# Om Algebra Crash Course

Aniruddha Madhava

December 31, 2025

## Contents

# 1   Quotient Groups and Homomorphisms

## 1.1   The Isomorphism Theorems

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

  Let $\varphi : G \to H$ 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

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

  This implies that $gKg^{-1} \subseteq K$ for all $g \in G$, and so $K$ is a normal subgroup of $G$. Now let $\widetilde{\varphi} : G/\ker \varphi \to \varphi(G)$ as follows: $\widetilde{\varphi}(gK) = \varphi(g)$. First, we start by showing that $\widetilde{\varphi}$ is well-defined. Suppose $g_1 K = g_2 K$, which means that $g_1 g_2^{-1} \in K$. Therefore,

  $$\varphi(g_1 g_2^{-1}) = 1 \implies \varphi(g_1) = \varphi(g_2) \implies \widetilde{\varphi}(g_1 K) = \widetilde{\varphi}(g_2 K). \tag{2}$$

  We need to show that $\widetilde{\varphi}$ is an isomorphism. Suppose $\widetilde{\varphi}(g) = \widetilde{\varphi}(h)$. 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 $\widetilde{\varphi}$ is surjective. Finally, if $g_1 K, g_2 K \in G/K$, then

  $$\widetilde{\varphi}(g_1 K \cdot g_2 K) = \widetilde{\varphi}(g_1 g_2 K) = \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = \widetilde{\varphi}(g_1 K)\widetilde{\varphi}(g_2 K). \tag{3}$$

  Hence, $\widetilde{\varphi}$ 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 $\varphi : A \to AB/B$ 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:

  $$A \ni a \in \ker \varphi \iff aB = 1B \iff a \in B. \tag{4}$$

  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

  $$(G/H)/(K/H) \cong G/K. \tag{5}$$

  First, we will show that $K/H \trianglelefteq G/H$. Define the map $\varphi : G/H \to G/K$ by $\varphi(gH) = gK$. First, we need to show that this map is well-defined. Suppose $g_1 H = g_2 H$. Then $g_1 = g_2 h$ for some $h \in H$. Since $H \leq K$, $h \in K$, which shows that $g_1 K = g_2 K$. 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,

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

## 1.2 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,

$$p = |G : H| = |G : HK| \cdot |HK : H|. \tag{6}$$

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

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

---

**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

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

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:

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

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

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

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 $P/(P \cap N) \cong PN/N$, $|PN/N| = |P|/|P \cap N| = p^{a-b}$.

## 1.3   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

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

is called a *composition series* if $N_i \trianglelefteq N_{i+1}$ 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 $\{1, 2, \ldots, r\}$ such that

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

- **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

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_s = G \tag{13}$$

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

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

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

Hence, the chain

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_n = N = G_0 \trianglelefteq \cdots \trianglelefteq G_m = G \tag{15}$$

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

## 1.4   Exercises

**Exercise 1.** Prove that if $G$ is an abelian simple group then $G \cong Z_p$ 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 $\varphi : \mathbb{Z} \to G$ 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 $\varphi : \mathbb{Z}/p\mathbb{Z} \to G$ 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. We will proceed by complete induction; assume that the result holds true for all groups of order less than $|G|$.

# 2   Group Actions

# 3   Direct and Semidirect Products and Abelian Groups