GORE HALL 1840

HARVARD UNIVERSITY

ARCHIVES

Classical Linear Groups over Finite Fields

Michael Emanuel

April 5, 1999

Special thanks to my advisor, Peter Kronheimer, for his invaluable assistance.

Classical Linear Groups over Finite Fields

1 Introduction

The classical linear groups are the isometry groups of vector spaces preserving certain bilinear forms. The most familiar example is the orthogonal group over $\mathbb{R}^n$ which preserves the standard inner product $(x, y) = \sum_{k=1}^{n} x_k y_k$; so a transformation A on $\mathbb{R}^n$ is orthogonal when $(Ax, Ay) = (x, y)$ for any x, y. For $\mathbb{R}^3$, the orthogonal group $O_3(\mathbb{R})$ is the familiar group of rotations and reflections. We explore four families of linear groups here. The simplest groups are the general linear groups, which don't preserve any bilinear form. We have already seen the orthogonal group, which preserves a symmetric bilinear form. The symplectic groups preserve skew-symmetric forms; they frequently arise in connection with Hamiltonian dynamics. When the field F has an automorphism of order 2, the unitary group preserves the Hermitian- symmetric inner product on V, and is analagous to transformations preserving the standard complex inner product.

The classical groups over $\mathbb{R}$ and $\mathbb{C}$ are very well understood and have been studied for many years, hence the term "classical." They provide a bridge between the ideas of differential geometry and algebra via the idea of the Lie algebra. If we embed a classical group G in $F^{n\times n}$, we can think of the Lie algebra as the space of vectors tangent to G at the identity. More recently, group theorists working on finite groups discovered that each family of classical groups has analogues over finite fields. This is an extremely interesting fact in its own right, since it allows us to write these groups concretely, and to use the ideas of linear algebra on group-theoretic problems. But there is an even more remarkable fact about these groups. Each classical group has a subgroup consisting of transformations of determinant one; we call this the special classical group. The center of each special classical linear group consists only of homotheties, or scalar multiples of the identity. When we pass to the quotient modulo these homotheties, we call the resulting group a projective group. The marvelous fact about the classical linear groups is that except for a few exceptions when the rank n and the order of the field are small, *all the projective special classical linear groups are simple.*

Simple groups are of central importance in the theory of finite groups. The two most familiar classes of simple groups are the cyclic groups of prime order (the only Abelian simple groups) and the alternating group A_n when $n \geq 5$. The monumental classification theorem for finite simple groups says that in addition to these two families of groups and 26 so- called sporadic groups, every simple group is of Lie type. In fact, finite simple groups are classified by the isomorphsim class of their associated Lie algebras. The best way to understand the more complicated linear groups is to use the heavy machinery of Lie algebra and algebraic groups. But the finite classical groups can be attacked directly by methods similar to those used over the real and complex numbers. That is the approach used exclusively herein. It sacrifices generality, but has the advantages of concreteness and greater accessibility. The major results we prove here are that the projective special linear groups $PSG_n(q)$ are simple.

2 Spaces with Forms

Let V be a finite dimensional vector space over a field F. We define a *bilinear form* b as a map

$$b : V \times V \to F$$

with the properties that for $x, y, z \in V$ and $a \in F$,

$$b(x+y,z) = b(x,z) + b(y,z) \qquad b(x,y+z) = b(x,y) + b(x,z)$$

$$b(ax,y) = ab(x,y) = b(x,ay)$$

If θ is an involution of F (i.e. an automorphism of order 2), then we define a *sesquilinear form* similarly. It is still linear in each of its variables, but scalars in front of the second component come out twisted by θ: that is, $b(ax,y) = ab(x,y)$, but $b(x,ay) = a^\theta b(x,y)$. So sesquilinear forms behave like the usual complex inner product, $(x,y) = \sum_{k=1}^{n} x_k \bar{y_k}$. For brevity we usually write (x,y) as shorthand for $b(x,y)$. Note that we have written the map θ to the right of its argument a; in general we will adopt this convention, so that the composition $x \xrightarrow{\alpha} \alpha(x) \xrightarrow{\beta} \beta(\alpha(x))$ will be written $(x)\alpha\beta$.

Suppose that b is a bilinear form. We say that b is *symmetric* if $(y,x) = (x,y)$ for all $x, y \in V$. On the other hand, b is *skew symmetric* if $(y,x) = -(x,y)$. If b is a sesquilinear form, b is *Hermitian symmetric* when $(y,x) = (x,y)^\theta$. Observe that for any of these symmetry types, $(x,y) = 0 \Leftrightarrow (y,x) = 0$. To motivate these definitions, we can think of the usual inner product on $\mathbb{R}^n$ as a typical example of a symmetric bilinear form, while the inner product on $\mathbb{C}^n$ is an example of a Hermitian symmetric form.

The usual notion of orthogonality on vector spaces carries over. We say that x is *orthogonal* to y and write $x \perp y$ when $(x,y) = 0$. If $X \subset V$, then we define the *orthogonal complement* of X to be the set $X^\perp = \{v \in V : x \perp v\ , \forall x \in X\}$. If $\langle X \rangle$ represents the subset generated by X, then $X^\perp = \langle X \rangle^\perp$.

Now for some terminology. A subspace W is a *hyperplane* when it has codimension 1. We define the *radical* of V to be the subspace $V^\perp$, and say that b is *nondegenerate* if the radical of V is 0. We say that a vector x is *isotropic* if $(x,x) = 0$, and a subspace U is *totally isotropic* when the restriction of b to U is trivial, so $b(u,v) = 0$ for all $u, v \in U$. The maximal dimension of a totally isotropic subspace is called the *Witt index* of the space. U is said to be *nonsingular* when the restriction of b to U is nondegenerate. In terms of the relation between U and $U^\perp$, v is isotropic when $v \in v^\perp$, U is totally isotropic when $U \subset U^\perp$ and U is nondegenerate when $U \cap U^\perp = 0$.

Lemma 2.1 For $x \in V$, $x^\perp = \ker(\alpha)$, where $\alpha \in \mathrm{Hom}_F(V,F)$, $y\alpha = (y,x)$. The dimension $\dim(x^\perp) \geq n-1$, with equality when $x \notin V^\perp$.

Proof: α as defined is certainly an F-linear transformation with kernel $x^\perp$ by definition. Applying the rank- nullity theorem, when $x \notin V^\perp$, α will be

surjective and thus have rank one, leaving its kernel with dimension $n-1$. And obviously if $x \in V^\perp$, α is the zero map and its kernel has dimension n. □

Lemma 2.2 Let U be a subspace of an n-dimensional nondegenerate space V. Then $\dim(U^\perp) = \text{codim}(U)$.

Proof: The proof is by induction on $m = \dim(U)$. If $m = 0$ the result is trivial since $U = 0$ and $U^\perp = V$. V is nondegenerate so we can find some $x \in V - U^\perp$. By the previous lemma, $W = U \cap x^\perp$ has codimension 1 in U. Now by the inductive hypothesis, $\dim(W^\perp) = n - m + 1$. Then $\dim(U) > \dim(W)$ so we can choose some $u \in U - W$, and $U^\perp = W^\perp \cap u^\perp$. Now $x \in W^\perp - u^\perp$ so $U^\perp$ is a hyperplane of $W^\perp$ and $\dim(U^\perp) = \dim(W^\perp) - 1 = n - m$ as required. □

Using these two lemmas, we can prove a

Proposition 2.3 If V is a nondegenerate space, the Witt Index is at most $n/2$.

Proof: Suppose that U is a totally isotropic space. Then $U \subset U^\perp$. In particular, $\dim(U) \leq \dim(U^\perp)$. But $\dim(U^\perp) = n - \dim(U)$ by the previous lemma. Thus $\dim(U) \leq n - \dim(U) \Rightarrow \dim(U) \leq n/2$ as required. □

We now define the three classes of forms we will study in connection with the classical groups. b is *orthogonal* if it is symmetric and nondegenerate. When $\text{char}(F) = 2$, we impose the additional requirement that $(x, x) = 0$ for all $x \in V$. We say that b is *symplectic* if it is skew symmetric and nondegenerate. Again, when $\text{char}(F) = 2$ we require $(x, x) = 0$. Finally, a nondegenerate Hermitian symmetric form b is called a *unitary* form. Observe that we we don't lose any of the structure associated with the form by assuming that it is nondegenerate. If $\text{Rad}(V) = W$, we could always work over the quotient V/W and b would still be well-defined.

To every symmetric inner produce (x, y) we have an associated *quadratic form* $Q : V \to F$ such that (1) $Q(ax) = a^2 Q(x)$ for all $a \in F, x \in V$ and (2) $Q(x + y) = Q(x) + Q(y) + b_Q(x, y)$ for some bilinear form b_Q called the associated bilinear form. Observe that when the characteristic of F is not 2, every inner product gives rise to a quadratic form $Q(x) = (x, x)$ that has $2(x, y)$ as its associated bilinear form. This is true because for any symmetric bilinear form,

$$(x + y, x + y) = (x, x) + (y, y) + 2(x, y)$$

So when $\text{char}(F) \neq 2$, there is a complete equivalence between the notions of quadratic forms and symmetric bilinear forms. We will thus use the two interchangeably; given the symmetric bilinear form $b(x, y)$ we take $Q(x) = (x, x)$ and given a form $Q(x)$ we define $b(x, y) = \frac{1}{2}(Q(x + y) - Q(x) - Q(y))$. The obvious example for this on $\mathbb{R}^n$ is the norm that can be associated to any inner product: $||x||^2 = (x, x)$. In characteristic 2, things are a bit messier. We can still associate each quadratic form with a symmetric bilinear form by taking $b(x, y) = Q(x + y) - Q(x) - Q(y)$, but in order to write $Q(x) = b(x, x)$ we can no longer assume that b is symmetric. For this reason we essentially exclude altogether the case of characteristic 2 in the following discussions.

Let V be an orthogonal space with a basis $X = (x_1, \ldots, x_n)$. Relative to this basis, we can define the matrix of the bilinear form $b(x, y)$ by $J(X, b) = a_{ij}$ for $a_{ij} = b(x_i, x_j)$. If $v = \sum_i c_i x_i$, and $w = \sum_i d_i x_i$, then by bilinearity $b(v, w) = \sum_{ij} a_{ij}\, c_i d_j$. So if we write v and w as column vectors in the basis X, $v_X = (c_1, \ldots, c_n)^T, w_X = (d_1, \ldots, d_n)^T$ then we have $b(v, w) = v_x^T J(X, b) w_X$. Since b is symmetric, $b(x_i, x_j) = b(x_j, x_i) \Rightarrow a_{ij} = a_{ji}$ and $J(X, b)$ is a symmetric matrix: $J^T = J$. Conversely, given any matrix J we can define a bilinear form this way, and this form will be symmetric if and only if J is symmetric.

Observe that this construction goes through without difficulty if b is symplectic or bilinear; the symmetry properties of J just change. If b is symplectic, $b(x_i, x_j) = -b(x_j, x_i)$ and $J(X, b)$ is skew-symmetric: $J^T = -J$. If b is sesquilinear, we have $b(v, w) = \sum_{ij} c_i \bar{d}_i$ where $\bar{d}_i = d_i^\theta$. If we write $(d_1, \ldots, d_n)^\theta$ for the vector whose entries are $(\bar{d}_1, \ldots, \bar{d}_n)$ then we have the formula $b(v, w) = v_X^T J(X, b) w_X^\theta$. Of course the resulting matrix $J(X, b)$ is Hermitian symmetric: $(y, x) = (x, y)^\theta$ so $J^T = J^\theta$. If we want to write one set of formulas with full generality, we can adopt the convention that when b is orthogonal or symplectic, θ represents the trivial automorphism. Then $J(X, b)$ is still $b(x_i, x_j)$ and $b(v, w) = v_X^T J(X, b) w_X^\theta$.

We now compute the effect of a change of basis on the matrix representation $J(X, b)$. Suppose that we change to the basis $Y = (y_1, \ldots, y_n)$ where A is the transformation such that $Ax_i = y_i$. Let $v = c_1 y_1 + \cdots + c_n y_n$, so $v_Y = (c_1, \ldots, c_n)^T$. We compute v_X by noting that

$$v = c_1(a_{11}x_1 + \cdots + a_{1n}x_n) + \cdots + c_n(a_{n1}x_1 + \cdots + a_{nn}x_n)$$

so $v = (a_{11}c_1 + \cdots + a_{n1}c_n)x_1 + \cdots + (a_{1n}c_1 + \cdots + a_{nn}c_n)$. In matrix form,

$$v_X = \begin{pmatrix} a_{11} & \cdots & a_{n1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = A^T v_Y$$

So we want $J(Y, b)$ to be related to $J(X, b)$ such that

$$\begin{aligned} v_X^T J(X, b) w_X^\theta &= v_Y^T J(Y, b) w_Y^\theta \\ (A^T v_Y)^T J(X, b)(A^T w_Y)^\theta &= v_Y^T J(Y, b) w_Y^\theta \\ v_Y^T (A J(X, b) A^{T\theta}) w_Y^\theta &= v_Y^T J(Y, b) w_Y^\theta \end{aligned}$$

By taking $v = y_i, w = y_j$ for all pairs (i, j) we find that

$$J(Y, b) = A J(X, b) A^{T\theta}.$$

Let us say that two matrices J and J' are *congruent* when $J' = A J A^{T\theta}$ for some invertible matrix A. Then we have essentially proven that if J and J' represent the same bilinear form in different bases, J and J' are congruent. Conversely, if J is the matrix for the form b w.r.t. a basis X, and J and J' are congruent via A, then transforming X by A will define a new basis $Y = AX$ in which the form b has matrix J'. This proves

Proposition 2.4 Two matrices represent the same bilinear form in different bases if and only they are congruent. □

Let us define an *isometry* of the inner product spaces (V, b) and (V', b') to be an isomorphism of vector spaces that preserves the inner product. That is, $\alpha : V \to V'$ is an isometry if it is an isomorphism and if $b'(x\alpha, y\alpha) = b(x, y)$. We say that the spaces V and V' are *isometric* in this case. We can define a similar notion of *similarity* of spaces, where we relax the requirement that α strictly preserves the inner product and allow it to multiply b by a scalar. That is, an isomorphism α is a similarity if $b'(x\alpha, y\alpha) = \lambda(x, y)$ for some $\lambda \neq 0$. Let us write $O(V)$ for the group of isometries of the space V, and $\Delta(V)$ for the group of similarities of V.

Note that in characteristic not 2 we can also define an isometry as a map such that $Q'(x\alpha) = Q(x)$, and a similarity as $Q'(x\alpha) = \lambda Q(x)$. If α is an isometry and $X = (x_1, \ldots, x_n)$ is a basis for V, then $X' = (x_1\alpha, \ldots, x_n\alpha)$ is a basis for V' such that the matrices for the two forms b and b' are the same; so two spaces will be isometric if and only if the matrices of their forms are congruent.

We now develop a convenient criterion for determining when a space is degenerate (recall that a space V is degenerate if its radical $V^\perp$ is nonzero). Suppose that $b(v, w) = v_x^T J w_x^\theta$. The radical of V consists of those vectors u such that $b(u, x_i) = 0$ for all i, so $u_x^T J = 0$. This can be solved if and only if J is a singular matrix, so we have

Proposition 2.5 A space is degenerate if and only if the matrix of its form in any basis is singular. □

When we change basis in an orthogonal space, we have $J' = AJA^T$, so the determinant of J is not an invariant of the form. However, this transformation multiplies $\det(J)$ by a square: $\det(J') = \det(J)\det(A)^2$. So the quadratic character of $\det(J)$ is preserved under a change of coordinates, and thus defines an invariant of the space which is called the *determinant* of the space V. Here is an example: if the field is $\mathbb{R}$, the squares are just the positive numbers. So this says that the determinant of the space is the sign of $\det(J)$.

If V is a unitary space, $\det(J') = \det(J)\det(A)\det(A)^\theta$, so the residue of $\det(J)$ in the multiplicative group F^* modulo the subgroup $\{a\bar{a} : a \in F^*\}$ is an invariant. For example, if our field is $\mathbb{C}$ then $\{a\bar{a} : a \in \mathbb{C}\} = \mathbb{R}_+$, and the argument $\arg(\det(J))$ is invariant under changes of coordinates. We will later show that every symplectic matrix has determinant 1, so the determinant is not an interesting invariant.

Let us now classify the orthogonal spaces on finite fields up to isometry. Our real aim is to understand the orthogonal groups of linear transformations that preserve the inner product structure on a space. That is why we are interested in classifying the various types of spaces only up to isometry (indeed, up to similarity) because similar spaces give rise to isomorphic orthogonal groups.

Proposition 2.6 If two inner product spaces V and V' are similar, then their orthogonal groups $O(V)$ and $O(V')$ are isomorphic.

Proof: A matrix A is in the orthogonal group of a space when $AJA^{T\theta} = J$. So if V and V' are similar spaces, there are bases $X = (x_i)$ and $X' = (x_i')$ such that when we write J and J' in these bases, $J' = \lambda J$. Let the map effecting this basis change be $\alpha : V \to V'$. Consider the map $\phi : GL(V) \to GL(V')$, with $A\phi = \alpha A \alpha^{-1}$. Then ϕ is certainly an isomorphism from $GL(V)$ to $GL(V')$; we must show that it is bijective from $O(V)$ to $O(V')$. If $A \in O(V)$, then $AJA^{T\theta} = J$. So

$$\begin{aligned}(A\phi)J'(A\phi)^{T\theta} &= (\alpha A\alpha^{-1})(\lambda\alpha J\alpha^{-1})(\alpha A\alpha^{-1})^{T\theta} \\ &= \lambda\alpha AJA^{T\theta}\alpha^{-1} = \lambda\alpha J\alpha^{-1} = J'\end{aligned}$$

and $A\phi$ is indeed in $O(V')$. By the same argument in reverse, ϕ^{-1} sends $O(V')$ to $O(V)$, so we conclude that ϕ is an isomorphism as claimed. □

If V_1 and V_2 are orthogonal spaces with quadratic forms Q_1 and Q_2, we define their *orthogonal sum* to be the vector spaces $V_1 \oplus V_2$ equipped with the form

$$Q(v_1 + v_2) = Q_1(v_1) + Q_2(v_2)$$

for $v_i \in V_i$. We denote this new space by $V_1 \perp V_2$ to emphasize that it is an orthogonal direct sum. This definition of Q matches with our intuition from $\mathbb{R}^n$ that if V and W are mutually orthogonal subspaces, $||v + w||^2 = ||v||^2 + ||w||^2$ by the usual Pythagorean identity. If Q_1 and Q_2 have matrices J_1 and J_2, then the matrix for Q is $\begin{pmatrix} J_1 & 0 \\ 0 & J_2 \end{pmatrix}$.

