

# Om Algebra Crash Course

Aniruddha Madhava

December 31, 2025

---

## Contents

<b>1</b>	<b>Quotient Groups and Homomorphisms</b>	<b>2</b>
1.1	The Isomorphism Theorems . . . . .	2
1.1.1	Exercises . . . . .	3
1.2	Composition Series and the Hölder Program . . . . .	4
1.2.1	Exercises . . . . .	5
<b>2</b>	<b>Group Actions</b>	<b>6</b>
2.1	Group Actions and Permutation Representations . . . . .	6
2.1.1	Exercises . . . . .	6
2.2	Groups Acting on Themselves by Left Multiplication . . . . .	7
2.2.1	Exercises . . . . .	8
2.3	Groups Acting on Themselves by Conjugation . . . . .	9
2.4	Sylow's Theorems . . . . .	9
2.4.1	Application of Sylow's Theorem . . . . .	10
2.4.2	Exercises . . . . .	10
<b>3</b>	<b>Direct and Semidirect Products and Abelian Groups</b>	<b>12</b>

---

# 1 Quotient Groups and Homomorphisms

## 1.1 The Isomorphism Theorems

- **Thm. 16. (First Isomorphism Theorem)** If  $\varphi : G \rightarrow H$  is a group homomorphism, then  $\ker \varphi \trianglelefteq G$  and  $G/\ker \varphi \cong \varphi(G)$ .

Let  $\varphi : G \rightarrow H$  be a group homomorphism with kernel  $K$ . First, we will prove that the kernel is a normal subgroup. Let  $g \in G$  and  $k \in \ker \varphi$ . Then

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1 \implies gkg^{-1} \in K. \quad (1)$$

This implies that  $gKg^{-1} \subseteq K$  for all  $g \in G$ , and so  $K$  is a normal subgroup of  $G$ . Now let  $\tilde{\varphi} : G/\ker \varphi \rightarrow \varphi(G)$  as follows:  $\tilde{\varphi}(gK) = \varphi(g)$ . First, we start by showing that  $\tilde{\varphi}$  is well-defined. Suppose  $g_1K = g_2K$ , which means that  $g_1g_2^{-1} \in K$ . Therefore,

$$\varphi(g_1g_2^{-1}) = 1 \implies \varphi(g_1) = \varphi(g_2) \implies \tilde{\varphi}(g_1K) = \tilde{\varphi}(g_2K). \quad (2)$$

We need to show that  $\tilde{\varphi}$  is an isomorphism. Suppose  $\tilde{\varphi}(g) = \tilde{\varphi}(h)$ . Then  $\varphi(g) = \varphi(h) \iff gh^{-1} \in K \iff gK = hK$ . This proves injectivity. Now let  $\varphi(g) \in \varphi(G)$ . Hence clearly  $gK \mapsto g$  so that  $\tilde{\varphi}$  is surjective. Finally, if  $g_1K, g_2K \in G/K$ , then

$$\tilde{\varphi}(g_1K \cdot g_2K) = \tilde{\varphi}(g_1g_2K) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \tilde{\varphi}(g_1K)\tilde{\varphi}(g_2K). \quad (3)$$

Hence,  $\tilde{\varphi}$  is indeed an isomorphism of groups.

- **Thm. 18. (Diamond Isomorphism Theorem)** Let  $G$  be a group,  $A$  and  $B$  be subgroups of  $G$ , and assume that  $A \leq N_G(B)$ . Then (1)  $AB$  is a subgroup of  $G$ , (2)  $B \trianglelefteq AB$ , (3)  $A \cap B \trianglelefteq A$ , and (4)  $AB/B \cong A/A \cap B$ .

(1) Since  $A \leq N_G(B)$ , it automatically follows that  $AB$  is a subgroup of  $G$ . (2) Since  $A \leq N_G(B)$  and  $B \leq N_G(B)$ , then  $AB \leq N_G(B)$ , which is to say that  $B$  is a normal subgroup of  $AB$ . (3 - 4) Consider the map  $\varphi : A \rightarrow AB/B$  defined by  $\varphi(a) = aB$ . It is straightforward to see that  $\varphi$  is a surjective group homomorphism, which means that  $\varphi(A) = AB/B$ . Now we will determine the kernel:

$$A \ni a \in \ker \varphi \iff aB = 1B \iff a \in B. \quad (4)$$

Hence,  $\ker \varphi = A \cap B$ . By the first Isomorphism Theorem,  $A \cap B \trianglelefteq A$  and  $A/A \cap B \cong AB/B$ .

- **Thm. 19. (Third Isomorphism Theorem)** Let  $G$  be a group and let  $H$  and  $K$  be normal subgroups of  $G$  with  $H \leq K$ . Then  $K/H \trianglelefteq G/H$  and

$$(G/H)/(K/H) \cong G/K. \quad (5)$$

First, we will show that  $K/H \trianglelefteq G/H$ . Define the map  $\varphi : G/H \rightarrow G/K$  by  $\varphi(gH) = gK$ . First, we need to show that this map is well-defined. Suppose  $g_1H = g_2H$ . Then  $g_1 = g_2h$  for some  $h \in H$ . Since  $H \leq K$ ,  $h \in K$ , which shows that  $g_1K = g_2K$ . Hence,  $\varphi$  is well-defined. It is straightforward to see that  $\varphi$  is a surjective homomorphism. Finally, we can easily show that  $\ker \varphi = K/H$ . This means that (1)  $K/H$  is a normal subgroup of  $G/H$ , and (2) by the First Isomorphism Theorem,  $(G/H)/(K/H) \cong G/K$ .

