, and $g \in G$, then $gMg^T = M$ so $\det(g) = \det(M(g^T)^{-1}M^{-1}) = (\det g)^{-1}$.

The elements of determinant 1 form a subgroup of index 2, called the *special orthogonal group* $\mathrm{SO}_n(q)$. The only scalars in the orthogonal groups are ± 1, and -1 is in the special orthogonal group if and only if the dimension is even. The corresponding quotient groups are the *projective orthogonal* groups $\mathrm{PO}_n(q)$ and *projective special orthogonal* groups $\mathrm{PSO}_n(q)$. In contrast to the other three families of classical groups, however, these groups are not in general simple. There is in most cases (the exceptions are the groups $\mathrm{PSO}^\varepsilon_{2m}(q)$ where $q^m + \varepsilon \equiv 0 \bmod 4$, as we show at the end of this section) a further subgroup of index 2, defined as the kernel of another invariant, called the *spinor norm*.

This invariant works in much the same way as the concept of even and odd permutations. We first write our arbitrary element of the special orthogonal group as a product of reflections. Since a reflection may be defined by the property that it negates a certain 1-space $\langle v \rangle$ and fixes all vectors orthogonal to v, it may be

defined by the formula

$$r_v \quad : \quad x \mapsto x - 2\frac{f(x,v)}{f(v,v)}v \tag{3.13}$$

Since reflections have determinant -1, this product contains an even number of reflections. Now there are two types of reflections: those which negate a vector of norm 1, and those which negate a vector of norm a non-square α. So there is a subgroup of the special orthogonal group (of index 1 or 2) consisting of those elements which are a product of a set of reflections, consisting of an even number of each type (these are called the elements of spinor norm 1). To show that this subgroup has index 2, it suffices to show that there is an element which cannot be written in this way (these are called the elements of spinor norm -1), or to show that the identity element cannot be written as such a product, with an odd number of reflections of each type. This is surprisingly difficult to prove..

The kernel of the spinor norm map is denoted $\Omega(V,f)$ or $\Omega_n^{\pm}(q)$ as appropriate, and the quotients $\Omega(V,f)/\{\pm 1\}$ by $\mathrm{P}\Omega(V,f)$ etc. The groups $\mathrm{P}\Omega_n^{\pm}(q)$ for q odd are always simple if $n \geq 5$.

Note that in even dimensions -1 has spinor norm 1 if and only if there is an orthonormal basis, that is if and only if $q^m \equiv \varepsilon \bmod 4$, where the orthogonal group is $\mathrm{O}^{\varepsilon}_{2m}(q)$. In particular, if this condition does not hold then $\mathrm{SO}^{\varepsilon}_{2m}(q) = 2\times\Omega^{\varepsilon}_{2m}(q)$ and $\mathrm{PSO}^{\varepsilon}_{2m}(q) = \mathrm{P}\Omega^{\varepsilon}_{2m}(q)$.

3.4.2 Orders of orthogonal groups

To calculate the orders of these groups we first prove (by induction) a formula for the number of isotropic vectors in an orthogonal space. Then we show that the stabilizer of an isotropic vector in $\mathrm{O}^{\varepsilon}_n(q)$ is $q^{n-2}{:}\mathrm{O}^{\varepsilon}_{n-2}(q)$. Thus we obtain (by induction again) a formula for the order of the orthogonal group.

The inductive argument does not depend on the characteristic of the field, though the base case is slightly different in characteristic 2. For the base case we need to know the orders of the 1- and 2-dimensional orthogonal groups. Now $\mathrm{SO}_1(q)$ is the trivial group for all q. For q odd and $n = 2$ we can choose an orthogonal basis such that the quadratic form is $x^2 + \lambda y^2$, with either $\lambda = 1$ or λ a fixed non-square. For the $+$ type, there are just two solutions of $(x/y)^2 + \lambda = 0$, so (up to multiplication by scalars) just two isotropic vectors. In both $+$ type and $-$ type the stabilizer in $\mathrm{O}^{\varepsilon}_2(q)$ of a non-isotropic vector v has order 2 (consisting of the reflection in $v^{\perp}$), and therefore (since by Witt's Lemma the orthogonal group acts transitively on the vectors of any given norm) the number of vectors of norm 1 is equal to the number of vectors of norm α (a fixed non-square). In particular, there are up to sign just $\frac{1}{2}(q+1)$ vectors of norm 1 in $\mathrm{O}^{-}_2(q)$, and $\frac{1}{2}(q-1)$ in $\mathrm{O}^{+}_2(q)$. Therefore $|\mathrm{O}^{+}_2(q)| = 2(q-1)$ and $|\mathrm{O}^{-}_2(q)| = 2(q+1)$. In fact these are dihedral groups, since they may be generated by two reflections,