We can generalize this construction to any inner product spaces. For arbitrary inner product spaces V_1 and V_2 with forms b_1, b_2 , we define $V_1 \perp V_2$ to be the vector space $V_1 \oplus V_2$ with the inner product

$$b(v_1 + v_2, w_1 + w_2) = b_1(v_1, w_1) + b_2(v_2, w_2)$$

for all $v_i, w_i \in V_i$. Again, observe that the matrix J for b is $\begin{pmatrix} J_1 & 0 \\ 0 & J_2 \end{pmatrix}$. Note that this broader definition is consistent with the definition given for orthogonal spaces since $Q(v) = (v, v)$.

Using the notion of orthogonal sums, let us show directly how we can reduce to the case of nonsingular spaces.

Proposition 2.7 Let V be an inner product space, $V = V^\perp \oplus U$. Then $V = V^\perp \perp U$, U is nonsingular, and U is determined up to isometry by V.

Proof: U is orthogonal to $V^\perp$ so we immediately conclude that $V = V^\perp \perp U$. Furthermore, $U^\perp = V^\perp$ and $U \cap V^\perp = 0$, so $U^\perp \cap U = 0$ and U is nonsingular. Next, since the inner product (x, y) vanishes when either x or y is in $V^\perp$, we can define an inner product on the quotient $V/V^\perp$ by taking $(\bar{x}, \bar{y}) = (x, y)$ where $x \mapsto \bar{x}$ is the natural projection $V \to V/V^\perp$. Then it is clear that $V/V^\perp$ is isometric to U, hence U is unique up to isometry. □

U is the *nonsingular part* of V, and its dimension is called the *rank* of V.

Our next result shows how to decompose any inner product space into the orthogonal direct sum of subspaces.

Proposition 2.8 Let V be an inner product space and U a nonsingular subspace. Then $V = U \perp U^\perp$

Proof: U is nonsingular, so $U \cap U^\perp = 0$. Let $(x_1, \ldots, x_r)$ be a basis for U. Given $v \in V$, take $v = \sum c_i x_i + y$. We will find c_i such that $y \in U^\perp$, establishing the fact that $V = U \oplus U^\perp$. $(v, x_i) = 0$ if $(\sum c_i x_i, x_i) = (x, x_i)$. That is, we want to solve the equations $\sum c_i (x_i, x_j) = (x, x_j)$. But the matrix $J = (x_i, x_j)$ is nonsingular because U is nondegenerate, so this system of equations has a unique solution, and $V = U \oplus U^\perp$. This sum is clearly orthogonal because if $x_1, x_2 \in U, y_1, y_2 \in U^\perp$,

$$(x_1 + y_1, x_2 + y_2) = (x_1, x_2) + (x_1, y_2) + (y_1, x_2) + (y_1, y_2)$$

The middle terms (x_1, y_2) and (x_2, y_1) are zero by orthogonality, so we have $(x_1, x_2) + (y_1, y_2)$ as required. □

Corollary 2.9 If U is a subspace of V and σ is an isometry of V such that $U\sigma = U$, then $U^\perp \sigma = U^\perp$.

Proof: Suppose that $u' \in U^\perp$; we claim that $u'\sigma \in U^\perp$ as well. Given any $u \in U$, we have $(u, u'\sigma) = (u\sigma^{-1}, u')$ since σ is an isometry. Also, $u\sigma^{-1} \in U$ since $U\sigma = U$. Thus $(u, u'\sigma) = 0$ and $u'\sigma \in U^\perp$ as claimed. □

We now show that when the characteristic isn't 2, every orthogonal space is the orthogonal sum of 1-dimensional subspaces: that is, every form has an orthogonal basis.

Theorem 2.10 Let V be an orthogonal space over a field F of characteristic $\neq 2$. Then V is the orthogonal sum of 1-dimensional subspaces.

Proof: Let Q be the quadratic form on V. If $Q = 0$ any basis is orthogonal. Otherwise, let x_1 be a vector such that $Q(x_1) \neq 0$. Let $U = \text{span}(x_1)$; then U is nonsingular and by the previous Proposition, $V = U \perp U^\perp$. Now the result follows by induction on the dimension of V. □

Let us define an *orthogonal basis* to be a basis $(x_1, \ldots, x_n)$ such that $(x_i, x_j) = 0$ if $i \neq j$. We have shown that every orthogonal space has an orthogonal basis if $\text{char}(F) \neq 2$. In this basis the quadratic form has a diagonal matrix $\text{diag}(a_1, \ldots, a_n)$. Let us write $\langle a_1, \ldots, a_n \rangle$ for the orthogonal space whose matrix takes this form. If we change to a new basis $(c_1 x_1, \ldots, c_n x_n)$ the matrix for the form will change to $\text{diag}(c_1^2 a_1, \ldots, c_n^2 a_n)$ so we see that $\langle a_1, \ldots, a_n \rangle \cong \langle c_1^2 a_1, \ldots, c_n^2 a_n \rangle$. Observe that if $Q(x) = a$, then by the above Theorem $V = \text{span}(x) \perp V'$ when $V' = x^\perp$, i.e. $V = \langle a \rangle \perp V'$. We say that a quadratic form Q *represents* $a \in F$ if $Q(x) = a$ for some $x \in V$. Then we have just shown

Corollary 2.11 Let V be an orthogonal space over a field F of characteristic $\neq 2$ with quadratic form Q. If Q represents a then $V = \langle a \rangle \perp V'$. $\square$

Corollary 2.12 If every element in F of characteristic $\neq 2$ is a square, then two inner product spaces are isometric if and only if they have the same dimension and rank.

Proof: This condition is certainly necessary since the rank and dimension are preserved under isometry. It is sufficient because $\langle a \rangle$ is isometric to $\langle 1 \rangle$ since a is a square. Thus every space of dimension n and rank r is isometric to $\langle 1^r, 0^{n-r} \rangle$. $\square$

Now we are ready to classify quadratic forms over finite fields. We say that a form Q is *universal* if it represents every nonzero $a \in F$. A useful lemma about finite fields tells us that all quadratic forms of rank ≥ 2 over a finite field are universal.

Proposition 2.13 A quadratic form Q with rank ≥ 2 over a finite field F is universal.

Proof: First we handle the case where the characteristic is not 2. Since we can pick an orthogonal basis and choose coefficients $c_3, \ldots, c_n$ all equal to zero, it is sufficient to show that we can solve the equation $ax^2 + by^2 = c$ for any $c \in F$ given nonzero a, b. Let S be the set of elements $S = \{ax^2 : x \in F\}$, T the set $T = \{c - by^2 : y \in F\}$. Now if F has order q, it has $\frac{q+1}{2}$ squares: consider the group endomorphism $x \mapsto x^2$ on F^*. This has kernel ± 1 of order 2, so it has image of order $\frac{q-1}{2}$. 0 is also a square, so there are $\frac{q+1}{2}$ squares as claimed. Both S and T have order $\frac{q+1}{2}$ so their intersection must be nonempty. If $z \in S \cap T$, then it leads to a solution since $z = ax^2$ and $z = c - by^2$ so $ax^2 + by^2 = c$.

Now if $\mathrm{char}(F) = 2$ every element of F is a square. This follows because the above group endomorphism $x \mapsto x^2$ has kernel $\pm 1 = 1$ of order 1, so it is actually an isomorphism. But then as long as there is some x with $Q(x) = a \neq 0$, to represent c we take $\lambda^2 = c/a$ so $Q(\lambda x) = c$. $\square$

One useful corollary that we will apply later is that in any finite field every element can be written as the sum of two squares. For our present purpose of classifying quadratic forms over finite fields, we note that $\langle a, a \rangle \cong \langle 1, 1 \rangle$ for any $a \neq 0$. For the form $\langle a, a \rangle$ represents 1, so by Corollary 2.11 $\langle a, a \rangle \cong \langle 1, b \rangle$ for some b. Now isometries preserve determinants, so the quadratic character of b is the same as the quadratic character of a^2, i.e. b is a square. So $\langle b \rangle$ represents 1 and $\langle b \rangle \cong \langle 1 \rangle$. We conclude that $\langle a, a \rangle \cong \langle 1, 1 \rangle$ as claimed. We can now prove the main classification theorem for quadratic forms over finite fields:

Theorem 2.14 If F is a finite field of characteristic $\neq 2$, all nonsingular quadratic forms of rank n on F are isometric to one of $\langle 1^n \rangle$ or $\langle 1^{n-1}, \lambda \rangle$ where λ is not a square. Q is isometric to $\langle 1^n \rangle$ when its determinant is 1, and $\langle 1^{n-1}, \lambda \rangle$ otherwise.

Proof: By Theorem 2.10 we can construct an orthogonal basis for V such that $Q(x_i) = a_i$. Since λ is not a square, every one of the a_i can be changed to 1 or λ by multiplying through by a square, depending on the quadratic character of a_i. Then we have $V \cong \langle 1^r, \lambda^{n-r} \rangle$. But by our remark that $\langle \lambda, \lambda \rangle \cong \langle 1, 1 \rangle$ we have $V \cong \langle 1^n \rangle$ or $\langle 1^{n-1}, \lambda \rangle$. Since the determinant of a space is unchanged under isometries, the case $\langle 1^n \rangle$ arises when $\det(V)$ is a square, the case $\langle 1^{n-1}, \lambda \rangle$ when $\det(V)$ isn't a square. □

We make the further observation that if n is odd, say $n = 2k + 1$, the two isometry classes of forms differ by a scalar λ, for the form $\langle 1^{2k}, \lambda \rangle \cong \langle \lambda^n \rangle$. This is important because later when we consider the orthogonal group of transformations that preserve the quadratic form, the orthogonal groups corresponding to these two spaces will be isomorphic.

We now proceed to classify the unitary spaces over finite fields; this will be easier because we have already done most of the work. The answer is also simpler: all unitary spaces have an orthonormal basis, so in that basis the matrix J for the form is the identity. Before we show this, we make some observations about finite fields to make matters more concrete. Suppose that F is a finite field and that θ is a non-trivial involution of F. Let $E = \mathrm{Fix}(\theta)$ be the subfield of F fixed by θ. Since θ has order 2 in the Galois group $\mathrm{Gal}_{F/E}$, it follows that F is a quadratic extension of E. But since these are finite fields,it follows that $F \cong E[t]/(p(t))$ for some irreducible quadratic polynomial $p(t)$. The upshot of this is that the order of F must be a square $q^2 = p^{2r}$, and the fixed field E is just the copy of the finite field of order q lying in F. This also allows us to explicitly identify the involution θ. We know from finite field theory that the automorphism group of F is cyclic of order $2r$ and generated by the Frobenius automorphism $x\phi = x^p$. The only element of order 2 in this group is $\theta = \phi^r$, so $x\theta = x^q$. We note a pair of results that will be useful later:

Lemma 2.15 $\mathrm{Fix}(\theta) = \{x\bar{x} : x \in F\}$. In fact, the equation $x\bar{x} = a$ has $q + 1$ solutions in F when a is a nonzero element in the fixed field of θ.

Proof: Clearly $x\bar{x}$ is fixed by θ. Conversely, suppose that $a \in \mathrm{Fix}(\theta)$. If $a = 0$, the result holds trivially, so assume w.l.o.g. that $a \neq 0$. F^* is cyclic, so we have $a = \zeta^n$ for a $(q^2-1)^{st}$ root of unity ζ. Then since a is fixed, $\bar{a} = (\zeta^n)^q = \zeta^{qn} = \zeta^n$ Thus $qn - n \equiv 0 \mod q^2 - 1$ and $q^2 - 1$ divides $n(q-1) \Rightarrow (q+1)$ divides n. Let $n = k(q+1)$ and take $x = \zeta^k$. Then $x\bar{x} = \zeta^k(\zeta^k)^q = \zeta^{k(q+1)} = \zeta^n$ and $a = x\bar{x}$ as claimed. The polynomial $x^{q+1} = 1$ has at most $q+1$ roots in F because that is its degree. They are distinct here since $\{x, \zeta^{q-1}x, \zeta^{2(q-1)}x, \ldots, \zeta^{q(q-1)}x\}$ are all roots. □

Theorem 2.16 If V is a nondegenerate unitary space and $\mathrm{Fix}(\theta) = \{a\bar{a} : a \in F\}$ then every form on V admits an orthonormal basis. In particular, this holds if V is a unitary space over a finite field.

Proof: We start by constructing an orthogonal basis; the proof is similar to the proof for orthogonal spaces. The first step is to construct an anisotropic vector x_1. Choose any vector $x \neq 0$ in V. Since V is nonsingular, we can find

y with $(x,y) \neq 0$. By multiplying y by a scalar we can assume w.l.o.g. that $(x,y) = 1$. If either x or y is anisotropic, we are done, so we may assume w.l.o.g. that $(x,x) = (y,y) = 0$. Then $(ax+by, ax+by) = a\bar{b} + b\bar{a}$. If $\mathrm{char}(F) \neq 2$ we can choose $a = b = 1$, so $(x+y, x+y) = 2 \neq 0$. If $\mathrm{char}(F) = 2$, we can take take $a = 1$ and any $b \neq \bar{b}$. Then $(x+by, x+by) = b + \bar{b} = b - \bar{b} \neq 0$. So we have an anisotropic vector x_1 in both cases. Now by Proposition 2.8 it follows that $V = \langle x_1 \rangle \perp \langle x_1 \rangle^\perp$. Since $x_1^\perp$ is again nonsingular, we can find an orthogonal basis $(x_1, \ldots, x_n)$ by induction on the dimension n.

Now we normalize the x_i to make $(x_i, x_i) = 1$. Let $(x_i, x_i) = a_i$. a_i is fixed by θ because in general, $(y,x) = (x,y)^\theta$. But by hypothesis, $a_i = b_i\bar{b_i}$, for some b_i, so $(b_i^{-1}x_i, b_i^{-1}x_i) = 1$ and $(b_i^{-1}x_i)$ is an orthonormal basis as claimed. □

We now turn to the symplectic spaces. We will show that every symplectic space has even dimension, and that all symplectic spaces of a given dimension over F are equivalent to the standard symplectic space. We define a basis $(u_1, \ldots, u_n, v_1, \ldots, v_n)$ to be a *symplectic basis* if $(u_i, v_j) = \delta_{ij}, (u_i, u_j) = (v_i, v_j) = 0$. So in a symplectic basis, the matrix for the form b is

$$J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$$

We define a pair (x,y) of singular vectors to be a *hyperbolic pair* if $(x,y) = 1$. A two-dimensional space U is a *hyperbolic plane* if it has a hyperbolic pair as a basis.

Theorem 2.17 Let V be a symplectic space, U any nonsingular subspace and U_0 a maximal totally isotropic subspace of U. Then $\dim(U) = 2\dim(U_0)$ and any basis $u_1, \ldots, u_r$ of U_0 can be completed to a basis $u_1, \ldots, u_r, v_1, \ldots, v_r$ of U such that (u_i, v_i) are mutually orthogonal hyperbolic pairs. The basis of U can be completed to a symplectic basis for V, and in particular, V is an orthogonal sum of hyperbolic planes.

Proof: Consider the natural homomorphism $\Phi : U \to \mathrm{Hom}(U, F)$ where $v \mapsto \phi_v$ and ϕ_v is the functional $x\phi_v = (x,v)$. v is in the kernel of Φ when $x\phi_v = 0$ for all $x \in U$, i.e. when $v \in U^\perp$. So when U is nonsingular, Φ is injective. On the other hand, U and its dual U^* have the same dimension, so when U is nonsingular, Φ is an isomorphism. Furthermore, if W is any subspace of U we have a map $\Psi : U \to \mathrm{Hom}(W, F)$ defined by setting $\Psi(v)$ to be the restriction of ϕ_v to W. Since every functional on W extends to one on U and Φ is surjective, Ψ is also surjective. So we have shown an analogue of the Riesz Representation Theorem: if W is a subspace of a nonsingular space U, then any linear functional λ on W equals ϕ_v for some $v \in U$. Using this lemma, it is easy to prove the theorem.

Let $u_1, \ldots, u_r$ be a basis of U_0. Let f_1 be the functional on U_0 sending u_1 to 1 and u_i to 0 for $i \neq 1$. Now choose $v_1 \in U$ such that $\phi_v = f_1$. Then $(u_1, v_1) = 1$ and $(u_i, v_1) = 0$. We claim also that v_1 is linearly independent of $u_1, \ldots, u_n$; this is obvious because since U_0 is totally isotropic, any vector w in U_0 has $(u_1, w) = 0$. Now we define f_2 to be the functional on $\langle U_0, v_1 \rangle$

sending u_2 to 1, the other u_i and v_1 to 0. Pick v_2 with $\phi_{v_2} = f_2$. Then v_2 is independent of $(u_1, \ldots, u_n, v_1)$ since any vector $w = u + av_1$ in their span has $(u_2, w) = (u_2, u) + a(u_1, v_1) = 0$. In general, given $v_1, \ldots, v_k$ such that $(u_i, v_j) = \delta_{ij}$ and $(v_i, v_j) = 0$, we can extend to v_{k+1} by exactly the same argument: find v_k mapping to the functional f_k, and show linear independence since nothing in the span of the u_i, v_i already chosen has nonzero inner product with u_k. Thus we have a collection $B = (u_1, \ldots, u_r, v_1, \ldots, v_r)$ such that (u_i, v_i) are mutually orthogonal hyperbolic pairs.

We claim that B is a basis. Suppose that there were some vector $w \in U$ not in the span of B. Let $a_i = (u_i, w)$ and define $u = w - \sum_{i=1}^{r} a_i v_i$. Then u is not in U, but we have $(u_i, u) = 0$ for all i. Thus $\langle U_0, u \rangle$ is a totally isotropic space containing U_0, contradicting the maximality of U_0. Finally, we show that B can be extended to a symplectic basis of V. Since U is nonsingular, by Proposition 2.8 $V = U \perp U^{\perp}$, and $U^{\perp}$ is also nonsingular because $U^{\perp} \cap (U^{\perp})^{\perp} = U^{\perp} \cap U = 0$. Then we can construct a symplectic basis $(u_{r+1}, \ldots, u_n, v_{r+1}, \ldots, v_n)$ for $U^{\perp}$ so that $(u_1, \ldots, u_n, v_1, \ldots, v_n)$ is a symplectic basis for V. □

3 The Special Linear Group $SL_n(F)$

Given a field F, we define the *general linear group* $GL_n(F)$ to be the group of all invertible n by n matrices over F. Alternately, we can think of it as the set of invertible linear transformations of the vector space $V = F^n$. We use the shorthand $GL_n(q)$ to indicate $GL_n(F)$ when F is the field of order q.

Proposition 3.1 The order of $GL_n(q)$ is

$$(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}) = \prod_{k=0}^{n-1} q^n - q^k$$

Proof: We start by observing that any k-dimensional subspace of V has order q^k because there are q different possible values for the coefficient of each vector spanning the subspace, and each choice gives rise to a different vector because of the linear independence of the basis. The first column vector v_1 of $A \in G$ can be any nonzero vector, of which there are $q^n - 1$. Since A must be invertible, the second column v_2 cannot be in the span of v_1, but any other choice is possible; so there are $q^n - q$ choices for v_2. Continuing in this fashion we see that there are $q^n - q^{k-1}$ possibilities for v_k, and derive the above formula. □

We define the *special linear group* $SL_n(F)$to consist of the subgroup of $GL_n(F)$ of transformations with determinant 1. Since $SL_n(F)$ is the kernel of the group homomorphism det : $GL_n(F) \to F^*$, $SL_n(F)$ is normal in $GL_n(F)$. We can also use this map to compute the order of $SL_n(q)$.

