II.C. Symplectic groups

Continuing with the notation of §II.A, assume char($\mathbb{F}$) $\neq 2$ and let $B$ be a skew-symmetric, hence alternating, bilinear form on $V$. Then for any basis $e$ of $V$, the entries $B_{ij}$ of the matrix $[B]_e$ satisfy $B_{ij} = −B_{ji}$, and in particular $B_{ii} = 0$, for all $i, j = 1, \ldots, n$.

The next result says that the rank of such a form (i.e. of its matrix) is always even. What is perhaps more surprising is that, since any two bases are related by an isomorphism, all alternating forms of a given rank are equivalent in the sense of II.A.8:

II.C.1. Theorem. There exists a basis $e$ such that $[B]_e$ is a block-diagonal matrix $\text{diag}\{J, \ldots, J, 0, \ldots, 0\}$, where $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. (The zeroes are “1 × 1” blocks, and the nondegenerate case is the one with no zeroes.)

**Proof.** If $B = 0$, we are done (since any basis will do). Otherwise, there exist $u, v$ such that $b := B(u, v) \neq 0$. They are necessarily independent (why?). Put $u_1 := u$ and $v_1 := b^{-1}v$, so that $B(u_1, v_1) = 1 = −B(v_1, u_1)$.

Inductively assume that there exists a linearly independent set $e^{(k)} = \{u_1, v_1, \ldots, u_k, v_k\}$, such that $B(u_i, v_i) = 1 = −B(v_i, u_i)$ and all other $B(x, y) = 0$ (for $x, y \in e^{(k)}$). Writing $V_k := \text{span}(e^{(k)})$, we obviously have $[B|_{V_k}]_{e^{(k)}} = \text{diag}\{J, \ldots, J\}$, whence $B|_{V_k}$ is nondegenerate and (by II.A.3) $V_k \cap V_k^\perp = \{0\}$.

Now for any $x \in V$, put $y := x − \sum_{i=1}^{k} B(x, v_i)u_i + \sum_{i=1}^{k} B(x, u_i)v_i$ and notice that

\[B(y, u_j) = B(x, u_j) + \underbrace{B(x, u_j)B(v_j, u_j)}_{=0} = 0\]

and

\[B(y, v_j) = B(x, v_j) − \underbrace{B(x, v_j)B(u_j, v_j)}_{=0} = 0\]

for all $j$. Hence $y \in V_k^\perp$, and $x \in V_k + V_k^\perp$. So $V = V_k + V_k^\perp$, which together with $V_k \cap V_k^\perp = \{0\}$ gives $V = V_k \oplus V_k^\perp$.

Finally, apply the first paragraph to $B|_{V_k^\perp}$: if this is zero, the induction terminates and we add any basis of $V_k^\perp$ to $e^{(k)}$. If it is not zero, add the resulting $u_{k+1}, v_{k+1}$ to our basis to get $e^{(k+1)}$, and continue. 

$\square$
II.C.2. Corollary. Let \( M = -^t M \in M_n(\mathbb{F}) \). Then \( 2 | \text{rank}(M) \) and \( \det M \in \mathbb{F}^2 \).

Proof. Thinking of \( M \) as \([B]_\varepsilon\) for some bilinear form on \( V \), take \( S := \varepsilon[1]_\varepsilon \) for \( \varepsilon \) as in II.C.1. Then
\[
M = ^t S [B]_\varepsilon S = ^t S \cdot \text{diag}\{J, \ldots, J, 0, \ldots, 0\} \cdot S
\]
gives \( \det M = (\det S)^2 \) or 0; and \( \text{rank}(M) \) is \( 2 \times \) the number of \( J \)'s. \( \square \)

II.C.3. Corollary. Two skew-symmetric matrices are cogredient if and only if they have the same rank.

Proof. Only the reverse implication needs to be checked. Again, we interpret the matrices as \([B]_\varepsilon\) and \([\tilde{B}]_\varepsilon\), which applying II.C.1 become \( ^t S J S \) and \( ^t \tilde{S} J \tilde{S} \) (with \( J \) the \( J \)-block diagonal matrix of that rank). So they are cogredient by \( S^{-1} \tilde{S} \). \( \square \)

II.C.4. Definition. (i) Let \( V \) be an \( \mathbb{F} \)-vector space of dimension \( n = 2r \), and \( B \) a nondegenerate alternating bilinear form. Then \((V, B)\) is called a symplectic vector space, and \( B \) a symplectic form.

