18.704 Gabe Cunningham
3/9/05 gcasey@mit.edu

Sylow Theorems and The General Linear Group

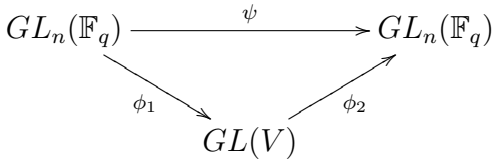
Theorem 1 (First Sylow Theorem) *Let G be a group of order n with $p|n$. Write $n = p^a m$ where p does not divide m. Then G has a subgroup S of order p^a, called a* Sylow p-subgroup *of G.*

Recall from our last discussion that $|GL_n(\mathbb{F}_q)| = \prod_{k=0}^{n-1}(q^n - q^k) = q^{n(n-1)/2}\prod_{k=1}^{n}(q^k - 1)$. If $q = p^r$, the First Sylow Theorem tells us that $GL_n(\mathbb{F}_q)$ has a Sylow p-subgroup of order $q^{n(n-1)/2}$. Now I'll describe one such group.

Proposition 1 *Let $q = p^r$; let $MT_n(\mathbb{F}_q)$ be the group of upper triangular matrices with 1's along the diagonal. Then $MT_n(\mathbb{F}_q)$ is a Sylow p-subgroup of $GL_n(\mathbb{F}_q)$.*

Proof: It's clear that $MT_n(\mathbb{F}_q)$ is a subgroup of $GL_n(\mathbb{F}_q)$, so it suffices to show that $MT_n(\mathbb{F}_q)$ has order $q^{n(n-1)/2}$. This follows simply; each of the $n(n-1)/2$ entries strictly above the diagonal can be any element of $\mathbb{F}_q$, for a total of $q^{n(n-1)/2}$ elements.

Now for a bit of a diversion. Let V be an n-dimensional vector space over $\mathbb{F}_q$. We define $GL(V)$ to be the group of invertible linear transformations from V to itself. There is a natural isomorphism between $GL(V)$ and $GL_n(\mathbb{F}_q)$; fix a basis for V and consider the matrices of the linear transformations in $GL(V)$ with respect to that basis. By picking two different bases, B_1 and B_2, we can compose the isomorphisms obtained from each choice of basis to get an isomorphism ψ from $GL_n(\mathbb{F}_q)$ to itself as follows:



Let's consider an example. Let $A = \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right) \in GL_2(\mathbb{F}_5)$. Let V be a two-dimensional vector space over $\mathbb{F}_5$; let $e_1 = (1, 0)$ and $e_2 = (0, 1)$. Then by considering A as the matrix of some linear transformation T with respect to the standard basis of V (i.e., the basis (e_1, e_2)), we can map A to T by requiring that $T(e_1) = e_1$ and $T(e_2) = 2e_1 + e_2$; this fully determines $T \in GL(V)$. Now we fix a new basis, say, $(e_1 + e_2, e_1 - e_2)$. Since $T(e_1 + e_2) = 3e_1 + e_2 = 2(e_1 + e_2) + (e_1 - e_2)$ and $T(e_1 - e_2) = -e_1 + e_2 = -(e_1 - e_2)$, the matrix of T with respect to this new basis is $\left(\begin{smallmatrix} 2 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. So in our isomorphism ψ, the matrix $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$ is mapped to $\left(\begin{smallmatrix} 3 & -1 \\ 1 & 1 \end{smallmatrix}\right)$.

Now, let's consider the subgroup $H = \psi(MT_n(\mathbb{F}_q))$ of $GL_n(\mathbb{F}_q)$. H is, of course, also a Sylow p-subgroup of $GL_n(\mathbb{F}_q)$. By considering several changes of basis, we can find several subgroups H_1, H_2, etc., all isomorphic to $MT_n(\mathbb{F}_q)$. Two natural questions arise. The first is whether all Sylow p-subgroups are isomorphic by a change-of-basis isomorphism. The second is whether there's an easier way to describe the relationship between these Sylow p-subgroups. Thankfully, the answer to both questions is yes.

