15 Cauchy's theorem and Sylow's theorem part 1 (10/27)

Theorem 15.1 (Cauchy's theorem)**.** *Let G be a finite group and p a prime number dividing $|G|$. Then, G has an element of order p.*

Proof. We will use induction and the abelian case of the theorem established in Exercise 14.2. Assume the result is true for all groups of order less than $|G|$. Note that it is true for groups of order 1, trivially. Recall the class equation

$$|G| = |Z(G)| + \sum_{\mathcal{O} \in G//G \text{ non-central}} |G : N_G(x_{\mathcal{O}})|,$$

where $x_{\mathcal{O}} \in \mathcal{O}$. If some normalizer $N_G(x_{\mathcal{O}})$ has order divisible by p, then it has an element of order p by our inductive hypothesis. Thus, assume that $N_G(x_{\mathcal{O}})$ has no element of order p for any of the non-central conjugacy classes $\mathcal{O}$. It follows from the inductive hypothesis that p does not divide $|N_G(x_{\mathcal{O}})|$ so that p *does* divide the index $|G : N_G(x_{\mathcal{O}})|$. Thus, since p also divides $|G|$, p must divide $|Z(G)|$. But, $|Z(G)| > 1$, so that $Z(G)$ is an abelian group whose order is divisible by p. By the special case of Cauchy's theorem for abelian groups, $Z(G)$ has an element of order p, which is also of order p in G. $\square$

Question 15.2. Having established that there are elements of order p in groups whose order is divisible by p, it is natural to ask about subgroups of other types. Specifically, if $|G| = p^r n$ where $(n, p) = 1$, is there a subgroup of G of order p^r?

Definition 15.3 (p-Sylow subgroups)**.** If G has order $p^r n$ where p is a prime, $r \geqslant 0$, and $(p, n) = 1$, then any subgroup of G of order p^r is called a **p-Sylow** subgroup. The previous question asks if p-Sylow subgroups exist.

Remark 15.4. The next result is the first part of the Sylow theorems. It establishes the existence of p-Sylow subgroups. Later, we will prove that all p-Sylow subgroups are conjugate (and hence isomorphic) and give a way to count them.

Theorem 15.5 (Sylow 1)**.** *Suppose that G is a finite group of order $p^r n$ where p is a prime, $r \geqslant 0$, and $(p, n) = 1$. Then, G contains a p-Sylow subgroup.*

Proof. The theorem trivially holds when G is the trivial group, of order 1. Assume that it holds for all groups of order less than $|G| = p^r n$. If p divides the order of $Z(G)$, then there is a central element of G of order p. This element generates a cyclic subgroup $N \subseteq Z(G)$ isomorphic to $\mathbf{Z}/p$. Since it is a subgroup of $Z(G)$, it is normal. The quotient G/N has order $p^{r-1}n$, which is less than $p^r n$. By the inductive hypothesis, G/N has a p-Sylow subgroup Q of order p^{r-1}. Writing $f \colon G \to G/N$ for the quotient map, $f^{-1}(Q)$ is a p-Sylow subgroup of G.

Now, suppose that p does not divide the order of $Z(G)$. Then, since p divides $|G|$, the class equation implies that for some non-central orbit $\mathcal{O}$, p does not divide $|G : N_G(x_{\mathcal{O}})|$. But, this means that $|N_G(x_{\mathcal{O}})| = p^r m$ for some m prime-to-p. By induction, $N_G(x_{\mathcal{O}})$ contains a p-Sylow subgroup of order p^r, which is then a p-Sylow subgroup in G as well. $\square$

Example 15.6. Let $G = S_3$. There are three 2-Sylow subgroups isomorphic to $\mathbf{Z}/2$, each generated by a transposition, and one 3-Sylow subgroup.

Example 15.7. Let p be a prime. In the dihedral group D_{2p}, there is a unique p-Sylow subgroup, which is normal, generated by the rotation r of angle $\frac{2\pi}{p}$. How many 2-Sylow subgroups are there? Each sr^a has order 2 as $(sr^a)(sr^a) = s^2 r^{-a} r^a = e$. There are thus 2-Sylow subgroups for each $s, sr, \ldots, sr^{p-1}$, so there are p of them.

15.1 Exercises

Exercise 15.1. Let p be a prime number and let $p \leqslant n \leqslant 2p-1$. Describe the p-Sylow subgroups of S_n, including how many there are.

Exercise 15.2. Describe the Sylow subgroups of D_{12}.

Exercise 15.3 (From Herstein)**.** Prove that a group of order 108 contains a normal subgroup of order 9 or 27.

Exercise 15.4. Let G be a finite *abelian* group of order $p_1^{r_1} \cdots p_k^{r_k}$. Let $P_1, \ldots, P_k$ be p_i-Sylow subgroups of G for $1 \leqslant i \leqslant k$. Show that G is isomorphic to the product $P_1 \times P_2 \times \cdots \times P_k$, consisting of k-tuples $(a_1, \ldots, a_k)$ where $a_i \in P_i$ for $1 \leqslant i \leqslant k$.