18.704 Supplementary Notes
March 18, 2005

Symplectic groups

These notes cover most of what I did in the seminar on March 14, in a slightly more coordinate-free way. The general setting is

(1)(a) $$V = 2n\text{-dimensional vector space over a field } F,$$

(1)(b) $$B = \text{non-degenerate symplectic form on } V.$$

(1)(c) $$Sp(V) = \{g \in GL(V) \mid B(gv, gw) = B(v, w) \quad (v, w \in V)\}.$$

This is the symplectic group of the form B.

The goal is to work out the structure of certain subgroups of $Sp(V)$, and to use that structure to calculate the orders of symplectic groups over finite fields.

Recall first of all the projective space

(2) $$\mathbb{P}(V) = \text{set of lines in } V.$$

If u is a non-zero vector in V, we write $[u] = \{au \mid a \in F\}$ for the line through u. The group $Sp(V)$ (like any subgroup of $GL(V)$) acts on $\mathbb{P}(V)$.

Lemma 3 (text, Proposition 3.2). *The action of $Sp(V)$ on $V - \{0\}$ is transitive; consequently the action on $\mathbb{P}(V)$ is transitive as well.*

From now on we fix a non-zero vector $u \in V$. (Such a vector exists if $n \geq 1$.) The goal is to understand the group

(4) $$\begin{aligned} \mathrm{Stab}_{Sp(V)}([u]) &= \{g \in Sp(V) \mid g[u] = [u]\} \\ &= \{g \in Sp(V) \mid gu = ku, \quad \text{some } k \in F^\times\}. \end{aligned}$$

There at least three reasons to understand this group. First, when F is a finite field we can use the formula

(5) $$|Sp(V)| = |\mathbb{P}(V)| \cdot |\,\mathrm{Stab}_{Sp(V)}([u])|$$

to compute the order of the symplectic group. Second, we'll be able to use the structure of this group together with Iwasawa's theorem to deduce that $PSp(V)$ (the quotient of $Sp(V)$ by its center) is almost always a simple group. Third, the structure of the stabilizer is interesting for its own sake: this is a group that plays an important part in lots of current mathematics.

So here we go. In order to work out the structure of the stabilizer of the line $[u]$, we're going to write down lots of linear transformations in the stabilizer. In order to do that, we need to make one more choice. Because B is non-degenerate and u is non-zero, we can choose a vector v so that

(5)(a) $$B(u, v) = 1.$$

Because the form B is symplectic, we deduce that

(5)(b) $$B(u,u) = B(v,v) = 0, \qquad B(u,v) = -B(v,u) = 1.$$

This means that the vectors u and v span a hyperbolic plane. The matrix of the form B on this plane is $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, which has determinant $+1$; so B is non-degenerate on this plane. Define

(6)(a) $$W = \{w \in V \mid B(u,w) = B(v,w) = 0\} = \mathrm{span}(u,v)^{\perp}.$$

According to Proposition 2.9 of the text,

(6)(b) $$B_W = \text{restriction of } B \text{ to } W$$

is a non-degenerate symplectic form on the $(2n-2)$-dimensional vector space W, and

(6)(c) $$V = \mathrm{span}(u,v) \oplus W.$$

I am going to describe a lot of linear transformations on V with three pieces of information: what happens to u; what happens to v; and what happens to vectors in W. Formally, this means that I'll specify the linear transformation T on V by specifying

(1) the vector $T(u)$;
(2) the vector $T(v)$; and
(3) the linear transformation T_W = restriction of T to W, which is a linear map from W to V.

