Notes on Serge Lang's Algebra

Amanuel Tewodros

March 9, 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 $p \mid q-1$ $\square$

Theorem 3 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Let A be a finite abelian group and let $A(p)$ be the subgroup of all elements with order that is a power of p. Then*

$$\prod_{A(p)\neq\{1\}} A(p) = A.$$

Proof. Clearly the map $\phi : \prod_p A(p) \to A$ defined by $\phi((x_p)) = \prod_p x_p$ is an endomorphism. We show that ϕ is injective and surjective. Let $\phi((x_p)) = 1$ for some $x = (x_p) \in \prod_p A(p)$. Let q be a prime with $A(q) \neq \{1\}$. Then

$$x_q = \prod_{p\neq q} x_p^{-1}.$$

Let m be the least common multiple of the primes powers on the right hand side, i.e. powers of $p \neq q$. Then $x_q^m = 1$. But, $x_q^{q^r} = 1$ too. Consequently, $x_q^{(m,q^r)} = x_q^1 = x_q = 1$. Thus $\prod_p x_p = 1$ iff all $x_p = 1$ and $\ker\phi = \{1\}$.

To prove surjectivity, let $x \in A$ with $x^m = 1$ such that $m = \prod p_i^{r_i}$. By Euclidean algorithm, $1 = \sum_i u_i \prod_{j\neq i} p_j^{r_j}$ and thus $x = \prod_i x^{u_i \prod_{j\neq i} p_j^{r_j}}$ with $x^{u_i \prod_{j\neq i} p_j^{r_j}} \in A(p_i)$. $\square$

Why nilpotence and the existence of normal Sylow sub-groups are equivalent?: If $P, Q \in \mathrm{Syl}_p(G)$ then $N_P(Q) = P \cap Q < P, Q$ and thus $Z(G)$ is always $< G$. Thus $P = Q \iff G$ nilpotent.

The number of ways G acts on H: $= \#$ of homomorphisms from G to $\mathrm{Aut}(H) = \#$ subgroups of order $|G|/|H^*|$.

Theorem 4. *If $n \geq 5$ then S_n is not solvable.*

Proof. Let S_n decompose as $S_n = H_m \supset \cdots \supset H_0 = \{1\}$. Clearly, S_n contains all 3-cycles. We also know since H_n/H_{n-1} is abelian $(abc)(ade)(acb)(aed) = (adebc)(aedcb) = (abd) \in H_{m-1}$. By induction all 3 cycles are in $\{1\}$, a contradiction. $\square$

Theorem 5. *A_n is simple for all $n \geq 5$.*

A priori: A_n can be generated by 3-cycles and 3-cycles are conjugates.

Proof. Let $N \trianglelefteq A_n$. Let $\sigma \in N$. We show that σ is a 3-cycle or $\sigma = \mathrm{id}$. The former implies $N = A_n$ and the latter implies N is the trivial subgroup. Let σ have the maximal number of fixed points in N.

Lrt all σ's orbits have size 2 and it does not fix elements i, j. If σ is (ijk) for some k, we are done. Otherwise, $\langle\sigma\rangle > \langle(ij)(rs)\rangle$ for some r, s because σ is an even permutation and not a 3-cycle. Let $\tau = (rsk)$ for some k. Then $\tau' = \tau\sigma\tau^{-1}\sigma^{-1} \in N$.

But $\tau' = (i, j)\sigma$ contradicting σ fixes the maximal number of points. Thus at least one σ's orbit has more than 2 elements.

Therefore, $\sigma = (ijk)(rs)\theta$ where θ is possible identity permutation. By similar argumenta as above picking $\tau' = (rsk)$, σ can not be the element of N with maximal fixed points unless it contains all of A_n. $\square$