Dillan Marroquin
MATH 331.1001
Scribing Week 9
Due. 25 October 2021

Lecture 21

<u>Q:</u> Is the image of a group homomorphism $\varphi : G \to H$ a normal subgroup of H?
<u>A:</u> Nope! As an example, take $G = \mathbb{Z}$, $H = S_3$, $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Then $\mathrm{im}\varphi = \{\varphi(k) | k \in \mathbb{Z}\} = \{\tau^k | k \in \mathbb{Z}\} = \langle \tau \rangle$. We know from past lectures that $\langle \tau \rangle \leq S_3$ is not a normal subgroup.

Permutation Groups

Definition (21.1)**.** Let X be a set. The <u>**permutation group of** X</u> is the set $\Sigma(X) := \{f : X \to X | f \text{ is a bijection}\}$ with binary operator being function composition, $\circ$, and identity element $e(x) = x$, $\forall x \in X$.

Most important example: $X = \mathbb{n} = \{1, \ldots, n\}$, $n \geq 1$. Then $\Sigma(X) = S_n$ is the <u>**symmetric group on n-letters** ($\mathrm{Sym}_{\mathbf{n}}$, $\Sigma_{\mathbf{n}}$)</u>.

Proposition (21.2)**.** Let $X = \{x_1, \ldots, x_n\}$ be an n-element set. Then $\Sigma(X) \cong S_n$.

Permutation Group of a Group: $\Sigma(G)$

Remark. Paulin uses the idea of a "group action." This is important, but we'll ignore it.

Let G be a group. Then $\Sigma(G) := \{f : G \to G | f \text{ is a set-theoretic bijection}\}$.
Let $g \in G$. Define a function $L_g : G \to G$, $L_g(x) := gx$, $\forall x \in G$. Note that L_g is not a group homomorphism if $g \neq e_G$, but it is a bijection.

Example. Let $G = \mathbb{Z}$. Then $L_g(a) = g *_G a = a + n$ (translation by n).

Lemma (21.3)**.** Let G, H be groups and let $\varphi : G \to H$ be a group homomorphism. If φ is injective, then φ induces a group isomorphism $G \cong \mathrm{im}\varphi \leq H$.

Theorem (21.4 Cayley's Theorem)**.** Let G be a group, $\Sigma(G)$ be the permutation group of the SET G. Let $\varphi : G \to \Sigma(G)$ be the function $\varphi(g) := L_g$. Then

1. φ is a group homomorphism and
2. φ induces a group isomorphism between G and the subgroup $\mathrm{im}\varphi \leq \Sigma(G)$.

Corollary (21.5)**.** Every finite group is isomorphic to a subgroup of S_n.

Lecture 22

Proof of Theorem 21.4.

1. Want to show $\forall g, g' \in G$, $\varphi(gg') = \varphi(g) \circ \varphi(g')$ i.e. we want to show $L_{gg'} = (L_g \circ L_{g'})(x)$. The left-hand side $= gg'x$ and the right-hand side $= L_g(L_{g'}(x)) = L_g(g'x) = gg'x$.
2. Suffices to show $\varphi : G \to \mathrm{im}\varphi$ is injective since any function is surjective onto its image (Lemma 21.3). By Prop. 17.1, we want to show $\ker\varphi = \{e_G\}$. Suppose $g \in \ker\varphi$. Then $\varphi(g) = \mathrm{id}_G$, i.e. $\forall x \in G$, $L_g(x) = \mathrm{id}_G(x) = x$. Since $x \in G$, $x^{-1} \in G$. Therefore $gx = x$ implies $g = e_G$. Thus injective.

■

Corollary (21.5)**.** Every finite group G of order n is isomorphic to a subgroup of $S_n = \Sigma(\{1, 2, \ldots, n\}$.

Structure of Symmetric Group S_n

S_n is B I G! $|S_n| = n!$, so it's too hard to write the elements of S_n as $\left(\begin{smallmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 6 & 1 & \cdots & 7 \end{smallmatrix}\right)$.

Definition (22.1). Let $i_1, i_2, \ldots, i_k$ be distinct elements of $\mathbb{n} = \{1, \ldots, n\}$ with $1 \leq k \leq n$. Then $(i_1, i_2, \ldots, i_k) \in S_n$ denotes the function $i_1 \mapsto i_2, i_2 \mapsto i_3, \ldots, i_{k-1} \mapsto i_k, i_k \mapsto i_1$. Every other element of $\mathbb{n}$ gets mapped to itself. $(i_1, \ldots, i_k)$ is a **k-cycle**. 2-cycles are **transpositions**.

