Lecture notes for Modern Algebra I: Lecture 21 + 22

1 Sylow theorems

1.1 Sylow theorems and p-groups

Definition 1. A p-group is a group where all elements have order a power of p. A subgroup of a group is a p-subgroup if it is p-group.

Theorem 2. *(Cauchy) Let G be a finite group and p a prime such that p divides the order of G. Then G contains a subgroup of order p.*

Proof. We will use induction on the order of the group G. If $|G| = p$, then clearly G itself is the required subgroup. We now assume that every group of order k, where $p \leq k < n$ and p divides k, has an element of order p. Assume that $|G| = n$ and $p|n$ and consider the class equation of G:

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_k)].$$

We have two cases.
Case 1. Suppose the order of one of the centralizer subgroups, $C(x_i)$, is divisible by p for some index $i = 1, \ldots, k$. In this case, by our induction hypothesis, we are done. Since $C(x_i)$ is a proper subgroup of G and p divides $|C(x_i)|$, $C(x_i)$ must contain an element of order p. Hence, G must contain an element of order p.
Case 2. Suppose the order of no centralizer subgroup is divisible by p. Then p divides $[G : C(x_i)]$, the order of each conjugacy class in the class equation; hence, p must divide the order of the center of G, $|Z(G)|$. Since $Z(G)$ is abelian, it must have a subgroup of order p by the Fundamental Theorem of Finite Abelian Groups. Therefore, the center of G already contains an element of order p. □

Corollary 3. *Let G be a finite group. Then G is a p-group if and only if $|G| = p^n$*

Example 4. Let us consider the group A_5. We know that $|A_5| = 60$. By Cauchy's Theorem, we are guaranteed that A_5 has subgroups of orders $2, 3$ and 5. The Sylow Theorems will give us even more information about the possible subgroups of A_5.

Theorem 5. *(Sylow first theorem) Let G be a finite group and p a prime such that p^r divides the order of G. Then G contains a subgroup of order p^r.*

Proof. We induct on the order of G once again. If $|G| = p$, then we are done. Now suppose that the order of G is n with $n > p$ and that the theorem is true for all groups of order less than n, where p divides n. We shall apply the class equation once again:

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_k)].$$

First suppose that p does not divide $[G : C(x_i)]$ for some i. Then $p^r||C(x_i)|$, since p^r divides $|G| = |C(x_i)| \cdot [G : C(x_i)]$. Now we can apply the induction hypothesis to $C(x_i)$. Hence, we may assume that p divides $[G : C(x_i)]$ for all i. Since p divides $|G|$, the class equation says that p must divide the order of the center $|Z(G)|$; hence, by Cauchy's Theorem, $Z(G)$ has an element of order p, say g. Let N be the group generated by g. Clearly, N is a normal subgroup of $Z(G)$ since $Z(G)$ is abelian; therefore, N is normal in G since every element in $Z(G)$ commutes with every element in G. Now consider the factor group G/N of order $|G|/p$. By the induction hypothesis, the group G/N contains a subgroup H of order p^{r-1}. Now, the inverse image of H under the map $G \longrightarrow G/N$ is a subgroup of order p^r in G. □

Definition 6. A Sylow p-subgroup P of a group G is a maximal p-subgroup of G.

Definition 7. Let H be a subgroup of G. The normalizer subgroup of H in G is the maximal subgroup where H is normal, given by:

$$N(H) = \{g \in G \,|\, gHg^{-1} = H\}.$$

Lemma 8. *Let P be a Sylow p-subgroup of a finite group G and let x have as its order a power of p. If $x^{-1}Px = P$, then $x \in P$.*

Proof. Certainly $x \in N(P)$, and the cyclic subgroup, $\langle xP \rangle \subset N(P)/P$, has as its order a power of p. By the Correspondence Theorem there exists a subgroup H of $N(P)$ containing P such that $H/P = \langle xP \rangle$. Since $|H| = |P||\langle xP \rangle|$, the order of H must be a power of p. However, P is a Sylow p-subgroup contained in H. Since the order of P is the largest power of p dividing $|G|$, we get $H = P$. Therefore, H/P is the trivial subgroup and $xP = P$, or $x \in P$. □

Lemma 9. *Let H and K be subgroups of G. The number of distinct H-conjugates of K is $[H : N(K) \cap H]$.*

