18.704 Gary Sivek
April 15, 2005 gsivek@mit.edu

PSp(V) is (Almost Always) Simple

Recall that PSp($2n, q$) denotes the projective symplectic group on the vector space $\mathbb{F}_q^{2n}$. On Wednesday we worked through most of the proof that this group is almost always simple. To be exact, our goal was:

Theorem 1: Except for PSp(2,2), PSp(2,3), and PSp(4,2), every group PSp(V) is simple.

The proof was to follow Iwasawa's Theorem, restated here for convenience:

Theorem (Iwasawa): Suppose that G is faithful and primitive on a set S and that $G' = G$, where G' is the derived group of G. Fix $s \in S$ and set $H = \mathrm{Stab}_G(s)$. Suppose there is a solvable subgroup $K \triangleleft H$ such that $G = \langle \cup \{K^x : x \in G\} \rangle$. Then G is simple.

Our first result showed that the center of the symplectic group is $Z(Sp(V)) = \{\pm 1\}$, from which we define $\mathrm{PSp}(V) = \mathrm{Sp}(V)/Z(\mathrm{Sp}(V))$. We know that if $\mathcal{T}$ is the subgroup of $\mathrm{Sp}(V)$ generated by symplectic transvections, then $\mathcal{T}$ acts transitively on $V \setminus \{0\}$, and we saw in a previous lecture that in fact $\mathcal{T} = \mathrm{Sp}(V)$. Since $\mathrm{Sp}(V)$ acts on $\mathbb{P} = \mathbb{P}_{n-1}(V)$ with kernel $Z(\mathrm{Sp}(V))$, we see that $\mathrm{PSp}(V)$ acts faithfully and transitively on $\mathbb{P}$.

Proposition 2: $\mathrm{Sp}(V)$ is primitive on $\mathbb{P}$.
Proof: If $n = 2$ then $\mathrm{Sp}(n, q) = \mathrm{SL}(n, q)$, and $\mathrm{SL}(2, q)$ is always doubly transitive and hence primitive. So assume $n \geq 4$, and assume for the sake of contradiction that there exists a block $S \subseteq \mathbb{P}$ with $|S| > 1$ and either $\sigma S = S$ or $\sigma S \cap S = \emptyset$ for all $\sigma \in \mathrm{Sp}(V)$.

First we show there exist $[u], [v] \in S$ such that $B(u, v) \neq 0$, where B is the nondegenerate alternate form associated with the symplectic space V. If this is false, then pick $[u] \neq [v]$ and choose a function $f \in V*$ satisfying $f(u) = 1$ and $f(v) = 0$. Using a result from chapter 2 of Grove, since B is nondegenerate we can find $x \in V$ such that $B(u, x) = f(u) = 1$ and $B(v, x) = f(v) = 0$; then $W = \mathrm{Span}(u, x)$ is hyperbolic and we can define $H = \{\sigma \in \mathrm{Sp}(V) : \sigma|_W = 1_W\}$. Every $\sigma \in \mathrm{Sp}(W^\perp)$ extends to a $\sigma' \in \mathrm{Sp}(V) = \mathrm{Sp}(W \oplus W^\perp)$ with $\sigma'|_W = 1_W$, so $\mathrm{Sp}(W^\perp) = \{\tau|_{W^\perp} : \tau \in H\}$. Choose a nonzero $w \in W^\perp$; since the transvections act transitively, we can find $\tau \in H$ such that $\tau v = w$; furthermore, since $u \in W$ we know $\tau u = u$, so that $[u] \in S \cap \tau S$ and thus $\tau S = S$. Now $[w] = \tau[v] \in S$ and w was arbitrary; since $W^\perp$ is nonzero it contains some hyperbolic pair (y, z), and $[y], [z] \in S$. But since they are hyperbolic, $B(y, z) = 1$, a contradiction.