(ii) Continuing with the assumptions of (i), the group
\[
\text{Sp}_n(\mathbb{F}) := \{ T \in \text{Aut}_\mathbb{F}(V) \mid B(Tx, Ty) = B(x, y) \ (\forall x, y \in V)\},
\]
which up to isomorphism\(^4\) is independent of the choice of \( B \), is called the symplectic group of degree \( n \) over \( \mathbb{F} \). Note that the elements \( T \) are exactly the (self-)isometries of \((V, B)\).

(iii) A basis in which \( B \) has matrix \( J_n := \text{diag}\{J, \ldots, J\} \) (with \( r = \frac{n}{2} \) blocks) is called a symplectic basis for \((V, B)\). More explicitly, this is of the form \( \{u_1, v_1, \ldots, u_r, v_r\} \) with \( B(u_i, u_j) = 0 = B(v_i, v_j) \) and \( B(u_i, v_j) = \delta_{ij} = -B(v_i, u_j) \).

I should point out that, given a symplectic basis \( \varepsilon = \{\varepsilon_i\}_{i=1}^n \) of \((V, B)\), the transformations \( T \) for which \( T(\varepsilon) \) is another symplectic basis

\(^4\)The notation might still be a bit deceptive; it is perhaps more honest to write \( \text{Aut}(V, B) \), and say that it is conjugate to any other \( \text{Aut}(V, B') \) (\( B' \) also nondegenerate alternating) inside \( \text{Aut}(V) \), and isomorphic to the group \( \text{Sp}_n(\mathbb{F}) := \text{Aut}(\mathbb{F}^n, J_n) \) (where \( J_n \) is the bilinear form with matrix \( J_n \) with respect to the standard basis).
II. LINEAR ALGEBRAIC GROUPS

basis are exactly the elements of \( \text{Sp}_n(\mathbb{F}) \). (If \( B(Tx, Ty) = B(x, y) \)
fails for some \((x, y)\), then \( B(T(\varepsilon_i), T(\varepsilon_j)) = B(\varepsilon_i, \varepsilon_j) (= [J_n]_{ij}) \)
fails for some \((i, j)\).) In matrix terms, this condition on \( T \) is precisely that
\[
[B]_{T(\varepsilon)} = \epsilon T([\mathbf{1}]_{T(\varepsilon)}) \quad \text{for all } \varepsilon.
\]

We now introduce some terminology and technical lemmas which will be instrumental in showing that the quotient of the symplectic group by its center is simple.

II.C.5. Definition. Let \( U \subset V \) be a subspace of a symplectic vector space. The radical of \( U \) is the subspace \( U \cap U^\perp \). If \( U \) is its own radical (i.e. \( U \subset U^\perp \), or \( B(U, U) = 0 \)), then \( U \) is isotropic.

II.C.6. Examples. (a) Obviously radicals are isotropic.

(b) Notice that if \( \varepsilon = \{u_1, v_1, \ldots, u_r, v_r\} \) is a symplectic basis, then \( \mathbb{F}\langle u_1, \ldots, u_r \rangle \) and \( \mathbb{F}\langle v_1, \ldots, v_r \rangle \) are isotropic – in fact, maximally so, as any enlargement is no longer isotropic.

II.C.7. Lemma. Given a subspace \( U \) of a symplectic space \((V, B)\) with radical \( R \), \( B \) is well-defined on \( U := U/R \),\(^5\) and gives it the structure of a symplectic vector space.

Proof. Well-definedness follows from \( B(u + r, u' + r') = B(u, u') \)
since \( R \) is \( \perp \) to everything in \( U \). It is left to check that \( B|_U \) (which is not nondegenerate) descends to a nondegenerate alternating form on \( U \), which is simply because in \( U \) only 0 is \( \perp \) to everything. \( \square \)

II.C.8. Lemma. Any maximal isotropic subspace \( U \) of a symplectic space \((V, B)\) has \( \dim U = \frac{1}{2} \dim V \).