- **Thm. 20. (Lattice Isomorphism Theorem)** Let  $G$  be a group and  $N$  a normal subgroup of  $G$ . Every subgroup of  $G/N$  is of the form  $A/N$ , where  $A$  is a subgroup of  $G$  containing  $N$ . Moreover, for all  $A, B \leq G$ , with  $N \leq A$  and  $N \leq B$ ,

- (1)  $A \leq B$  if and only if  $A/N \leq B/N$ .
- (2) If  $A \leq B$ , then  $|B : A| = |B/N : A/N|$ .
- (3)  $\langle A, B \rangle / N = \langle A/N, B/N \rangle$ .
- (4)  $(A \cap B)/N = (A/N) \cap (B/N)$ .

(5)  $A \trianglelefteq G$  if and only if  $A/N \trianglelefteq G/N$ .

- **Def. (Factoring Through)** In some of the above proofs of the isomorphism theorems, we have had to define a map  $\varphi$  on quotient groups  $G/N$  defined by giving the value of  $\varphi$  on the coset  $gN$  in terms of the representative  $g$  alone. In essence, this defines a homomorphism  $\Phi$  on  $G$ , itself, by specifying the value of  $\varphi$  at  $g$ . Hence, a map on a quotient group  $G/N$  is well-defined if and only if  $N \leq \ker \Phi$ . In this case, we say that the homomorphism  $\Phi$  *factors through*  $N$  and  $\varphi$  is the induced homomorphism on  $G/N$ . Pictorially,

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/N \\ & \searrow \Phi & \downarrow \varphi \\ & & H \end{array}$$

### 1.1.1 Exercises

**Exercise 3.** Prove that if  $H$  is a normal subgroup of  $G$  of prime index  $p$  then for all  $K \leq G$  either

- (i)  $K \leq H$  or
- (ii)  $G = HK$  and  $|K : K \cap H| = p$ .

Let  $H$  be a normal subgroup of  $G$  of prime index  $p$ , and let  $K$  be an arbitrary fixed *nontrivial* subgroup of  $G$ . If  $K \leq H$ , we are done; so assume that  $K$  is not a subgroup of  $H$ . Since  $K \leq G = N_G(H)$ , we conclude by the Second Isomorphism Theorem that  $HK$  is a subgroup of  $G$  and that  $K \cap H$  is a normal subgroup of  $K$ . Hence, we have the chain  $H \leq HK \leq G$ . Therefore,

$$p = |G : H| = |G : HK| \cdot |HK : H|. \quad (6)$$

Since  $p$  is a prime, either  $|G : HK| = 1$  (in which case  $G = HK$ ), or  $|HK : H| = 1 \implies HK = H \implies K \leq H$ . By our hypothesis, the latter is not possible. Therefore,  $G = HK$ . From this, we observe that

$$1 = \frac{|HK|}{|G|} = \frac{|H||K|}{|G||K \cap H|} = \frac{p^{-1}|K|}{|K \cap H|} \implies p = \frac{|K|}{|K \cap H|} = |K : K \cap H|. \quad (7)$$

**Exercise 4.** Let  $C$  be a normal subgroup of the group  $A$  and let  $D$  be a normal subgroup of the group  $B$ . Prove that  $(C \times D) \trianglelefteq (A \times B)$  and  $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$ .

Let  $C$  be a normal subgroup of the group  $A$  and  $D$  be a normal subgroup of the group  $B$ . Define the map,

$$\begin{aligned} \varphi : A \times B &\longrightarrow C \times D \\ (a, b) &\longmapsto (aC, bD). \end{aligned}$$

First, we will show that  $\varphi$  is a group homomorphism. Let  $a_1, a_2 \in A$  and  $b_1, b_2 \in B$ . Then

$$\begin{aligned} \varphi(a_1 a_2, b_1 b_2) &= (a_1 a_2 C, b_1 b_2 D) \\ &= (a_1 C, b_1 D) \cdot (a_2 C, b_2 D) \\ &= \varphi(a_1, b_1) \cdot \varphi(a_2, b_2). \end{aligned} \quad (8)$$

This confirms that  $\varphi$  is a group homomorphism;  $\varphi$  is clearly surjective since for any  $(aC, bD) \in (A/C) \times (B/D)$ ,  $\varphi : (a, b) \mapsto (aC, bD)$ . Now we identify the kernel of this map:

$$\begin{aligned} \ker \varphi &= \{(a, b) \in A \times B : aC = 1C \text{ and } bD = 1D\} \\ &= \{(a, b) \in A \times B : a \in C \text{ and } b \in D\} \\ &= C \times D. \end{aligned} \quad (9)$$

Hence, the conclusion proceeds from the First Isomorphism Theorem.

**Exercise 9.** Let  $p$  be a prime and let  $G$  be a group of order  $p^a m$ , where  $p$  does not divide  $m$ . Assume  $P$  is a subgroup of  $G$  of order  $p^a$  and  $N$  is a normal subgroup of  $G$  of order  $p^b n$ , where  $p$  does not divide  $n$ . Prove that  $|P \cap N| = p^b$  and  $|PN/N| = p^{a-b}$ . (The subgroup  $P$  of  $G$  is called a Sylow  $p$ -subgroup of  $G$ . This exercise shows that the intersection of any Sylow  $p$ -subgroup of  $G$  with a normal subgroup  $N$  is a Sylow  $p$ -subgroup of  $N$ .)

Assume all of the given hypotheses. We have the following results:

- (i) since  $P \leq G = N_G(N)$ ,  $PN \leq G$  by the Diamond Isomorphism Theorem;
- (ii)  $P \cap N \leq P$ , which means that  $|P \cap N| = p^j$  for some nonnegative integer  $j \leq a$ ;
- (iii)  $PN \leq G$  implies, by Lagrange's Theorem, that there exists a positive integer  $k$  such that

$$|G| = p^a m = k \cdot |PN| = k \cdot \frac{|P||N|}{|P \cap N|} = k \cdot \frac{p^a p^b n}{p^j} \implies m = k \cdot p^{b-j} n. \quad (10)$$

This shows that  $p^{b-j} \mid m$ . Since  $p \nmid m$ , we must necessarily have  $p^{b-j} = 1 \implies b-j = 0 \implies j = b$ . Therefore,  $|P \cap N| = p^b$ . Next, by the Diamond Isomorphism Theorem, since  $P/(P \cap N) \cong PN/N$ ,  $|PN/N| = |P|/|P \cap N| = p^{a-b}$ .

