18.704 Supplementary Notes: Sylow Subgroups of The Symplectic Group

Rachel Lee

Friday, April 29, 2005

Sylow Subgroups

Definition: A *Sylow p-subgroup* of G is a maximal p-subgroup of G.

This means the Sylow subgroup is a subgroup of G which is a p-group, and is not a proper subgroup of any other p-subgroup of G.

Our interest is to find the Sylow p-subgroup of the Symplectic group. Since we know all Sylow subgroups of a given group are isomorphic to each other, we need to only find one of these such groups.

First we will find the order of the Sylow subgroup so that we can construct a subgroup of that order.

Sylow Subgroups of the Symplectic Group

Order of the Sylow Subgroup

From previous lectures, we know the order of the Symplectic group $Sp(2n, F_q)$:

$$|Sp(2n, F_q)| = q^{n^2}(q^{2n} - 1)......(q^2 - 1)$$

The largest power of q that divides the order of the Symplectic group is q^{n^2} since none of the other terms have factors of q, this is our largest p, and therefore the order of the Sylow subgroup.

Finding Elements of the Sylow Subgroup

There are two directions we can go in to find the Sylow Subgroup of $Sp(2n, F_q)$. We can look only at the order of known subgroups, or we can start with a nice basis and construct the member matrices. First let's look at orders:

Dealing with Order to Find the Sylow Subgroup

Let V be our $2n - dimensional$ Symplectic space. We can find an $S \subset V$ such that S is an $n - dimensional$ isotropic subspace of V. The stabilizer of S is $P(S)$.

$$P(S) = g \in Sp(V) | gS = S$$

From previous lectures, we know the stabilizer of an isotropic subspace

$$P(S) \simeq GL(n, F_q) \cdot Sp(2(n-k)) \cdot N(S)$$

Where k is the dimension of S. If $k = n$, the middle term disappears. We know $GL(n, F_q)$ has a Sylow subgroup of order $q^{\frac{n(n-1)}{2}}$. We also know $N(S)$ is composed of $n \times n$ symmetric matrices with entries in F_q, and $dim(N(S)) = \frac{n(n+1)}{2}$ so the order of $N(S)$ is $|N(S)| = q^{\frac{n(n+1)}{2}}$.

Since $|N(S)| \cdot |\text{sylow subgroup of} GL(n, F_q)| = q^{\frac{n(n-1)}{2}} \cdot q^{\frac{n(n+1)}{2}} = q^{n^2}$, this is the order we established for the sylow subgroup of $Sp(2n, F_q)$, and all sylow subgroups of a given group are ispmorphic to each other, we need only to construct this one subgroup within $Sp(2n, F_q)$.

Constructing the Matrices in the Sylow Subgroup

The normal subgroup of S:

$$N(S) = \begin{pmatrix} I_n & A \\ 0_n & I_n \end{pmatrix}$$

Where A is a symmetric $n \times n$ matrix.

Show $N(S)$ symplectic:

Consider a symplectic form $B(v, w)$. We need to show that

$$B\left(\begin{pmatrix} I_n & A \\ 0_n & I_n \end{pmatrix} \begin{pmatrix} s_1 \\ t_1 \end{pmatrix}, \begin{pmatrix} I_n & A \\ 0_n & I_n \end{pmatrix} \begin{pmatrix} s_2 \\ t_2 \end{pmatrix} \right) = B\left(\begin{pmatrix} s_1 \\ t_1 \end{pmatrix}, \begin{pmatrix} s_2 \\ t_2 \end{pmatrix} \right)$$

Apply the Symplectic form B to the left side:

$$B\left(\begin{pmatrix} I_n & A \\ 0_n & I_n \end{pmatrix} \begin{pmatrix} s_1 \\ t_1 \end{pmatrix}, \begin{pmatrix} I_n & A \\ 0_n & I_n \end{pmatrix} \begin{pmatrix} s_2 \\ t_2 \end{pmatrix} \right) = B\left(\begin{pmatrix} s_1 + At_1 \\ t_1 \end{pmatrix}, \begin{pmatrix} s_2 + At_2 \\ t_2 \end{pmatrix} \right)$$

$= s_1t_2 + At_1t_2 - (s_2t_1 + At_2t_1)$

Since A is symmetric, the two terms with A cancel, and we are left with:

$$s_1t_2 - s_2t_1$$

which is exactly the inner product $B\left(\begin{pmatrix} s_1 \\ t_1 \end{pmatrix}, \begin{pmatrix} s_2 \\ t_2 \end{pmatrix} \right)$.

So N is symplectic. □

Together $N(S)$ and $GL(n, F_q)$ form the maximal parabolic subgroup. This is a little larger than the Sylow subgroup we are looking for.

Now consider the Sylow subgroup M of $GL(n, F_q)$ found in a previous lecture:

$$M = \begin{pmatrix} \begin{pmatrix} 1 & .. & * \\ .. & .. & .. \\ 0 & .. & 1 \end{pmatrix} & 0 \\ 0 & \begin{pmatrix} 1 & .. & 0 \\ .. & .. & .. \\ * & .. & 1 \end{pmatrix} \end{pmatrix}$$

M and $N(S)$ together form the Sylow subgroup of $Sp(2n, F_q)$.

To prove this we will use the following theorem.

Theorem

Suppose G is a group. G has normal subgroup N, and another subgroup H. (H is the quotient group G/N.) Assume every element $g \in G$ is uniquely $g = \{h \cdot n | h \in H, n \in N\}$. Then:

(1) If $M \subset H$ is any subgroup of G, then $M \cdot N$ is a subgroup of G since N is normal.

(2) This is all subgroups of G containing N.

Proof that $M \cdot N$ is a Sylow subgroup of $Sp(2n, F_q)$

We know $GL(n, F_q)$ is a subgroup of $P(S)$. M is the sylow subgroup of $GL(n, F_q)$ so it is also a subgroup of $P(S)$. $N(S)$ is the normal subgroup of $P(S)$ by definition. From the theorem, $M \cdot N$ is a subgroup of $P(S)$, which also makes it a subgroup of $Sp(2n, F_q)$ transitively. Previously we mentioned that the order $|N(S)| = q^{\frac{n(n+1)}{2}}$, and the order of the Sylow subgroup of $GL(n, F_q)$, or the order of M as we now know it, is $|M| = q^{\frac{n(n-1)}{2}}$. So the order of $|M \cdot N| = q^{\frac{n(n-1)}{2}} \cdot q^{\frac{n(n-1)}{2}} = q^{n^2}$. Therefore, $M \cdot N$ is a sylow subgroup of $Sp(2n, F_q)$ because it is a subgroup with order q^{n^2}. □