Notes on Serge Lang's Algebra

Amanuel Tewodros

April 12, 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. □

Properties of Common Non-Abelian Groups

- *Dihedral Group*: D_{2n}
  - $\cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ acting by inversion
  - $= \{a, b | a^n, b^2, baba\}$
- *Binary Dihedral Group/ Dicyclic Group*: $\mathrm{DiC}(4n)$
  - $\cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ acting by inversion
  - $= \{a, b | a^n, b^4, baba\}$
- *Generalized Quaternions*: $Q_{2^{n+2}}$
  - $\cong \mathbb{Z}/2^n\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ acting by inversion
  - $= \{a, b | a^{2^n}, b^4, baba\}$
- *Holomorph Group*: $\mathrm{Hol}(G)$
  - $\cong G \rtimes \mathrm{Aut}(G)$
  - if G is $\mathbb{Z}/p\mathbb{Z}$, p prime, $\mathrm{Hol}(G)$ is isomorphic to the *generalized affine group*

Notes on Category Theory

- A category $\mathcal{C}$ is a collection of **objects** $\mathrm{Ob}(\mathcal{C})$, along with a set of maps, called **morphisms** between any two objects $A, B \in \mathrm{Ob}(\mathcal{C})$ denoted by $\mathrm{Mor}(A, B)$.
- Morphisms follow the law of composition.
- Three axioms
  1. **CAT 1** $\mathrm{Mor}(A, B)$ and $\mathrm{Mor}(A', B')$ are disjoint unless $(A, B) = (A', B')$, in which case they are equal.
  2. **CAT 2** For every $A \in \mathrm{Ob}(\mathcal{C})$, there exists a morphism, id_A in $\mathrm{Mor}(A, A)$ that acts as a left and right identity for the elements of $\mathrm{Mor}(A, B)$ and $\mathrm{Mor}(B, A)$ resp. for all B.
  3. **CAT 3** The law of composition of morphisms is associative.
- The **operation** of a group G on an object $A \in \mathrm{Ob}(\mathcal{C})$ is a homomorphism from G to $\mathrm{Aut}(A)$. It is also called a **representation.**

- Given a category $\mathcal{C}$, we can construct a new category $\mathcal{D}$ where the objects are the morphisms of $\mathcal{C}$ and the morphisms between two objects f, f' are defined by a pair of momorphism (ϕ, ψ) that make the following diagram commute:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\phi"'] & B \arrow[d, "\psi"] \\ A' \arrow[r, "f'"'] & B' \end{tikzcd}$$

- An object P of a category $\mathcal{C}$ is called **universally attracting** (resp. **universally repelling**) if there is exists a *unique* morphism from (resp. to) every object to(resp. from) P. If it is both, it is called **universal object**.

Chapter 2

Rings

Proposition 6. *For two ideals* $\mathfrak{a}, \mathfrak{b}$ *of a ring* A*, if* $\mathfrak{a} + \mathfrak{b} = A$*, then* $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

Proof. Clearly, $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Thus, it suffices to prove the contra-positive relation. Since $1 = a + b$ for some $a \in \mathfrak{a}, b \in \mathfrak{b}$, $c = c \cdot a + c \cdot b$ for all $c \in A$. Of course, if $c \in \mathfrak{a} \cap \mathfrak{b}$, $c \cdot a + c \cdot b \in \mathfrak{a}\mathfrak{b}$. □

Let A be a ring and let $\lambda : \mathbb{Z} \to A$ given by

$$\lambda(n) = \underbrace{1_A + \cdots + 1_A}_{n \text{ times}}.$$

Then $\ker \lambda = \langle n \rangle$ for some $n \geq 0$. If $\langle n \rangle$ is a prime ideal, then we say A has characteristic n.

Proposition 7. *If* S *is a set with more than two elements and* A *is a ring with* $1_A \neq 0_A$*, then* $\mathrm{Map}(S, A)$ *is not an integral domain.*

Proof. Let $\{\} \neq T \subset S$

$$f(x) = \begin{cases} 1_A \text{ if } x \in T \\ 0_A \text{ if } x \in S - T \end{cases} \qquad \text{and } g(x) = 1_A - f(x).$$

$fg = 0_{\mathrm{Map}(S,A)}$. □

If $\mathfrak{p}$ is a prime ideal in a ring A, then it means

1. $A/\mathfrak{p}$ is an integral domain.

2. $xy \in \mathfrak{p} \implies x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

The ideal $\{0_A\}$ *is a prime ideal of* A *iff* A *is an integral domain.*

Proof. ($\implies$) $A/\{0_A\} \cong A$, thus A should be an integral domain.