in vectors with suitable norms and inner product. The special orthogonal groups $\mathrm{SO}_2^\varepsilon(q)$ are cyclic of order $q-\varepsilon$, and $\Omega_2^\varepsilon(q)$ is cyclic of order $(q-\varepsilon)/2$.

Now we are ready for the first induction, which is really three separate inductions. Let z_m denote the number of (non-zero) isotropic vectors in an orthogonal space of dimension $2m$ or $2m+1$. Our inductive hypothesis is that $z_m = q^{2m}-1$ in dimension $2m+1$, $z_m = (q^m-1)(q^{m-1}+1)$ for a space of plus type in $2m$ dimensions, and $z_m = (q^m+1)(q^{m-1}-1)$ for a space of minus type in $2m$ dimensions. Note that these formulae give $z_0 = 0$ for a 1-space, $z_1 = 2(q-1)$ for a plus-type 2-space, and $z_1 = 0$ for a minus-type 2-space, so the induction starts.

For the inductive step, we split the $(n+2)$-space V as $V = U \oplus W$, where U is a 2-space of plus type, and W is an orthogonal space of dimension n, of the same type as the original space V. Now every isotropic vector is of the form $u+w$, where $u \in U$ and $w \in W$. Either u and w both have norm 0 (but are not both the zero vector), or u has norm $\lambda \neq 0$ and w has norm $-\lambda$. Since U contains $2q-1$ vectors of norm 0 (including the zero vector), and $q-1$ vectors of every non-zero norm, we count $z_{m+1} = (2q-1)(1+z_m)+(q-1)(q^n-1-z_m)-1$. This simplifies to $z_{m+1} = qz_m + (q-1)(q^n+1)$, and it is a simple matter to complete the proof by induction in each of the three cases.

Next we determine the stabilizer of an isotropic vector v_0. Certainly this is contained in the stabilizer of the flag $0 < \langle v_0\rangle < v_0^\perp < V$. Fixing v_0 implies that the quotient $V/v_0^\perp$ is also fixed. The possible actions on $v_0^\perp/\langle v_0\rangle$ form a group $\mathrm{SO}_{n-2}(q)$. By choosing a basis $\{v_0, w_1, \ldots, w_{n-2}, v_1\}$ such that $w_i \perp v_0$, we see that the maps f_i defined by $f_i : w_i \mapsto w_i + v_0, v_1 \mapsto v_1 - w_i, w_j \mapsto w_j$ generate the kernel of this action. Hence the stabilizer of v_0 has order $q^{n-2}|\mathrm{SO}_{n-2}(q)|$. Moreover, we can choose v_1 orthogonal to $w_1, \ldots, w_{n-2}$, so that V is the orthogonal direct sum of $\langle v_0, v_1\rangle$ and $\langle w_1, \ldots, w_{n-2}\rangle$. Therefore if n is even then the orthogonal space $\langle w_1, \ldots, w_{n-2}\rangle$ has the same type (+ or −) as V.

