Foreword

Usage

- Notes are presented in two columns: main notes on the left, and sidenotes on the right. Main notes will have a larger margin.
- The following is the color code for the notes:

Blue	Definitions
Red	Important points
Yellow	Points to watch out for / comment for incompletion
Green	External definitions, theorems, etc.
Light Blue	Regular highlighting
Brown	Secondary highlighting

- The following is the color code for boxes, that begin and end with a line of the same color:

Blue	Definitions
Red	Warning
Yellow	Notes, remarks, etc.
Brown	Proofs
Magenta	Theorems, Propositions, Lemmas, etc.

- Hyperlinks are underlined in magenta. If your PDF reader supports it, you can follow the links to either be redirected to an external website, or a theorem, definition, etc., in the same document. Note that this is only reliable if you have the full set of notes as a single document, which you can find on: `https://japorized.github.io/TeX_notes`

15 Lecture 15 Jun 04 2018

15.1 Group Action

15.1.1 Cayley's Theorem

Theorem 42 (Cayley's Theorem)

If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.

Proof

Since G is finite, let $G = \{g_1, g_2, ..., g_n\}$ and let S_G be the permutation group of G. By identifying g_i with i, where $1 \leq i \leq n$, we see that $S_G \cong S_n$ [1]. Therefore, it suffices to find an injective homomorphism[2] $\sigma : G \to S_G$.

Consider the function $\mu_a : G \to G$, where $a \in G$, such that $\mu_a(g) = ag$ for all $g \in G$. Clearly, μ_a is surjective. Suppose $\mu_a = \mu_b$, where $b \in G$. Then $a = \mu_a(1) = \mu_b(1) = b$. Thus μ_a is also injective. It follows that $\mu_a \in S_G$ by definition.

Now define the function $\sigma : G \to S_G$ such that $\sigma(a) = \mu_a$. Clearly, σ is injective, since $\sigma(a) = \sigma(b) \implies \mu_a = \mu_b$. Observe that $\sigma(ab) = \mu_{ab} = ab = \mu_a\mu_b$. Thus σ is a group homomorphism. Note that $\ker\sigma = \{1\}$, the trivial group. It follows from the First Isomorphism Theorem that $G \cong \operatorname{Im}\sigma \leq S_G \cong S_n$.[3] [4] $\square$

Cayley's Theorem is, however, too strong at times. We can certainly find a smaller integer m such that G is contained in S_m. Con-

[1] S_G is the permutation group of G. We can think of S_G as a group of permutations that permutes the index of the elements of G. Since there are n indices, there are $n!$ ways to permute the indices, and so $|S_G| = n! = |S_n|$. Then we can certainly find some isomorphism from S_G to S_n, and so $S_G \cong S_n$.

[2] **Why do we need injectivity?** We need homomorphicity in order to invoke the First Isomorphism Theorem so that we can get $G \cong \operatorname{im}\sigma \leq S_G \cong S_n$.

[3] We shall use $H \leq G$ to denote that H is a subgroup of G from here on.

[4] This is a result from Proposition 36

sider the following example.

Example 15.1.1

Let $H \leq G$ with $[G : H] = m < \infty$. Let $X = \{g_1 H, g_2 H, ..., g_m H\}$ be the set of all distinct left cosets of H in G [5]*. For $a \in G$, define $\lambda_a : X \to X$ by $\lambda_a(gH) = agH$, $gH \in X$.*

Note that λ_a is a bijection[6]*, and so $\lambda_a \in S_X$, the permutation group of X. Consider the mapping $\tau : G \to S_X$ defined by $\tau(a) = \lambda_a$ for $a \in G$. Note that $\forall a, b \in G$, $\lambda_{ab} = \lambda_a \lambda_b$. Thus τ is a homomorphism. Note that if $a \in \ker \tau$, then $aH = H$ which implies $a \in H$ by Proposition 22. Thus $\ker \tau \subseteq H$.*

[5] This is simply a consequence of $[G : H] = m$.

[6] This is true as shown in the proof above, but it can also serve as a tiny exercise.

From the example above, if we apply the First Isomorphism Theorem, then

$$G / \ker \tau \cong \operatorname{im} \tau \leq S_X \cong S_m \leq S_n.$$

This is the result that we desired.

Theorem 43 (Extended Cayley's Theorem)

Let $H \leq G$ with $[G : H] = m < \infty$. If G has no normal subgroup contained in H except for the trivial subgroup $\{1\}$, then G is isomorphic to a subgroup of S_m.

Proof

By our assumption, let X be the set of all distinct left cosets of H in G. Then we have that $|X| = m$ and so $S_X \cong S_m$ [7]*. From Example 15.1.1, we have that there exists a group homomorphism $\tau : G \to S_X$ with $K := \ker \tau \subseteq H$. So by the First Isomorphism Theorem, we have that*

$$G / K \cong \operatorname{im} \tau.$$

Since $K \subseteq H$ and $K \triangleleft G$, we have, by assumption, that $K = \{1\}$. It follows that

$$G \cong \operatorname{im} \tau \leq S_X \cong S_m.$$

$\square$

[7] This is as argued in the proof of Cayley's Theorem.

Corollary 44

Let $|G| = m \in \mathbb{N}$ and p the smallest prime such that $p \mid m$. If $H \leq G$ with $[G : H] = p$, then $H \lhd G$.

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 $k = p_1^{a_1} p_2^{a_2} ... p_m^{a_m}$, 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 distint primes, $b_i < b_{i+1}$, and $c_i \in \mathbb{N} \cup \{0\}$,

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

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

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

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.*