## 1.2 Composition Series and the Hölder Program

- **Prop. 21. (Element of Prime Order)** If  $G$  is a finite abelian group and  $p$  is a prime dividing  $|G|$ , then  $G$  contains an element of order  $p$ .
- **Def. (Simple Group)** A (finite or infinite) group  $G$  is called *simple* if  $|G| > 1$  and the only normal subgroups of  $G$  are 1 and  $G$ .
- **Def. (Composition Series)** In a group  $G$  a sequence of subgroups

$$1 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_{k-1} \leq N_k = G \quad (11)$$

is called a *composition series* if  $N_i \triangleleft N_{i+1}$  and  $N_{i+1}/N_i$  is a simple group for all  $0 \leq i \leq k-1$ . The quotient groups  $N_{i+1}/N_i$  are called *composition factors* of  $G$ .

- **Thm. 22. (Jordan-Hölder)** Let  $G$  be a finite group with  $G \neq 1$ . Then
  - (1)  $G$  has a composition series and
  - (2) the composition factors in a composition series are unique, namely, if  $1 = N_0 \leq N_1 \leq \cdots \leq N_r = G$  and  $1 = M_0 \leq M_1 \leq \cdots \leq M_s = G$  are two composition series for  $G$ , then  $r = s$  and there is some permutation,  $\pi$ , of  $\{1, 2, \dots, r\}$  such that

$$M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1}, \quad 1 \leq i \leq r. \quad (12)$$

- **Thm. (Feit-Thompson)** If  $G$  is a simple group of odd order, then  $G \cong Z_p$  for some prime  $p$ .
- **Def. (Solvable Group)** A group  $G$  is *solvable* if there is a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_s = G \quad (13)$$

such that  $G_{i+1}/G_i$  is abelian for  $i = 0, 1, \dots, s-1$ .

- **Obs. (Solvability of Groups in Terms of Subgroups)** Let  $G$  be a group and  $N$  a normal subgroup of  $G$ . If  $N$  and  $G/N$  are solvable, then  $G$  is solvable.

Let  $\overline{G} = G/N$ ,  $1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_n = N$  be a chain of subgroups of  $N$  such that  $N_{i+1}/N_i$  is abelian for all  $0 \leq i \leq n-1$  and let  $\overline{1} = \overline{G}_0 \trianglelefteq \overline{G}_1 \trianglelefteq \cdots \trianglelefteq \overline{G}_m = \overline{G}$  be a chain of subgroups such that  $\overline{G}_{i+1}/\overline{G}_i$  is abelian for  $0 \leq i \leq m-1$ . By the Lattice Isomorphism Theorem, there are

subgroups  $G_i$  of  $G$  with  $N \leq G_i$  such that  $G_i/N = \overline{G}_i$  and  $G_i \trianglelefteq G_{i+1}$ ,  $0 \leq i \leq m-1$ . By the Third Isomorphism Theorem,

$$\overline{G}_{i+1}/\overline{G}_i = (G_{i+1}/N)/(G_i/N) \cong G_{i+1}/G_i. \quad (14)$$

Hence, the chain

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_n = N = G_0 \trianglelefteq \cdots \trianglelefteq G_m = G \quad (15)$$

is a composition series for  $G$ , which proves that  $G$  is solvable.

### 1.2.1 Exercises

**Exercise 1.** Prove that if  $G$  is an abelian simple group then  $G \cong \mathbb{Z}_p$  for some prime  $p$  (do not assume  $G$  is a finite group).

Let  $G$  be a nontrivial, abelian, simple group. Since  $G$  is nontrivial, it must contain some nonidentity element  $x \in G$ . Consider the subgroup  $\langle x \rangle$  generated by this element. Since  $G$  is abelian,  $\langle x \rangle$  is a normal subgroup of  $G$ . And since  $G$  is simple,  $\langle x \rangle = G$ . Therefore,  $G$  is a cyclic group.

Suppose  $G$  is an infinite group. Then  $G \cong \mathbb{Z}$  via the isomorphism  $\varphi : \mathbb{Z} \rightarrow G$  that maps  $n \mapsto x^n$ . However,  $\mathbb{Z}$  is not a simple group, since for example, the subgroup  $4\mathbb{Z}$  is a proper normal subgroup of  $\mathbb{Z}$ . Hence, by contradiction,  $G$  must be a finite group.

Assume  $|G| = pm$  for some prime  $p$ . By Cauchy's Theorem,  $G$  contains an element  $y$  of order  $p$ ; since  $G$  is abelian, the subgroup  $\langle y \rangle$  of index  $m$  generated by this element is proper unless  $m = 1$ . But if  $m = 1$ ,  $G$  is a cyclic group of prime order  $p$ . Then it is easily shown that the map  $\varphi : \mathbb{Z}/p\mathbb{Z} \rightarrow G$  defined by  $\varphi(n) = x^n$  is an isomorphism. Therefore,  $G$  is isomorphic to  $\mathbb{Z}_p$  for some prime  $p$ .

**Exercise 4.** Use Cauchy's Theorem and induction to show that a finite abelian group has a subgroup of order  $n$  for each positive divisor  $n$  of its order.