Proposition 3.2 The order of $SL_n(q)$ is $|GL_n(q)|/(q-1) = \frac{1}{q-1} \prod_{k=0}^{n-1} q^n - q^k$

Proof: Let $H = SL_n(q)$ be a subgroup of $G = GL_n(q)$. The determinant is a surjective group homomorphism from G to the multiplicative group F^* of

order $q-1$. Since H is the kernel of this map we have $|G|/|H| = |F^*|$ so $|H| = |G|/|F^*|$.□

Let $(e_1, \ldots, e_n)$ be a basis for F^n and define E_{ij} to be the matrix with (i,j) entry of 1 and all others 0. We define the *elementary matrix* $B_{ij}(a) = I + aE_{ij}$ and the diagonal matrix $\text{diag}(a_1, \ldots, a_n) = \sum a_i E_{ii}$. We note that $B_{ij}(a)$ has determinant 1 and inverse $B_{ij}(-a)$. The elementary matrices are special cases of transvections. We define a *transvection along* u in $GL_n(F)$ to be an element T such that $xT = x + \lambda(x)u$ for some linear functional $\lambda(x)$ such that $\lambda(u) = 0$. In other words, $xT - x$ is always a multiple of u, and T fixes u. So $B_{ij}(a)$ is a transvection because if $x = \sum c_i e_i$ then $xB_{ij}(a) = x + ac_i e_j$.

Proposition 3.3 $SL_n(F)$ is generated by the elementary matrices

Proof: This is trivial for $n = 1$ so assume w.l.o.g. that $n > 1$. Let A be in $SL_n(F)$. We note that multiplying A by $B_{ij}(a)$ on the left corresponds to the row operation of adding a times the j^{th} row to the i^{th} row, while multiplying by it on the right is the column operation of adding a times the i^{th} column to the j^{th} column. Using these operations, we will reduce A to the identity. Note that the matrix

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

is generated by elementary matrices, so we can interchange the i^{th} row and minus the j^{th} row. Now A is invertible so its first column cannot be all zeroes. If $a_{i1} \neq 0$ we can apply the above transformation so $a_{11} \neq 0$. Next, we also note that $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ is generated by the elementary matrices since it is the product

$$\begin{pmatrix} 1 & 0 \\ \lambda^{-1} & 1 \end{pmatrix}\begin{pmatrix} 1 & \lambda - 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & \lambda^{-1} - 1 \\ 0 & 1 \end{pmatrix}$$

Taking $\lambda = a_{11}^{-1}$, we can make $a_{11} = 1$. Now by applying appropriate row operations we can make the first column $(1, 0, \ldots, 0)^T$, while by column operations we can make the first row $(1, 0, \ldots, 0)$. Then we have A in the form $\begin{pmatrix} 1 & 0 \\ 0 & B \end{pmatrix}$ where B is an $n-1$ by $n-1$ matrix of determinant 1. Then by induction on n we conclude that A can be reduced to the identity by elementary matrices. □

Let us prove another useful result about transvections:

Proposition 3.4 The transvections form a conjugacy class in $GL_n(F)$ for $n > 1$ and in $SL_n(F)$ for $n > 2$

Proof: Let T be a transvection, $xT = x + \lambda(x)v_1$. We will show that T is conjugate to the matrix $B_{12}(1)$. λ is a nonzero functional so there is some v_2 such that $\lambda(v_2) = 1$. Then $v_2 T = v_1 + v_2$. Since $T - I = \langle v_1 \rangle$, $T - I$ has rank 1 and null-space $n-1$. Thus T fixes an $(n-1)$ dimensional subspace of V which

includes v_1. Complete this to a basis $(v_1, v_3, \ldots, v_n)$ for $\mathrm{Fix}(T)$. Then in the basis $(v_1, \ldots, v_n)$, $T = B_{12}(1)$. This shows that T is conjugate to $B_{12}(1)$ in $GL_n(F)$. Suppose that the change-of-basis matrix P has determinant $\Delta \neq 1$. Then if $n > 2$ we define Q by $Qe_i = v_i$ for $i < n$ and $Qe_n = \Delta^{-1} v_n$. Then $\det(Q) = 1$ and clearly $QTQ^{-1} = PTP^{-1} = B_{12}(1)$.

On the other hand, any matrix that is conjugate to $B_{12}(1)$ is clearly a transvection; for if $(v_1, \ldots, v_n)$ is the basis in which $T = B_{1,2}(1)$, then $xT = x + \lambda(x)v_1$ where $\lambda(x)$ is the coefficient a_2 in front of v_2 when we write $v = \sum a_i v_i$. □

We can already see the broad outlines of a computational proof that some large quotient $SL_n(F)/Z$ is simple. We have shown that the transvections (1) generate $SL_n(F)$ and (2) form a conjugacy class. So to show that $SL_n(F)/Z$ is simple for $n > 2$ it is enough to show that any normal subgroup N strictly containing Z contains a single transvection. The original proof of this theorem, due to Dickson, was achieved in exactly this way: given some matrix A not in N, manipulate it by taking products of A and its conjugates to produce a transvection. In fact, the original proofs that all of the classical linear groups were simple followed a similar recipe: first find a small generating set for the group, consisting of several families of generators, each of which is a conjugacy class. Then to show that the center Z is a maximal normal subgroup, play the same game of constructing a member of each family from a non-central element A and its conjugates. Fortunately, there are now much slicker and cleaner group-theoretic proofs of these results. But lurking beneath the surface of all of them lie the patient computations of an earlier generation of group theorists.

We recall that the *commutator* of x and y in a group G is defined to be $[x, y] = x^{-1}y^{-1}xy$. The *commutator subgroup* $G' = [G, G]$ is the subgroup generated by commutators, $G' = \langle [x, y] : x, y \in G \rangle$. We say that a group G is *perfect* if $G = G'$.

Lemma 3.5 If N is a normal subgroup of G, the quotient group G/N is Abelian if and only if $N \supset G'$

Proof: If G/N is Abelian, then for all x, y, $(xN)(yN) = (yN)(xN)$. So $xyN = yxN$, whence $x^{-1}y^{-1}xyN = N$. We conclude that $x^{-1}y^{-1}xy \in N$ and $N \supset G'$. Conversely, if $N \supset G'$, then G/N is Abelian because $(xN)(yN) = xyN = xynN$ for any $n \in N$. Take $n = y^{-1}x^{-1}yx$ and $xynN = yxN$ as required. □

We now establish a useful lemma on the commutators of GL_n and SL_n.

Theorem 3.6 For any field F and $n \geq 2$, $SL_n(F)' = GL_n(F)' = SL_n(F)$ except when $n = 2$ and $|F| \leq 3$. In particular, $SL_n(F)$ is perfect with the above exceptions.

Proof: Clearly $SL_n(F)' \subset GL_n(F)' \subset SL_n(F)$, since the determinant of any commutator is $\det(A^{-1}B^{-1}AB) = 1$. Since $SL_n(F)$ is generated by elementary matrices, it is sufficient to show that each elementary matrix is a commutator. For i, j, k distinct, we compute $[B_{ik}(a), B_{kj}(1)] = B_{ik}(-a)B_{kj}(-1)B_{ik}(a)B_{kj}(a)$.

Writing our matrices in terms of the basis (e_i, e_j, e_k) we find that this is

$$\begin{pmatrix} 1 & 0 & -a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

This is just $B_{ij}(a)$ again, so for $n \geq 3$ we are done. If $n = 2$ we compute the commutator

$$\left[\begin{pmatrix} b^{-1} & 0 \\ 0 & b \end{pmatrix}, \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} 1 & (1-b^2)c \\ 0 & 1 \end{pmatrix}$$

Now if F has an element b such that $b \neq 0$ and $b^2 \neq 1$ then we have $B_{12}(a)$ equal to the above commutator by choosing $c = (b^2 - 1)^{-1}a$. There are at most two square roots of 1 in any field, so excluding them and 0 there must be such a b if $|F| > 3$. We can get $B_{21}(a)$ by an analagous construction, so when $|F| > 3$ we have all the elementary matrices as required. □

We remark that the exceptions noted are not just holes in the proof but are in fact exceptional cases. Our main goal in this section is to show that the *projective special linear group* $PSL_n(F)$ defined to be $SL_n(F)$ modulo its center Z is a simple group when it does not fall into one of the two exceptions noted above. Let us first identify the center.

Proposition 3.7 The center Z of $SL_n(F)$ consists of the homotheties or scalar multiples of the identity λI such that $\lambda^n = 1$.

Proof: Clearly every homothety λI such that $\lambda^n = 1$ is in $SL_n(F)$ and commutes with all its members. Conversely, suppose that $A \in Z$. The result is trivial if $n = 1$ so assume that $n > 1$. A commutes with all of $SL_n(F)$ so in particular it commutes with the elementary matrices. For any pair $i \neq j$, $B_{ij}(1)A = AB_{ij}(1)$. Looking at the (i,i) entry we see that $a_{ii} + a_{ji} = a_{ii} \Rightarrow a_{ji} = 0$. So A must be diagonal. Furthermore, if we now look at the (i,j) entry we see that $a_{ij} + a_{jj} = a_{ij} + a_{ii} \Rightarrow a_{ii} = a_{jj}$ So if we set $\lambda = a_{11}$ we find $A = \lambda I$. Finally, $\det(A) = 1 \Rightarrow \lambda^n = 1$ as claimed. □

In order to show that $PSL_n(F)$ is simple, we will develop a criterion for simplicity when G admits a certain kind of permutation representation on a set S, and then show that the action of $PSL_n(F)$ on projective n-space meets this criterion. First we recall some ideas on permutation representations. We say that a group G acts on a finite set $S = \{s_1, \ldots, s_n\}$ when there is a homomorphism $\rho : G \to \mathrm{Sym}(S)$. We write sg for $s(g\rho)$, and $\mathrm{Stab}(s)$ for the *stabilizer* of s, which is the set $\{g \in G : sg = s\}$. We define the *orbit* of s to be the set $\{t \in S : t = sg \text{ for some } g \in G\}$.

G acts *faithfully* when ρ is injective, i.e. when the only element in G fixing all of S is 1. G acts *transitively* on S when given $s, t \in S$ there is some g such that $sg = t$. That is, G acts transitively on S when there is only one G orbit. More generally, we say that G acts *n-fold transitively* on S when given n-tuples of distinct elements $s_1, \ldots, s_n$ and $t_1, \ldots, t_n$, there is some g with $s_i g = t_i$.

Finally, we recall the notion of a primitive permutation representation. Suppose that $S = \Omega_1 \cup \ldots \cup \Omega_r$ is a partition of S such that each g permutes the Ω_i among themselves (i.e. $\Omega_i g = \Omega_j$). Clearly the two trivial partitions of S with (1) $\Omega_1 = S$ and (2) $\Omega_i = \{s_i\}$ satisfy this requirement. Any other such partition is called a *system of imprimitivity.* We define a faithful, transitive G-action to be *primitive* when there are no systems of imprimitivity. Alternately, we can characterize primitivity as follows:

Lemma 3.8 G acts imprimitively on S if and only if there is a proper subset S_0 of S such that either $S_0 g = S_0$ or $S_0 g \cap S_0 = \emptyset$, and $|S_0| > 1$.

Proof: On the one hand, if such an S_0 exists then the partition $\Omega_1 = S_0, \Omega_2 = S - S_0$ is a system of imprimitivity: each g permutes the Ω_i by hypothesis, and $\Omega_1 = S_0$ is a proper subset with more than one element, so this isn't a trivial partition. On the other hand, given a system of imprimitivity $\{\Omega_i\}$, there must by at least one proper subset Ω_j with more than one element. Set $S_0 = \Omega_j$, and then S_0 is as described. □

Corollary 3.9 If G is two-fold transitive on S, G acts primitively on S

Proof: Suppose $|S_0| > 1$. Pick a pair $x, y \in S_0$. Then by two-fold transitivity, for any z there is some g fixing x and sending y to z. Since $S_0 g$ contains x, $S_0 g$ meets S_0 and is thus equal to S_0. So every z is in S_0, and S_0 is not a proper subset of S. □

Lemma 3.10 Suppose that G acts primitively on a set S. Then any non-trivial normal subgroup N is transitive, and $G = \mathrm{Stab}(p)N$ for any point $p \in S$.

Proof: Consider the orbits $\{\Omega_1, \ldots, \Omega_r\}$ of S under the action of N. The Ω_i are disjoint because they are orbits, and for any $p \in S, g \in G$, we have $pNg = pgN$ since for N normal, $Ng = gN$. But $pgN = pN$ if $pg \in pN$, otherwise $pgN = qN$ is a different orbit and is thus disjoint from pN. Since N is nontrivial and G acts faithfully on S, pN cannot just be p for each p. So by primitivity we conclude that there can be only one orbit $pN = S$.

Now fix some $p \in S$ and choose any $g \in G$. $pg = pn$ for some $n \in N$ by the transitivity of N, so $pgn^{-1} = p$ whence $gn^{-1} \in \mathrm{Stab}(p)$ and $g \in \mathrm{Stab}(p)N$. So $G = \mathrm{Stab}(p)N$ as claimed. □

We are now ready to establish a criterion for the simplicity of G.

Lemma 3.11 Suppose that G is a perfect group and G acts primitively on a set S. If there exists a point $p \in S$ such that (1) $\mathrm{Stab}(p)$ contains an Abelian normal subgroup A, and (2) G is generated by A and its conjugates, then G is simple.

Proof: Suppose that $N \neq 1$ is a normal subgroup of G. We show that $N = G$. We recall that N is a normal subgroup of G if and only if $gN = Ng$ for all $g \in G$. If N is normal, $HN = NH$ also for any subgroup H of G. Now by

Lemma 3.10, $G = \text{Stab}(p)N$, so the subgroup AN is also normal: any g can be written $g = sn$, with $s \in \text{Stab}(p)$ and $n \in N$, and

$$g(AN) = (sn)(NA) = s(NA) = s(AN) = (As)N = A(sn)N = AN(sn) = (AN)g.$$

Since it is normal, AN contains all the conjugates of A and hence $AN = G$ by hypothesis. Now by the third isomorphism theorem, $G/N \cong A/(A \cap N)$. But A is Abelian, so its quotient is also; and then by Lemma 3.5, N contains the commutator G'. Finally, since G is perfect, $G = G'$ and we conclude that $N = G$ as claimed. □

Now we show that G is simple by examining its action on projective space. We define the *projective space* $\mathbb{P}^{n-1}(F)$ to be the set of all one-dimensional subspaces of $F^n = V$. We can write points $\langle x \rangle$ for $x \in F^n$ to be the span of x in F^n. So in this context, $x \neq 0$ and $\langle x \rangle = \langle \lambda x \rangle$ for all $\lambda \neq 0$. $PSL_n(F)$ acts naturally on $\mathbb{P}^{n-1}$: given $\bar{A} \in PSL_n(F), \langle x \rangle \in \mathbb{P}^{n-1}$, we define $\bar{A}\langle x \rangle = \langle Ax \rangle$, where A denotes any representative element for $\bar{A}$ in $SL_n(F)$. Clearly the choice of representative doesn't matter, since if A, A' represent the same element, they differ by a scalar. $PSL_n(F)$ acts faithfully since if $A \in GL_n(F)$ preserves every linear subspace, $A = \lambda I$ and $\bar{A} = \bar{I}$. Since each A is bijective, it will permute the one-dimensional subspaces. We thus have a faithful permutation representation of $PSL_n(F)$.

Theorem 3.12 Let F be a field and $n \geq 2$. Then $PSL_n(F)$ is simple unless $n = 2$ and $|F| \leq 3$.

Proof: We have already shown that $SL_n(F)$ is perfect; it follows that $PSL_n(F)$ is perfect. For by Lemma 3.5, G is perfect precisely when G/N is Abelian $\Rightarrow$ $N = G$. Thus any quotient G/H of a perfect group is perfect since $\frac{G/H}{N/H} \cong G/N$ is Abelian $\Rightarrow N = G \Rightarrow N/H = G/H$.

Consider the action of $G = PSL_n(F)$ on $\mathbb{P}^{n-1}$. We claim that this action is doubly transitive. Suppose that $\langle x_1 \rangle$ and $\langle x_2 \rangle$ are distinct projective points. Then x_1 and x_2 are linearly independent, so we can complete them to a basis $(x_1, \ldots, x_n)$. Now given distinct points projective points $\langle y_1 \rangle$ and $\langle y_2 \rangle$, we can again extend to a basis $(y_1, \ldots, y_n)$. Then there is some B in $GL_n(F)$ sending x_i to y_i. If its determinant is Δ is not 1, we define A by $Ax_1 = \Delta^{-1}y_1$, $Ax_i = y_i$ for $i > 1$. Then $A \in SL_n(F)$ and $\bar{A}$ sends $\langle x_1 \rangle, \langle x_2 \rangle$ to $\langle y_1 \rangle, \langle y_2 \rangle$ as claimed. Thus by Corollary 3.9 G acts primitively on $\mathbb{P}^{n-1}$.

Let p be the projective point $\langle (1, 0, \ldots, 0) \rangle$. Now p is fixed by any matrix $\begin{pmatrix} a & b \\ 0 & Q \end{pmatrix}$ where $a \in F^*$ and Q is any invertible $(n-1)$ by $(n-1)$ matrix. On the other hand, any matrix fixing p must have first column $(a, 0, \ldots, 0)^T$, and since the determinant will then be $a \det(Q)$, Q is invertible. So $\text{Stab}(p)$ is precisely the matrices of this form. We now define a subgroup A consisting of matrices of the form $\begin{pmatrix} 1 & b \\ 0 & I \end{pmatrix}$ This is an Abelian subgroup since

$$\begin{pmatrix} 1 & b \\ 0 & I \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & I \end{pmatrix} = \begin{pmatrix} 1 & b+c \\ 0 & I \end{pmatrix}$$

Furthermore, A is normal in Stab(p) because the conjugate

$$\begin{pmatrix} a & b \\ 0 & Q \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & I \end{pmatrix}\begin{pmatrix} a^{-1} & -a^{-1}bQ^{-1} \\ 0 & Q^{-1} \end{pmatrix} = \begin{pmatrix} 1 & acQ^{-1} \\ 0 & I \end{pmatrix}$$

is again in A. To finish the proof then we need only show that $PSL_n(F)$ is generated by A and its conjugates. But this is an easy result beause A contains the elementary matrix $B_{12}(1)$ which is a transvection. If $n > 2$, the transvections form a conjugacy class that generates $SL_n(F)$ by Proposition 3.4. If $n = 2$ we recall from Proposition 3.3 that $SL_n(F)$ is generated by elementary matrices for all n. The only elementary matrices in SL_2 are $B_{12}(a)$ and $B_{21}(a)$, and we already have $B_{12}(a)$ for all a. So the conjugate

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$$

which is $B_{21}(a)$ is also accounted for. Thus all the hypotheses of Lemma 3.11 are met and we conclude that $PSL_n(F)$ is simple. □

4 The Symplectic Group $Sp_{2n}(F)$

In the first part we showed that all symplectic spaces have even dimension, and that for each field F, all symplectic spaces of dimension $2n$ are isometric to the space V with the standard symplectic form $J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$. The *symplectic group* $Sp_{2n}(F)$ is defined as the group of isometries of (V, J). A more concrete characterization can be given in terms of matrices:

$$Sp_{2n}(F) = \{P \in GL_{2n}(F) : PJP^T = J\}$$

The main goal of this section is to show that the *projective symplectic group* $PSp_{2n}(F)$ is simple, where $PSp_n(F)$ is defined analagously to $PSL_n(F)$ as the group modulo its center. So $PSp_n(F) = Sp_n(F)/Z$.

