Group Theory (Math 311)
Final on Sylow Subgroups of $\mathrm{Sym}(n)$

Fall 2005
Ali Nesin

January 19, 2005

Question. *Study the structure of the Sylow p-subgroups of* $\mathrm{Sym}(n)$.

Proposition 1 *Let $n \in \mathbb{N}$ and p a prime. Let $k = [n/p]$. Then a Sylow p-subgroup of $\mathrm{Sym}(n)$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^k \rtimes P$ where P is a Sylow p-subgroup of $\mathrm{Sym}(k)$ and P acts on $(\mathbb{Z}/p\mathbb{Z})^k$ by permuting the components.*

The generators of $(\mathbb{Z}/p\mathbb{Z})^k$ can be taken to be the cycles

$$\sigma_i = ((i-1)p+1, \ldots, ip)$$

for $i = 1, \ldots, k$. The element $\sigma_1\sigma_2\ldots\sigma_k$ is in the center of the Sylow p-subgroup. And the center of the Sylow p-subgroup is in $(\mathbb{Z}/p\mathbb{Z})^k$.

Proof: Let P be a Sylow p-subgroup of $\mathrm{Sym}(n)$. We first note that $|P| = p^{[n/p]+[n/p^2]+\cdots}$.

If p does not divide n, then $P \leq \mathrm{Sym}(n-1) \leq \mathrm{Sym}(n)$. So we may assume that p divides n. Let $n = kp$. Now we have $|P| = p^{[n/p]+[n/p^2]+\cdots} = p^{k+[k/p]+[k/p^2]\cdots}$.

Since P has a nontrivial center, there is an element z of order p in $Z(P)$. Conjugating if necessary, we may assume that

$$z = z_i = (1, 2, \ldots, p)(p+1, p+2, \ldots, 2p)\ldots((i-1)p+1, (i-1)p+2, \ldots, ip)$$

for some $i = 1, \ldots, k$. Thus $P \leq C_{\mathrm{Sym}(n)}(z_i)$. Now we compute $|C_{\mathrm{Sym}(n)}(z_i)|$ and choose i so that $p^{[n/p]+[n/p^2]+\cdots}$ (which is equal to $p^{k+[k/p]+[k/p^2]\cdots}$) divides $|C_{\mathrm{Sym}(n)}(z_i)|$.

It is clear that

$$|z_i^{\mathrm{Sym}(n)}| = \frac{\binom{n}{p}(p-1)!\binom{n-p}{p}(p-1)!\ldots\binom{n-(i-1)p}{p}(p-1)!}{i!} = \frac{n!}{p^i i!}$$

Thus

$$|C_{\mathrm{Sym}(n)}(z_i)| = |\,\mathrm{Sym}(n)|/|z_i^{\mathrm{Sym}(n)}| = p^i i!$$

The maximal power of p that divides $p^i i!$ is $p^i p^{[i/p]+[i/p^2]+\cdots} = p^{i+[i/p]+[i/p^2]+\cdots}$. Thus if we take $i = k$, then $C_{\mathrm{Sym}(n)}(z_i)$ will be large enough to contain P.

We now find $C_{\mathrm{Sym}(n)}(z_k)$. Recall that it has $p^k k!$ elements. Let

$$\sigma_i = ((i-1)p+1, \ldots, ip)$$

for $i = 1, \ldots, k$. Then

$$(\mathbb{Z}/p\mathbb{Z})^k \simeq \langle \sigma_1, \sigma_2, \ldots \sigma_k \rangle = \langle \sigma_1 \rangle \oplus \langle \sigma_2 \rangle \oplus \ldots \oplus \langle \sigma_k \rangle \leq C_{\mathrm{Sym}(n)}(z_k).$$

Also the elements of $\mathrm{Sym}(n)$ that permute the cycles of σ_i are in $C_{\mathrm{Sym}(n)}(z_k)$. Consider the ones of the form $\{\sigma :$ for all $i = 1, \ldots, k$, $\sigma(ip) = jp$ for some j and $\sigma(ip - \ell) = \sigma(ip) - \ell$ for all $\ell = 1, \ldots, p-1\} \simeq \mathrm{Sym}(k)$. It is easy to see that $C_{\mathrm{Sym}(n)}(z_k) \simeq (\mathbb{Z}/p\mathbb{Z})^k \rtimes \mathrm{Sym}(k)$, where $\mathrm{Sym}(k)$ permutes the components. Thus P is isomorphic to a Sylow p-subgroup of $(\mathbb{Z}/p\mathbb{Z})^k \rtimes \mathrm{Sym}(k)$, which is $(\mathbb{Z}/p\mathbb{Z})^k \rtimes Q$ for some Sylow p-subgroup Q of $\mathrm{Sym}(k)$. The last statements are easy to prove. □

Corollary 2 *If $p \neq 2$ then Sylow p-subgroup of* $\mathrm{Sym}(n)$ *are in* $\mathrm{Alt}(n)$.

If $p = 2$, then with the notation of the theorem above, a Sylow 2-subgroup of $\mathrm{Alt}(n)$ *is isomorphic to*

$$\{(a_0, \ldots, a_{k-1}) : \sum_{i=0}^{k-1} a_i \text{ is even}\} \rtimes P$$

where P is a Sylow 2-subgroup of $\mathrm{Sym}(k)$ *and it acts on the normal part by permuting the components.*

Corollary 3 *Let G be a finite p-group. Then there is a finite p-subgroup P such that $G \leq P$ and $Z(P) \simeq \mathbb{Z}/p\mathbb{Z}$.*