Let  $G$  be a finite abelian group of order  $n$ . Assume that the result holds for all groups of order less than  $n$ . Let  $d$  be a divisor of  $n$ . Decompose  $d$  into the product  $kp$ , where  $p$  is some prime; by Cauchy's Theorem,  $G$  contains a subgroup of order  $p$ . Since  $G$  is finite abelian, this subgroup,  $P$ , is normal so that we can examine the quotient group  $G/P$ . Since  $|G/P| < n$ , the inductive hypothesis holds for this quotient group. Since  $k \mid |G/P|$ , by the hypothesis and the Lattice Isomorphism Theorem, there exists a subgroup  $P \leq K \leq G$  such that  $K/P$  has order  $k$ . Hence,  $|K| = k|P| = kp = d$ . Hence, this concludes the proof.

## 2 Group Actions

### 2.1 Group Actions and Permutation Representations

#### 2.1.1 Exercises

**Exercise 1.** Let  $G$  act on the set  $A$ . Prove that if  $a, b \in A$  and  $b = g \cdot a$  for some  $g \in G$ , then  $G_b = gG_ag^{-1}$  ( $G_a$  is the stabilizer of  $a$ ). Deduce that if  $G$  acts transitively on  $A$ , then the kernel of the action is  $\bigcap_{g \in G} gG_ag^{-1}$ .

Let  $G$  be a group acting on the set  $A$ , and assume that  $b = g \cdot a$  for some  $g \in G$ . Then

$$\begin{aligned} h \in G_b &\iff h \cdot b = b \iff h \cdot (g \cdot a) = (g \cdot a) \iff (g^{-1}hg) \cdot a = a \iff g^{-1}hg \in G_a \\ &\iff h \in gG_ag^{-1}. \end{aligned} \quad (16)$$

Now suppose that  $G$  acts transitively on  $A$ . Fix  $a \in A$ ; by transitivity, for each  $b \in A$ , there exists some  $g \in G$  such that  $b = g \cdot a$ . This means that for each  $b \in A$ , there exists some  $g \in G$  such that  $G_b = gG_ag^{-1}$ . Now, we observe that a group element is contained in the kernel of the group action if and only if the element stabilizes every  $b \in A$ . Therefore, if  $\alpha : G \times A \rightarrow A$  denotes the group action,

$$h \in \ker \alpha \iff h \in \bigcap_{b \in A} G_b \iff h \in \bigcap_{g \in G} gG_ag^{-1}. \quad (17)$$

**Exercise 2.** Let  $G$  be a *permutation group* on the set  $A$  (i.e.,  $G \leq S_A$ ), let  $\sigma \in G$ , and let  $a \in A$ . Prove that  $\sigma G_a \sigma^{-1} = G_{\sigma(a)}$ . Deduce that if  $G$  acts transitively on the set  $A$ , then

$$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = 1. \quad (18)$$

Let  $G$  be a permutation group on the set  $A$ , and let  $\sigma \in G, a \in A$ . Then

$$\begin{aligned} \tau \in G_{\sigma(a)} &\iff \tau \cdot \sigma(a) = \sigma(a) \iff (\sigma^{-1}\tau\sigma)(a) = a \iff \sigma^{-1}\tau\sigma \in G_a \\ &\iff \tau \in \sigma G_a \sigma^{-1}. \end{aligned} \quad (19)$$

This proves the first claim. Now assume that  $G$  acts transitively on the set  $A$ . Fix  $a \in A$ ; by transitivity, for every  $b \in A$ , there exists some  $\sigma \in G$  such that  $b = \sigma(a)$ . But then, this implies that  $G_b = G_{\sigma(a)} = \sigma G_a \sigma^{-1}$ . Therefore, if  $\alpha : G \times A \rightarrow A$  denotes the group action, then

$$\tau \in \ker \alpha \iff h \in \bigcap_{b \in A} G_b = \bigcap_{\sigma \in G} G_{\sigma(a)} = \bigcap_{\sigma \in G} \sigma G_a \sigma^{-1}. \quad (20)$$

On the other hand, by uniqueness of the identity in a group, it follows that the only permutation that fixes *every* element of  $A$  is the identity. This means that  $\ker \alpha = 1$ . Hence, the proof concludes.

**Exercise 9.** Assume  $G$  acts transitively on the finite set  $A$  and let  $H$  be a normal subgroup of  $G$ . Let  $\mathcal{O}_1, \dots, \mathcal{O}_r$  be the distinct orbits of  $H$  on  $A$ .

- (a) Prove that  $G$  permutes the sets  $\mathcal{O}_1, \dots, \mathcal{O}_r$  in the sense that for each  $g \in G$  and each  $i \in \{1, \dots, r\}$  there is a  $j$  such that  $g\mathcal{O}_i = \mathcal{O}_j$ , where  $g\mathcal{O} = \{g \cdot a : a \in \mathcal{O}\}$ . Prove that  $G$  is transitive on  $\{\mathcal{O}_1, \dots, \mathcal{O}_r\}$ . Deduce that all orbits of  $H$  on  $A$  have the same cardinality.

- (a) Remember that orbits of an action are equivalence classes under the equivalence relation  $b \sim a$  iff  $b = h \cdot a$  for some  $h \in H$ . For each of the  $r$  orbits of  $H$  on  $A$ , let  $a_j \in A$  be a representative element; that is, for each  $j = 1, \dots, r$ , suppose that

$$\mathcal{O}_j = \{h \cdot a_j : h \in H\}. \quad (21)$$

Since the orbits of  $H$  on  $A$  partition  $A$ , for each  $i \in \{1, \dots, r\}$  and  $g \in G$ ,  $g \cdot a_i$  lies in some orbit  $\mathcal{O}_j$ . We claim that  $g\mathcal{O}_i = \mathcal{O}_j$ . Suppose  $g \cdot a_i = h' \cdot a_j$  for some  $h' \in H$ . Then

$$\begin{aligned} g\mathcal{O}_i &= \{g \cdot (h \cdot a_i) : h \in H\} = \{(gh) \cdot a_i : h \in H\} \\ &= \{h'' \cdot (g \cdot a_i) : h'' \in H\} \quad (\text{by normality of } H \text{ in } G) \\ &= \{h'' \cdot (h' \cdot a_j) : h'' \in H\} = \{h \cdot a_j : h \in H\} \\ &= \mathcal{O}_j. \end{aligned} \tag{22}$$