Proof. Given \( V_0 \subset V \), by the proof of II.A.4 \( \dim V_0^\perp = 2r - \dim V_0 \). So if \( \dim V_0 > r \), we cannot have \( V_0 \subset V_0^\perp \). On the other hand, if \( V_0 \) is isotropic and \( \dim V_0 < r \), we have \( V_0 \subsetneq V_0^\perp \), and for any \( v \in (V_0)^\perp \setminus V_0 \), \( V_0 + \mathbb{F}\langle v \rangle \) is still isotropic,\(^6\) and enlarges \( V_0 \). \( \square \)

---

\(^5\)Granted, one would not want to use this notation in a context where it could be confused with complex conjugation . . .

\(^6\)Remember, in a symplectic space, every vector is self-orthogonal.
II.C.9. Lemma. Any isometry \( \theta : (\mathcal{U}, B|_{\mathcal{U}}) \rightarrow (\mathcal{\hat{U}}, B|_{\mathcal{\hat{U}}}) \) between subspaces extends to a (self)-isometry of \((V, B)\), i.e. is induced by an element \( T \in \text{Sp}_n(F) \).

Proof. Taking a symplectic basis \( \mathcal{v}' = \{\mathcal{u}_1, \mathcal{v}_1, \ldots, \mathcal{u}_k, \mathcal{v}_k\} \) for \( \mathcal{U} \) (possible by II.C.7), let \( \mathcal{v}' := \{u_1, v_1, \ldots, u_k, v_k\} \) be any lift to \( \mathcal{U} \), and write \( \mathcal{v}^\circ := \{v_{k+1}, \ldots, v_m\} \) for any basis of \( R = \mathcal{U} \cap \mathcal{U}^\perp \). Put \( \mathcal{U}' := F\langle \mathcal{v}' \rangle \), and observe that \( \mathcal{U}' \cap R = \{0\} \): since \( B' := B|_{\mathcal{U}'} \) is nondegenerate, a nonzero element of \( \mathcal{U}' \) cannot belong to \( (\mathcal{U}')^\perp \) (which contains \( R \)). So \( \mathcal{U} = \mathcal{U}' \oplus R \), and \( \mathcal{v}' \cup \mathcal{v}^\circ \) is a basis of \( \mathcal{U} \).

We now extend this to a symplectic basis of \((V, B)\). Write \( \mathcal{U}'' := \mathcal{U}'^\perp \) and \( \mathcal{B}'' := B|_{\mathcal{U}''} \). By nondegeneracy of \( \mathcal{B}' \) we have \( V = \mathcal{U}' \oplus \mathcal{U}'' \). Since \( \mathcal{B} \) is nondegenerate and \( \mathcal{L}_\mathcal{B} = \mathcal{L}_{\mathcal{B}'} \mathcal{L}_{\mathcal{B}''}, \mathcal{B}'' \) must also be nondegenerate. Let \( \mathcal{W} \subset \mathcal{U}'' \) be a maximal isotropic subspace containing \( R \), and extend \( \mathcal{v}^\circ \) to a basis \( \mathcal{v} \) of \( \mathcal{W} \). By II.C.8, \( \dim \mathcal{W} = \frac{1}{2} \dim \mathcal{U}'' = r - k \), so we can write \( \mathcal{v} = \{v_{k+1}, \ldots, v_{r}\} \); and one easily checks\(^7\) that there exist \( u_{k+1}, \ldots, u_r \) in \( \mathcal{U}'' \) completing this to a symplectic basis \( \mathcal{v}'' \) of \( (\mathcal{U}'', \mathcal{B}'') \). Now \( \mathcal{v} := \mathcal{v}' \cup \mathcal{v}'' \) gives the desired basis of \( V \).

Finally, define a basis of \( \mathcal{\hat{U}} \) by \( \theta(\mathcal{v}' \cup \mathcal{v}^\circ) \). Since \( \theta \) is an isometry, \( \theta(\mathcal{v}') \) is symplectic and \( \theta(\mathcal{v}^\circ) \) spans the radical of \( \mathcal{\hat{U}} \). So we may extend this to a symplectic basis \( \mathcal{\hat{v}} \) of \( V \) in the same way. Now simply let \( T \) be the linear map sending \( \mathcal{v} \mapsto \mathcal{\hat{v}} \). This sends a symplectic basis to a symplectic basis, and is thus in \( \text{Sp}_n(F) \). \( \square \)

**Transvections.**

In order to prove simplicity of \( \text{Sp}_n \) modulo its center (and that the latter is just \( \{ \pm 1 \} \)), the next big ingredient we need is a result which is important in its own right, to the effect that certain special kinds of transformations generate \( \text{Sp}_n \). To get a feel for this let’s consider the \( n = 2 \) case first.