Proof. We define a bijection between the H-conjugacy classes of K and the right cosets of $N(K) \cap H$ by doing

$$h^{-1}Kh \mapsto (N(K) \cap H)h.$$

To show that this map is a bijection, consider two elements $h_1, h_2 \in H$ and suppose that $(N(K) \cap H)h_1 = (N(K) \cap H)h_2$ Then $h_2h_1^{-1} \in N(K)$. Therefore,

$$K = h_2h_1^{-1}Kh_1h_2^{-1} \;\Rightarrow\; h_1^{-1}Kh_1 = h_2^{-1}Kh_2,$$

and the map is an injection. It is easy to see that this map is surjective; hence, we have a one-to-one and onto map between the H-conjugates of K and the right cosets of $N(K) \cap H$ in H. □

Theorem 10. *(Second Sylow Theorem) Let G be a finite group and p a prime dividing $|G|$. Then all Sylow p-subgroups of G are conjugate. That is, if P_1 and P_2 are two Sylow p-subgroups, there exists and element $g \in G$ such that $gP_1g^{-1} = P_2$.*

Proof. Let P be a Sylow p-subgroup of the group G and suppose that the order $|G| = p^r m$ with $|P| = p^r$. Let S be the set

$$S = \{P = P_1, P_2, \ldots, P_k\}$$

consisting of the distinct conjugates of P in G. By lemma 9, the number k is the index $k = [G : N(P)]$. Notice that $|G| = p^r m = |N(P)| \cdot [G : N(P)] = |N(P)| \cdot k$. Given any other Sylow p-subgroup Q, we must show that $Q \in S$. Consider the Q-conjugacy classes of each P_i. Clearly, these conjugacy classes partition S. The size of the partition containing P_i is $[Q : N(P_i) \cap Q]$ by lemma 9. Lagrange's Theorem tells us that the order of Q, $|Q| = [Q : N(P_i) \cap Q] \cdot |N(P_i) \cap Q|$. Thus, $[Q : N(P_i) \cap Q]$ must be a divisor of $|Q| = p^r$.
Hence, the number of conjugates in every equivalence class of the partition is a power of p. However, since p does not divide k, one of these equivalence classes must contain only a single Sylow p-subgroup, say P_j. In this case, $x^{-1}P_jx = P_j$ for all $x \in Q$. By 8, the grup $P_j = Q$. □

Theorem 11. *(Third Sylow theorem) Let G be a finite group and let p be a prime dividing the order of G. Then the number n_p of Sylow p-subgroups satisfy the two conditions:*

(a) $n_p \equiv 1 \, (mod\, p)$,

(b) n_p *divides the order* $|G|$ *of the group.*

Proof. Let P be a Sylow p-subgroup acting on the set of Sylow p-subgroups,

$$S = \{P = P_1, P_2, \ldots, P_k\}$$

by conjugation. From the proof of the Second Sylow Theorem, the only P-conjugate of P is itself and the order of the other P-conjugacy classes is a power of p. Each P-conjugacy class contributes a positive power of p toward $k = |S|$ except the equivalence class $\{P\}$. Since $|S|$ is the sum of positive powers of p and 1, we have $|S| \equiv 1 (\bmod p)$. Now suppose that G acts on S by conjugation. Since all Sylow p-subgroups are conjugate, there can be only one orbit under this action. For $P \in S$,

$$|S| = |\text{ orbit of } P| = [G : N(P)].$$

by Lemma 9. But $[G : N(P)]$ is a divisor of $|G|$; consequently, the number of Sylow p-subgroups of a finite group must divide the order of the group. □

Example 12. If $p < q$ are primes and q is not congruent to 1 modulo p, then the only group G of order pq up to isomorphism is the cyclic group C_{pq}. Suppose that H and K denotes p-Sylow subgroups of order q and p respectively. Let us denote by n_q and n_p the number of conjugates of H and K respectively. We must satisfy the conditions:

$$n_q \equiv 1 \bmod q, \quad n_q | p \qquad \text{and} \qquad n_p \equiv 1 \bmod p\,, \quad n_p | q,$$

which gives $n_q = 1$ and $n_p = 1$. So we have two normal subgroups H and K of order q and p and they satisfy the criteria for direct product, $G \cong H \times K \cong C_q \times C_p \cong C_{pq}$.