Let us begin our investigation by explicitly calculating the matrix form of members of $Sp_n(F)$.

Lemma 4.1 The matrix $P = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ where A, B, C, D are all n by n matrices, is in $Sp_{2n}(F)$ if and only if (1) $AB^T = BA^T$, (2) $CD^T = DC^T$ and (3) $AD^T - BC^T = I$.

Proof: We compute $PJP^T =$

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} AB^T - BA^T & AD^T - BC^T \\ CB^T - DA^T & CD^T - DC^T \end{pmatrix}$$

and set this equal to J. This immediately implies conditions (1), (2) and (3). Conversely, if A, B, C, D meet conditions 1-3, then we note that the lower-left

entry $CB^T - DA^T = (BC^T - AD^T)^T = -I^T = -I$ so $PJP^T = J$ and P is symplectic. □.

These conditions suggest a few cases in which they are easily satisfied. If $B = C = 0$, we are left only with $AD^T = I$, i.e. $D = A^{-1T}$. If $C = 0$ and $A = D = I$, we have only $B = B^T$. So the matrices

$$S_P = \begin{pmatrix} P & 0 \\ 0 & P^{-1T} \end{pmatrix} \quad \text{and} \quad R_Q = \begin{pmatrix} I & Q \\ 0 & I \end{pmatrix}$$

are symplectic when $Q = Q^T$. Over a two-dimensional space, the blocks A, B, C, D are just elements of the field. So conditions (1) and (2) are vacuous because the field is commutative, while (3) says that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Sp_2(F)$ if and only if $ad - bc = 1$. So $Sp_2(F)$ and $SL_2(F)$ are identical as matrix groups and we have:

Corollary 4.2 For any field F, $Sp_2(F)$ is isomorphic to $SL_2(F)$. □

In studying $SL_n(F)$ the transvections proved to be a very useful class. Let us determine the structure of the symplectic transvections. Suppose that T is a symplectic transvection along u, $xT = x + \lambda(x)u$. The entire space V is definite, so as we saw in the proof of Theorem 2.17 on the existence of a symplectic basis, the functional $\lambda(x) = (x, v)$ for some $v \in V$. Now since T is symplectic, $(xT, yT) = (x, y)$ for every pair $x, y \in V$. So

$$\begin{aligned} (x + (x,v)u, y + (y,v)u) = (x,y) + (y,v)(x,u) + (x,v)(u,y) &= (x,y) \\ (y,v)(x,u) + (x,v)(u,y) &= 0 \end{aligned}$$

Using skew-symmetry, we see that $(y, v)(x, u) = (x, v)(y, u)$. This condition will obviously be met when v is a multiple of u. This motivates our definition of the symplectic transvection $\tau_{u,c}$ as the map $x\tau_{u,c} = x + c(x, u)u$. In fact, every symplectic transvection takes this form. We can sum up these results, and some other elementary facts about symplectic transvections, in the following

Lemma 4.3 If V is a symplectic space and $u \in V$, then (1) the map $\tau_{u,c}$ is a symplectic transvection; (2) every symplectic transvection fixing $u^\perp$ takes the form $\tau_{u,c}$ for some c; (3) $\tau_{u,c}\tau_{u,d} = \tau_{u,c+d}$; (4) for $\alpha \in F^*$, $\tau_{\alpha u,c} = \tau_{u,\alpha^2 c}$; and (5) for any $\sigma \in Sp_{2n}(F)$, $\sigma^{-1}\tau_{u,c}\sigma = \tau_{u\sigma,c}$.

Proof: We have already verified (1). For (2), suppose T is a transvection. Then it fixes a $2n - 1$ dimensional subspace whose orthogonal complement is $\langle u \rangle$ for some $u \in V$. Thus the kernel of λ is $u^\perp \Rightarrow \lambda(x) = c(u, x)$ for some constant c. The result is trivial if T is the identity, so we may assume that $c \neq 0$. We have now written T in the form $xT = x + c(x, u)z$ for some z. We claim that z is proportional to u. Let (u, v) be a hyperbolic pair, so $z = au + bv + w$ with w in $W = \langle u, v \rangle^\perp$. First, T is a transvection so it must fix $z \Rightarrow (au + bv + w, u) = b = 0$. Next, if $w \neq 0$, we can find some $w' \in W$ such that $(w, w') = 1$;

then $(v, w') = (v + c(v,u)(au + w), w') = (v, w') - c(w, w')$ contradicting the orthogonality of T. So $v = du$ and changing to $c' = cd$ we conclude $T = \tau_{u,c'}$. (3) is immediate:

$$x\tau_{u,c}\tau_{u,d} = \big(x + c(x,u)u\big)\tau_{u,d} = x + c(x,u)u + d(x,u)u = x\tau_{u,c+d}.$$

(4) follows since $x\tau_{\alpha u,c} = x + c(x,\alpha u)(\alpha u) = x + \alpha^2 c(x,u) = x\tau_{\alpha^2 u,c}$. And finally we have

$$x\sigma^{-1}\tau_{u,c}\sigma = \big(x\sigma^{-1} + c(x\sigma^{-1}, u)u\big)\sigma = (x\sigma^{-1} + c(x, u\sigma)u)\sigma = x + c(x, u\sigma)u\sigma$$

so $\sigma^{-1}\tau_{u,c}\sigma = \tau_{u\sigma,c}$ as claimed. □

The formula (5) for the conjugate of $\tau_{u,c}$ allows us to identify the center of $Sp_{2n}(F)$:

Corollary 4.4 The center Z of $Sp_{2n}(F)$ consists of the scalars I and $-I$.

Proof: Suppose that $\sigma \in Z$. Then in particular σ commutes with each transvection $\tau_{u,1}$ so $\tau_{u,1} = \sigma^{-1}\tau_{u,1}\sigma = \tau_{u\sigma,1}$ Thus $x + (x,u)u = x + (x,u\sigma)u\sigma \Rightarrow (x,u)u = (x,u\sigma)u\sigma$. Now this equation can only hold when $u\sigma$ is a multiple of u, i.e. $u\sigma = \lambda(u)u$ for some functional $\lambda(u)$. We can see that $\lambda(u) = \pm 1$ since $(x,u)u = (x,cu)cu = c^2(x,u)u \Rightarrow c^2 = 1$. In fact, $\lambda(u)$ is a constant c. If the field characteristic is 2, then obviously $\lambda(u) = 1$. If not, suppose w.l.o.g. that for linearly independent vectors u, v, $\lambda(u) = 1$, $\lambda(v) = -1$, and take some $x \notin (u+v)^\perp$. Then we cannot possibly have

$$(x, u+v)(u+v) = (x, (u+v)\sigma)(u+v)\sigma = (x, u-v)(u-v)$$

because $u+v$ and $u-v$ are linearly independent. We conclude that σ is either I or $-I$. □

Our proof of simplicity will closely parallel the one given for the special linear group. As was the case for $SL_n(F)$, we will soon see that the symplectic transvections generate $Sp_{2n}(F)$. But we can see immediately that the symplectic group cannot be two-fold transitive: since it preserves inner products, it must send one hyperbolic pair into another. So it is a natural question to ask if $Sp_{2n}(F)$ acts transitively on the hyperbolic pairs. As we will see in the next theorem, the symplectic group is trying as hard as it can to act doubly transitively, and the answer is yes.

Theorem 4.5 For any field F, the symplectic group $Sp_{2n}(F)$ is transitive on hyperbolic pairs, and it is generated by the symplectic transvections.

Proof: Let T be the subgroup generated by the symplectic transvections. We break the proof up into three parts. First we show that T is transitive on nonzero vectors, then we show it is transitive on hyperbolic pairs, and finally we show that T is the whole of $Sp_{2n}(F)$.

(1) Let x, y be two nonzero vectors. If $(x,y) \neq 0$, take $c = (x,y)^{-1}$ and $u = x - y$ so that $x\tau_{u,c} = x + c(x, x-y)(x-y) = x - c(x,y)(x-y) = x - (x-y) = y$

and $\tau_{u,c}$ in T sends x to y. On the other hand, suppose $(x,y) = 0$. $\langle x,y\rangle$ has dimension 1 or 2. If it is a linear subspace, y is a multiple of x. So we can pick any vector z not orthogonal to x and it will also not be orthogonal to y. Now by the first part we can find transvections τ_1 and τ_2 sending x to z and z to y respectively, so $x\tau_1\tau_2 = y$. If x and y are linearly independent, by Theorem 2.17 we can find vectors v, w such that (x,v) and (y,w) are orthogonal hyperbolic pairs. Then we can take $z = v - w$ so that $(x,z) = (z,y) = 1$. Now by the argument directly above, we can find transvections τ_i so $x \xrightarrow{\tau_1} z \xrightarrow{\tau_2} y$.

(2) Next, suppose that (u_i, v_i) are two hyperbolic pairs. By (1) we can find $\tau \in T$ such that $u_1\tau = u_2$. So we can assume w.l.o.g. that $u_1 = u_2 = u$. If $(v_1, v_2) \neq 0$, we will use a symplectic transvection along $v_1 - v_2$ to send v_1 into v_2 as in part (1). Furthermore, this will fix u because $u\tau_{v_1-v_2,c} = u + c(v_1 - v_2, u)(v_1 - v_2)$ and both v_1 and v_2 are orthogonal to u. On the other hand, suppose that $(v_1, v_2) = 0$. We just showed that we can send the hyperbolic pair (x,y) to (x,z) as long as $(y,z) \neq 0$. So we must take a slight detour and use the hyperbolic pair $(u, v_1 + u)$. Since $(v_1, v_1 + u) = (v_1, u) = -1$, we have a transvection τ_1 mapping $(u, v_1) \to (u, v_1 + u)$. Next, $(v_1 + u, v_2) = (u, v_2) = 1$ so another transvection τ_2 finishes the job by sending $(u, v_1 + u)$ to (u, v_2).

(3) We show that $T = Sp_{2n}(F)$ by induction on n. For $n = 1$, this follows because $Sp_2(F)$ is isomorphic to $SL_2(F)$ by Corollary 4.2, and the transvections generate $SL_2(F)$ by Proposition 3.3. So say $n > 1$ and suppose that $\sigma \in Sp_{2n}(F)$. Take any hyperbolic pair (u,v): σ is symplectic, so $(u\sigma, v\sigma)$ is a hyperbolic pair as well. Thus by (2) there is some $\tau \in T$ sending (u,v) to $(u\sigma, v\sigma)$, so $\sigma\tau^{-1}$ fixes $\langle u,v\rangle$. But then $\sigma\tau^{-1}$ must also send $W = \langle u,v\rangle^\perp$ into itself by Corollary 2.9. Thus $\sigma\tau^{-1}$ is an isometry on W and by the inductive hypothesis $\sigma\tau^{-1}_{|W} = \tau_1' \cdots \tau_n'$ where τ_i' are symplectic transvections on W. Extend each τ_i' to a symplectic transvection τ_i on V by making it fix u and v. Then we have $\sigma = \tau_1 \cdots \tau_n\tau$ and $\sigma \in T$ as claimed. □

Since every transvection has determinant 1, we have

Corollary 4.6 Every symplectic transformation has determinant 1. □

The next step is to show that the symplectic group is (usually) perfect. Since the transvections generate it, the obvious strategy is to try to replicate our proof for the special linear group and write each transvection as a commutator.

Theorem 4.7 The group $Sp_{2n}(F)$ is perfect, unless $n = 1$ and $|F| \leq 3$, or $n = 2$ and $|F| = 2$.

Proof: For $n = 1$, this follows immediately since we have already shown that $Sp_2(F) \cong SL_2(F)$ [Corollary 4.2] and $SL_2(F)$ is perfect unless $|F| \leq 3$ [Theorem 3.6]. So supose that $n > 1$ and $|F| > 3$. The conjugate $\sigma^{-1}\tau_{u,c}\sigma$ is $\tau_{u\sigma,c}$; so if we want to make the commutator $[\sigma, \tau_{u,c}]$ equal to $\tau_{u,d}$, we can take σ such that $u\sigma = \alpha u$ by the transitivity of the symplectic group on nonzero vectors [Theorem 4.5]. Then

$$\sigma^{-1}\tau_{u,-c}\sigma\tau_{u,c} = \tau_{\alpha u,-c}\tau_{u,c} = \tau_{u,-\alpha^2 c}\tau_{u,c} = \tau_{u,(1-\alpha^2)c}$$

As long as we can find $\alpha \neq 0$ in F such that $\alpha^2 \neq 1$, we can take $c = (1-\alpha^2)^{-1}d$ to make $[\sigma, \tau_{u,c}] = \tau_{u,d}$. Of course, when $|F| > 3$ there will be such an α because there are at least 3 nonzero elements of the field, and at most two of them can be roots of the equation $x^2 - 1 = 0$.

We still have the case where $|F|$ is 2 or 3. We observe here that it is enough to produce a single transvection which is a commutator. For if $\tau_{u,a} \in G'$, then so is the commutator $[\sigma, \tau_{u,-a}] = \sigma^{-1}\tau_{u,a}\sigma\tau_{u,-a} = \tau_{u\sigma,a}\tau_{u,-a}$. Multiplying on the right by $\tau_{u,a}$ we find that $\tau_{u\sigma,a} \in G'$. By the transitivity of G on nonzero vectors, then, we have $\tau_{v,a} \in G'$ for all nonzero $v \in V$. In F_2 there is only one nonzero element, so we are already done; and in F_3, $\tau_{v,a}^2 = \tau_{v,2a}$ covering both nonzero elements ± 1. Then since the transvections generate G by Theorem 4.5, we conclude that G is perfect.

So suppose now that $n = 2$ and $|F| = 3$. We compute the commutator $[S_A, R_B]$

$$\begin{pmatrix} A^{-1} & 0 \\ 0 & A^T \end{pmatrix}\begin{pmatrix} I & -B \\ 0 & I \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & A^{-1T} \end{pmatrix}\begin{pmatrix} I & B \\ 0 & I \end{pmatrix} = \begin{pmatrix} I & C \\ 0 & I \end{pmatrix}$$

Where $C = B - A^{-1}BA^{T-1}$. As long as C has precisely one nonzero entry, this will be a symplectic transvection. The matrices $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$ do the job because $C = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$. When $n > 2$, we use the same argument, making A act as the identity on the other coordinates and B act as zero on them.

Suppose finally that $n = 3$ and $|F| = 2$. This time the matrices

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

produce $C = E_{11}$. We extend the argument for $n > 3$ by the same method we did for $|F| = 3$. So in all cases but the listed exceptions we have shown that $Sp_{2n}(F)$ is a perfect group. □

We are now ready to show that $PSp_{2n}(F)$ is simple when it does not fall into the exceptions given above. The proof is along the same lines as the proof for $PSL_n(F)$.

Theorem 4.8 The projective symplectic group $PSp_{2n}(F)$ is simple unless $n = 1$ and $|F| \leq 3$ or $n = 2$ and $|F| = 2$.

Proof: Since $PSL_2(F)$ is simple when $|F| > 3$ [Theorem 3.12] and SL_2 is isomorphic to $Sp_{2n}(F)$, we merely note that the center $Z = \pm I$ in both cases and conclude that $PSp_2(F)$ is simple as well. When $n > 1$ we employ the same group action on the projective space $\mathbb{P}^{2n-1}(F)$ we did for $PSL_n(F)$. Since we no longer have two-fold transitivity, we must show directly that this action is primitive. Suppose that S is a subset of $\mathbb{P}^{2n-1}$ such that either $Sg = S$ or

$Sg \cap S = \emptyset$, and $|S| \geq 2$. We claim that $S = \mathbb{P}^{2n-1}$. Since $|S| \geq 2$, we have at least two projective points $\langle x \rangle$ and $\langle y \rangle$ in S.

Let us first suppose that $(x, y) \neq 0$, so w.l.o.g. (x, y) is a hyperbolic pair. Then given a third subspace $\langle z \rangle$ where $(x, z) \neq 0$, we may again assume w.l.o.g. that (x, z) is a hyperbolic pair as well. Then by the transitivity of $Sp_{2n}(F)$ on hyperbolic pairs [Theorem 4.5] we can find $\sigma \in Sp_{2n}(F)$ sending (x, y) to (x, z), and $\bar{\sigma} \in PSp_{2n}(F)$ sends $\langle x \rangle, \langle y \rangle$ to $\langle x \rangle, \langle z \rangle$. Since $S\bar{\sigma}$ meets S at $\langle x \rangle$ and $\langle z \rangle \in S\bar{\sigma}$, we conclude that $\langle z \rangle \in S$ (here $\bar{\sigma}$ is the image of σ in the projective group). On the other hand, if $(x, z) = 0$, then $\langle x, z \rangle$ is a totally singular subspace. So by Theorem 2.17 we can find vectors v_1 and v_2 to make (x, v_1) and (z, v_2) orthogonal hyperbolic pairs. Now if we set $w = v_1 + v_2$, $(x, w) = (z, w) = 1$, so by the previous argument we can find symplectic maps σ_i such that $(x, y) \xrightarrow{\sigma_1} (x, w) \xrightarrow{\sigma_2} (x, z)$. Taking $\tau = \sigma_1 \sigma_2$ we conclude that $\langle z \rangle \in S$ by applying $\bar{\tau}$.

We next suppose that $(x, y) = 0$, so $\langle x, y \rangle$ is a totally singular two dimensional space. So we can pick w such that (x, w) is a hyperbolic pair and $(y, w) = 0$. Let $H = \langle x, w \rangle$ be the hyperbolic plane spanned by x and w. Since H is definite, by Proposition 2.8 $V = H \perp H^{\perp}$ and $y \in H^{\perp}$. So if $0 \neq z \in H^{\perp}$, we can find a symplectic map σ on $H^{\perp}$ sending y to z and then extend it to a symplectic map on V fixing x. Once again, $S\sigma$ meets S, and we conclude that $z \in S$. In particular, $w \in H^{\perp}$ so $w \in S$ and we have a hyperbolic pair $(x, w) \in S$. Now by the first part $S = \mathbb{P}^{2n-1}$.