Hence, this concludes the proof that  $G$  permutes the orbits of  $H$  on  $A$ . Now, since  $G$  acts transitively on  $A$ , for each pair  $(i, j) \in \{1, \dots, r\}$ , there exists some  $g \in G$  such that  $g \cdot a_i = a_j$ . By our previous observation, this implies that for each pair of orbits  $(\mathcal{O}_i, \mathcal{O}_j)$ , there exists some  $g \in G$  such that  $g\mathcal{O}_i = \mathcal{O}_j$ . Hence,  $G$  acts transitively on the set of orbits of  $H$  on  $A$ . Finally, given any pair  $\mathcal{O}_i, \mathcal{O}_j$  of orbits of  $H$  on  $A$ , the map  $\varphi : \mathcal{O}_i \rightarrow \mathcal{O}_j$  given by  $\varphi(a) = g \cdot a$  for all  $a \in \mathcal{O}_i$  and where  $g \in G$  is the group element such that  $g\mathcal{O}_i = \mathcal{O}_j$  can be easily shown to be a bijection by the above reasoning.

## 2.2 Groups Acting on Themselves by Left Multiplication

- **Thm. 3. (Action on Set of Left Cosets)** Let  $G$  be a group,  $H$  a subgroup of  $G$ , and let  $G$  act by left multiplication on the set  $A$  of left cosets of  $H$  in  $G$ . Let  $\pi_H$  be the associated permutation representation afforded by this action. Then

- (1)  $G$  acts transitively on  $A$
- (2) the stabilizer in  $G$  of the point  $1H \in A$  is the subgroup  $H$ .
- (3) the kernel of the action (i.e., the kernel of  $\pi_H$ ) is  $\bigcap_{x \in G} xHx^{-1}$ , and  $\ker \pi_H$  is the largest normal subgroup of  $G$  contained in  $H$ .

Assume the given hypotheses.

- (1) Let  $aH, bH \in A$ , where  $a, b \in G$ . Then  $ba^{-1} \in G$ . Hence,  $(ba^{-1})aH = bH$ . Therefore, the arbitrary cosets  $aH$  and  $bH$  lie in the same orbit, which proves that  $G$  acts transitively on  $A$ .
- (2)  $g \in G_{1H} \iff g \cdot 1H = 1H \iff gH = 1H \iff g \in H$ . Hence,  $G_{1H} = H$ .
- (3) By definition of  $\pi_H$ , we must have

$$\begin{aligned} \ker \pi_H &= \{g \in G : gxH = xH \forall x \in G\} \\ &= \{g \in G : (x^{-1}gx)H = H \forall x \in G\} \\ &= \{g \in G : x^{-1}gx \in H \forall x \in G\} \\ &= \{g \in G : g \in xHx^{-1} \forall x \in G\} = \bigcap_{x \in G} xHx^{-1}. \end{aligned} \tag{23}$$

Now, we need to prove that  $\ker \pi_H$  is the largest normal subgroup of  $G$  contained in  $H$ . First observe that  $\ker \pi_H \trianglelefteq G$  and  $\ker \pi_H \leq H$ . Let  $N$  be a normal subgroup of  $G$  contained in  $H$ , which means that  $N = xNx^{-1} \leq xHx^{-1}$  for all  $x \in G$ . Hence,

$$N \leq \bigcap_{x \in G} xHx^{-1} = \ker \pi_H. \tag{24}$$

- **Cor. 4. (Cayley's Theorem)** Every group is isomorphic to a subgroup of some symmetric group. If  $G$  is a group of order  $n$ , then  $G$  is isomorphic to a subgroup of  $S_n$ .

Let  $H = 1$  and apply the preceding theorem to obtain a homomorphism of  $G$  into  $S_G$  (here, we identify the cosets of the identity subgroup with the elements of  $G$ ). Since the kernel of this homomorphism is contained in  $H = 1$ ,  $G$  is isomorphic to its image in  $S_G$ .

- **Cor. 5. (Subgroups of Smallest Prime Index)** If  $G$  is a finite group of order  $n$  and  $p$  is the smallest prime dividing  $|G|$ , then any subgroup of index  $p$  is normal.

Suppose  $H \leq G$  and  $|G : H| = p$ . Let  $\pi_H$  be the permutation representation afforded by multiplication on the set of left cosets of  $H$  in  $G$ , let  $K = \ker \pi_H$ , and let  $|H : K| = k$ . Then  $|G : K| = |G : H||H : K| = pk$ . Since  $H$  has  $p$  left cosets,  $G/K$  is isomorphic to a subgroup of  $S_p$  by the First Isomorphism Theorem. By Lagrange's Theorem,  $pk = |G/K|$  divides  $p!$ . Therefore,  $k \mid (p-1)!$ . But all of the prime divisors of  $(p-1)!$  are less than  $p$ , and by the minimality of  $p$ , every prime divisor of  $k$  is greater than or equal to  $p$ . This forces  $k = 1$  so that  $H = K \trianglelefteq G$ , completing the proof.

### 2.2.1 Exercises

**Exercise 8.** Prove that if  $H$  has finite index  $n$  then there is a normal subgroup  $K$  of  $G$  with  $K \leq H$  and  $|G : K| \leq n!$ .

