Notes on Serge Lang's Algebra

Amanuel Tewodros

March 5, 2025

Contents

Chapter 1

Groups

Theorem 1 (Sylow Theorems)**.** *Let G be a finite group with p divides $|G|$, where p is a prime. Then*

1. *There exists a Sylow p-subgroup of G.*

2. *The number of Sylow p-subgroups of G is congruent to 1 modulo p and divides $|G|$.*

3. *All Sylow p-subgroups of G are conjugate.*

Proof. If $H \leq G$ with $[G : H]$ coprime with p, then by induction H and therefore G contains a Sylow p-group. Otherwise, by the class equation,

$$|G| = |Z(G)| + \sum_x [G : N_x(G)],$$

it follows $Z(G)$ is divisible by p and thus $\langle g \rangle \leq Z(G)$ for some $g \in Z(G)$ with exponenet = p. Inducting on the order of G, $G/\langle g \rangle$ contains a Sylow p-subgroup, say $S/\langle g \rangle$ that is the image of $S \leq G$ that is a Sylow p-subgroup of G.

Let $P, Q \in \mathrm{Syl}_p(G)$. P does not normalize Q because otherwise $PQ \leq G$ and $p^m = |PQ| > |P|$, a contradiction. Let $S = \{P_1, \ldots, P_k\}$ be the conjugates of P and let $\mathcal{O}_i$ be the orbit of P_i by the action P on the set S by conjugation. Then $|\mathcal{O}_i| = [P : N_P(P_i)] = [P : N_G(P_i) \cap P] = [P : P_i \cap P] \implies k = 1 \mod p$.

If $P, Q \in \mathrm{Syl}_p(G)$ are not conjugates, then Q is not conjugate with conjugates of P. Consider the action of the elements of Q on the set $\{gPg^{-1} : g \in G\} = \{P_1, \ldots, P_m\}$. Then

$$|\mathcal{O}_{P_i}| = [Q : N_Q(P_i)] = [Q : P_i \cap Q],$$

where the latter equality follows because $P_i(N_G(P_i) \cap Q)$ is a p-group that contains P_i with order $\leq |P_i|$(a Sylow p-group) and thus $N_G(P_i) \cap Q \leq P_i$. Since Q is not a conjugate of P, $[Q : Q \cap P_i] = p^k, k > 0$ and $\mathcal{O}_{P_i}$ is divisible by p and the number of conjugates of P which is $\sum_i |\mathcal{O}_{P_i}| = 0 \mod p$, a contradiction. $\square$

Theorem 2. *If $|G| = pq$ for primes $p < q$, then $G = \mathbb{Z}/pq\mathbb{Z}$ if $p \nmid q - 1$ else $G = \mathbb{Z}/pq\mathbb{Z}$ of $G = \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ for some non-trvial semi-direct product.*

Proof. If $q > p$, $n_q = 1$ and thus $Q \in \mathrm{Syl}_q(G)$ is normal. $|\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})| = q - 1$, therefore, there is a nontrivial map $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ if $p \mid q - 1$ □