Now choose any projective point $\langle x \rangle$. We claim that the subgroup $A = \{\bar{\tau}_{x,c} : c \in F\}$ of symplectic transvections along x (plus the identity) is Abelian and normal in $\mathrm{Stab}(\langle x \rangle)$, and that A and its conjugates generate the entire projective symplectic group. First, we have already shown that A is Abelian since $\tau_{u,c}\tau_{u,d} = \tau_{u,c+d}$ by Lemma 4.3. Next, A is normal in $\mathrm{Stab}(\langle x \rangle)$: if $\bar{\sigma}$ stabilizes $\langle x \rangle$, then $x\sigma = \alpha x$ and $\sigma^{-1}\tau_{x,c}\sigma = \tau_{x\sigma,c} = \tau_{x,\alpha^2 c} \in A$. Finally, A and its conjugates generate $PSp_{2n}(F)$ because the symplectic transvections generate $Sp_{2n}(F)$ and the symplectic group is transitive on nonzero vectors. So given any symplectic transvection $\tau_{u,c}$ we can find σ sending x to u; then $\sigma^{-1}\tau_{x,c}\sigma = \tau_{u,c}$ as desired. We have met all the requirements of our simplicity criterion [Lemma 3.11], and conclude that $PSp_{2n}(F)$ is simple. □

We remark, as we did after the simplicity theorem for $PSL_n(F)$, that the exceptions listed above are in fact non-simple groups. We can also use this group action to give a formula for the size $Sp_{2n}(q)$, the symplectic group over the finite field with q elements.

Proposition 4.9 The order of $Sp_{2n}(q)$ is $\prod_{k=1}^{n} q^{2k-1}(q^{2k} - 1)$, and $|PSp_{2n}(q)| = |Sp_{2n}(q)|/\varepsilon$ where $\varepsilon = 1$ when q is even, 2 otherwise.

Proof: We use the orbit stabilizer theorem $|G| = |\mathrm{Stab}(x)| \cdot |\mathrm{Orb}(x)|$ to get a recursive formula for the size of $Sp_{2n}(q)$. Consider the action of $G = Sp_{2n}(q)$ on the set of hyperbolic pairs in $V \times V$. G preserves inner products, so it sends one hyperbolic pair to another. As we have already shown, G acts transitively on hyperbolic pairs. Thus the size of any orbit is equal to the number of hyperbolic

pairs in a $2n$-dimensional space. We claim that this number is $q^{2n-1}(q^{2n}-1)$. There are $q^{2n}-1$ choices for the first vector u, since any nonzero vector will do. Then if we complete $u = u_1$ to a symplectic basis and write $v = \sum a_i u_i + b_i v_i$, we see that (u, v) is a hyperbolic pair precisely when $b_1 = 1$, so there are q^{2n-1} choices for v. The stabilizer of any hyperbolic pair, though, is isomorphic to the smaller symplectic group $Sp_{2n-2}(q)$ by the obvious inclusion map. So we conclude that $|Sp_{2n}(q)| = q^{2n-1}(q^{2n}-1)|Sp_{2n-2}(q)|$. $Sp_2(q)$ is isomorphic to $SL_2(q)$ and $|SL_2(q)| = q(q^2-1)$; so the product formula for the size of $Sp_{2n}(q)$ agrees with this for $n = 1$. The general result immediately follows by induction. To figure out the size of the projective group, we merely divide by the size of the center Z. Since $Z = \pm I$, it consists only of the identity when q is even; otherwise $|Z| = 2$, and the formula follows. □

5 The Orthogonal Group $O(V)$

If V is an orthogonal space with quadratic form Q, the *orthogonal group* $O(V)$ is the set of transformations that preserve Q, while the *special orthogonal group* $SO(V)$ is the subgroup of $O(V)$ consisting of transformations of determinant 1. Throughout this section we assume that the field characteristic is not 2, so we work interchangably with the bilinear form (x, y) and the associated quadratic form $Q(x) = (x, x)$. We also almost always assume that our quadratic spaces are nondegenerate (i.e. that the radical $V^\perp = 0$). We say that V is a *regular quadratic space* when V is nondegenerate and the field characteristic is not 2. We have already shown in Section 2 that two quadratic spaces are isometric if they have the same rank and determinant, and that the only isometry classes of nondegenerate quadratic forms of dimension n are $\langle 1^n \rangle$ and $\langle 1^{n-1}, \lambda \rangle$ where λ is any non-square in the field F. When n is odd, we saw that these two forms were still similar to each other, so there is only one orthogonal group which we may denote $O_n(F)$. When n is even, these two groups will not in general be the same; so we write $O_n^+(F)$ for the group when $V = \langle 1^n \rangle$ and $O_n^-(F)$ when $V = \langle 1^{n-1}, \lambda \rangle$.

In $\mathbb{R}^n$ it is well known that the orthogonal transformations are rotations and reflections. While rotations are difficult to generalize, reflections can be described algebraically in a natural way. Suppose that ρ is a reflection on $\mathbb{R}^n$, say $\mathbb{R}^3$ so we may visualize it easily. Then ρ fixes some subspace W (the plane of the reflection) and inverts its orthogonal complement $W^\perp$, by sending $x \mapsto -x$ there. Since $V = W \oplus W^\perp$ this completely determines ρ. Geometrically, we usually think of W as having dimension $n-1$ so ρ inverts a linear subspace, but the construction also works for any orthogonal decomposition of V. Given an orthogonal decomposition $V = U \perp U'$, we define the *reflection* $\rho_{U,U'}$ to be the unique linear map that sends $x \in U$ to $-x$ and fixes U'. We recall that the definition of an orthogonal decomposition is that $Q(u+u') = Q(u) + Q(u')$ when $u \in U, u' \in U'$. ρ is orthogonal because if $x = u+u'$, $Q(x\rho) = Q(u-u') = Q(u) + Q(-u') = Q(u) + Q(u') = Q(x)$. ρ also obviously has order two, since it fixes U and for U', $u'\rho^2 = -u'\rho = u'$.

So every reflection is an orthogonal transformation of order two. The converse also holds: every orthogonal involution is a reflection:

Lemma 5.1 Let V be a regular quadratic space. If $\alpha \in O(V)$ is an involution, then α is a reflection.

Proof: If the claim is in fact true, we can easily identify U and U': U is reversed so it must be precisely $\{x : x\alpha = -x\}$, while U' is fixed by α. So we define $U_+ = \{x : x\alpha = x\}$ and $U_- = \{x : x\alpha = -x\}$. We claim that $V = U_+ \perp U_-$. Clearly $U_+ \cap U_- = 0$ since if x is in both sets we have $x = x\alpha = -x \Rightarrow 2x = 0$. We are not in characteristic 2 so $x = 0$. Also, $V = U_+ + U_-$ since if we write $u = \frac{x+x\alpha}{2}$ and $v = \frac{x-x\alpha}{2}$, $x = u + v$ and $u\alpha = \frac{x\alpha+x\alpha^2}{2} = \frac{x+x\alpha}{2} = u \Rightarrow u \in U_+$ and $v\alpha = \frac{x\alpha-x\alpha^2}{2} = \frac{x\alpha-x}{2} = -v \Rightarrow v \in U_-$. Finally, U_+ and U_- are orthogonal to each other since if $x \in U_+$, $y \in U_-$, then $(x, y) = (x\alpha, y\alpha) = (x, -y) \Rightarrow (x, y) = 0$. □

Just as is true on $\mathbb{R}^n$, the reflections act transitively on vectors of the same length:

Lemma 5.2 Let V be a regular quadratic space. If $Q(u) = Q(v) \neq 0$, then there is a reflection ρ sending $u \mapsto v$.

Proof: We use the same trick and take $x = \frac{u+v}{2}$, $y = \frac{u-v}{2}$. Then x and y are orthogonal since $(x, y) = \frac{1}{4}(u + v, u - v) = \frac{1}{4}(Q(u) - Q(v)) = 0$. Furthermore, x and y cannot both be isotropic because $x + y = u$ and $Q(u) = Q(x + y) = Q(x) + Q(y) \neq 0$. If $Q(x) \neq 0$ we want to reverse the component orthogonal to x: so take $U = x^\perp$, $U' = \langle x \rangle$. Then $x\rho_{U,U'} = x$ while $y\rho_{U,U'} = -y$, so $u\rho_{U,U'} = (x + y)\rho_{U,U'} = x - y = v$. On the other hand, if $Q(y) \neq 0$, we use the same argument, but instead reverse $\langle y \rangle$ while fixing $y^\perp$, so we again have $u\rho = v$. □

If the dimension of U is p, we say that $\rho_{U,U'}$ is a reflection of *type* p. The reflections of type 1 correspond to our usual geometric notion of a reflection that fixes an $n-1$ dimensional space and inverts a linear space. They are particularly important, so we reserve the special term *symmetry* to describe a reflection of type 1. If $\rho_{U,U'}$ is to be a symmetry, U must be a one dimensional nonsingular space, so $U = \langle u \rangle$ for some anisotropic vector u. Thus we write σ_u for the symmetry $\rho_{\langle u \rangle, u^\perp}$. We can explicitly describe a reflection in terms of the inner product: σ_u reverses only the component along u, so $x\sigma_u = x - \lambda(x)u$ for some linear functional $\lambda(x)$ on V. σ_u will be orthogonal when $Q(x) = Q(x - \lambda(x)u) = Q(x) - 2\lambda(x)(x, u) + \lambda(x)^2 Q(u)$, so cancelling $Q(x)$ we see that $\lambda(x) = \frac{2(x,u)}{Q(u)}$. Thus

$$x\sigma_u = x - \frac{2(x, u)}{Q(u)}\, u$$

Observe that if we take orthogonal bases $e_1, \ldots, e_p$ for U and $e_{p+1}, \ldots, e_n$ for U', the reflection $\rho_{U,U'} = \begin{pmatrix} -I_p & 0 \\ 0 & I_{n-p} \end{pmatrix}$. As a corollary, we see that every

reflection of type p is the product of the p symmetries $\sigma_{e_1} \cdots \sigma_{e_p}$. We now show that the reflections generate the orthogonal group:

Theorem 5.3 If V is a regular quadratic space of dimension n, every $\alpha \in O(V)$ can be written as the product of at most n reflections.

Proof: The proof is by induction on n. For $n = 1$, the result is trivial since the only orthogonal transformations are $\pm I$ and $-I$ is a reflection. Now if $\dim(V) = n$, choose some anisotropic vector $e_1 \in V$. Since α is orthogonal, $Q(e_1\alpha) = Q(e_1)$. The reflections are transitive on vectors of the same length, so there exists some reflection ρ_1 mapping e_1 to $e_1\alpha$; thus $\alpha\rho_1$ fixes e_1. Then by Corollary 2.9 $\alpha\rho_1$ sends $W = e_1^{\perp}$ to itself. Applying the inductive hypothesis, we can write $\alpha\rho_{1|W} = \rho_n' \cdots \rho_2'$ where ρ_i' is an isometry on W. ρ_i' can be extended to an isometry ρ_i of V by making it fix e_1. Then we have $\alpha\rho_1 = \rho_n \cdots \rho_2$ since they are equal on both W and $\langle e_1 \rangle$. We conclude that $\alpha = \rho_n \cdots \rho_1$. □

Since every reflection is a product of symmetries, we have a

Corollary 5.4 The orthogonal group $O(V)$ is generated by symmetries. □

We can use the reflections to identify the center of $O(V)$.

Proposition 5.5 If V is a regular quadratic space and $(n, |F|) \neq (2, 3)$, then the center Z of $O(V)$ is $\pm I$.

Proof: Clearly $\pm I$ are in Z, since they are orthogonal and commute with every transformation. Suppose that $\alpha \in Z$. Then for every anisotropic vector u, α commutes with σ_u and $(u\alpha)\sigma_u = (u\sigma_u)\alpha = -u\alpha$. But the only vectors inverted by σ_u are the multiples of u, so $(u\alpha) \in \langle u \rangle$. Furthermore, since α is an isometry, $u\alpha = \pm u$ whenever u is anisotropic.

Choose an orthogonal basis $(u_1, \ldots, u_n)$ and reorder it such that $u_i\alpha = u_i$ when $i \leq k$, $u_i\alpha = -u_i$ if $i > k$. We claim that $k = 0$ or $k = n$. Suppose not: first consider $v = u_1 + u_n$. If v is anisotropic, we will have a contradiction since $v\alpha = u_1 - u_n$ is neither v nor $-v$ by the linear independence of u_1, u_n. Then if the dimension $n \geq 3$, we are done because $v = u_1 + u_2 + u_n$ is anisotropic as $Q(v) = Q(u_1 + u_n) + Q(u_2) = Q(u_2) \neq 0$. Then by the same argument, there is no way that $v\alpha$ is $\pm v$. On the other hand, if $n = 2$, we have assumed that $|F| > 3$. The forms are $\langle 1, 1 \rangle$ and $\langle 1, \lambda \rangle$ for λ a non-square. In the first case, we can pick u_i such that $Q(u_1) = Q(u_2) = 1 \Rightarrow Q(u_1 + u_2) = 2 \neq 0$. In the second case, if $\mathrm{char}(F) \neq 2$, there are at least $\frac{|F|-1}{2}$ nonsquares, so here there are at least two of them. Thus we can find a nonsquare $\lambda \neq -1$, and again $Q(u_1) + Q(u_2) = 1 + \lambda \neq 0$. So we see that either all of the u_i are fixed and $\alpha = I$, or they are all reversed and $\alpha = -I$. □.

As an excuse to work out the structure of the orthogonal group on a hyperbolic plane, we note that the exceptional group $O_2^-(F_3)$ is Abelian and does not have center $\pm I$. Suppose V is hyperbolic, so it has basis (x, y) with inner product $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. The transformation $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ will be orthogonal

when $AJA^T = J$. Since $AJA^T = \begin{pmatrix} 2ab & ad+bc \\ ad+bc & 2bc \end{pmatrix}$, we get the equations $ab = cd = 0$, and $ad + bc = 1$. If $b = 0$, $ad = 1 \Rightarrow c = 0$ and we get the solution $\lambda_a = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$. If $b \neq 0$, then $a = 0 \Rightarrow c = b^{-1}$. So rewriting this we have the matrix $\lambda_a \tau = \begin{pmatrix} 0 & a \\ a^{-1} & 0 \end{pmatrix}$ where $\tau = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Clearly $\lambda_a \lambda_b = \lambda_{ab}$, so $\{\lambda_a : a \in F^*\}$ forms a subgroup isomorphic to F^*, and $O(V)$ is the extension of F^* by a group $\langle \tau \rangle$ of order 2, where τ acts via $\tau \lambda_a \tau = \lambda_{a^{-1}}$. Since the matrix corresponding to τ has determinant -1, the special orthogonal group $SO(V) = \{\lambda_a\}$. In particular, for the case of F_3 we find that

$$O_2^-(F_3) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \right\}$$

is isomorphic to the Klein 4-group, so it is Abelian.

The symmetry σ_u only makes sense when u is non-isotropic. Let us try to construct an analogue of a symmetry that fixes an isotropic vector u. We write this map $x\rho = x + \lambda(x)u$ for some linear functional $\lambda(x)$. In order for ρ to be an isometry, $Q(x + \lambda(x)u) = Q(x) + 2\lambda(x)(x, u)$ should equal $Q(x)$, i.e. $\lambda(x)(x, u) = 0$. We only want to assume that ρ fixes u, so rather than insisting that $\lambda(x) = 0$ when $(x, u) \neq 0$, we can instead use this definition only for $u^\perp$. So to finish specifying ρ, we choose any vector v such that (u, v) is a hyperbolic pair. Then $V = \langle u, v \rangle \perp \langle u, v \rangle^\perp = \langle v \rangle \perp u^\perp$. So we need only specify ρ on v as well to complete the map. Now since V is nondegenerate, $\lambda(x) = (x, z)$ for some vector $z \in V$. Take $W = \langle u, v \rangle^\perp$ so $z = au + bv + w$ for a unique $w \in W$. This is only operative for $x \in u^\perp$, so we can assume that $a = 0$ w.l.o.g., while $u\rho = u + (u, bv + w)u = (1 + b)u$. Since we want ρ to fix u, we also have $b = 0$. We thus arrive at the following definition: when u is isotropic, choose some vector v so (u, v) is a hyperbolic pair. Then for any $w \in W$, define the transformation $\rho_{u,w}$ by $\begin{cases} x\rho_{u,w} = x + (x, w)u \text{ when } x \in u^\perp \\ v\rho_{u,w} = v - \frac{1}{2}Q(w)u - w \end{cases}$

We can motivate the choice of $v\rho$ in the following lemma. In fact, it is the only choice that is compatible with the orthogonality of $\rho_{u,w}$:

Lemma 5.6 If $x\rho = x + (x, w)u$ for $x \in u^\perp$ and (u, v) is a hyperbolic pair, then $v\rho = v - \frac{1}{2}Q(w)u - w$.

Proof: We can write $v\rho = au + bv + w'$ for some $w' \in W$. First, we observe that $b = 1$ since $(u, v) = (u\rho, v\rho) = (u, au + bv + w') = b = 1$. Next,

$$\begin{aligned} (w', v) &= (w'\rho, v\rho) = (w' + (w', w)u, v + au + w') \Rightarrow Q(w') + (w', w) = 0 \\ (w, v) &= (w\rho, v\rho) = (w + Q(w)u, v + au + w') \Rightarrow Q(w) + (w', w) = 0 \end{aligned}$$

Combining these two results, we have $Q(w') = Q(w)$ and $(w', w) = -(w, w)$. We get a by taking $Q(v) = Q(v\rho) = Q(v - au) + Q(w') = 2a + Q(w) = 0 \Rightarrow a = -\frac{1}{2}Q(w)$.

Now pick an orthogonal basis $w_1, \ldots, w_n$ for W with $w_1 = w$. We can see that w' must be a multiple of w since if $i > 1$, we have

$$(w_i, v) = (w_i\rho, v\rho) = (w_i + (w_i, w_1)u, v + au + w') = (w_i, w') = 0$$

So if we write $w' = cw$, $(w, w') = c(w, w) = -(w, w) \Rightarrow c = -1$. We conclude that $v\rho = v - \frac{1}{2}Q(w)u - w$ as claimed. □

In order to prove the simplicity of the special orthogonal group, we will let it act on the set of isotropic vectors in V. As a first step, we show that the transformations $\rho_{u,w}$ we have developed will form a normal Abelian subgroup in the stabilizer of u.

Lemma 5.7 Let V be a regular quadratic space of dimension ≥ 3 and containing a hyperbolic pair (u, v). Let $W = \langle u, v\rangle^\perp$. Then the set of transformations $A_u = \{\rho_{u,w} : w \in W\}$ is an Abelian subgroup of $O(V)$ that is normal in $\mathrm{Stab}(u)$.