If we were to choose a basis $\{w_1, \ldots, w_{2n-2}\}$ of W and think in terms of matrices (in the basis $\{u, v, w_1, \ldots, w_{2n-2}\}$ of V), then Tu is the first column of the matrix of T; Tv is the second column; and T_W is the last $2n-2$ columns. In order to check whether $T \in Sp(V)$, we have to check

(7)(a) $$B(T(u), T(v)) = B(u,v);$$

(7)(b) $$B(T(u), T_W(w)) = B(T(v), T_W(w)) = 0 \qquad (w \in W);$$

(7)(c) $$B(T_W(w), T_W(w')) = B(w,w') \qquad (w, w' \in W).$$

So here are some easy elements in the stabilizer of $[u]$; I apologize that the notation doesn't match what I used in class. For any non-zero $k \in F$, we have

(8) $$A_k(u) = ku, \quad A_k(v) = k^{-1}v, \quad A_k(w) = w \quad (w \in W).$$

The relations in (7) are easy to check: (7)(c) is trivial, (7)(b) is nearly trivial, and for (7)(a), we have

$$B(A_k(u), A_k(v)) = B(ku, k^{-1}v) = k \cdot k^{-1} \cdot B(u,v) = B(u,v).$$

So A_k belongs to $\mathrm{Stab}_{Sp(V)}([u])$.

For any $x \in F$, we can define

$$Z_x(u) = u, \quad Z_x(v) = v + xu, \quad Z_x(w) = w \quad (w \in W). \tag{9}$$

Here again conditions (7)(c) and (7)(b) are almost obvious. For (7)(a),

$$B(Z_x(u), Z_x(v)) = B(u, v + xu) = B(u, v) + xB(u, u) = B(u, v)$$

since $B(u, u) = 0$. So Z_x belongs to $\mathrm{Stab}_{Sp(V)}([u])$.

The next elements require a little more thought. If u is mapped to itself by a symplectic map, then v must be mapped to some v' such that $B(u, v') = 0$. In Z_x we chose v' to be v plus a multiple of u. In the next elements, we'll choose v' to be v plus something in W. The complication now arises in trying to arrange (7)(b). Here are the maps. For any $w \in W$, define

$$N_{w_1}(u) = u, \quad N_{w_1}(v) = v + w_1, \quad N_{w_1}(w) = w + B(w_1, w)u \quad (w \in W). \tag{10}$$

Conditions (7)(a) and (7)(c) are very simple to check. For (7)(b), we compute (for any $w \in W$)

$$\begin{aligned} B(N_{w_1}(u), N_{w_1}(w)) &= B(u, w + B(w_1, w)u) \\ &= B(u, w) + B(w_1, w)B(u, u) \\ &= B(u, w) = 0, \end{aligned}$$

since $B(u, u) = 0$ and $B(u, w) = 0$. Similarly,

$$\begin{aligned} B(N_{w_1}(v), N_{w_1}(w)) &= B(v + w_1, w + B(w_1, w)u) \\ &= B(v, w) + B(w_1, w)B(v, u) + B(w_1, w) + B(w_1, w)B(w_1, u) \\ &= -B(w_1, w) + B(w_1, w) + B(w_1, w) \cdot 0 = 0. \end{aligned}$$

At the last step we use $B(v, u) = -1$ (cf. (5)(a)). Therefore N_{w_1} belongs to $\mathrm{Stab}_{Sp(V)}([u])$.

The final class of elements is a large one, but easy to deal with. Suppose R is any element of $Sp(W)$, the symplectic group of the form B_W on W. Define

$$M_R(u) = u, \quad M_R(v) = v, \quad M_R(w) = R(w) \quad (w \in W). \tag{11}$$

Verification that M_R satisfies the conditions (7) is almost trivial; the only interesting one is (7)(c), and that is just the requirement that R belong to $Sp(W)$. Therefore M_R belongs to $\mathrm{Stab}_{Sp(V)}([u])$.