Example.

1. Our friends $\sigma, \tau \in S_3$, where $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$ and $\tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$. ☺ In cycle notation we have $\sigma = (1\ 2\ 3)$ and $\tau = (2\ 3)$
2. Let $\rho = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{smallmatrix}\right) \in S_4$. Then $\rho = (1\ 4\ 3\ 2)$.
3. $\mathrm{id}_{\mathbb{n}} \in S_n$ and $\mathrm{id}_{\mathbb{n}} = (1) = (2) = (3) = \cdots$.

Remark.

1. Example 3 shows there are multiple ways to express cycles- Ex 1: $\sigma = (3\ 1\ 2) = (2\ 3\ 1)$, $\tau = (2\ 3) = (3\ 2)$.
2. Without context, it's unclear where these cycles live. e.g. $(1\ 2\ 3)$ could be in S_3 or S_4 corresponding to $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{smallmatrix}\right)$.

Proposition. Let $\sigma = (i_1\ i_2\ \ldots\ i_k) \in S_n$ be a k-cycle. Then:

1. $|\sigma| = k$ and
2. $\sigma^{-1} = (i_k\ i_{k-1}\ \ldots\ i_2\ i_1)$.

Lecture 23

Remark. This is important! Not every element in S_n is a cycle!

Example. $\eta = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right) \in S_4$. Note that $|\eta| = 2$. Prop. 22.1(1) implies $\eta = (i_1\ i_2)$. So η leaves 2 elements of $\{1, 2, 3, 4\}$ fixed, which is false.

Composition of Cycles: "Important" Group Operation in S_n into Cycle Notation

Example.

1. Let $\sigma = (1\ 3\ 5\ 2)$, $\tau = (2\ 5\ 6) \in S_6$. Then $\sigma \circ \tau = \sigma\tau = (1\ 3\ 5\ 2)(2\ 5\ 6) = (1\ 3\ 5\ 6)$.
2. Let $\sigma = (1\ 3\ 5\ 2)$, $\tau = (1\ 6\ 3\ 4) \in S_6$. Then $\sigma\tau = (1\ 3\ 5\ 2)(1\ 6\ 3\ 4) = (1\ 6\ 5\ 2)(3\ 4)$ which is NOT a cycle!

Observation: $\alpha = (1\ 6\ 5\ 2)$, $\beta = (3\ 4)$ commute: $\alpha\beta = \beta\alpha$.

Definition (23.1). 2 cycles $(i_1\ i_2\ \ldots\ i_r)$ and $(j_1\ j_2\ \ldots\ j_s)$ are **disjoint** iff $\forall k = 1, \ldots, r$, $i_k \neq j_l$, $\forall l = 1, \ldots, s$.

Proposition (23.2). If $\sigma, \tau \in S_n$ are disjoint cycles, $\sigma\tau = \tau\sigma$.

Proof. We want to show $\forall m \in \mathbb{n}$, $\sigma\tau(m) = \tau\sigma(m)$. Let $I := \{i_1, \ldots, i_r\}$, $J := \{j_1, \ldots, j_k\}$. Let $m \in \mathbb{n}$. We observe 3 different cases:
Case 1: $m \notin I$, $m \notin J$. By definition of cycle, $\tau(m) = m$ and $\sigma(m) = m$. Therefore $\sigma\tau(m) = m = \tau\sigma(m)$.
Case 2: $m \in I$. Consider $\sigma\tau(m)$. Since $m \in I$, $m \notin J$ and therefore $\tau(m) = m$ which implies $\sigma\tau(m) = \sigma(m)$. Consider $\tau\sigma(m)$. Then $\sigma(m) \in I$ which implies $\sigma(m) \notin J$ and therefore $\tau\sigma(m) = \sigma(m)$.
Case 3: $m \in J$. Same as Case 2, just swap the roles of I, J. ■

Remark. Let $\sigma = (1\ 2\ 3)$ and $\tau = (2\ 3) \in S_3$. Then $\sigma\tau = (1\ 2\ 3)(2\ 3) = (1\ 2) \neq (1\ 3) = (2\ 3)(1\ 2\ 3) = \tau\sigma$.

Corollary (23.3). Let $\alpha \in S_n$ be the product of disjoint cycles $\sigma_1, \sigma_2, \ldots, \sigma_k \in S_n$. Then $|\sigma| = \mathrm{lcm}\{|\sigma_1|, |\sigma_2|, \ldots, |\sigma_k|\}$.