Proof: A_u is an Abelian subgroup since if $w, w' \in W$, for $x \in x^\perp$ we have

$$\begin{aligned} x\rho_{u,w}\rho_{u,w'} &= (x + (x, w)u)\rho_{u,w'} = x + (x, w)u + (x + (x, w)u, w')u \\ &= x + (x, w)u + (x, w')u = x + (x, w + w')u = x\rho_{u,w+w'} \end{aligned}$$

By the previous lemma, $\rho_{u,w}$ is completely determined by its effect on $u^\perp$, so it follows that $\rho_{u,w}\rho_{u,w'} = \rho_{u,w+w'}$. Next we show normality. Suppose that $\sigma \in O(V)$. Then for $x \in u^\perp$,

$$x\sigma^{-1}\rho_{u,w}\sigma = (x\sigma^{-1} + (x\sigma^{-1}, w)u)\sigma = x + (x, w\sigma)u\sigma = x\rho_{u\sigma,w\sigma}$$

Again, the map is determined by its action on $u^\perp$ so $\sigma^{-1}\rho_{u,w}\sigma = \rho_{u\sigma,w\sigma}$. Thus if σ fixes u, the conjugate of $\rho_{u\sigma,w\sigma}$ is again in A_u. □

Our next goal is to show that the commutator subgroup $O(V)'$ is generated by the A_u most of the time. It is clear that we must impose some conditions on the space V, however, to guarantee that there is an adequate supply of isotropic vectors. It is enough to take $\dim(V) \geq 3$.

Lemma 5.8 Let V be a regular quadratic space of dimension ≥ 3. Then (1) for any isotropic $u \in V$, A_u is transitive on the linear isotropic subspaces $\langle v\rangle$ not orthogonal to u. (2) For any two linearly independent isotropic vectors u_1, u_2 there is a vector v and constants λ_1, λ_2 such that $(\lambda_i u_i, v)$ are hyperbolic pairs. (3) The subgroup Ω in $O(V)$ generated by the A_u (over all isotropic vectors u) is transitive on hyperbolic pairs.

Proof: (1) Let $\langle x\rangle$ and $\langle y\rangle$ be isotropic subspaces not orthogonal to u, so w.l.o.g. $(u, x) = (u, y) = 1$. Then since $V = \langle x, y\rangle \oplus \langle x, y\rangle^\perp$ we can write $y = au + bx + z$ for $z \in \langle x, y\rangle^\perp$. $(u, y) = 1 \Rightarrow b = 1$, and $Q(y) = 0 \Rightarrow 2a + Q(z) = 0$. So $y = x - \frac{1}{2}Q(z)u + z = x\rho_{u,-z}$. Then A_u acts transitively as claimed.

(2) Suppose that u_i are linearly independent isotropic vectors. If $(u_1, u_2) \neq 0$ we can assume that $(u_1, u_2) = 1$ w.l.o.g. by scaling λ_2. Then since $\langle u_1, u_2\rangle$ is

nonsingular, $\langle u_1, u_2\rangle^\perp$ is nonsingular as well and of positive dimension, so it contains an anisotropic vector w. Set $v = u_1 - \frac{1}{2}Q(w)u_2 + w$. Then $Q(v) = Q(u_1 - \frac{1}{2}Q(w)u_2) + Q(w) = -Q(w)(u,v) + Q(w) = 0$ so v is isotropic. Furthermore, $(u_1, v) = (u_1, u_1 - \frac{1}{2}Q(w)u_2) = -\frac{1}{2}Q(w)u_2$ and $(u_2, v) = (u_2, u_1 - \frac{1}{2}Q(w)u_2) = 1$. So if we take $\lambda_1 = -\frac{2}{Q(w)}$, $\lambda_2 = 1$ we have $(\lambda_i u_i, v) = 1$ as desired.

On the other hand, suppose that $(u_1, u_2) = 0$. Since (u_1, u_2) are linearly independent and V is nondegenerate, we can find vectors v_1, v_2 such that $(u_i, v_j) = \delta_{i,j}$. Then if $v' = v_1 + v_2$, $(u_i, v') = 1$. We still need to make v' isotropic; we do that by setting $v = v' - au_1$ so that $Q(v) = Q(v') - 2a$ which can be set to zero by choosing $a = Q(v')/2$.

(3) Suppose that (u_i, v_i) are two hyperbolic pairs. If u_1 and u_2 are linearly independent, then by (2) we can find v, λ_i such that $(\lambda_i u_i, v)$ are hyperbolic pairs. Then by (1) there is a map $\sigma \in A_{v_1}$ sending $\langle u_1\rangle$ into $\langle u_2\rangle$, so that $u_1\sigma = cu_2$. Then $(u_1\sigma, v_1\sigma) = (cu_2, v_1\sigma)$ and (u_2, v_2) are both hyperbolic pairs. So again applying (1), we can find $\tau \in A_{u_2}$ mapping v_1 to v_2; then $(u_1, v_1) \xrightarrow{\sigma} (cu_2, v_1) \xrightarrow{\tau} (cu_2, v_2)$. Now by orthogonality, $(u_1, v_1) = c(u_2, v_2) \Rightarrow c = 1$ and $\sigma\tau$ is the desired transformation. If instead u_1 and u_2 are linearly dependent, we can use (1) to send (u_1, v_1) to a hyperbolic pair (u', v') where u' is linearly independent of u_2. Then we have reduced to the case we solved above. □

Before we prove our next proposition on the commutators of $O(V)$ and $SO(V)$, we make two useful observations that will help in the proof.

Lemma 5.9 (1) The square of any orthogonal transformation α is in $O(V)'$. (2) When $\dim(V) \geq 3$, $O(V)' = SO(V)'$

Proof: (1) Since $O(V)$ is generated by symmetries, $\alpha = \sigma_1 \cdots \sigma_n$. Then $\alpha^2 = \sigma_1 \cdots \sigma_n \sigma_1 \cdots \sigma_n$. If we are willing to absorb a commutator, we can change the order of any two terms, since in any group $yx = (xx^{-1})yx(y^{-1}y) = x(x^{-1}yxy^{-1})y = x[x,y]y$ Thus $\alpha^2 \equiv \sigma_1^2 \cdots \sigma_n^2 \equiv 1 \pmod{O(V)'}$. (2) We use a similar argument here. Obviously $SO(V)' \subset O(V)'$. On the other hand, suppose that σ_1 and σ_2 are symmetries. Since they both fix $n-1$ dimensional spaces and $n \geq 3$, both σ_1 and σ_2 must fix some common nonzero vector v. Let τ be the reflection that inverts v, so τ commutes with σ_i. Then the commutator $[\sigma_1, \sigma_2] = \sigma_1\sigma_2\sigma_1\sigma_2 = (\sigma_1\tau)(\sigma_2\tau)(\tau\sigma_1)(\tau\sigma_2) = [\tau\sigma_1, \tau\sigma_2]$ is also in $SO(V)'$ because $\det(\tau\sigma_i) = 1$. So given any commutator in $O(V)'$, we can reorder the symmetries in it while changing it by a factor in $SO(V)'$. Now by the same trick we saw in (1), for any $\rho_1, \rho_2 \in O(V)$, $[\rho_1, \rho_2] \equiv 1 \pmod{SO(V)'}$ as desired. □

Let Ω be the subgroup generated by the A_u over isotropic vectors u. We now show that Ω is usually the commutator subgroup of $O(V)$, and is thus a perfect group.

Theorem 5.10 Let V be a regular quadratic space of dimension ≥ 3 and Witt index $\nu > 0$. Then $\Omega = \Omega' = O(V)'$ except when n = 4 and $\nu = 2$, or $n = 3$ and $|F| = 3$.

Proof: We start by showing that $\Omega \supset O(V)'$. Because the Witt index is positive, we can fix some hyperbolic pair (u, v) and take O_H to be $O(\langle u, v\rangle)$, $W = \langle u, v\rangle^\perp$. We claim that every symmetry is conjugate to a symmetry in O_H under the action of Ω. Suppose x is anisotropic. Then the vector $y = u + \frac{1}{2}Q(x)v$ has norm $Q(y) = Q(x)(u, v) = Q(x)$, so since $O(V)$ is transitive on vectors of the same length [Lemma 5.2], there is some $\rho \in O(V)$ sending $y \to x$. But now by Lemma 5.8 there is some $\alpha \in \Omega$ mapping the hyperbolic pairs $(u\rho, v\rho) \xrightarrow{\alpha} (u, v)$ as shown. Now since $y \in \langle u, v\rangle$, $x = y\rho \in \langle u\rho, v\rho\rangle \Rightarrow x\alpha = y\rho\alpha \in \langle u, v\rangle$. Then we have the conjugate of σ_x by a member of Ω in O_H as promised since $\alpha^{-1}\sigma_x\alpha = \sigma_{x\alpha}$ and $x\alpha \in \langle u, v\rangle$.

$O(V)$ is generated by symmetries and every symmetry has determinant -1, so every $\rho \in SO(V)$ can be written as the product of an even number of symmetries, $\rho = \sigma_1 \cdots \sigma_{2r}$. By the first part $\sigma_i = \omega_i^{-1}\tau_i\omega_i$ where τ_i is a symmetry in O_H and $\omega_i \in \Omega$, so $\rho = (\omega_1^{-1}\tau_1\omega_1)\cdots(\omega_{2r}^{-1}\tau_{2r}\omega_{2r})$. But Ω is a normal subgroup of $O(V)$ [Lemma 5.7] so $\tau\omega = \tilde{\omega}\tau$ where $\tilde{\omega} \in \Omega$. Thus we can pass all the τ's to the right and rewrite this as $\rho = \omega\tau_1 \cdots \tau_{2r}$. We conclude that $SO(V) \subset \Omega SO_H$. $\Omega \subset SO(V)$, so taking quotients, we have $SO(V)/\Omega \cong SO_H/SO_H \cap \Omega$. But when we calculated the orthogonal group of a hyperbolic plane, we saw that SO_H was isomorphic to F^*; in particular, it was Abelian. Now by Lemma 3.5, G/N is Abelian if and only if $N \supset G'$, so we conclude that $\Omega \supset SO(V)'$.

To finish the proof, we show that Ω is perfect, for then we have $\Omega = \Omega' = SO(V)'$. Ω is generated by maps $\rho_{u,w}$ so it is suffifficient to show that all such maps are in Ω'. Assume w.l.o.g. that u, v, W, O_H are the ones we have already chosen. The commutator $[\tau, \lambda_a] = \tau\lambda_{a^{-1}}\tau\lambda_a = \lambda_a\lambda_a = \lambda_{a^2}$ is in Ω since we have already shown that $\Omega \supset O(V)'$. Then the commutator

$$\lambda_{a^2}^{-1}\rho_{u,w}{}^{-1}\lambda_{a^2}\rho_{u,w} = \rho_{a^2u,w}{}^{-1}\rho_{u,w} = \rho_{u,-a^2w}\rho_{u,w} = \rho_{u,(1-a^2)u}$$

is in Ω'. Now when $|F| > 3$, we can always find $a \neq 0$ with $a^2 \neq 1$; then scaling the original w we chose by $(1 - a^2)^{-1}$ we have $\rho_{u,w} \in \Omega'$ as claimed.

We must handle the case where $|F| = 3$ separately. Here either $n \geq 4$ or $n = 4$ and the Witt index is 1. So $\dim(W) \geq 2$ and we can pick an orthogonal basis $(w, w_2, \ldots, w_n)$ for W. If $Q(w_1) = Q(w_2)$ then the map α which is $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ on the first two coordinates and the identity on the others is an isometry. Furthermore, $\alpha^2 \in O(V)'$ by Lemma 5.9, and $w\alpha^2 = w$. Then we have the commutator $\rho_{u,w}{}^{-1}\alpha^{-2}\rho_{u,w}\alpha^2 = \rho_{u,-w}\rho_{u,-w} = \rho_{u,-2w}$ and $\rho_{u,w} \in \Omega'$ as claimed. Finally, then, let us show why we can find w_2 with length equal to that of w. The only possibilities for $Q(w)$ are ± 1. If $n = 4$, the Witt index is 1 and $\langle u, v\rangle$ is already an isotropic space. So W cannot contain any isotropic vectors z or $\langle u, z\rangle$ would be a 2-dimensional totally isotropic space. Thus the two basis vectors must have the same length (either 1 or -1) so that $Q(w_1 + w_2) = Q(w_1) + Q(w_2) \neq 0$. When $n \geq 5$, $W \cap w^\perp$ is a nondegenerate space of dimension at least 2, so by Proposition 2.13 any quadratic form on it must be universal. In particular, W must contain some w' which is orthogonal to w and has equal length. Thus in all cases we have shown an orthogonal basis

for W of the desired form. □

Corollary 5.11 For any isotropic $u \in V$, A_u and its conjugates generate Ω.

Proof: Since Ω is generated by A_v over all v, it is sufficient to show that the conjugates of A_u for some particular u include each A_v. Given any isotropic vector v and $\rho_{v,w} \in A_v$, find $\sigma \in SO(V)$ that sends $u \to v$ by the transitivity of Ω on hyperbolic pairs [Lemma 5.8]. There is some y such that (v, y) is a hyperbolic plane and $w \in \langle v, y \rangle^{\perp}$, so we can take $y' = y\sigma^{-1}$ and (u, y') will be a hyperbolic plane since $Q(y') = Q(y) = 0$ and $(u, y') = (v\sigma^{-1}, y\sigma^{-1}) = (v, y) = 1$. Thus we can choose $w' = w\sigma^{-1}$ and $\rho_{u,w'}$ will be in A_u as w' is orthogonal to both u and y'. Then the conjugate $\sigma^{-1}\rho_{u,w'}\sigma = \rho_{u\sigma,w'\sigma} = \rho_{v,w}$ as desired. □

The pieces are now in place to prove the main result: the quotient $P\Omega$ of Ω by its center Z is a simple group.

Theorem 5.12 Let V be a regular quadratic space of dimension $n \geq 3$ and of positive Witt index ν. Then $P\Omega$ is simple unless $n = 4$, $\nu = 2$ or $n = 3$, $|F| = 3$.

Proof: Consider the action of $P\Omega$ on the quadric cone of null vectors in the projective space, $N = \{\langle x \rangle \in \mathbb{P}(V) : Q(x) = 0\}$. This is clearly a faithful group action because the orthogonal group preserves length and we have quotiented out the only transformations that act trivially. In Lemma 5.7, we showed that A_u is normal in the stabilizer $\mathrm{Stab}(u)$. And in the above theorem, we just proved that Ω (and hence its quotient $P\Omega$) is perfect; as a corollary we saw that A_u and its conjugates generate Ω. So by our simplicitity criterion Lemma 3.11 it remains only to show that $P\Omega$ acts primitively on N.

In the transitivity lemma [Lemma 5.8] we saw that Ω acts transitively on N. So suppose that S is a subset of N that is compatible with the action of G and that $|S| > 1$. We show that $S = N$. If $\nu = 1$, then every pair x, y of linearly independent isotropic vectors in V has $(x, y) \neq 0$. Now since we are working with projective spaces, if $\langle x \rangle \neq \langle y \rangle$, then w.l.o.g. $(x, y) = 1$. In this case by the transitivity of Ω on hyperbolic pairs, we have G acting two-fold transitively on N, so it acts primitively as well [Corollary 3.9]. Thus we assume henceforth that $\nu \geq 2$. Since the Witt Index is at most $n/2$ by Proposition 2.3 and we have excluded the case $n = 4, \nu = 2$ we can take $n \geq 5$. We are given two projective points $\langle x_1 \rangle$ and $\langle x_2 \rangle$ in S. If $(x_1, x_2) = 0$, then by the argument used in Theorem 2.17 we can find (y_1, y_2) such that (x_i, y_i) are orthogonal hyperbolic pairs. Now if we let $W = \langle x_2, y_2 \rangle^{\perp}$, by the transitivity lemma we can find $\alpha \in \Omega$ such that α fixes x_2, y_2 while sending $x_1 \to y_1$. Then S meets $S\alpha$ at $\langle x \rangle$ so $S = S\alpha$, and we conclude that $\langle y_1 \rangle \in S$. But now if $\langle z \rangle$ is any point other than $\langle x_1 \rangle$, we can find a vector v such that (x_1, v) and (z, v) are hyperbolic pairs; here we have set the factors λ_i to 1 since we are working on projective space and can choose whatever representatives we like. Now we see that $\langle z \rangle \in S$ in two steps. First take $\beta \in \Omega$ so $(x_1, y_1) \xrightarrow{\beta} (x_1, v)$; S meets $S\beta$ at $\langle x_1 \rangle \Rightarrow \langle v \rangle \in S$. Now take γ so $(x_1, v) \xrightarrow{\gamma} (z, v)$; so we have $\langle z \rangle \in S$. Since $\langle z \rangle$ was arbitrary, $S = N$ as claimed.

We have thus reduced to the case where our two given points x_1, x_2 are a hyperbolic pair. Given $\langle z \rangle \neq \langle x_1 \rangle$, find v making (x_i, v) hyperbolic pairs and $\beta \in \Omega$ mapping $(x_1, x_2) \to (x_1, v)$. Then $S\beta = S$ and $\langle v \rangle \in S$. Now when we take γ which sends $(x_1, v) \to (z, v)$, $S\gamma$ meets S at $\langle v \rangle$ and $\langle z \rangle \in S$ as claimed. Thus the action of $P\Omega$ on N is indeed primitive, and by the simplicity criterion it follows that $P\Omega$ is simple. □

We remark that over finite fields, the condition that the Witt index ν is at least 1 is always satisfied when $n \geq 1$: if v and w are orthogonal vectors of length a and b in V, $xv + yw$ will be isotropic when $ax^2 + by^2$ is zero. But by Proposition 2.13, every quadratic form of rank 2 represents zero in a finite field.

We conclude this section by computing the order of the orthogonal group. We start with some preliminary lemmas on the number of solutions to various polynomials over finite fields. Define the *quadratic symbol* of a in the field of order q, written $\left(\frac{a}{q}\right)$, to be 1 if a is a square, -1 if a is a non-square, and zero if $a = 0$.

Lemma 5.13 The equation $ax^2 + by^2 = c$ has $q - \nu$ solutions if $c \neq 0$ and $q + (q-1)\nu$ solutions when $c = 0$, where $\nu = \left(\frac{-ab}{q}\right)$ and $a \neq 0$.

Proof: First change variables to $x' = x/a$ so the equation is $x'^2 + aby^2 = ac$; since this changes neither the number of solutions that exist nor the number produced by our formula, we can assume w.l.o.g. that we can write the equation as $x^2 + aby^2 = ac$. If $-ab = t^2$ is a square, then our equation becomes $(x+ty)(x-ty) = ac$. If we write $u = x+ty$, $v = x-ty$, we have $uv = ac$. This obviously has $q-1$ solutions when $c \neq 0$: given any nonzero u, only $v = cu^{-1}$ works. If $c = 0$, the formula is again correct: $(u, 0)$ and $(0, v)$ are solutions for all values of u and v, giving $2q - 1$ solutions. So suppose insead that $-a$ is not a square. Then by adjoining a square-root t of $-a$ we get a finite field E containing F of order q^2. In E the equation factors as $(x + ty)(x - ty) = (x + ty)\overline{(x + ty)} = (x + ty)^{q+1} = ac$. This equation has $q + 1$ roots in F by Lemma 2.15 when $c \neq 0$. When $c = 0$, $x + ty = 0$ and the unique solution with x and y in F is $x = y = 0$. □

Corollary 5.14 The number of solutions $(x_1, \ldots, x_{2n})$ to $\sum_{i=1}^{2n} a_i x_i^2 = c$ is $q^{2n-1} - \nu q^{n-1}$ if $c \neq 0$ and $q^{2n-1} + \nu(q^n - q^{n-1})$ if $c = 0$, where ν is the quadratic symbol of $(-1)^n a_1 \cdots a_{2n}$.