Proposition 12. *Suppose that u is a non-zero vector in the symplectic vector space V. Choose another vector v so that $B(u, v) = 1$, and let W be the subspace orthogonal to u and v (see (5) and (6) above). Define elements A_k, Z_x, N_{w_1}, and M_R of $\mathrm{Stab}_{Sp(V)}([u])$ as in (8)–(11) above.*

1. *The collection A of elements $\{A_k \mid k \in F^\times\}$ is a subgroup of $Sp(V)$, isomorphic to the multiplicative group $F^\times$ of F.*
2. *The collection Z of elements $\{Z_x \mid x \in F\}$ is a subgroup of $Sp(V)$, isomorphic to the additive group of F.*

(3) *The collection N of elements $\{N_{w_1}Z_x \mid w \in W, x \in F\}$ is a subgroup of $Sp(V)$. The expression of each element of N as a product $N_{w_1}Z_x$ is unique. The group law is*

$$(N_{w_1}Z_{x_1})(N_{w_2}Z_{x_2}) = N_{w_1+w_2}Z_{x_1+x_2+B(w_1,w_2)}.$$

Consequently Z is a normal subgroup of N (equal to the center of N if the characteristic is not 2), and the quotient group N/Z is isomorphic to the additive group of the vector space W.

(4) *The collection M of elements $\{M_R \mid R \in Sp(W)\}$ is a subgroup of $Sp(V)$, isomorphic to $Sp(W)$.*

(5) *The collection L of elements $\{M_R A_k \mid R \in Sp(W), k \in F^\times\}$ is a subgroup of $Sp(V)$, isomorphic to the product group $Sp(W) \times F^\times$.*

(6) *The groups A and M act by conjugation on N, according to the formulas*

$$A_k(N_{w_1}Z_x)A_k^{-1} = N_{kw_1}Z_{k^2x},$$

$$M_R(N_{w_1}Z_x)M_R^{-1} = N_{Rw_1}Z_x.$$

(7) *Every element of $T \in \mathrm{Stab}_{Sp(V)}([u])$ has a unique representation as a product*

$$T = M_R A_k N_{w_1} Z_x \quad (R \in Sp(W), k \in F^\times, w_1 \in W, x \in F).$$

The subgroups N and Z are normal in $\mathrm{Stab}_{Sp(V)}([u])$. The quotient group $\mathrm{Stab}_{Sp(V)}([u])/N$ is isomorphic to the product $L = A \times M$.

(8) *Suppose that $F = \mathbb{F}_q$. Then*

$$|\mathrm{Stab}_{Sp(V)}([u])| = (q-1) \cdot q^{2n-1} \cdot |Sp(W)|;$$

here $2n$ is the dimension of V. Furthermore

$$|Sp(V)| = (q^{2n}-1) \cdot q^{2n-1} \cdot |Sp(W)|.$$

Notice that the collection of elements N_{w_1} does *not* constitute a group: it is not closed under multiplication.

Proof. To prove (1), we just compute from (8) that $A_k A_{k'} = A_{kk'}$. Part (2) is similar. For (3), we calculate

$$\begin{aligned} &N_{w_1}Z_{x_1}(u) = u, \\ &N_{w_1}Z_{x_1}(v) = N_{w_1}(v + x_1 u) = v + w_1 + x_1 u, \\ &N_{w_1}Z_{x_1}(w) = N_{w_1}(w) = w + B(w_1, w)u. \end{aligned} \tag{13}$$

A first consequence of these formulas is that

$$N_{w_1}Z_{x_1}(v) - v = x_1 u + w_1.$$

From this formula it is evident that x_1 and w_1 are determined uniquely by $N_{w_1}Z_{x_1}$, which proves the second claim of (3). To check the displayed formula, it is straightforward to compute the action of the linear transformations $(N_{w_1}Z_{x_1})(N_{w_2}Z_{x_2})$ on u, v, and an element $w \in W$; for example,

$$\begin{aligned}(N_{w_1}Z_{x_1})(N_{w_2}Z_{x_2})(v) &= (N_{w_1}Z_{x_1})(v + w_2 + x_2u)\\ &= (v + w_1 + x_1u) + (w_2 + B(w_1, w_2)u) + x_2u\\ &= v + (w_1 + w_2) + (x_1 + x_2 + B(w_1, w_2))u.\end{aligned}$$

Now one has only to check that these formulas agree with the ones in (13) for $N_{w_1+w_2}Z_{x_1+x_2+B(w_1,w_2)}$. This is trivial for the action on u (which is fixed in both cases), and clear for the action on v written above. The case of $w \in W$ is similar. This proves the formula for multiplication. That N is a subgroup follows very easily. The remaining assertions in (3) are easy consequences of the formula for the group law.