Proposition 2 *Let T be a linear transformation from V to itself, and let A be the matrix of T with respect to a particular basis B. Then the matrices A' that represent T with respect to different bases are of the form*

$$A' = PAP^{-1}$$

for $P \in GL_n(\mathbb{F}_q)$.

I'm not going to prove this proposition, but you can find a proof in Artin's *Algebra* on pages 115 and 116, or in many other places, I'm sure. This proposition tells us that A and $\psi(A)$ are conjugate (or in the language of linear algebra, *similar*), for any change-of-basis isomorphism ψ. Thus, the Sylow p-subgroups $MT_n(\mathbb{F}_q)$ and $\psi(MT_n(\mathbb{F}_q))$ are conjugate as well. As it turns out, all of the Sylow p-subgroups of a group G are conjugate; this is Sylow's second theorem.

Theorem 2 (Second Sylow Theorem) *The Sylow p-subgroups of a group G are conjugate.*

Finally, let us turn to the third Sylow theorem.

Theorem 3 (Third Sylow Theorem) *Let s be the number of Sylow p-subgroups of G; let $|G| = p^a m$ where p does not divide m. Then s divides m and s is congruent to 1 (mod p).*

We've seen already that we get one Sylow p-subgroup of $GL_n(\mathbb{F}_q)$ by taking the group of upper triangular matrices with 1's along the diagonal. In similar fashion, the group of *lower* triangular matrices with 1's along the diagonal is a Sylow p-subgroup. Since for $n \geq 2$ these two groups aren't the same (and when $n = 1$, p doesn't divide the order of $GL_n(\mathbb{F}_q)$), the number of Sylow p-subgroups of $GL_n(\mathbb{F}_q)$ is greater than 1, so it is at least $p+1$. We notice that $p+1$ divides $q^2 - 1$, so it is an allowable number of Sylow p-subgroups. Unfortunately, even for small q and n, $GL_n(\mathbb{F}_q)$ is large and there are a lot of choices of s that fulfill the requirements of the third Sylow theorem. In principle, it shouldn't be difficult to find s; we know one easily described Sylow p-subgroup, and we just need to conjugate it to find all the others. This is tedious, but I don't know of a better way to count the Sylow p-subgroups.

Addendum: We discussed in class how to count the number of Sylow p-subgroups of $GL_n(\mathbb{F}_q)$. Let X be the set of Sylow p-subgroups. The second Sylow theorem tells us that if we let $GL_n(\mathbb{F}_q)$ act on X by conjugation, the action is transitive. Let $H = MT_n(\mathbb{F}_q)$; let N be the normalizer of H (that is, the set of $g \in GL_n(\mathbb{F}_q)$ such that $gHg^{-1} = H$). Then, by the counting formula,

$$|GL_n(\mathbb{F}_q)| = |N| \cdot |X|$$

So if we can find the normalizer of H and count the elements of it, we can find the number of Sylow p-subgroups, s. (Note that this argument holds for any finite group G; indeed, it is the basis on which the third Sylow theorem is proved.) Without getting into details,

it turns out that the normalizer of H is the group of upper triangular matrices, which has $(q-1)^n q^{n(n-1)/2}$ elements. Therefore,

$$\begin{aligned} s &= \frac{q^{n(n-1)/2}\prod_{k=1}^{n}(q^k-1)}{q^{n(n-1)/2}(q-1)^n} \\ &= \frac{1}{(q-1)^n}\prod_{k=1}^{n}(q^k-1) \\ &= \prod_{k=1}^{n}\frac{q^k-1}{q-1} \\ &= \prod_{k=1}^{n}(q^{k-1}+q^{k-1}+\cdots+1) \\ &= [n!]_q \end{aligned}$$