\(^7\) The \( F\langle v_{k+2}, \ldots, v_r \rangle \cap \mathcal{U}'' \) has dimension \( r - k + 1 \) and contains \( W \). Take any vector \( u \) in the complement; since \( u \) isn’t in \( W \) and is \( \perp \) to \( v_{k+2}, \ldots, v_r \), it cannot be \( \perp \) to \( v_{k+1} \). Scale it to make \( B(u, v_{k+1}) = 1 \), and then you have your \( u_{k+1} \).
II.C.10. EXAMPLE. The condition that a $2 \times 2$ matrix $M$ satisfy $^tMJM = J$ implies that $\det M = \pm 1$. But let’s look more closely: writing $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we get $^tMJM = \begin{pmatrix} 0 & ad-bc \\ bc-ad & 0 \end{pmatrix}$. This forces $\det M = 1$, and there are no further conditions: $\text{Sp}_2(\mathbb{F}) = \text{SL}_2(\mathbb{F})$.

Now it is easy to see that you can write all the elements of $\text{SL}_2(\mathbb{F})$ as products of a the type of elementary matrices associated to “replace” operations: any $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of determinant 1 and $b \neq 0$ can be written as $\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix}$, by taking $y = b$, $x = \frac{d-1}{b}$, and $z = \frac{a-1}{b}$.

The case $c \neq 0$ is similar, while (say, having done that case) you take $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix}$ to get the remaining case ($b = 0 = c$) $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$.

To do something similar for $n > 2$, we slightly expand and generalize these elements as follows:

II.C.11. DEFINITION. Let $(V, B)$ be a symplectic $\mathbb{F}$-vector-space. The linear transformations (for each $u \in V$ and $c \in \mathbb{F}$)

$$\tau_{u,c}: V \to V$$

$$x \mapsto x + cB(x, u)u$$

are called symplectic transvections (in the direction $u$).

Of course, we should check that they deserve their name:

II.C.12. LEMMA. $\tau_{u,c} \in \text{Sp}_n(\mathbb{F})$ for every $u, c$.

PROOF. $\mathbb{F}$-linearity is clear. We must check they are isometries: so compute $B(\tau_{u,c}(x), \tau_{u,c}(y)) = B(x + cB(x, u)u, y + cB(y, u)u) = B(x, y) + cB(x, u)\{B(y, u) + B(u, y)\} + c^2B(x, u)B(u, y)B(u, u)^0 = B(x, y)$, done. □

For reference, here is a list of their properties:

II.C.13. PROPERTIES. (Proofs are easy and left to you.)

(i) $\tau_{u,c} \tau_{u,c''} = \tau_{u,c+c''}$, and $\tau_{u,0} = 1 \iff c = 0$; hence $c \mapsto \tau_{u,c}$ defines an injective group homomorphism $(\mathbb{F}, +) \hookrightarrow \text{Sp}_n(\mathbb{F})$.

(ii) $T\tau_{u,c}T^{-1} = \tau_{(Tu),c}$ for all $T \in \text{Sp}_n(\mathbb{F})$. 


II.C SYMPLECTIC GROUPS

(iii) \( \tau_{au,c} = \tau_{u,a^2c} \).

(iv) \( \tau_{u,c}(x) = x \) if \( x \in F(u)^\perp \); in particular, \( \tau_{u,c}(u) = u \).

(v) Set \( \eta_{u,c} = \tau_{u,c} - 1 : x \mapsto cB(x,u)u \). We may regard \( \eta_{u,c} \) as an element of \( \text{End}_F(V) \), with \( \eta_{u,c}^2 = 0 \). It is nilpotent, since \( \eta_{u,c}^2 = 0 \); and so \( \tau_{u,c} \) is unipotent, with \( \det([\tau_{u,c}]_e) = 1 \) (see the next Remark).

II.C.14. REMARK. Recall that an element of a ring \( R \) with zero as a power is called nilpotent. When this is true of \( \tau - 1 \), \( \tau \) is called unipotent. If \( R = \text{End}_F(V) \) is the endomorphism ring of a vector space, then by putting \( [\tau]_e \) in Jordan form one immediately sees that it must have diagonal entries all 1, hence determinant 1.