Parts (4) and (5) are extremely easy. For part (6), we compute the left sides acting on u, and v, and an element $w \in W$ (using (13)), and compare with the formulas in (13) for the right side. As an example, here is the calculation of the left side of the second display in (6) on an element $w \in W$:

$$\begin{aligned}M_R(N_{w_1}Z_x)M_R^{-1}(w) &= M_R(N_{w_1}Z_x)(R^{-1}w)\\ &= M_R\left(R^{-1}w + B(w_1, R^{-1}w)u\right)\\ &= w + B(w_1, R^{-1}w)u.\end{aligned}$$

Because R is symplectic, $B(w_1, R^{-1}w) = B(Rw_1, w)$. The left side is therefore

$$w + B(Rw_1, w)u = N_{Rw_1}Z_x(w),$$

using the formula in (13). This shows that the two sides agree on W. The other cases are similar but easier.

For part (7), we first address the uniqueness of the decomposition. Using (13), ((11), and (8), we compute

$$\begin{aligned}M_RA_kN_{w_1}Z_x(u) &= ku\\ M_RA_kN_{w_1}Z_x(v) &= k^{-1}v + Rw_1 + kxu\\ M_RA_kN_{w_1}Z_x(w) &= Rw + kB(w_1, w)u\end{aligned} \tag{14}$$

Suppose that we have two decompositions

$$M_RA_kN_{w_1}Z_x = M_{R'}A_{k'}N_{w_1'}Z_{x'}.$$

From the first equation in (14), we deduce that $k = k'$. From the third we deduce $R = R'$. From these two equalities and the second equations in (14), it finally follows that $kx = k'x'$ and $Rw_1 = R'w_1'$, so that $x = x'$ and $w_1 = w_1'$, as we wished to show.

We now prove the existence of the decomposition. Suppose $T \in \mathrm{Stab}_{Sp(V)}([u])$. This means that $Tu = ku$ for some non-zero scalar $k \in F^\times$. Hence

$$A_k^{-1}Tu = u.$$

Now $A_k^{-1}T$ is an element of $\mathrm{Stab}_{Sp(V)}([u])$ fixing u. It must therefore carry v to some element v' such that $B(u, v') = 1$. Such an element v' is necessarily of the form $v + xu + w_2$, with $w_2 \in W$:

$$A_k^{-1}Tv = v + xu + w_2.$$

From (13) we deduce

$$[N_{w_2}Z_x]^{-1}A_k^{-1}Tu = u, \qquad [N_{w_2}Z_x]^{-1}A_k^{-1}Tv = v.$$

Now $[N_{w_2}Z_x]^{-1}A_k^{-1}T$ is an element of $\mathrm{Stab}_{Sp(V)}([u])$ fixing both u and v. As a consequence of the orthogonal decomposition (6), such a symplectic transformation must be equal to M_R for some $R \in Sp(W)$. That is,

$$[N_{w_2}Z_x]^{-1}A_k^{-1}T = M_R,$$

or

$$T = A_k N_{w_2} Z_x M_R.$$

Set $w_1 = R^{-1}w_2$; then according to (6) of the Proposition,

$$T = M_R A_k N_{w_1} Z_x,$$

as we wished to show. The normality of N and Z follow easily from this decomposition and from (6). The decomposition also implies the last isomorphism in (7).

