4. Cauchy and Sylow Theorems

The Sylow Theorems

Background

Sylow's Theorem was proved in 1872.

- Sylow's original paper is available here.
- A brief biography of Sylow is given at the MacTutor Archive.

- The paper *The Early Proofs of Sylow's Theorem* by Waterhouse talks about the mathematics of the early work on this problem. (You'll need UConn library access, or JSTOR access, to access Waterhouse's paper).

The Theorems

Theorem: (Cauchy) Let G be a group of order n and suppose $p|n$. Then G has an element of order p.

Proof: We prove this by induction on the order of G. We have proved this if G is abelian, and in particular if $|G| = p$. Suppose G is not abelian. Consider its class equation

$$|G| = |Z(G)| + \sum_{g}[G : C_G(g)]$$

where the sum is over representatives for the conjugacy classes of G of size greater than one. Since G is nonabelian there is at least one such class. Since the left side of this equation is divisible by p, so is the right side. If $|Z(G)|$ is divisible by p then, since $Z(G)$ is abelian, it contains an element of order p. Otherwise, at least one of $[G : C_G(g)]$ is not divisible by p. Therefore by Lagrange's theorem $|C_G(g)|$ is divisible by p. Since $C_G(g)$ is smaller then G, it contains an element of order p by induction.

Theorem: Let G be a finite group of order n and let p be a prime number.

1. There exists a subgroup P of p-power order such that $[G : P]$ is prime to p. Such a subgroup is called a Sylow p-subgroup of G.

2. If P is any Sylow p-subgroup of G, and H is any subgroup of G of prime power order, then some conjugate of H is contained in P. In particular, all Sylow p-subgroups are conjugate.
3. Let n_p be the number of Sylow p-subgroups in G. Then $n_p \equiv 1 \pmod{p}$ and $n_p|n$.

Note: One proof is given in DF, Chapter 4, page 139-140. We follow Keith Conrad's approach.

We will construct our Sylow p-subgroup by constructing an increasing sequence of groups $H_1 \subset H_2 \subset \cdots$ where H_i has order p^i and the process stops when the index of H_i in G becomes prime to p.

We recall this lemma about group actions.

Lemma: Suppose X is a set on which a group G acts transitively.
Let $x \in X$ and let H be the stabilizer of x in G. Let $N = N_G(H)$. Then N permutes the fixed points of H transitively, so the number of such fixed points is $[N : H]$.

Proof: Suppose H fixes x. If H also fixes x', write $x' = gx$ for some $g \in G$. Then gHg^{-1} fixes x' so $gHg^{-1} = H$ and $g \in N_G(H)$. Conversely, if $g \in N_G(H)$, then gHg^{-1} fixes gx so H fixes gx.

We will need the following lemma about the action of p groups on finite sets.

Lemma: Suppose X is a finite set with an action of a finite p-group H. Let $\mathrm{Fix}_H(X)$ be the set of points in X that are fixed by H. Then

$$|X| \equiv |\mathrm{Fix}_H(X)| \pmod{p}.$$

Proof: Under the action of H, X breaks up into orbits of varying sizes; these sizes divide the order of H, which is a power of p. The orbits of size bigger than one all of size divisible by p. The orbits of size one are the fixed points. So the number of elements in X is the number of fixed points plus a sum of powers of p.

Proof of Sylow:

Part 1. 1. By Cauchy there is a subgroup H of order p in G.
2. Suppose now that H is a subgroup of order p^i. If $[G : H]$ is prime to p, we are done. 3. Consider the action of H on the homogeneous space of cosets $X = G/H$. 4. X breaks up into orbits under the action of H, each orbit being of size 1 or a power of p.
5. By the second Lemma above, the number of elements of X fixed by H is divisible by p. 6. By the first lemma, the index $[N_G(H) : H]$ is divisible by p. 7. By Cauchy's theorem, the group $N_G(H)/H$ has a subgroup of order p. 8. By the isomorphism theorems, the subgroups of $N_G(H)/H$ correspond to the subgroups of $N_G(H)$ containing H. Therefore there is a subgroup of $N_G(H)$ of order p^{i+1}. 9. We have shown that if p^k is the exact power of p dividing n, and

$i < k$, then any subgroup of order p^i is contained in a subgroup of order p^{i+1}. Thus there must be a subgroup of order p^k.

Part 2. 1. Let Q be a group of p-power order, and let P be a Sylow p-subgroup. The group Q acts on the homogeneous space G/P, which has prime-to-p order.
2. Since Q is a p-group, we know that

$$|G/P| \equiv |\mathrm{Fix}_Q(G/P) \pmod{p}.$$

3. Since the left side isn't zero, there must be a coset kP which is stabilized by Q.
4. This means kQk^{-1} stabilizes P, which means $Q \subset P$.

Part 3. 1. Let P be a Sylow p-subgroup and let P act on the set of Sylow p-subgroups by conjugation.
P fixes Q provided $gQg^{-1} = Q$ for all $g \in P$, or, in other words, if $P \subset N_G(Q)$.
2. Now Q is also in $N_G(Q)$, and both P and Q are Sylow p-subgroups in $N_G(Q)$.
3. That means P and Q are conjugate in this group by part (2) of Sylow's theorems.
4. On the other hand Q is normal in $N_G(Q)$, which means $P = Q$. 5. We've shown that P is the only fixed point under conjugation by P, and the other orbits under conjugation have size divisible by p. 6. Therefore the number of conjugates is 1 mod p. 7. On the other hand, since G permutes the Sylow p-subgroups transitively under conjugation by part (2), we know that the number of such subgroups (being the size of an orbit) is a divisor of n.