

List of Theorems

Proposition 1	18
Proposition 2	Properties of S_n	20
Theorem 3	Cycle Decomposition Theorem	21
Proposition 4	Group Identity and Group Element Inverse	23
Proposition 5	26
Proposition 6	Cancellation Laws	29
Proposition 7	31
Proposition 8	Intersection of Subgroups is a Subgroup ..	35
Proposition 9	Finite Subgroup Test	35
Theorem 10	Parity Theorem	37
Theorem 11	Alternating Group	38
Proposition 12	Cyclic Group as A Subgroup	40
Proposition 13	Properties of Elements of Finite Order ...	41
Proposition 14	Property of Elements of Infinite Order ...	43
Proposition 15	Orders of Powers of the Element	43
Proposition 16	Cyclic Groups are Abelian	44
Proposition 17	Subgroups of Cyclic Groups are Cyclic ...	45
Proposition 18	Other generators in the same group	46
Theorem 19	Fundamental Theorem of Finite Cyclic Groups	47
Proposition 20	Properties of Homomorphism	50
Proposition 21	Isomorphism as an Equivalence Relation ..	51

14 Lecture 14 Jun 01 2018

14.1 Isomorphism Theorems (Continued 2)

14.1.1 Isomorphism Theorems (Continued)

Note (Recall)

In First Isomorphism Theorem 38, we had that for a group homomorphism $\alpha : G \rightarrow H$ where G and H are groups,

$$G/\ker \alpha \cong \operatorname{im} \alpha$$

Now let $\alpha : G \rightarrow H$ be a group homomorphism, $K = \ker \alpha$, $\phi : G \rightarrow G/K$ be the coset map, and $\bar{\alpha}$ be as defined in the proof of First Isomorphism Theorem 38. We then have the following commutative diagram to illustrate the relationship between the three groups.

$$\begin{array}{ccc} G & \xrightarrow{\alpha} & H \\ \phi \downarrow & \nearrow \bar{\alpha} & \\ G/K & & \end{array}$$

A natural question to ask after seeing the relationship is: Is $\bar{\alpha}\phi = \alpha$? If it is, is the definition of $\bar{\alpha}$ unique? The answer is: **YES!** on both accounts.

Proof

Let $g \in G$. Then

$$\bar{\alpha}\phi(g) = \bar{\alpha}(\phi(g)) = \bar{\alpha}(Kg) = \alpha(g)$$

Suppose $\alpha = \beta\phi$ where $\beta : G/K \rightarrow H$. Then

$$\beta(Kg) \stackrel{(1)}{=} \beta(\phi(g)) = \beta\phi(g) = \alpha(g) = \bar{\alpha}(Kg)$$

where (1) is because ϕ is surjective by Proposition 35. Therefore, we observe that $\beta = \bar{\alpha}$ for any $Kg \in G/K$. This proves that $\bar{\alpha}$ is the unique homomorphism such that $G/K \rightarrow H$ satisfying $\alpha = \bar{\alpha}\phi$. \square

With that, we have the following proposition.

Proposition 39

Let $\alpha : G \rightarrow H$ be a group homomorphism, where G and H are groups. Let $K = \ker \alpha$. Then α factors uniquely as $\alpha = \bar{\alpha}\phi$ where $\phi : G \rightarrow G/K$ is the coset map and $\bar{\alpha} : G/K \rightarrow H$ is defined by

$$\bar{\alpha}(Kg) = \alpha(g).$$

Note that ϕ is surjective and $\bar{\alpha}$ is injective.

In such a scenario, we also say that α **factors through** ϕ .¹

¹ Reference for the terminology: <https://math.stackexchange.com/questions/68941/terminology-a-homomorphism-factors>.

Example 14.1.1

Let $G = \langle g \rangle$ be a cyclic group. Consider $\alpha : \mathbb{Z} \rightarrow G$, defined as

$$\forall k \in \mathbb{Z} \quad \alpha(k) = g^k,$$

which is a group homomorphism. By definition, α is surjective. Note that

$$\ker \alpha = \{k \in \mathbb{Z} : g^k = 1\}.$$

We have, therefore, two cases to consider.

- G is an infinite group

This would imply that $\ker \alpha = \{0\}$ since only $g^0 = 1$. Then by First Isomorphism Theorem 38, we have that

$$\mathbb{Z}/\ker \alpha \cong G$$

Note that²

$$\mathbb{Z}/\ker \alpha = \{(\ker \alpha)k : k \in \mathbb{Z}\} = \{0 + k : k \in \mathbb{Z}\} = \mathbb{Z}.$$

² We are assuming that the group \mathbb{Z} here works under the operation of addition, otherwise, if we employ multiplication, then \mathbb{Z} would not be a group and α would not be a group homomorphism.

Therefore

$$\mathbb{Z} \cong G$$

- G is a finite group

Suppose that $|G| = o(g) = n \in \mathbb{N}$, which is valid by Corollary 24. Then

$$\ker \alpha = n\mathbb{Z}$$

Then by the First Isomorphism Theorem 38, we have

$$\mathbb{Z}/n\mathbb{Z} \cong G.$$

Observe that

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z} + k : k \in \mathbb{Z}\} = \mathbb{Z}_n$$

since the set in the middle is the definition of the set of integers modulo n .³ Therefore,

$$\mathbb{Z}_n \cong G$$

Therefore, we have that

$$\mathbb{Z} \cong G \text{ or } \mathbb{Z}_{o(g)} \cong G$$

³ This is why we often see texts from various authors using $\mathbb{Z}/n\mathbb{Z}$ to represent the set of integers modulo n .

Theorem 40 (Second Isomorphism Theorem)

Let H and K be the subgroups of a group G with $K \triangleleft G$. Then

- HK is a subgroup of G ;
- $K \triangleleft HK$;
- $H \cap K \triangleleft H$; and
- $HK/K \cong H/H \cap K$.

Proof

Since $K \triangleleft G$, by Lemma 29 and Proposition 30, we have that $HK = KH$ is a subgroup of G . Consequently, we have $K \triangleleft HK$, since K is clearly a subgroup of HK and $K \triangleleft G$, and so $\forall x \in HK \subseteq G$ we have that $gK = Kg$.

Consider $\alpha : H \rightarrow HK/K$, defined by⁴

⁴ Note that $Kh \in HK/K$ since $h \in H \subseteq HK$.