In part (8), the unique decomposition of (7) lets us count the elements of the stabilizer of $[u]$. The formula for $|Sp(V)|$ then follows from Lemma 3 and the counting formula for group actions. We use also the fact that $|\mathbb{P}(V)| = (q^{2n} - 1)/(q - 1)$. □

Corollary 15. *Suppose that V is a symplectic vector space of dimension $2n$ over a finite field $\mathbb{F}_q$. Then*

$$|Sp(V)| = (q^{2n} - 1)(q^{2n-2} - 1) \cdots (q^2 - 1) \cdot q^{n^2}.$$

W. e can apply the counting formula of Proposition 12(8) for $|Sp(V)|$ again to $Sp(W)$, as long as W has dimension greater than 0 (so that we can find a non-zero vector u to start the argument). In the end we come down to the symplectic group of the zero vector space, which consists of the identity element alone. The resulting formula is

$$|Sp(V)| = (q^{2n} - 1) \cdot q^{2n-1} \cdot (q^{2(n-1} - 1) \cdot q^{2(n-1)-1} \cdots (q^2 - 1) \cdot q.$$

The powers of q can be collected, giving a total exponent of

$$\sum_{k=1}^{n} (2k - 1) = n^2.$$

□

I will just give a few hints about the second application of the structure theorem for $\mathrm{Stab}_{Sp(V)}([u])$. We showed that Z is an abelian normal subgroup of the stabilizer. Notice that the elements of Z_x of Z are precisely the symplectic transvections (called $\tau_{u,x}$ in the text) in the direction u. If T is any element of $Sp(V)$, then it's more or less obvious that

$$TZT^{-1} = \text{transvections in the direction Tu.}$$

So the group generated by all conjugates of Z is the group generated by all symplectic transvections. Yaim Cooper showed in her presentation that this is all of $Sp(V)$. That is,

$$Sp(V) = \text{group generated by all conjugates of } Z.$$

This is one of the requirements for Iwasawa's Theorem, to try to prove that $PSp(V)$ is a simple group. The main additional requirement is that $Sp(V)$ be its own commutator subgroup.

Theorem 16. *Suppose that V is a symplectic vector space of dimension $2n$ over a field F.*

1. *If $|F| \geq 4$, then the derived group of $Sp(V)$ is equal to $Sp(V)$.*
2. *If $\dim V \geq 4$ and $|F| \geq 3$, then the derived group of $Sp(V)$ is equal to $Sp(V)$.*
3. *If $\dim V \geq 6$, then the derived group of $Sp(V)$ is equal to $Sp(V)$.*

F. or part (1), suppose u is any non-zero vector in V. Use the notation of (5)–(11) above. Since $|F| \geq 4$, we can choose an element $b \in F$ not equal to 0 or to ± 1. It follows that $b^2 - 1 \neq 0$. Using the first formula in Proposition 12(6), we can compute the commutator

$$A_b Z_{x/(b^2-1)} A_b^{-1} Z^{-1} Z_{x/(b^2-1)} = Z_{xb^2/(b^2-1)} Z_{-x/(b^2-1)} = Z_{x(b^2-1)/(b^2-1)} = Z_x.$$

This shows that the transvection $Z_x = \tau_{u,x}$ is a commutator. Since u was arbitrary, every transvection is a commutator. Since the transvections generate $Sp(V)$, (1) follows.

Part (2) is done in the text as Proposition 3.8, and part(3) as Proposition 3.9; I won't repeat the arguments. □

Corollary 17. *Except for the cases $|F| = 2$ and $\dim V = 2$ or 4, and $|F| = 3$ and $\dim V = 2$, the group $PSp(V)$ (the quotient of $Sp(V)$ by its center $\pm I$) is a simple group.*

The proof given in the text (Theorem 3.11) works perfectly well for infinite fields also. I won't include the details.

The third reason I gave for studying the stabilizer was that the group was simply interesting. The group N (Proposition 12(3)) is at the heart of that. As a set, it's just a the product of a symplectic vector space W and the ground field F; but the group structure is very interesting.