Proof: This is true for $n = 1$ by the previous Lemma. Now the proof follows by induction. Solving the given equation is equivalent to simultaneously solving $\sum_{i=3}^{2n} a_i x_i^2 = c - b$ and $a_1 x_1^2 + a_2 x_2^2 = b$. For each of the $(q-2)$ nonzero pairs (c, b) we get $q^{2n-3} - \mu q^{n-2}$ and $q - \lambda$ solutions for the former and latter equations, where λ and μ are the quadratic symbols for $-a_1 a_2$ and $(-1)^{n-1} a_3 \cdots a_n$ respectively. When $c = b$, we have $q + (q-1)\nu$ and $q^{2n-3} - \mu q^{n-2}$ solutions for the two equations, while for $b = 0$, we have $q - \lambda$ and $q^{2n-3} + \mu(q^{n-1} - q^{n-2})$.

So adding these all up we find a total of

$$\begin{aligned}(q-2)[(q-\lambda)(q^{2n-3}+\mu q^{m-2})] &+ [q+(q-1)\lambda][q^{2n-3}-\mu q^{m-2}] \\ &+ (q-\lambda)[q^{2n-3}+\mu(q^{n-1}-q^{n-2})]\end{aligned}$$

solutions. Simplifying this and using the fact that the quadratic character is multilicative so $\lambda\mu = \nu$, we find a total of $q^{n-1}(q^n - \nu)$ solutions as claimed. The argument when $c = 0$ is exactly the same. □.

Finally, we compute the number of ways to represent c as the sum of an odd number of squares.

Corollary 5.15 The number of solutions $(x_1, \ldots, x_{2n})$ to $\sum_{i=1}^{2n+1} a_i x_i^2 = c$ is $q^{2n} + \omega q^n$ where ω is the quadratic symbol of $(-1)^n a_1 \cdots a_{2n+1} c$.

Proof: The idea of the proof is to apply the same trick we did above, this time breaking the sum up into the two pieces $\sum_{i=1}^{2n} a_i x_i^2 = c - b$ and $a_{n+1}x_{n+1}^2 = b$. Then it is a routine computation. □

Now we have the tools at our disposal to find the size of the orthogonal groups.

Proposition 5.16 The sizes of the special orthogonal groups over an even dimensional space are

$$\begin{aligned}|SO_{2n}^+(q)| &= (q^{2n-1} - \nu q^{n-1}) \cdot |SO_{2n-1}(q)| \\ |SO_{2n}^-(q)| &= (q^{2n-1} + \nu q^{n-1}) \cdot |SO_{2n-1}(q)|\end{aligned}$$

where ν is the quadratic symbol of $(-1)^n$.

Proof: $SO_{2n}^+(q)$ is transitive on the set of unit vectors in $2n$-dimensional space, while the stabilizer of any unit vector is isomorphic to $SO_{2n-1}(q)$. So if we let Γ_n be the set of unit vectors in n dimensional space, by the orbit- stabilizer theorem we have $|SO_{2n}^+(q)| = |\Gamma_{2n}| \cdot |SO_{2n-1}(q)|$. Let $(e_1, \ldots, e_{2n})$ be an orthonormal basis for V. The vector $\sum_{i=1}^{2n} a_i e_i$ has length 1 when $\sum_{i=1}^{2n} a_i^2 = 1$. By Lemma 5.14 there are $q^{2n-1} - \nu q^{n-1} = |\Gamma_{2n}|$ solutions to this equation. In the case of $SO_{2n-1}^-(q)$, the argument is exactly the same, except that the length of a vector is $\sum_{i=1}^{2n-1} a_i^2 + \lambda a_{2n}^2$ where λ is a non-square. So the quadratic symbol ν is reversed here, giving the second formula. □

Now we compute the size of $SO_{2n+1}(q)$ in terms of $SO_{2n}^+(q)$ to develop a formula for $|SO_{2n+1}(q)|$.

Proposition 5.17 The size of the special orthogonal group $SO_{2n+1}(q)$ is $\prod_{k=1}^{n} (q^{2k} - 1)q^{2k-1}$.

Proof: The proof is by induction. When $n = 0$, the result is trivial since $|SO_1(q)| = 1$. Now by the same orbit-stabilizer argument used above, we have $|SO_{2n+1}(q)| = |\Gamma_{2n+1}| \cdot |SO_{2n}^+(q)| = |\Gamma_{2n+1}| \cdot (q^{2n} - \nu q^{n-1}) \cdot |SO_{2n-1}(q)|$. We know that $|\Gamma_{2n+1}|$ is the number of solutions of $\sum_{i=1}^{2n+1} x_i^2$ which is $q^{2n} + \omega q^n$ by

our Lemma. Now ω and ν are both equal to the quadratic symbol of $(-1)^n$ which is ± 1, so we have $(q^{2n}+\omega q^n)(q^{2n-1}-\nu q^{n-1}) = q(q^{2n-1}+q^{n-1})(q^{2n-1}-q^{n-1}) = q^{2n-1}(q^{2n}-1)$. The result follows immediately by induction. □

If we substitute this into the formulas for $|SO_{2n}(q)|$ we can state the following:

Theorem 5.18 The order of the special orthogonal group over an odd dimensional space is

$$|SO_n(q)| = (q^{n-1}-1)q^{n-2}(q^{n-3}-1)q^{n-4}\cdots(q^2-1)q$$

while over an even-dimensional space

$$|SO_{2m}(q)| = (q^{2m-1}-\varepsilon q^{m-1})(q^{2m-2}-1)q^{2m-3}\cdots(q^2-1)q$$

where ε is the quadratic symbol of $(-1)^m\Delta$ and Δ is the determinant of the quadratic form. □

6 The Unitary Group $U_n(F)$

Let F be a quadratic extension of E and θ the nontrivial automorphism of F fixing E. We have defined the unitary group $U(V)$ of a unitary space V of dimension n over F to be the group of isometries of V. As long as F has the property that every member of E takes the form $a\bar{a}$ for some $a \in F$, we showed in Theorem 2.16 that all unitary spaces of dimension n were equivalent to the standard unitary space with an orthonormal basis $(e_1, \ldots, e_n)$. So whenever F has this property, the notation $U_n(F)$ is unambiguous. In particular, this is true when F is a finite field of square order, which is the case which concerns us here. For clarity, we will write the unitary group of the finite field of order q^2 as $U_n(q^2)$. We can think of the unitary group concretely as a matrix group: $U_n(F) = \{A : AA^* = I\}$ where we have used the shorthand A^* for the conjugate-transpose $A^{T\theta}$ of A. The *special unitary group* $SU_n(F)$ is the subgroup of $U_n(F)$ consisting of the transformations of determinant 1, while the *projective special unitary group* $PSU_n(F)$ is the quotient of $U_n(F)$ modulo its center Z of homotheties. Our major goal in this section is to show that the projective special unitary group is almost always simple when $n \geq 2$.

Before we begin, let us make a few simple remarks about the structure of F and its subfield E. E is a finite field of order $q = p^r$ and F is a quadratic extension of E, so F has order q^2. The involution θ sends $x \mapsto x^q$, but it is usually more productive to think of it as an involution analagous to complex conjugation. The subfield E plays the role of the reals in $\mathbb{C}$, and E is precisely the subfield fixed by θ. In exploring unitary groups, we will also often encounter the counterparts of pure imaginary numbers, namely field elements a such that $a + \bar{a} = 0$. Sometimes we will write field elements in the form $a + bt$ where $a, b \in E$, in the spirit of the notation $z = a + bi$. When we do this, we have written $F = E[t]$ where we suppose w.l.o.g. that $t^2 = \lambda$ is in E. Since θ must

permute the roots of the polynomial $x^2 - \lambda = 0$ and it cannot fix $t \notin E$, we have $t\theta = -t$. So t is the analogue of the imaginary unit i, and "pure imaginary number" in F are its multiples bt where $b \in E$. We start by calculating the order of $SU_n(q^2)$.

Proposition 6.1 The order of the group $SU_n(q^2)$ is

$$(q^n - (-1)^n)q^{n-1}(q^{n-1} - (-1)^{n-1})q^{n-2} \cdots (q^2 - 1)1 = \prod_{k=2}^{n} q^{2k-1} + (-q)^{k-1}.$$

Proof: $SU_n(q^2)$ is transitive on vectors of unit length: for if x_1 and y_1 have length 1, they can both be completed to orthonormal bases $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$. Then the map sending x_i to y_i is unitary. So let $(e_1, \ldots, e_n)$ be an orthonormal basis for V, and let Γ_n be the set of unit vectors in V. The stabilizer of e_n is equal to the full special unitary group on the span of $e_1, \ldots, e_{n-1}$, so applying the orbit-stabilizer theorem we conclude that $|SU_n(q^2)| = |\Gamma_n| \cdot |SU_{n-1}(q^2)|$.

For $n = 1$, this formula is trivially correct, as only I has determinant 1. So to complete an inductive proof we must show that $|\Gamma_n| = q^{2n-1} + (-q)^{n-1}$. This is straightforward. The vector $\sum a_i e_i$ has length one if and only if $\sum_{i=1}^{n} a_i^{q+1} = 1$. The polynomial $x^{q+1} = c$ has $q+1$ roots in F as long as $c \in E$ by Lemma 2.15. If the sum $\sum_{i=1}^{n-1} a_i^{q+1} = \alpha$ is different from 1, then the $q+1$ distinct roots to $x^{q+1} = 1 - \alpha$ can all be chosen for a_n (α is a sum of norms so it is in E). On the other hand, if $\alpha = 1$, then we have only one choice, $a_n = 0$. Thus we get the recursive formula

$$|\Gamma_n| = \left((q^2)^{n-1} - |\Gamma_{n-1}|\right)(q+1) + |\Gamma_{n-1}| = q^{2n-1} + q^{2n-2} - q|\Gamma_{n-1}|.$$

We have already shown that $|\Gamma_1| = (q+1)$, so it immediately follows by induction that $|\Gamma_n| = q^{2n-1} + (-q)^{n-1}$ as claimed. □

With the aid of this formula, we can determine the structure of $SU_2(q^2)$.

Proposition 6.2 The special unitary group $SU_2(q^2)$ is isomorphic to the special linear group $SL_2(q)$.

Proof: Let V be the unitary space written as a hyperbolic plane, so $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. With t and λ defined as above, so $F = E[t]$ where $t^2 = \lambda \in E$, consider the map $\phi : SL_2(E) \to SU_2(F)$ defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \phi = \begin{pmatrix} a & bt/\lambda \\ ct & d \end{pmatrix}$$

ϕ preserves determinants as $\det(A\phi) = ad - (bt\lambda)(ct) = ad - bc$; and we verify that the image of A is unitary by computing $(A\phi)J(A\phi)^*$

$$\begin{pmatrix} a & bt/\lambda \\ ct & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & bt/\lambda \\ ct & d \end{pmatrix}^*$$

$$= \begin{pmatrix} bt/\lambda & a \\ d & bt\lambda \end{pmatrix} \begin{pmatrix} a & -ct \\ -bt/\lambda & d \end{pmatrix} = \begin{pmatrix} 0 & ad - bc \\ ad - bc & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

so ϕ does indeed send $SL_2(E)$ to $SU_2(F)$. ϕ is also a homomorphism, since

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\phi\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}\phi = \begin{pmatrix} a_1 & b_1 t/\lambda \\ c_1 t & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 t/\lambda \\ c_2 t & d_2 \end{pmatrix}$$

$$= \begin{pmatrix} a_1a_2 + b_1c_2 & (a_1b_2 + b_1d_2)t/\lambda \\ (c_1a_2 + d_1c_2)t & c_1b_2 + d_1d_2 \end{pmatrix} = \left[\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}\right]\phi\,.$$

ϕ is obviously injective, because its kernel is I. We finish the proof by showing that ϕ is surjective. But this is easily accomplished with a counting argument. By the previous Proposition, the order of $SU_2(q^2)$ is $q^3 - q$. But this is equal to the order of $SL_2(q)$ by Proposition 3.2, so we conclude that ϕ is an isomorphism. □

As a corollary we see that $PSU_2(q^2)$ is simple when $q > 3$. Since we understand $PSU_2(q^2)$, we will assume henceforth that $n > 2$. We now consider the unitary transvections. Suppose that u is an isotropic vector in V and $a \in E$. We define the unitary transvection $\tau_{u,a}$ by $x\tau_{u,a} = x + at(x,u)u$. Observe that the coefficient at in front of $(x,u)u$ is "pure imaginary;" this is important, because if $a + \bar{a} \neq 0$ this map will not be unitary.

Lemma 6.3 The map $\tau_{u,a}$ is unitary, and every unitary transvection takes the form $\tau_{u,a}$ for some isotropic u and $a \in E$. Furthermore, if σ is unitary, the conjugate $\sigma^{-1}\tau_{u,a}\sigma = \tau_{u\sigma,a}$, and $\tau_{cu,a} = \tau_{u,c\bar{c}a}$.

Proof: $\tau_{u,a}$ is unitary, since for any $x, y \in V$ we have $(x\tau_{u,a}, y\tau_{u,a}) = (x + at(x,u)u, y + at(y,u)u) = (x,y) + at(x,u)(u,y) - at(u,y)(x,u) = (x,y)$. Here we have used that fact that $\overline{(s,t)} = (t,s)$. On the other hand, suppose that T is a unitary transvection along u, so $xT = x + \lambda(x)u$. First, we observe that u is isotropic: pick some v with $\lambda(v) = 1$. Then $(uT, vT) = (u, v + u) = (u,v) + (u,u) = (u,v)$ since T is unitary, so $(u,u) = 0$. The proof that $\lambda(x) = c(x,u)$ for some constant is exactly the same as it was in the symplectic case [Lemma 4.3]. Finally, c is pure imaginary because we if we take some v with $(u,v) = 1$, we have $(v,v) = (v + cu, v + cu) = (v,v) + c + \bar{c} \Rightarrow c + \bar{c} = 0$. We can compute the next two formulas directly: $\sigma^{-1}\tau_{u,a}\sigma = \tau_{u\sigma,a}$ since $(x\sigma^{-1} + a(x\sigma^{-1}, u)u)\sigma = x + a(x, u\sigma)u\sigma = x\tau_{u\sigma,a}$. And $x\tau_{cu,a} = x + at(x,cu)cu = x + ac\bar{c}t(x,u)u = x\tau_{u,c\bar{c}a}$. □

To show that the unitary group is perfect, we use the same strategy we have used before: show that it is generated by transvections, then show that every transvection is a commutator. But first we need a small lemma:

Lemma 6.4 Let G act transitively on S, $p \in S$ be a point, and H a subgroup of G. Then H is transitive on S if and only if $G = \mathrm{Stab}(p)G$.

Proof: If H is transitive on S, by the orbit-stabilizer theorem $|G| = |\mathrm{Stab}(p)| \cdot |S|$ and $|H| = |\mathrm{Stab}(p) \cap H| \cdot |S|$. Now in general, when H and K are subgroups, $|KH| = |K| \cdot |H|/|K \cap H|$. So here we see that $|\mathrm{Stab}(p)H| = |\mathrm{Stab}(p)| \cdot |H|/|\mathrm{Stab}(p) \cap H| = \big(|\mathrm{Stab}(p)| \cdot |H|\big)/\big(|H|/|S|\big) = |\mathrm{Stab}(p)| \cdot |S| = |G|$. Thus $\mathrm{Stab}(p)H = G$. Conversely, if $G = \mathrm{Stab}(p)H$, then suppose that $q = pg$ for

some $g \in G$. Since $G = \mathrm{Stab}(p)H$, $g = sh$ where s fixes p and $h \in H$. Then $q = p(sh) = ph$, and H is transitive on S as claimed. □

Proposition 6.5 When $n \geq 2$, the special unitary group $SU_n(q^2)$ is generated by transvections unless $|F| = 4$.

Proof: Let Γ be the set of unit vectors in V, $\Gamma = \{v \in V : (v,v) = 1\}$ and T be the subgroup generated by unitary transvections. We claim that T acts transitively on Γ. The claim is enough to prove the proposition since if $\mathrm{Stab}(e_1) = SU_{n-1}(q)$ is in T and T is transitive on the span of e_i for $i > 1$, then by the previous lemma $G = \mathrm{Stab}(e_1)T$. Now the result follows immediately by induction since T contains $SU_{n-1}(q)$. Let us now prove the claim. Suppose that we are given two vectors x, y. If $W = \langle x, y\rangle$ is a nondegenerate plane, then the claim is true because transvections generate SL_2 and our isomorphism sends the elementary matrix B_{ij} to a unitary transvection in SU_2. And SU_2 certainly acts transitively on Γ, since if $y = ax + by$, the matrix $A = \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix}$ sending x to y will be special unitary as $a\bar{a} + b\bar{b} = (y,y) = 1$. So suppose that $0 \neq u \in \mathrm{Rad}(W)$; it is sufficient to show that we can find $z \in \Gamma$ with $\langle x, z\rangle$ and $\langle y, z\rangle$ nondegenerate. If $n > 3$ this is easy since we can just choose $z \in u^{\perp}$ with $\langle x, z\rangle$ nondegenerate. So assume that $n = 3$ and let (u, v) be a hyperbolic basis for $y^{\perp}$. Choose $x = y + u$ so $x^{\perp} = \langle u, y - v\rangle$. If $z = au - v + y$, $\langle y, z\rangle \cap y^{\perp} = \langle au - v\rangle$. So it is enough to show that we can choose a so z and $au - v$ are nonsingular, i.e. such that $a + \bar{a} \neq 0$ and $a + \bar{a} \neq 1$. The set of a satisfying each of these equations is a coset of E in F, and there are $|E|$ such cosets. Since $|E| > 2$, we can pick a different coset which gives us the desired a. □

We remark that in fact, this result is true except when $n = 3$ and $|F| = 4$, but a separate proof is required. We are now prepared to show that $SU_n(q)$ is perfect.

Theorem 6.6 The special unitary group $SU_n(q^2)$ is perfect unless $n = 2$ and $q \leq 3$, or $n = 3$ and $q = 2$.

Proof: When $n = 2$, we have shown that $SU_2(q^2) \cong SL_2(q)$, and $SL_2(q)$ is perfect when $q > 3$ by Theorem 3.6. So suppose that $n > 2$; then by the previous Proposition it is sufficient to show that every transvection is a commutator.