Let  $G$  be an arbitrary group, and  $H$  a subgroup of  $G$  of finite index  $n$ . Let  $G$  act on the set  $A$  of left cosets of  $H$  by left multiplication, and denote the afforded permutation representation as  $\pi_H$ . Define  $K = \ker \pi_H \trianglelefteq G$  such that  $K \leq H$ . By the First Isomorphism Theorem,  $G/K$  is isomorphic to the subgroup  $\pi_H(G) \leq S_A$ . Since  $H$  has  $n$  left cosets,  $|S_A| = n!$  so that  $|\pi_H(G)| \mid n!$ . In particular, this implies that  $|\pi_H(G)| \leq n!$ , which then implies that  $|G/K| \leq n!$ .

**Exercise 9.** Prove that if  $p$  is a prime and  $G$  is a group of order  $p^\alpha$  for some  $\alpha \in \mathbb{Z}^+$ , then every subgroup of index  $p$  is normal in  $G$ . Deduce that every group of order  $p^2$  has a normal subgroup of order  $p$ .

Let  $p$  be a prime and  $G$  a group of order  $p^\alpha$  for some  $\alpha \in \mathbb{Z}^+$ . Since  $p$  is the smallest prime dividing the order of  $G$ , we conclude by Corollary 5 that any subgroup of index  $p$  must be normal in  $G$ . Now let  $G$  be a group of order  $p^2$ . If  $G$  has a subgroup of order  $p$ , then since  $p^2/p = p$ , the index of the subgroup is  $p$ ; by the previous observation, this subgroup must be normal in  $G$ . Therefore, it suffices to show that such subgroups necessarily exist. But existence is straightforward: since  $p$  divides  $|G|$ , then by Cauchy's Theorem,  $G$  has to contain an element of order  $p$ . Then the subgroup generated by this element has to have order  $p$ , which then concludes the claim.

**Exercise 10.** Prove that every non-abelian group of order 6 has a nonnormal subgroup of order 2. Use this to classify groups of order 6. [Produce an injective homomorphism into  $S_3$ .]

We argue by contradiction; let  $G$  be a non-abelian group of order 6. By Cauchy's Theorem,  $G$  must contain *at least one* element of order 2. Considering the subgroup generated by this element,  $G$  must contain a subgroup of order 2. Assume to the contrary that every subgroup of order 2 is normal in  $G$ , and let  $P = \{1, a\}$  be such a subgroup. By definition of normality,  $gag^{-1} = a$  for all  $g \in G$ , which implies  $ga = ag$  for all  $g \in G$ , which then implies that  $a \in Z(G)$ . I.e.,  $|Z(G)| \geq 2$ .

- (i) Suppose  $|Z(G)| = 2$ . Then  $|G/Z| = 3$ , which means  $G/Z$  is cyclic, and so  $G$  is abelian - contradicting our assumption that  $|Z(G)| = 2$ .
- (ii) Suppose  $|Z(G)| = 3$ . Then  $|G/Z| = 2$ , which means  $G/Z$  is cyclic, and so  $G$  is abelian - contradicting our assumption that  $|Z(G)| = 3$ .
- (iii) Suppose  $|Z(G)| = 6$ . Then  $G$  is abelian, which contradicts our hypothesis that  $G$  is non-abelian.

Hence, we must have  $|Z| = 1$ , but this contradicts our hypothesis that every subgroup of order 2 is normal. Hence,  $G$  must contain a nonnormal subgroup of order 2.

**Exercise 14.** Let  $G$  be a finite group of composite order  $n$  with the property that  $G$  has a subgroup of order  $k$  for each positive integer  $k$  dividing  $n$ . Prove that  $G$  is not simple.



Let  $G$  be a finite group of composite order  $n$  with the property that  $G$  has a subgroup of order  $k$  for each positive integer  $k$  dividing  $n$ . Let  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$  be the prime factorization of  $n$ , and  $p_1$  be the smallest prime in the factorization (possibly after rearranging and renumbering). Then since  $j = p_1^{\alpha_1-1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \mid n$ ,  $G$  contains a subgroup  $J$  of order  $j$ . By Lagrange's Theorem,  $[G : J] = p_1$ . Hence, by Corollary 5, this subgroup must be a proper normal, nontrivial, subgroup of  $G$  which means that  $G$  cannot be simple.

### 2.3 Groups Acting on Themselves by Conjugation

- **Prop. 6. (Number of Conjugates of a Subset)** Let  $G$  be a group and  $S$  a subset of  $G$ . Then the number of conjugates of  $S$  is equal to  $|G : N_G(S)| = |G : C_G(S)|$ . In particular, the number of conjugates of an element  $s$  is the index of the centralizer of  $s$ ,  $|G : C_G(s)|$ .
- **Thm. 7. (Class Equation)** Let  $G$  be a finite group and let  $g_1, g_2, \dots, g_r$  representatives of the distinct conjugacy classes of  $G$  not contained in the center  $Z(G)$  of  $G$ . Then

$$|G| = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|. \quad (25)$$

- **Thm. 8. (Groups of Order  $p^2$ )** If  $p$  is a prime and  $P$  is a group of prime power  $p^\alpha$  for some  $\alpha \geq 1$ , then  $P$  has a nontrivial center:  $Z(P) \neq 1$ .

Consider the class equation:

$$|P| = |Z(P)| + \sum_{i=1}^r |P : C_P(g_i)|, \quad (26)$$

where  $g_1, \dots, g_r$  are representatives of the distinct non-central conjugacy classes. By definition,  $C_P(g_i) \neq P$  for  $i = 1, 2, \dots, r$  so that  $p \mid |P : C_P(g_i)|$ . Since  $p \mid |P|$ , it follows that  $p \mid |Z(P)|$ . Hence,  $|Z(P)|$  cannot be trivial.

- **Thm. 9. (Groups of Order  $p^2$ )** If  $|P| = p^2$  for some prime  $p$ , then  $P$  is abelian. More precisely,  $P$  is isomorphic to either  $\mathbb{Z}_{p^2}$  or  $\mathbb{Z}_p \times \mathbb{Z}_p$ .