We have discussed isotropic subspaces of \((V,B)\); another type of subspace is a hyperbolic plane \( H \), which is a subspace of the form \( H = \text{span}\{u,v\} \), with \( B(u,v) = 1 \) (that is, spanned by a hyperbolic pair). This will be used in the next proof.

II.C.15. THEOREM. \( \text{Sp}_n(F) \) is generated by symplectic transvections.

PROOF. As usual we take \( \text{Sp}_n(F) \) to mean the isometries of a given \( n \)-dimensional symplectic space \((V,B)\), i.e. invertible transformations preserving \( B \) in the sense that \( B(Tx,Ty) = B(x,y) \).

**Step 1:** Assume that for any two hyperbolic pairs \((u,v)\) and \((u',v')\), there exists a product of transvections \( T = \prod_i \tau_i \) such that \( \rho(u) = u' \) and \( \rho(v) = v' \). [Call this assumption \((*)\).] Then the result follows.

We induce on \( n \). Let \( g \in \text{Sp}_n(F) \), and \((u,v)\) a hyperbolic pair; then \((g(u),g(v))\) is also hyperbolic. So by \((*)\) there exists \( T = \prod_i \tau_i \) such that \( T(u) = g(u) \) and \( T(v) = g(v) \), and \( g' := T^{-1}g \) fixes \( u \) and \( v \) hence \( H := F(u,v) \).

Since \( g' \in \text{Sp}_n(F) \), it also stabilizes (but need not fix) \( U := H^\perp \). That is, it restricts to an self-isometry of \((U,B|_U)\), and may be regarded as an element of \( \text{Sp}_{n-2}(F) \). By induction, it is thus given by a product of transvections in directions in \( U \): \( g'|_U = \prod_j \tau_j'|_U \). But since both \( g' \) and the \( \tau_j' \) are the identity on \( H \), we have \( g' = \prod_j \tau_j' \).

Conclude that \( g = Tg' = \prod_i \tau_i \prod_j \tau_j' \).
Step 2: Given any $u, u' \in V$, there exists a product of transvections sending $u \mapsto u'$.

There are two cases to deal with. First, suppose $B(u, u') \neq 0$, and set $w := u - u'$. Then $\tau_{w,c}(u) = u + cB(u, w)w = u - cB(u, u')(u - u')$; and taking $c := B(u, u')^{-1}$, this is just $u'$.

Next suppose $B(u, u') = 0$. Then there exists $f \in V^\vee$ such that $f(u) \neq 0, f(u') \neq 0$. By nondegeneracy of $B$, there is a $u'' \in V$ such that $f(\cdot) = B(u'', \cdot)$. Hence $B(u'', u') \neq 0 \neq B(u'', u)$, and we can just apply the first case twice to get a product of two transvections sending $u \mapsto u'' \mapsto u'$.

Step 3: If $(u, v)$ and $(u, v')$ are hyperbolic pairs, there exists $\prod_i \tau_i$ fixing $u$ and sending $v \mapsto v'$.

Again, two cases: if $B(v, v') \neq 0$, then $\tau_{w,c}$ (with $w := v - v'$ and $c := B(v, v')^{-1}$) sends $v \mapsto v'$ by the same computation as before. Moreover, since $B(u, v) = 1 = B(u, v')$, we have $B(u, w) = 0$ hence $\tau_{w,c}(u) = u$.

If $B(v, v') = 0$, then we apply the first case to get transvections sending $(u, v) \mapsto (u, u + v)$ and $(u, u + v) \mapsto (u, v')$. Here $(u, u + v)$ is a hyperbolic pair since $B(u, u) = 0$; and $B(v, u + v) = B(v, u) = -1$ and $B(u + v, v') = B(u, v') = 1$ are both nonzero.

Finally, note that Step 3 implies $(\ast)$ by sending $(u, v) \mapsto (u, v')$ then $(-v', u) \mapsto (-v', u')$. \hfill \Box

II.C.16. Corollary. The center of $\operatorname{Sp}_n(\mathbb{F})$ is $\{\pm 1\}$.