So we have $[u], [v] \in S$ with $B(u, v)$ nonzero; assume by rescaling that (u, v) is in fact hyperbolic, and take any $[w] \in \mathbb{P}$. If $B(u, w) \neq 0$ then we may assume that (u, w) is also hyperbolic, and since $\mathcal{T}$ acts transitively on the set of hyperbolic pairs, we can find $\sigma \in \mathrm{Sp}(V)$ such that $\sigma u = u$ and $\sigma v = w$; since $u \in S \cap \sigma S$, we have $S = \sigma S$ and so $[w] \in S$, implying $S = \mathbb{P}$. Otherwise $B(u, w) = 0$; as before we can find $f \in V*$ with $f(u) = B(u, x) = 1$ and $f(w) = B(w, x) = 1$, so we have two hyperbolic pairs again and we can find $\tau \in \mathrm{Sp}(V)$ such that $\tau u = w$ and $\tau x = x$. By the same reasoning as before, $[x] \in S$ and so we must have

$\tau S = S$, implying since $[w] = \tau u \in \tau S = S$ that $S = \mathbb{P}$. Thus in either case we have $S = \mathbb{P}$ and so $\mathrm{Sp}(V)$ acts primitively. $\square$

Corollary: $\mathrm{PSp}(V)$ also acts primitively on $\mathbb{P}$.

In class on Wednesday we proved the following three results, so I will not do more than sketch their proofs here.

Proposition 3: If $q \geq 4$ then $\mathrm{Sp}'(n, q) = \mathrm{Sp}(n, q)$.

Proposition 4: If $q = 3$ and $n \geq 4$ then $\mathrm{Sp}'(n, q) = \mathrm{Sp}(n, q)$.

Proposition 5: If $q = 2$ and $n \geq 6$ then $\mathrm{Sp}'(n, q) = \mathrm{Sp}(n, q)$.

We proved Proposition 3 by picking an arbitrary $a \in \mathbb{F}^*$, setting $c = a/(1 - b^2)$, setting $d = -b^2c$, choosing $\sigma \in \mathrm{Sp}(V)$ such that $\sigma u = bu$, and showing that $\tau_{u,c}\sigma\tau_{u,c}^{-1}\sigma^{-1} = \tau_{u,a}$, thus constructing an arbitrary generator of $\mathrm{Sp}(V)$. Propositions 4 and 5 were proved by fixing symplectic bases and carefully selecting two linear transformations on those basis elements such that a specific conjugate of their commutator was an arbitrary generator of $\mathrm{Sp}(V)$.

Proof of Theorem 1: We know now that $\mathrm{PSp}(V)$ is primitive and faithful on $\mathbb{P}$, and that it is its own derived group. Fix $[u] \in \mathbb{P}$ and set $H = \mathrm{Stab}_{\mathrm{Sp}(V)}([u])$. Then define $\overline{H} = H/\{\pm 1\} = \mathrm{Stab}_{\mathrm{PSp}(V)}([u])$ and $K = \{\tau_{u,a} : a \in \mathbb{F}_q\}$. It can be shown that $K \triangleleft H$, and since $\tau_{u,a}\tau_{u,b} = \tau_{u,a+b}$ we have $K \cong \mathbb{F}_q^+$, so K is abelian. It is also a straightforward exercise to show that for $\sigma \in \mathrm{Sp}(V)$ we have ${}^{\sigma}K \supseteq \{\tau_{\sigma u,a} : a \in \mathbb{F}_q\}$, so since $\mathcal{T}$ acts transitively we see that $\cup\{{}^{\sigma}K : \sigma \in \mathrm{Sp}(V)\}$ contains all symplectic transvections and thus generates all of $\mathrm{Sp}(V)$. We conclude that $\langle \overline{{}^{\sigma}K} : \overline{\sigma} \in \mathrm{PSp}(V)\rangle = \mathrm{PSp}(V)$, completing the last condition for Iwasawa's Theorem. Thus all projective symplectic groups other than PSp(2,2), PSp(2,3), and PSp(4,2) are simple. $\square$

As a final note, we must remember that Iwasawa's Theorem gives *sufficient* conditions for simplicity, not *necessary* ones, so this does not by itself prove that those three exceptions are not simple. What we find, however, is that $\mathrm{PSp}(2, 2) \cong S_3$, $\mathrm{PSp}(2, 3) \cong A_4$, and $\mathrm{PSp}(4, 2) \cong S_6$, none of which are simple. The proof of these three isomorphisms is left as an exercise to the reader.

References

1. Grove, L.C. Classical groups and geometric algebra, American Mathematical Society, Providence, RI, 2002.

2. Eric W. Weisstein. "Projective Symplectic Group." From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/ProjectiveSymplecticGroup.html