Finally, since $\mathrm{SO}_1(q)$ is trivial we have

$$|\mathrm{SO}_{2m+1}(q)| = \prod_{k=1}^{m}((q^{2k}-1)q^{2k-1}) = q^{m^2}(q^2-1)(q^4-1)\cdots(q^{2m}-1).$$

Similarly, since $\mathrm{SO}_2^+(q)$ has order $q-1$ we have

$$\begin{aligned} |\mathrm{SO}_{2m}^+(q)| &= (q-1)\prod_{k=2}^{m}((q^k-1)(q^{k-1}+1)q^{2k-2}) \\ &= q^{m(m-1)}(q^2-1)(q^4-1)\cdots(q^{2m-2}-1)(q^m-1), \end{aligned} \tag{3.14}$$

and also $\mathrm{SO}_2^-(q)$ has order $q+1$ so

$$|\mathrm{SO}_{2m}^-(q)| = q^{m(m-1)}(q^2-1)(q^4-1)\cdots(q^{2m-2}-1)(q^m+1).$$

3.5 Orthogonal groups in characteristic 2

In characteristic 2, everything is different. The quadratic form has a different definition, the canonical forms are different, there are no reflections, the determinant tells us nothing, and there is no spinor norm. Nevertheless, the formulae for the group orders still hold, and (in even dimensions) there is still a mysterious subgroup of index 2, although to define it we need a new invariant, which is called the *quasideterminant* or *pseudodeterminant* (it is analogous to the determinant, rather than the spinor norm). Indeed, the structure of the orthogonal groups in characteristic 2 is simpler than in odd characteristic, since the determinants are all 1 and there are no non-trivial scalars in the orthogonal group (for if $Q(\lambda v) = Q(v) \neq 0$ then $\lambda^2 = 1$ so $\lambda = 1$). Recall from Section 3.1.7 that in characteristic 2 we have $\mathrm{O}_{2m+1}(q) \cong \mathrm{Sp}_{2m}(q)$ and therefore we do not need to consider the odd-dimensional case.

3.5.1 The quasideterminant and the structure of the groups

The elements which in characteristic 2 play the role played by the reflections in odd characteristic are the *orthogonal transvections* (some people even call them reflections). For each vector v of norm 1 define the corresponding orthogonal transvection t_v by $t_v : w \mapsto w + f(w, v)v$. Clearly this is a linear map, and it preserves the quadratic form since

$$Q(w + f(w, v)v) = Q(w) + f(w, v)^2 + f(w, v)^2 Q(v) = Q(w).$$

Now the orthogonal group can be generated by these transvections (we leave the proof as an exercise) and the quasideterminant of an element x is defined to be 1 or -1 according as x can be written as a product of an even or an odd number of orthogonal transvections. In order to prove that this is well-defined we show that the transvections act as odd permutationsof the set of maximal isotropic subspaces (in the case $\mathrm{O}^+_{2m}(q)$). I am grateful to Bill Kantor for supplying this elegant argument.

First consider the case $\mathrm{O}^+_2(q)$. Here we have just two isotropic 1-spaces, since if x is isotropic and y is scaled so that $f(x, y) = 1$, then $Q(\lambda x + y) = Q(y) + \lambda$ so is zero for exactly one value of λ. Choosing y to be isotropic, then, t_{x+y} swaps $\langle x \rangle$ and $\langle y \rangle$, as does every other orthogonal transvection (they are all of the form $t_{x+\lambda y}$).

More generally, we need to look at maximal isotropic subspaces in the $2m$-space for $\mathrm{O}^+_{2m}(q)$. Suppose we have a maximal isotropic subspace U, and a vector v of norm 1. Note that $v^\perp$ has codimension 1, and does not contain U since $v \notin U = U^\perp$. Therefore $v^\perp \cap U$ has codimension 1 in U, and we may choose a basis $u_1, \ldots, u_m$ for U so that $u_1, \ldots, u_{m-1}$ span $v^\perp \cap U$ and $f(u_m, v) = 1$. Then t_v fixes $u_1, \ldots, u_{m-1}$ and maps u_m to $u_m + v \notin U$, so t_v does not fix U. Hence

the transvections act fixed-point-freely on the set of totally isotropic subspaces of dimension m.