Proof. Let $T \in \operatorname{C}(\operatorname{Sp}_n(\mathbb{F}))$. For any $v \in V$, by nondegeneracy $\exists u \in V$ so that $(u, v)$ is a symplectic pair. So

$$
\tau_{v,c} = T^{-1} \tau_{v,c} T = \tau_{T^{-1}v,c} \quad (\forall c)
$$

$$
\implies \tau_{v,1}(u) - u = \tau_{T^{-1}v,1}(u) - u
$$

$$
\implies v = B(u, v)v = B(u, T^{-1}v)T^{-1}v
$$

$$
\implies Tv = B(u, T^{-1}v)v,
$$

whence $T$ stabilizes every line $\mathbb{F}\langle v \rangle$ in $V$.
For a basis \( e = \{e_1, \ldots, e_n\} \), this gives \([T]_e = \text{diag}\{\alpha_1, \ldots, \alpha_n\}\); and for any \( i \neq j \), it gives that \( \alpha_i e_i + \alpha_j e_j \) is a multiple of \( e_i + e_j \), forcing \( \alpha_i = \alpha_j \). So \( T = \alpha I \) for some \( \alpha \in \mathbb{F} \). Finally, for any hyperbolic pair \((u, v), 1 = B(u, v) = B(Tu, Tv) = \alpha^2 B(u, v) = \alpha^2 \implies \alpha = \pm 1. \]

Since transvections have determinant 1, we also have:

II.C.17. COROLLARY. \( T \in \text{Sp}_n(\mathbb{F}) \implies \det[T]_e = 1. \) That is, \( \text{Sp}_n(\mathbb{F}) \leq \text{SL}_n(\mathbb{F}) \).

Finally, the symplectic group is its own derived group (i.e. commutator subgroup):

II.C.18. COROLLARY. \( \text{Sp}_n(\mathbb{F}) = D\text{Sp}_n(\mathbb{F}) \) for \( |\mathbb{F}| > 3 \).

PROOF. By II.C.15, it suffices to show that an arbitrary transvection \( \tau_{z,c} \) is contained in \( D\text{Sp}_n(\mathbb{F}) \). Since \( |\mathbb{F}| > 3 \), \( \exists d \in \mathbb{F}^* \) with \( d^2 \neq 1 \). Put \( b := \frac{c}{1-d^2} \) and \( a := -d^2 b = \frac{-d^2 c}{1-d^2} \); then \( a + b = c \) and \( \tau_{z,c} = \tau_{z,a} \tau_{z,b} \).

Pick \( w \in V \) so that \( B(z, w) = 1 \), put \( U := \mathbb{F}\langle z, w \rangle \), and consider the linear map \( \theta: U \to U \) sending \( z \mapsto dz, w \mapsto d^{-1} w \). This \( \theta \) is an isometry, and by II.C.9 extends to \( V \): i.e., \( \exists T \in \text{Sp}_n(\mathbb{F}) \) with \( T(z) = dz \). Using II.C.13,

\[ T \tau_{z,b}^{-1} T^{-1} = T \tau_{z,-b} T^{-1} = \tau_{T(z),-b} = \tau_{dz,-b} = \tau_{z,-bd^2} = \tau_{z,a} \]

hence \( \tau_{z,c} = \tau_{z,a} \tau_{z,b} = T \tau_{z,b}^{-1} T^{-1} \tau_{z,b} = [T^{-1}, \tau_{z,b}] \in D\text{Sp}_n(\mathbb{F}). \) \( \square \)

Simplicity.

Certainly \( \text{Sp}_n(\mathbb{F}) \) itself is not simple, because its center is a (barely) nontrivial normal subgroup. Rather, as mentioned above, we aim to prove that the quotient by its center is simple. For that, we need a definition and two lemmas:

II.C.19. DEFINITION. (i) Let \( \mathbb{F}^* \) act on \( \mathbb{F}^{N+1} \setminus \{0\} \) by

\[ \alpha.(a_0, \ldots, a_N) := (aa_0, \ldots, aa_N). \]

The \( N \)-dimensional **projective space** is the set of orbits,

\[ \mathbb{P}^N(\mathbb{F}) := (\mathbb{F}^{N+1} \setminus \{0\}) / \mathbb{F}^*. \]
Orbits are regarded as “points” of the projective space, and are written \([a_0: \cdots : a_N]\). We can identify them with lines through 0.