The proof is almost exactly the same as the one given for the symplectic group in Theorem 4.7. So let $\sigma u = \alpha u$. In order to generate $\tau_{u,a}$ we take the commutator $[\sigma, \tau_{u,-b}] = \sigma^{-1}\tau_{u,b}\sigma\tau_{u,-b} = \tau_{\alpha u,b}\tau_{u,-b} = \tau_{u,(1-\alpha^2)b}$. When $|F| > 3$, we can find $\alpha \neq 0$ such that $(1 - \alpha^2) \neq 0$; then we can choose $b = a(1 - \alpha^2)^{-1}$. Note that α can be any constant in F, not just E, so we don't need to consider the case where $|F| < 3$ since $|F|$ is a square. Thus every transvection is a commutator, and it follows that $SU_n(q^2)$ is perfect. □

The next step in applying our simplicity criterion is to exhibit an Abelian normal subgroup A of $\mathrm{Stab}(u)$ such that A and its conjugates generate $SU_n(q)$. Of course we choose $A = A_u$, the subgroup of unitary transvections along u.

A is an Abelian subgroup because $\tau_{u,a}\tau_{u,b} = \tau_{u,a+b}$. And A is normal since if σ fixes $\langle u \rangle$, $\sigma^{-1}\tau_{u,a}\sigma = \tau_{u\sigma,a} = \tau_{cu,a} = \tau_{u,c\bar{c}a} \in A_u$. To show that A and its conjugates generate G, it is sufficient to show that every unitary transvection $\tau_{v,b}$ is conjugate to some $\tau_{u,a} \in A$. We claim that $SU_n(F)$ acts transitively on the projective space $\mathbb{P}^{n-1}(F)$. Then we can find σ sending u to cv, and $\sigma^{-1}\tau_{u,c}\sigma = \tau_{cv,a} = \tau_{v,c\bar{c}a}$ is our desired map when we choose $a = b/c\bar{c}$. Now let us prove the claim:

Lemma 6.7 When $n > 2$, $SU_n(F)$ is transitive on the the cone of null vectors in projective space, $N = \{\langle x \rangle : (x,x) = 0\}$. In fact, $SU_n(F)$ is transitive on the hyperbolic pairs in projective space.

Proof: Let (u,v) and (u',v') be hyperbolic pairs. Let $U = \langle u,v \rangle$ be the hyperbolic plane spanned by u and v, and let W be its orthogonal complement. By the equivalence of unitary forms [Theorem 2.16] we can find an orthonormal basis $w_3, \ldots, w_n$ for W. Similarly we can take $U' = \langle u',v' \rangle$ with orthogonal complement W' equipped with an orthonormal basis (w_i'). Then the map A sending $u \to u'$, $v \to v'$ and $w_i \to w_i'$ is unitary because the matrix J for the form is the same in the basis $(u,v,w_3,\ldots,w_n)$ as it is in the basis $(u',v',w_3',\ldots,w_n')$. Now every unitary transformation has determinant of norm 1: since $AA^* = I$, it follows that $\det(A)\overline{\det(A)} = 1$. So if the determinant Δ of A is not 1, we can make A a special unitary transformation by sending w_n to $\Delta^{-1}w_n$. Then the new map certainly has determinant 1, and it is still length-preserving because $(Aw_n, Aw_n) = (1/\Delta\bar{\Delta})(w_n,w_n) = (w_n,w_n)$. So $SU_n(F)$ is transitive on hyperbolic pairs as claimed. □

We are now ready to prove the simplicity of $PSU_n(q^2)$.

Theorem 6.8 The projective special unitary group $PSU_n(q^2)$ is simple except when $n = 2$ and $q \leq 3$, or $n = 3, q = 2^r$.

Proof: We have already shown that $PSU_2(q^2) \cong SL_2(q)$. So the result is immediate for $n = 2$. We have met all the hypotheses of our simplicity criterion when $n > 2$ save that G acts primitively on the cone of null vectors. So suppose $\langle x \rangle$ and $\langle y \rangle$ are distinct isotropic lines in S. We will show that any third isotropic line $\langle z \rangle$ is also in S. We first handle the case where $(x,y) \neq 0$, so w.l.o.g. $(x,y) = 1$. Because G is transitive on hyperbolic pairs, any z with (x,z) or (y,z) different from zero is in S. Say $(x,z) = 1$ w.l.o.g. Then there is a special unitary map A sending (x,y) to (x,z). A fixes x, so $z = Ay$ is in S also.

On the other hand, suppose that $(x,z) = (y,z) = 0$. We can assume then that z is not in the span of x,y. Find some vector u orthogonal to x and y with $(u,z) = 1$. Then in the basis (x,y,z,u) we have

$$J = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and $A \in SU_n$ since $AJA^* = J$ and $\det(A) = 1$. Observe that $Ax = x + z$ while A fixes y, so $x + z \in S$. Now the map B interchanging the two hyperbolic pairs

so $(x,y) \leftrightarrow (z,u)$ is obviously special unitary, and it fixes $x+z$. Therefore the image $z = Bx$ is in S as desired.

We are left with the final case that $(x,y) = 0$. But this is simple because by non-degeneracy we can find some z such that $(x,z) = 1$ and $(y,z) = 0$. Then z will be in S as well, because the transformation A interchanging x and z and reversing y is unitary:

$$J = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \qquad A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

A fixes $\langle y \rangle$ so $z = Ax$ is in S. Then S contains the hyperbolic pair (x,z) and we have reduced to the case considered above. Now since the action of G on N is primitive, it follows from the simplicity criterion that G is a simple group. □

We remark that even though we did not show it here, when q is a power of 2, the group $PSU_n(q)$ is in fact simple except when $n = 3$.

7 Exceptions and Coincidences

By an *exception* we mean a group that is not simple even though it is a member of a family that contains infinitely many simple groups. For example, $PSL_2(2)$ and $PSL_2(3)$ are exceptional groups. By a *coincidence* we mean an "unexpected" isomorphism that arises between two groups in the families we have studied. For example, $PSL_2(4)$ and $PSL_2(5)$ are both isomorphic to the alternating group A_5. In this section we explore some of these exceptions and coincidences and explain them where they are accessible.

Let us begin with $PSL_n(q)$. The two exceptions are $PSL_2(2)$ and $PSL_2(3)$. They can both be easily understood by considering the action on the projective line $\mathbb{P}^1(F)$. We remark that as we saw after Lemma 3.11, this action is always faithful, so there is an injective group homomorphism from $PSL_2(q)$ to the symmetric group S_{q+1}.

Proposition 7.1 $PSL_2(2) \cong S_3$ and $PSL_2(3) \cong A_4$.

Proof: Consider the action of $PSL_2(2)$ on the projective line over F_2. $PSL_2(2)$ has order $(2+1)(2)(2-1) = 6$ by Prop 3.2 so the homomorphism $PSL_2(2) \to S_3$ is in fact an isomorphism. Thus $PSL_2(2)$ is not simple, because A_3 is normal in S_3. Now consider the action of $PSL_2(3)$ on the projective line. This gives rise to an injective homomorphism to S_4. The order of $PSL_2(3)$ is 12, so its image is a subgroup of index 2 in S_4. In general, the only subgroup of index 2 in the symmetric group S_n is A_n, so $PSL_2(3) \cong A_4$. $PSL_2(3)$ is not simple, then, because the Klein four-group is a normal subgroup in A_4. □

We remark that we can use the same method to show that $PSL_2(4) \cong A_5$. The linear group again acts faithfully on a projective space of 5 elements, and its order is $(5)(4)(3) = \frac{1}{2}5!$, so the image in S_5 is A_5 as claimed. $PSL_2(5)$ is also isomorphic to A_5. This is harder to prove directly because the natural action

is on 6 elements; the easiest way to do it is to show that all simple groups of order 60 are isomorphic. There are a few other isomorphisms which space does not permit us to prove here. There are two more projective groups that are isomorphic to alternating groups: $PSL_2(9) \cong A_6$ and $PSL_4(2) \cong A_8$. The only other coincidence among the special linear groups is that $PSL_2(7)$ and $PSL_3(2)$ of order 168 are isomorphic.

Let us now turn to the symplectic group. $Sp_2(q) \cong SL_2(q)$, so there aren't any new results there: all the previous results for $PSL_2(q)$ hold for $PSp_2(q)$. The only new exception is $PSp_4(2)$. Since the characteristic is 2, $PSp_4(2)$ is the same as $Sp_4(2)$.

Proposition 7.2 The projective symplectic group $Sp_4(2)$ is isomorphic to the symmetric group S_6.

Proof: Define a *pentagon* in V to be an unordered 5-tuple $\{u_1, u_2, \ldots, u_5\}$ such that $(u_i, u_j) = \delta_{ij}$. Every pentagon contains 20 (ordered) hyperbolic pairs, because every ordered pair (u_i, u_j) is a hyperbolic pair. In fact, every hyperbolic pair is in one and only one pentagon. For suppose that (u_1, u_2) is a hyperbolic pair. We can find an orthogonal hyperbolic pair (v_1, v_2). Then if we set $u_3 = u_1 + u_2 + v_1$, $u_4 = u_1 + u_2 + v_2$ and $u_5 = u_1 + u_2 + v_1 + v_2$ it is easily checked that $(u_i, u_j) = \delta_{ij}$. On the other hand, suppose that a pentagon contains a hyperbolic pair (u_1, u_2). Then $u_3 = a_1u_1 + a_2u_2 + a_3v_1 + a_4v_4$. $(u_2, u_3) = 1 \Rightarrow a_1 = 1$, and $(u_1, u_3) = 1 \Rightarrow a_2 = 1$. By an identical argument we can write $u_i = u_1 + u_2 + w_i$ for $i > 2$, where w_i are in the hyperbolic plane $W = \langle v_1, v_2 \rangle$. But there are only three nonzero vectors in W, so w_4, w_4, w_5 must be them; for if $w_3 = 0$, say, then $(u_3, u_4) = (u_1 + u_2, u_1 + u_2 + w_4) = 2 = 0$. By Proposition 4.9 there are a total of 120 hyperbolic pairs in V, so there are exactly 6 pentagons.

So consider the action of $Sp_4(2)$ on the set of pentagons. $A \in Sp_4(2)$ sends one pentagon to another because A preserves symplectic inner products. This action is also faithful, because any nonzero vector u is equal to the intersection of two pentagons. There are 15 nonzero vectors and 120 hyperbolic pairs, so for each $u \neq 0$, there are 8 vectors $v_1, \ldots, v_8$ such that (u, v_i) is a hyperbolic pair. Then the pentagon P_1 containing the hyperbolic pair (u, v_1) must have 4 of them, while the pentagon P_2 containing u and any missing v_i must have the other 4. Thus $P_1 \cap P_2 = u$. So if A fixes each pentagon, A fixes every nonzero vector and reduces to the identity. Now that we have an injective homomorphism from $Sp_4(2)$ to S_6, we conclude that the two groups are isomorphic since by Proposition 4.9 the order of $Sp_4(2)$ is $(15)(8)(3)(2) = 720 = |S_6|$. □

The most obvious exception for the orthogonal groups is when $n = 2$. We have already worked out $SO_2^-(F)$, i.e. SO_2 of a hyperbolic plane, in the section after Lemma 5.5, where we found it to be isomorphic to the multiplicative group F^*. Since this is Abelian, it is obviously not simple. $SO_2^+(F)$ is also Abelian. Every matrix A in $SO_2^+(F)$ takes the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ with $a^2 + b^2 = 1$; we can obtain this result by setting $A^{-1} = A^T$. Multiplying two generic group

members,

$$\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -(a_1b_2 + a_2b_1) & a_1a_2 - b_1b_2 \end{pmatrix}$$

Since this product obviously does not depend on the order, $SO_2^+(F)$ is also Abelian.

A more interesting example of a non-simple group is $P\Omega(V)$ when V has Witt index 2.

Proposition 7.3 Let V be a 4-dimensional vector space over F, of Witt index 2. Then there is a homomorphism from $PSO(V)$ to $SO_3(F) \times SO_3(F)$, and when restricted to $P\Omega$ it gives an isomorphism between $P\Omega$ and $\Omega_3 \times \Omega_3$, where $\Omega_3 = SO_3(F)'$.

Proof: Define W to be the space of skew-symmetric matrices on V. W has dimension 6 over F since it has a basis of $B_{ij} = E_{ij} - E_{ji}$ for $i < j$. We can put an inner product b on W by taking $b(B, C) = \text{trace}(BC^T)$. This is symmetric since $b(B, C) = \sum_{i,j} B_{ij}C_{ij}$. We remark that we can define an action of SO_4 on W via $B \mapsto ABA^T$. This preserves inner products:

$$b(B^A, C^A) = \text{tr}(ABA^T(ACA^T)^T) = \text{tr}(ABA^TAC^TA^T) = \text{tr}(ABC^TA^T)$$

since $AA^T = I$. Now since $\text{tr}(T_1T_2) = \text{tr}(T_2T_1)$ in general, $b(B^A, C^A) = \text{tr}(BC^T) = b(B, C)$. The idea of the proof is to produce an involution Φ of W which commutes with the action of $SO(V)$. Then by looking at the action of $SO(V)$ on the two eigenspaces W_+ and W_- of Φ we get a homomorphism into $SO_3 \times SO_3$.

We construct Φ by observing that the space $\Lambda^2(V)$ of differential 2-forms on V is naturally isomorphic to W. If ω is a 2-form, then $\omega = \sum b_{ij}\, dx_i \wedge dx_j$ and $b_{ji} = -b_{ij}$. So by sending ω to $B = b_{ij}$ we get an isomorphism into W. There is also a natural map from $\Lambda^2(V) \times \Lambda^2(V) \to \Lambda^4(V)$ given by sending ω_1, ω_2 to their wedge product $\omega_1 \wedge \omega_2$. But $\Lambda^4(V)$ is isomorphic to F because every 4-form is $a\, dx_1 \wedge dx_2 \wedge dx_3 \wedge dx_4$ for some constant $a \in F$. So this is a symmetric, bilinear form on $\Lambda^2(V)$ which we write as b'. In general, if b and b' are symmetric bilinear forms, we can find Φ such that $b'(B, C) = b(B, C\Phi)$. We compute Φ in this case to be the transformation that interchanges the three pairs (B_{12}, B_{34}), (B_{14}, B_{23}) and $(B_{13}, -B_{24})$. So $B_{12} \overset{\Phi}{\longleftrightarrow} B_{34}$, and so forth. Let us illustrate this by checking that $B_{12}\Phi = B_{34}$. $(\sum b_{ij}dx_i \wedge dx_j) \wedge (dx_1 \wedge dx_2) = b_{34}dx_3 \wedge dx_4 \wedge dx_1 \wedge dx_2 + b_{43}dx_4 \wedge dx_3 \wedge dx_1 \wedge dx_2 = 2b_{34}dx_1 \wedge dx_2 \wedge dx_3 \wedge dx_4$. So $b'(B, B_{12}) = 2b_{34} = b(B, B_{34})$. The calculation is analagous for the other basis vectors.

Now we can verify that A and Φ commute. A also preserves inner products on the diffferential form side, since if we change coordinates from x_i to Ax_i, the form $dx_1 \wedge dx_2 \wedge dx_3 \wedge dx_4$ is multiplied by a factor $\det(A)$. So as long as A has determinant 1, $b'(B^A, C^A) = b'(B, C)$. To check that $(C\Phi)^A = (C^A)\Phi$, it is enough to show that for any B, $b(B, (C^A)\Phi) = b(B, (C\Phi)^A)$. Thus

$b(B,(C^A)\Phi) = b'(B,ACA^T) = b'(A^TBA,C) = b(A^TBA,C\Phi) = b(B,(C\Phi)^A)$ as claimed. Now define W_+ and W_- to be the eigenspaces $W_+ = \{x : x\Phi = x\}$, $W_- = \{x : x\Phi = -x\}$. As we saw in the proof that every involution is a reflection [Proposition 5.1], $W = W_+ \oplus W_-$. A sends W_+ to W_+ because for $x \in W_+$, $(Ax)\Phi = A(x\Phi) = Ax$ which is also fixed by Φ. The same holds true for W_-, so by restricting A to W_+ and W_- we obtain orthogonal transformations over W, which in an orthogonal space of dimension 3, so we have a map $\psi : SO(V) \to O_3 \times O_3$. ψ has kernel $\pm I$ since if any transformation acts trivially on both W_+ and W_-, it acts trivially on all of W. Then it is readily verified that if $ABA^T = B$ for all B in W, $A = \pm I$. ψ in fact maps $\Omega(V)$ into $\Omega_3 \times \Omega_3$. For if A is a commutator, then so is its restriction to a subspace U: if $A = [B,C]$, then $A_{|U} = [B_{|U}, C_{|U}]$. Finally, by comparing the orders of these two groups we can see that ψ induces an isomorphism from $P\Omega(V)$ to $\Omega_3 \times \Omega_3$. Ω_3 is a subgroup of index 2 in $SO_3(q)$, so $|\Omega_3| = (q^2-1)q/2$ by our earlier result on the size of $SO_n(q)$. On the other hand, $\Omega(V)$ is a subgroup of index 2 in $SO(V)$, and its center $\pm I$ has order 2, so $|P\Omega| = (q^3-q)(q^2-1)q/4 = [(q^2-1)q/2]^2 = |\Omega_3 \times \Omega_3|$. □

8 Further Developments

This paper has focused exclusively on concrete and direct approaches to understanding the classical linear groups. While these work well for the classical groups, there are too many other families of more complicated linear groups to make it a good way to classify them. An approach which is better suited to classifying the linear groups is to study their associated Lie algebras. A theorem from geometry states that there are only 8 isomorphism classes of semi-simple Lie algebras. It turns out that the class of the Lie algebra almost completely specifies each family of groups. By bringing in several more abstract ideas like root systems and algebraic groups, it is possible to systematically work out the structures of all of the linear groups. The success of this theory in connection with this problem and the classification of finite simple groups represents the triumph of this abstruse, "high technology" approach to mathematics over an older, more ad hoc methodology. Nevertheless, before we are seduced by the glory of these slick and incomprehensible proofs, it would be well to remember that no one has ever invented one without first mastering the basics of his subject.

References

[1] ARTIN, M. *Algebra*, Prentice Hall, Englewood Cliffs, New Jersey (1991)

[2] ASCHBACHER, M. *Finite Group Theory*, Cambridge University Press, Cambridge (1986)

[3] COHN, P.M. *Algebra, Vol. 2 and 3*, John Wiley & Sons, Chichester (1977)

[4] DICKSON, L. E. *Linear Groups*, B.G. Teubner, Leipzig (1901)

[5] DIEUDONNÉ, J. *La Géométrie des Groupes Classiques*, Springer-Verlag, Berlin (1955)

[6] GORENSTEIN, D. *Finite Groups*, Chelsea Publishing Company, New York (1968)

[7] GORENSTEIN, D. *Finite Groups:An Introduction to Their Classification*, Plenum Press, New York (1982)

[8] GORENSTEIN, D., LYONS, R. and SOLOMON, R. *The Classification of the Finite Simple Groups, Number 3*, American Mathematical Society, Providence (1997)

[9] JACOBSON, N. *Basic Algebra II*, W. H. Freeman & Co., New York (1989)