

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

Proof

Let X be the set of all distinct left cosets of H in G . We have $|X| = p$ and so $S_X \cong S_p$. Let $\tau : G \rightarrow S_X \cong S_p$ be as defined in Example 15.1.1, with $K := \ker \tau \subseteq H$. By the First Isomorphism Theorem, we have that

$$G/K \cong \text{im } \tau \leq S_X \cong S_p,$$

i.e. G/K is isomorphic to a subgroup of S_p . Therefore, by Lagrange's

Theorem, we have that $|G/K| \mid p!$.

Also, since $K \subseteq H$, if $[H : K] = k \in \mathbb{N}$, then

$$|G/K| \stackrel{(1)}{=} \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = pk,$$

where (1) is by Proposition 35. Therefore we have that $pk \mid p!$ and so $k \mid (p-1)!$.

Note that $k \mid |H|$ ⁸, which divides $|G|$, and p is the smallest prime dividing $|G|$. Thus every prime divisor of k must be $\geq p$.⁹ Thus $k = 1$, which implies that $K = H$. Therefore, $H \triangleleft G$ as desired. \square

⁸ This is clear since $|H| = k|K|$.

⁹ By the **Fundamental Theorem of Arithmetic**, and since k is finite, let $k = p_1^{a_1} p_2^{a_2} \dots p_m^{a_m}$, where p_i 's are distinct primes and $a_i \in \mathbb{N}$ are the multiplicities of the i^{th} , and by the **Well-Ordering Principle**, let $p_i < p_{i+1}$. Then we have, for some $b = b_1^{c_1} b_2^{c_2} \dots b_j^{c_j} \in \mathbb{N}$ where the b_i 's are distinct primes, $b_i < b_{i+1}$, and $c_i \in \mathbb{N} \cup \{0\}$,

$$m = kb = p_1^{a_1} p_2^{a_2} \dots p_m^{a_m} b_1^{c_1} b_2^{c_2} \dots b_j^{c_j}.$$

Since p is the smallest prime that divides m , we have

$$\begin{aligned} p &= \min\{p_1, p_2, \dots, p_m, b_1, b_2, \dots, b_j\} \\ &= \min\{p_1, b_1\} \end{aligned}$$

15.1.2 Group Action**Definition 28 (Group Action)**

Let G be a group, X a non-empty set. A **group action** of G on X is a mapping $G \times X \rightarrow X$ denoted as $(a, x) \rightarrow ax$ such that

1. $1 \cdot x = x, x \in X$
2. $a \cdot (b \cdot x) = (ab) \cdot x, a, b \in G, x \in X$

In this case, we say G **acts on** X .

16 Lecture 16 Jun 06 2018

16.1 Group Action (Continued)

16.1.1 Group Action (Continued)

Remark

Let G be a group acting on a set X . For $a, b \in G$, and $x, y \in X$, we have that

$$a \cdot x = b \cdot y \iff (b^{-1}a) \cdot x = y.$$

In particular, we have

$$a \cdot x = a \cdot y \iff x = y.$$

For $a \in G$, define $\sigma_a : X \rightarrow X$ by $\sigma_a(x) = a \cdot x$ for all $x \in X$. In A3, we will be showing that¹:

1. $\sigma_a \in S_X$, the permutation group of X ; and
2. The function $\Theta : G \rightarrow S_X$ given by $\Theta(a) = \sigma_a$ is a group homomorphism with

$$\ker \Theta = \{a \in G : a \cdot x = x, x \in X\}.$$

Note that the group homomorphism $\Theta : G \rightarrow S_X$ gives an **equivalent definition** of a **Group Action** of G on X . If $X = G$, $|G| = n$ and $\ker \Theta = \{1\}$ ², then the map $\Theta : G \rightarrow S_G \cong S_n$ shows that G is isomorphic to a subgroup of S_n ³, which the equivalent statement of Cayley's Theorem.

Example 16.1.1

If G is a group, let G act on itself by $a \cdot x = a \cdot x \cdot a^{-1}$, for all $a, x \in G$. Note that the axioms of a group action is satisfied:

¹ This will be added after the assignment.

² This is also called a **faithful group action**.
³

Exercise 16.1.1

Verify that G is indeed isomorphic to a subgroup of S_n using the given information and the equivalent definition of a group action.

1. $1 \cdot x = 1 \cdot x \cdot 1^{-1} = x$; and
2. $a \cdot (b \cdot x) = a \cdot (b \cdot x \cdot b^{-1}) \cdot a = ab \cdot x \cdot (ab)^{-1} = (ab) \cdot x$.

In this case, we say that G **acts on itself by conjugation**.

Definition 29 (Orbit & Stabilizer)

Let G be a group acting on a set X , and $x \in X$. We denote by

$$G \cdot x = \{g \cdot x : \forall g \in G\}$$

the **orbit** of x and

$$S(x) = \{g \in G : g \cdot x = x\} \subseteq G$$

the **stabilizer** of x .

There is no standardized way of expressing the orbit and the stabilizer, i.e. the notation for orbit and stabilizers will be different across many references.

Proposition 45

Let G be a group acting on a set X and $x \in X$. Let $G \cdot x$ and $S(x)$ be the orbit and stabilizer of x respectively. Then

1. $S(x) \leq G$
2. there is a bijection from $G \cdot x$ to $\{gS(x) : g \in G\}$ and thus $|G \cdot x| = [G : S(x)]$.

Proof

1. Since $1 \cdot x = x$, we have $1 \in S(x)$. If $g, h \in S(x)$, then

$$gh \cdot x = g \cdot (h \cdot x) = g \cdot x = x$$

i.e. $S(x)$ is closed under "composition of group action". Also note that

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = 1 \cdot x = x.$$

Thus the inverse of each element is also in $S(x)$. Therefore, by the **Subgroup Test**, $S(x) \leq G$.

2. For the sake of simplicity, let us write $S = S(x)$. Consider the map

$$\phi : G \cdot x \rightarrow \{gS(x) : g \in G\}$$