(ii) If we want to avoid explicit coordinates, we can write instead \(\mathbb{P}V := (V \setminus \{0\})/\mathbb{F}^*\) for the projectivization of an \(\mathbb{F}\)-vector space (where \(\alpha v := \alpha v\), denoting its elements by \([v]\). Of course, with \(\dim V = n\), we have \(\mathbb{P}V \cong \mathbb{P}^{n-1}(\mathbb{F})\).

II.C.20. **Lemma.** \(\text{Sp}_n(\mathbb{F})\) acts primitively\(^8\) on \(\mathbb{P}^{n-1}(\mathbb{F}) (= \mathbb{P}V)\).

**Proof.** Here the action is just by \(g[v] := [gv]\). A **primitive** action is a particular sort of transitive group action. That the action here is transitive follows at once from II.C.9: for any \([u], [u'] \in \mathbb{P}V\), the map from \(U := \mathbb{F}\langle u \rangle\) to \(\tilde{U} := \mathbb{F}\langle u' \rangle\) sending \(u \mapsto u'\) is an isometry, since \(B(u, u) = 0 = B(u', u')\). So there is an element \(g \in \text{Sp}_n(\mathbb{F})\) with \(g[u] = [u']\). But primitivity asks a bit more.

Suppose we have a partition \(P\) of \(\mathbb{P}V\) into disjoint subsets, viz. \(\mathbb{P}V = \bigsqcup_{S \in P} S\), and that this partition is stabilized by \(\text{Sp}_n(\mathbb{F})\). (That is, for any \(g \in \text{Sp}_n(\mathbb{F})\) and \(S \in P\), we have \(gS \in P\).) The primitivity we are claiming says that \(P\) can only be the partition into singletons or the entire space; i.e., either every \(|S| = 1\) or the only \(S \in P\) is \(S = \mathbb{P}V\). The idea of the proof is to suppose that some \(S \in P\) contains two distinct elements \([x], [y] \in \mathbb{P}V\), and show that we can find \(g \in \text{Sp}_n(\mathbb{F})\) sending \([x] \mapsto [x]\) (so that \(gS = S\)) but \([y]\) to an arbitrary element other than \([x]\) (forcing \(S = \mathbb{P}V\)).

**Case 1:** \(B(x, y) \neq 0\). By rescaling the representatives of \([x], [y]\) we may assume \(B(x, y) = 1\). Let \([z] \in \mathbb{P}V \setminus \{[x]\}\) be arbitrary. If \(B(x, z) \neq 0\), scale \(z\) so \(B(x, z) = 1\) too. Taking \(U = \mathbb{F}\langle x, y \rangle\) and \(\tilde{U} = \mathbb{F}\langle x, z \rangle\), there is an obvious isometry \(\theta: U \rightarrow \tilde{U}\) sending \(x \mapsto x, y \mapsto z\). By II.C.9, this is the restriction of (the self-isometry of \(V\) given by) some \(g \in \text{Sp}_n(\mathbb{F})\). So \([z] \in S\) and we are done in this sub-case.

If \(B(x, z) = 0\), there exists \(w \in V\) such that \(B(x, w) = 1 = B(z, w)\), hence (by II.C.9) \(g \in \text{Sp}_n(\mathbb{F})\) sending \(x \mapsto x\) and \(y \mapsto w\). So \([w] \in S\). But II.C.9 also gives \(g' \in \text{Sp}_n(\mathbb{F})\) sending \(w \mapsto w\) and \(x \mapsto z\), and this gives \([z] \in S\).

\(^8\)defined in the proof
Case 2: $B(x, y) = 0$. There exists $u \in V$ such that $B(x, u) = 1$ and $B(y, u) = 0$. (Take a symplectic basis with $v_1 = x$ and $v_2 = y$, and let $u := u_1$.) Let $z \in \mathbb{F} \langle x, u \rangle \perp \{0\}$ be arbitrary, and consider the map from $U := \mathbb{F} \langle x, u \rangle$ to $\tilde{U} := \mathbb{F} \langle x, u, z \rangle$ fixing $x, u$ and sending $y \mapsto z$. Since $y \in \mathbb{F} \langle x, u \rangle \perp \{0\}$, this is an isometry, and so (by II.C.9) is induced by some $g \in \text{Sp}_n(\mathbb{F})$. This gives $[z] \in S$, but this time $[z]$ wasn’t arbitrary enough and we’re not quite finished.