By the previous theorem,  $Z(P)$  is nontrivial so that  $P/Z(P)$  is cyclic. Hence,  $P$  is abelian. If  $P$  contains an element of order  $p^2$ , then  $P$  is cyclic so that  $P \cong \mathbb{Z}_{p^2}$ . So suppose that every nontrivial element of  $P$  has order  $p$ . Let  $x, y$  be distinct nonidentity elements of  $P$ . Since  $|\langle x, y \rangle| > |\langle x \rangle| = p$ , we must have that  $P = \langle x, y \rangle$ . Since  $x$  and  $y$  have order  $p$ ,  $\langle x \rangle \times \langle y \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$ . Hence, the map  $\varphi : (x^a, y^b) \mapsto x^a y^b$  is an isomorphism from  $\langle x \rangle \times \langle y \rangle \rightarrow P$ , which completes the proof.

### 2.4 Sylow's Theorems

- **Def. (Sylow Subgroups)** Let  $G$  be a group and let  $p$  be a prime.
  - (1) A group of order  $p^\alpha$  for some  $\alpha \geq 1$  is called a  $p$ -group. Subgroups of  $G$  which are  $p$ -groups are called  $p$ -subgroups.
  - (2) If  $G$  is a group of order  $p^\alpha m$ , where  $p \nmid m$ , then a subgroup of order  $p^\alpha$  is called a Sylow  $p$ -subgroup of  $G$ .
- **Thm. 18. (Sylow's Theorem)** Let  $G$  be a group of order  $p^\alpha m$ , where  $p \nmid m$ .
  - (1)  $\text{Syl}_p(G) \neq \emptyset$ .
  - (2) Any two Sylow  $p$ -subgroups are conjugate in  $G$ .
  - (3) The number of Sylow  $p$ -subgroups of  $G$  divides  $m$  and satisfies the modular relation  $n_p \equiv 1 \pmod{p}$ .
- **Lem. 19. (Normalizers of Sylow  $p$ -Subgroups)** Let  $P \in \text{Syl}_p(G)$ . If  $Q$  is any  $p$ -subgroup of  $G$ , then  $Q \cap N_G(P) = Q \cap P$ .

- **Cor. 20. (Equivalent Statements for Sylow  $p$ -Subgroups)** Let  $P$  be a Sylow  $p$ -subgroup of  $G$ . Then the following are equivalent.
  - (1)  $P$  is the unique Sylow  $p$ -subgroup of  $G$ , i.e.,  $n_p = 1$ .
  - (2)  $P$  is normal in  $G$ .
  - (3)  $P$  is characteristic in  $G$ .
  - (4) All subgroups generated by elements of  $p$ -power order are  $p$ -groups, i.e., if  $X$  is any subset of  $G$  such that  $|x|$  is a power of  $p$  for all  $x \in X$ , then  $\langle X \rangle$  is a  $p$ -group.

### 2.4.1 Application of Sylow's Theorem

- **Exp. (Groups of Order  $pq$ ,  $p < q$  prime)** Let  $|G| = pq$  for primes  $p$  and  $q$  with  $p < q$ . Let  $P \in \text{Syl}_p(G)$  and  $Q \in \text{Syl}_q(G)$ . Then (1)  $Q$  is normal in  $G$ , and (2) if  $P$  is also normal in  $G$ , then  $G$  is cyclic.
  - (1) By Sylow's Theorems,  $n_q \in \{1, p\} \cap \{1, q+1, \dots\}$ . Since  $q > p$ ,  $n_q$  is forced to be 1. Hence,  $Q$  is normal by Corollary 20.
  - (2) [!! Complete Later !!]
- **Exp. (Groups of Order  $p^2q$ ,  $p$  and  $q$  Distinct)** Let  $G$  be a group of order  $p^2q$  for distinct primes  $p$  and  $q$ . We will show that  $G$  has a normal Sylow subgroup (for either  $p$  or  $q$ ).
  - (1) Consider first when  $p > q$ . Since  $n_p \mid q$  and  $n_p = 1 + kp$ , we must have  $n_p = 1$  so that  $P \trianglelefteq G$ .
  - (2) Consider now the case that  $q < p$ . If  $n_q = 1$ , then we are done. So suppose  $n_q = 1 + tq$  for some  $t > 0$ . Since  $n_q$  divides  $p^2$ ,  $n_q = p$  or  $n_q = p^2$ . Since  $q > p$ , we must have  $n_q = p^2$ . Hence,

$$tq = p^2 - 1 = (p-1)(p+1). \quad (27)$$

Since  $q$  is prime, either  $q \mid (p-1)$  or  $q \mid (p+1)$ . Since  $q > p$ ,  $q \mid (p+1)$ . But since  $q > p$ , we must have  $q = p+1$ . This forces  $q = 3$  and  $p = 2$  so that  $|G| = 12$ .

- (3) Consider the case  $|G| = 2^2 \cdot 3$ . If  $n_3 = 1$ , then we are done. So suppose  $n_3 = 4$ , which means  $G$  contains 8 elements of order 3. Let  $G$  act on  $\text{Syl}_3(G)$  by conjugation, which induces a homomorphism  $\varphi : G \rightarrow S_4$ . In particular, if  $K$  is the kernel of this homomorphism, then  $K \leq N_G(P) = P$ . Since  $P$  is not normal in  $G$  (by hypothesis),  $K = 1$  so that  $\varphi$  is injective. Hence,  $K \cong \varphi(G) \leq S_4$ . Since  $G$  contains 8 elements of order 3, and  $S_4$  contains exactly 8 elements of order 3, all contained in  $A_4$ ,  $\varphi(G)$  must intersect  $A_4$  in a subgroup of order at least 8. Since both groups have order 12, it follows that  $\varphi(G) \cong A_4$ , the latter of which has a normal Sylow 2-subgroup.