Now we count the number of such subspaces. Just as in the odd characteristic case, we see that the number of isotropic vectors is $(q^m - 1)(q^{m-1} + 1)$. Since $\mathrm{O}^+_{2m}(q)$ acts transitively on the isotropic vectors (this follows from our classification of the quadratic forms, as the form looks the same whichever isotropic vector we take as e_1), we may choose the first isotropic vector to be e_1. Then we see that the stabilizer of e_1 has the shape $q^{2m-2}{:}\mathrm{O}_{2m-2}(q)$. By induction, the number of m-dimensional totally isotropic subspaces is $\prod_{i=0}^{m}(q^i + 1)$ which is twice an odd number. Therefore t_v acts as an odd permutation on the set of m-dimensional totally isotropic subspaces. We can therefore define the quasideterminant of an element of $\mathrm{O}^+_{2m}(q)$ to be the sign of the permutation describing its action on this set. The kernel of the quasideterminant map is the subgroup $\Omega^+_{2m}(q)$ of index 2 in $\mathrm{O}^+_{2m}(q)$. (This subgroup is sometimes denoted $\mathrm{SO}^+_{2m}(q)$, but this can be confusing.)

For $\mathrm{O}^-_{2m}(q)$ this argument does not go through directly, since the maximal isotropic subspaces have dimension $m - 1$ and it is possible that $U \leq v^\perp$. However, if we extend the field to $\mathbb{F}_{q^2}$, we obtain maximal isotropic subspaces of dimension m, and can apply the preceding argument. (Incidentally, this shows that $\mathrm{O}^-_{2m}(q) < \mathrm{O}^+_{2m}(q^2)$.) In fact it is possible to extend this argument to show that the transvections in $\mathrm{O}^+_{2m}(q)$ interchange two families of maximal isotropic subspaces: two such subspaces U and W are in the same family if and only if $U \cap W$ has even codimension in each of them. Another useful fact is that an element x in $\mathrm{O}^\varepsilon_{2m}(q)$ is in Ω^ε_{2m} if and only if the rank of $1 + x$ (as a $2m \times 2m$ matrix) is even.

3.6 Maximal subgroups of classical groups

In order to understand how the nine types of subgroups of the linear groups behave in the presence of forms of various types, we need to look at the behaviour of the forms under the operations of tensor products, and restriction and extension of fields. (In Section 3.2.4 we looked at the subspaces in the case of the symplectic groups, and saw that we can restrict attention to non-singular subspaces and totally isotropic subspaces. It is clear that the same applies in the case of unitary and orthogonal groups.) Without going into too much detail at this stage, we can incorporate the forms into the Aschbacher–Dynkin theorem as follows. In this version, the natural classical groups are denoted $\tilde{G}$, and the corresponding projective groups by G. Thus for example we might have $\tilde{G} = \mathrm{Sp}_{2n}(q)$ and $G = \mathrm{PSp}_{2n}(q)$.

THEOREM 2. *If G_0 is a finite simple classical group, $G_0 \leq G \leq \mathrm{Aut}(G)$, and G does not involve the triality automorphism of $\mathrm{P}\Omega^+_8(q)$ or the graph automorphism*

of $\mathrm{PSp}_4(2^a)$*, and* M *is a maximal subgroup of* G*, not containing* G_0*, then either* M *stabilizes one of the following structures on the natural module for* $\tilde{G}$*:*

1. *a non-singular subspace;*
2. *a totally isotropic subspace;*
3. *a partition into isometric non-singular subspaces;*
4. *a partition into two totally isotropic subspaces;*
5. *a partition into non-singular subspaces defined over an extension field of prime degree;*
6. *a decomposition as a tensor product of two non-isometric spaces;*
7. *a decomposition as a tensor product of isometric spaces;*
8. *a proper subfield, of prime degree;*

or one of the following holds:

9. M *is a classical group of the same dimension and with the same field of definition as* G*;*
10. M *is an automorphism group of a simple group* S*, the representation of* $\tilde{S}$ *being irreducible and not writable over any proper subfield, where* $\tilde{S}$ *is the preimage of* S *in* $\tilde{G}$*;*
11. M *is an automorphism group of an extraspecial group* r^{1+2m} *with* r *dividing* d*, where* d *is the order of the generic part of the Schur multiplier of* G_0*; or of* $C_4 \circ 2^{1+2m}$ *when the generic part of the Schur multiplier has* C_4 *as a quotient.*