But since $B|_{\mathbb{F} \langle x, u \rangle}$ is nondegenerate, we can choose $z$ so that $B(z, y) \neq 0$ (and $[z], [y] \in S$). This puts us in Case 1, so we are done now.

For the next result, recall that $G_x$ denotes the stabilizer of $x$.

II.C.21. LEMMA. Let $G$ act on $X$, with $K \trianglelefteq G$ the kernel of the corresponding homomorphism (from $G \to \mathfrak{S}_X$). Then $G / K$ is simple if:

(i) $G$ acts primitively on $X$;
(ii) $G = DG$; and
(iii) there exist $x \in X$ and an abelian subgroup $A \trianglelefteq G_x$ such that the conjugates $\{gAg^{-1}\}_{g \in G}$ generate $G$.

PROOF. Suppose $K < H \trianglelefteq G$. Then $G$ stabilizes the partition of $X$ into $H$-orbits.\(^9\) Since (by (i)) $G$ acts primitively, this partition is either the one into singletons ($H$ acts trivially) or the entire set ($H$ acts transitively). Since $H \not\leq K$, it must be the latter.

Let $x \in rx$ satisfy (iii). Since $H$ acts transitively, for every $g \in G$ there is an $h \in H$ with $hx = gx$. So $G = HG_x \implies G \triangleright HA \implies HA$ contains every $gAg^{-1} \implies HA = G$ (by (iii)) \implies $G / H = A / (H \cap A)$ is abelian \implies $D(G / H) = \{1\} \implies H \supseteq DG \implies H \supseteq G$ (by (iii)) \implies $H = G$. Conclude that $G / K$ has no nontrivial proper normal subgroup, i.e. is simple.

II.C.22. THEOREM. The projective symplectic group

$$P\text{Sp}_n(\mathbb{F}) := \text{Sp}_n(\mathbb{F}) / \{\pm 1\}$$

is simple for $|\mathbb{F}| > 3$.

\(^9\)See the proof of I.L.6.
**Proof.** Consider the action of \( G := \text{Sp}_n(\mathbb{F}) \) on \( X := \mathbb{P}V \). We apply I.C.21, in which (i) and (ii) hold by II.C.20 and II.C.18. It remains to check (iii): fix \( x \in V \setminus \{0\} \), and set \( A := \{ \tau_{x,c} | c \in \mathbb{F} \} \). This is abelian, and normal in \( G_x \) since (for \( \gamma \in G_x \)) \( \gamma \tau_{x,c} \gamma^{-1} = \tau_{\gamma(x),c} = \tau_{x,c} \). Moreover, its conjugates give all transvections by II.C.13(ii), which generate \( G \) by II.C.15.

**II.C.23. Remark.** In complex algebraic geometry, we frequently study the topology of families of projective hypersurfaces, which is to say solution sets (in \( \mathbb{P}^N(\mathbb{C}) \)) of homogeneous polynomials in projective space as the coefficients vary. One typically considers an open subset \( U \) of the parameter space obtained by deleting those tuples of coefficients which make the variety singular, and calculates the action of various loops (around this deleted set) on a \( \mathbb{Q} \)-vector space \( H \) called the cohomology (of some fixed variety in the family). This space represents “topological cycles modulo boundaries”, and carries a nondegenerate bilinear form \( Q \) coming from intersection of cycles.

The action, which is called *monodromy*, measures how cycles do or do not return to themselves under analytic continuation, although the intersection numbers are always preserved. So it produces a homomorphism \( \rho: \pi_1(U) \to \text{Aut}(H, Q) \) from the fundamental group of the parameter space to the isometry group of \( (H, Q) \), which is symplectic when the (complex) dimension of the hypersurfaces is odd (i.e. \( N \) is even). One can show that the local monodromy transformations (images of simple loops) produce essentially all of the integral transvections.

These are not all of the rational transvections, and so we don’t get that \( \rho \) is surjective. Rather, what we are able to conclude from this is that the smallest linear algebraic group (over \( \mathbb{Q} \)) containing the image of \( \rho \) is the full symplectic group \( \text{Aut}(H, Q) \). It is still a beautiful and important statement. You can think of it as a topological analogue of the statement that the Galois group of a general polynomial of degree \( n \) is the full \( \mathfrak{S}_n \).