### 2.4.2 Exercises

**Exercise 13.** Prove that a group of order 56 has a normal Sylow  $p$ -subgroup for some prime  $p$  dividing its order.

Let  $G$  be a group of order  $56 = 2^3 \cdot 7$ . By Sylow's Theorem,  $n_7 \in \{1, 8\}$  and  $n_2 \in \{1, 7\}$ . If  $n_7 = 1$ , then we are done. So assume  $n_7 = 8$ . Since every element of  $G$  of order 7 lies in a Sylow 7-subgroup, each Sylow 7-subgroup has 6 nonidentity elements, and each pair of distinct Sylow 7-subgroups intersects trivially by Lagrange's Theorem,  $G$  must contain exactly 48 elements of order 7. This means that  $G$  contains at most 7 nonidentity elements whose order is some power of 2. Assume to the contrary that  $n_2 = 7$ , and let  $P_1, P_2$  be distinct Sylow 2-subgroups of  $G$ . By definition of distinct,  $P_2$  must contain at least one element that is not contained in  $P_1$ . Hence,  $|P_1 \cup P_2| \geq 9$ . Adding in the elements of  $G$  with order equal to 7, we see that  $|G|$  must be at least 57, which is a contradiction. Hence, by contradiction,  $n_2 = 1$ . The proof concludes.

**Exercise 14.** Prove that a group of order 312 has a normal Sylow  $p$ -subgroup for some prime  $p$  dividing its order.

Let  $G$  be a group of order 312. We start by considering the prime factorization of 312:

$$312 = 2^3 \cdot 3 \cdot 13. \quad (28)$$

By Sylow's Theorem:

$$\begin{aligned} n_2 &\in \{1, 3, 13, 39\} \cap \{1, 3, \dots\} = \{1, 3, 13, 39\}. \\ n_3 &\in \{1, 2, 4, 8, 13, 26, 52, 104\} \cap \{1, 4, 7, 10, 13, \dots, 52, \dots\} = \{1, 4, 7, 10, 52\}. \\ n_{13} &\in \{1, 2, 3, 4, 6, 8, 12, 24\} \cap \{1, 14, 27, \dots\} = \{1\}. \end{aligned} \quad (29)$$

Hence,  $G$  has a single Sylow 13-subgroup, which must be normal.

**Exercise 15.** Prove that a group of order 351 has a normal Sylow  $p$ -subgroup for some prime  $p$  dividing its order.

Let  $G$  be a group of order 351. We start by considering the prime factorization of 351:

$$351 = 3^3 \times 13. \quad (30)$$

By Sylow's Theorem,

$$\begin{aligned} n_{13} &\in \{1, 3, 9, 27\} \cap \{1, 14, 27, \dots\} = \{1, 27\}. \\ n_3 &\in \{1, 13\} \cap \{1, 4, \dots, 13, \dots\} = \{1, 13\}. \end{aligned} \quad (31)$$

If  $n_{13} = 1$ , we are done. So assume  $n_{13} = 27$ . Since every element of  $G$  of order 13 is contained in a Sylow 13-subgroup, each Sylow 13-subgroup of  $G$  contains 12 nonidentity elements, and by Lagrange's Theorem, Sylow 13-subgroups intersect trivially in  $G$ ,  $G$  must contain  $12(27) = 324$  elements of order 13. This means that  $G$  contains *at most* 27 elements whose order is a power of 3. Assume  $n_3 = 13$ , and let  $P_1, P_2$  be distinct Sylow 3-subgroups of  $G$ . Then by definition of distinct,  $P_2$  contains at least one element that is not contained in  $P_1$ . Since Sylow 3-subgroups of  $G$  contain 27 elements, it follows that  $|P_1 \cup P_2| \geq 28$ . But then  $G$  must contain at least  $28 + 324 = 352$  elements, which is a contradiction. Hence, by contradiction,  $n_3 = 1$  and the proof concludes.

**Exercise 17.** Prove that if  $|G| = 105$ , then  $G$  has a normal Sylow 5-subgroup and a normal Sylow 7-subgroup.

Let  $G$  be a group of order  $105 = 3 \cdot 5 \cdot 7$ . By Sylow's Theorem,

$$\begin{aligned} n_7 &\in \{1, 3, 5, 15\} \cap \{1, 8, 15, \dots\} = \{1, 15\}. \\ n_5 &\in \{1, 3, 7, 21\} \cap \{1, 6, 11, \dots\} = \{1, 21\}. \\ n_3 &\in \{1, 5, 7, 35\} \cap \{1, 4, 7, \dots\} = \{1, 7\}. \end{aligned} \quad (32)$$

We consider three separate cases.

- (i) Suppose  $G$  has neither a normal Sylow 7-subgroup nor a normal Sylow 5-subgroup, which means that  $n_7 = 15$  and  $n_5 = 21$ . Then  $G$  has 90 nonidentity elements of order 7 and 84 nonidentity elements of order 5, which means that  $|G| \geq 174$ , which is a contradiction. Hence, at least one of  $n_5$  and  $n_7$  must be one.
- (ii) Suppose  $n_5 = 1$  and  $n_7 = 15$ . Then  $G$  has 94 nonidentity elements whose order is not three. This leaves 10 nonidentity elements to be distributed amongst the Sylow 3-subgroups. But each Sylow 3-subgroup contains two nonidentity elements. Since the Sylow 3-subgroups all intersect trivially, this implies that there are 5 Sylow 3-subgroups which contradicts Sylow's Theorems. Hence, this is not a possible case.
- (iii) Finally, assume  $n_5 = 21$  and  $n_7 = 1$ .

### **3 Direct and Semidirect Products and Abelian Groups**