($\impliedby$). If A is an integral domain, then $xy \in \{0_A\} \implies x = \{0_A\}$ or $y \in \{0_A\}$. □

Theorem 8 (Chinese Remainder Theorem)**.** *Let $\mathfrak{a}_1, \dots \mathfrak{a}_n$ be ideals of a ring A such that $\mathfrak{a}_i + \mathfrak{a}_j = A$ for any $i \neq j$. Let x_i be elements of A. Then there is an element $x \in A$ such that $x \equiv x_i \mod \mathfrak{a}_i$.*

Proof. If $n = 2$, $A = \mathfrak{a}_1 + \mathfrak{a}_2$, and thus $1_A = a_1 + a_2$ for some $a_i \in \mathfrak{a}_i$. Then $x = x_1 a_1 + x_2 a_2$ satisfies the statement.

If $n > 2$, then $a_i + b_i = 1_A$ for some $a_i \in \mathfrak{a}_1$ and $b_i \in \mathfrak{a}_{j>1}$. Thus the product $\prod_i (a_i + b_i) = 1_A$. In other words,

$$A = \mathfrak{a}_1 + \prod_{i=2}^{n} \mathfrak{a}_i.$$

By the case for $n = 2$, there is an element y_1 such that,

$$y_1 \equiv 1_A \mod \mathfrak{a}_1 \text{ and } y_1 \equiv 0_A \mod \Big(\prod_{i=2}^{n} \mathfrak{a}_i\Big)$$

Since $\prod_{i=2}^{n} \mathfrak{a}_i \subseteq \bigcap_{i=2}^{n} \mathfrak{a}_i$, it follows that $y_1 \in \mathfrak{a}_i$ for all $i > 1$ and therefore, $y \equiv 0_A \mod \mathfrak{a}_i$ for $i > 1$. Carrying out the same procedure in similar fashion to obtain $y_2, \dots, y_n$ such that

$$y_i \equiv 1_A \mod \mathfrak{a}_i \text{ and } y_i \equiv 0_A \mod \mathfrak{a}_j, j \neq i,$$

we see that $x = \sum_{i=1}^{n} x_i y_i$ satisfies the statement of the theorem. □

A non-zero polynomial f of degree d over a commutitive ring A is homogenous iff for every set of $n+1$ algebraically independent elements $u, t_1, \dots, t_n$ over A,

$$f(ut_1, \dots, ut_n) = u^d f(t_1, \dots, t_n).$$

Proof. Let $f(X) = \sum_{(v)} a_{(v)} X_1^{v_1} \cdots X_n^{v_n}$. If f is homogenous of degree d, $v_1 + \cdots + v_n = d$ for all $a_{(v)} \neq 0$. $f(ut_1, \dots, ut_n) = \sum_{(v)} a_{(v)} (ut_1)^{v_1} \cdots (ut_n)^{v_n}$. Since A is commutitive, this is equal to $\sum_{(v)} a_{(v)} u^{v_1 + \cdots + v_n} t_1^{v_1} \cdots t_n^{v_n}$.

On the other hand, if $f(ut_1, \dots, ut_n) = u^d f(t_1, \dots, t_n)$m, then $\sum_{(v)} a_{(v)} u^{v_1 + \cdots + v_n} = f(u1_A, \dots, u1_A) = u^d f(1_A, \dots, 1_A) = u^d \sum_{(v)} a_{(v)}$. This is a polynomial in u over A and equality is assured iff $u^d = u^{v_1 + \cdots v_n}$.

□

Let G be a monid and let $A[G]$ be the set of all mappings $\alpha : G \to A$ such that $\alpha(x) = 0$ for almost all $x \in G$. Addition is defined ordinarily and multiplication is defined as

$$\alpha\beta(z) = \sum_{xy=z} \alpha(x)\beta(y).$$

Then $A[G]$ is a ring. A more convenient notation can be acheived if we define $a \cdot x$ as

$$a \cdot x(z) = \begin{cases} a \text{ if } z = x \\ 0 \text{ if otherwise.} \end{cases}$$

This way we can define, $\alpha = \sum_{x \in G} \alpha(x) \cdot x$, and

$$\left(\sum_{x \in G} a_x \cdot x\right)\left(\sum_{y \in G} b_y \cdot y\right) = \left(\sum_{x,y} a_x b_y \cdot xy\right)$$

$$\left(\sum_{x \in G} a_x \cdot x\right) + \left(\sum_{x \in G} b_x \cdot y\right) = \left(\sum_{x \in G} (a_x + b_x) \cdot x\right),$$

where $\{a_z\}_{z \in G}$, $\{b_z\}_{z \in G}$ are the elements of A, most of them equal to 0.

The injective homomorphisms $x \mapsto 1_A \cdot x$ and $a \mapsto a \cdot e$ show that G and A are embedded in $A[G]$.

