List of Theorems

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 $\tau : G \to S_X \cong S_p$ be as defined in Example 15.1.1, with $K := \ker \tau \subseteq H$. By the First Isomorphism Theorem, we have that

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

i.e. G/K is isomorphic to a subgroup of S_p. Therefore, by Lagrange's Theorem, we have that $\left| G/K \right| \,\Big|\, p!$.

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

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

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 evrey prime divisor of k must be $\geq p$.[9] Thus $k = 1$, which implies that $K = H$. Therefore, $H \lhd G$ as desired. □

[8] This is clear since $|H| = k\,|K|$.

[9] By the Fundamental Theorem of Arithmetic, and since k is finite, let $k = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$, 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 $b = b_1^{c_1} b_2^{c_2} \ldots b_j^{c_j} \in \mathbb{N}$ where the b_i's are distint primes, $b_i < b_{i+1}$, and $c_i \in \mathbb{N} \cup \{0\}$,

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

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

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

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 $G \times X \to X$ denoted as $(a, x) \to ax$ 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 $\sigma_a : X \to X$ by $\sigma_a(x) = a \cdot x$ for all $x \in X$. In A3, we will be showing that[1]:

1. $\sigma_a \in S_X$, the permutation group of X; and
2. The function $\Theta : G \to S_X$ 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 $\Theta : G \to S_X$ 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 $\Theta : G \to S_G \cong S_n$ shows that G is isomorphic to a subgroup of S_n [3], which the equivalent statement of Cayley's Theorem.

[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.

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. $1 \cdot x = 1 \cdot x \cdot 1^{-1} = x$; 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 an $x \in X$. 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

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

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*

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