Let A be a communtative ring and S be a multiplicative subset [1]. *For $a, a' \in A$ and $s, s' \in S$, we say*

$$(a, s) \sim (a', s')$$

if there is $s_1 \in S$ such that

$$s_1(as' - sa') = 0.$$

$\sim$ is an equivalance relation.

Proof. Symmetry and Reflexitvness are trivial. Transitivity can be verified as follows. Let $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then for some $s_1, s_2 \in S$, we have

$$s_1 ad = s_1 bc$$

$$s_2 de = s_2 cf$$

Multiplying both sides of first and the second equation by $s_2 f$ and $s_1 b$, it follows that $(s_1 s_2 d)(af - be) = 0$. $\square$

This construction of ring is called **ring of fraction of** A **by** S**,** $S^{-1}A$. The homomorphism $A \mapsto S^{-1}A$ defined by $a \mapsto a/1_A$ is a universal object (See 1). If A is an integral domain, then $S^{-1}A$ is the field of fractions.

If A has a unique maximal ideal, it is called **a local ring.** An intersting example is $A_{\mathfrak{p}} = S^{-1}A$,where S is the multiplicative subset $A - \mathfrak{p}$.

Principal Ideal Domains and Unique Factorization

Let A be an prinicipal integral domain. We say a divides b if $b = ac$ for some $c \in A$

Definition 9. d is called the greatest common divisor of a and b if and only if $c|a$ and $c|b \implies c|d$.

Proposition 10. *If $d = \gcd(a, b)$, then $ar + bs = d$ for some $r, s \in A$.*

[1] A subset containting 1_A and closed under multiplication

Proof. Let $a = dx$ and $b = dy$. Because d is a gcd of a and b, for $c \notin A^*$ $c \mid x \implies c \nmid y$ and vice versa, thus $\gcd(x, y)$ is a unit in A.

Now, $A \subseteqq \langle x, y\rangle$. To show that, let $\langle z\rangle = \langle x, y\rangle$. Since $x, y \in \langle x, y\rangle$, $x = w_1 z$ and $y = w_2 z$. But then z should be a unit in A and thus $1_A \in \langle x, y\rangle$. The proposition follows directly. □

The proof also shows if $\langle a, b\rangle = \langle c\rangle$, then $c = \gcd(a, b)$.

Definition 11. We call $p \in A$ **irreducible** if $p = ab$ for some $a, b \in A$, then $\{a, b\} \cap A^* \neq \emptyset$. If $c \in A$ can be written as a product of a unit in A and a product of some irreducibles in A, we call the product **a factorization** of c. If every non-zero element of A has a unique factorization (upto commutitivity) we call A a **unique factorization domain (UFD)** or **factorial ring**.

Theorem 12. *If A is a principal ideal domain, then A is a UFD.*

Proof. <u>Existence</u>: Let S be the set of ideals of A generated by elements a_i that don't have factorization. Let $S \neq \emptyset$. Then $\langle a_1\rangle \in S$.. Consider the chain,

$$\langle a_1\rangle \subsetneqq \langle a_2\rangle \subsetneqq \cdots \subsetneqq \langle a_n\rangle \subsetneqq \cdots$$

Because, A is a principal ideal domain $\cup_i \langle a_i\rangle = \langle a\rangle$ for some $a \in A$. However, $\langle a_i\rangle \subset \langle a_{i+1}\rangle$, $a \in \langle a_n\rangle$ for some n and the chain is finite. Thus if $\langle a\rangle \subsetneqq \langle b\rangle$, then b admits factorization.

Remark 13. The fact that A is a principal ideal domain is important in constructing the chain. Consider the following chain if $A = \mathbb{Q}$, for example

$$\langle 1/2\rangle \subsetneqq \langle 1/4\rangle \subsetneqq \cdots \subsetneqq \langle 1/2^n\rangle \subsetneqq \cdots$$

The union of these ideals = $\mathbb{Q}$ which is not a principal ideal.

Now, consider a. Clearly, a is not an irreducible. Thus Assume $a = bc$. But $\langle a\rangle \subsetneqq \langle b\rangle$. Thus b (and also c) admits factorization and by induction a does making S empty.

<u>Uniqueness</u> First, we prove that irreducibility implies primality. Let p be irreducible and let $p \mid ab$. If $p \nmid a$ then $\gcd(a, p) = 1_A$ and $1_A = ax + py \implies b = abx + pby = p(c'x + by)$ for some c.

If

$$a = up_1 \cdots p_r = vq_1 \cdots q_s,$$

$p_1 \mid q_1 \cdots q_s$ and WLOG, $q_1 = u_1 p_1$. Thus $up_2 \cdots p_r = vu_1 q_2 \cdots q_s$. The argument completes by induction. □