Math 493 Lecture 2

Professor Andrew Snowden

Transcribed by Thomas Cohn

9/9/2019

Defn: S_n is the symmetric group on n letters. As a group, it can be considered to be the set of bijections on $\{1, \ldots, n\}$ under composition.

$\text{ord}(S_n) = n!$, because an element of S_n is a permutation. There are n choices for the first number, $n-1$ choices for the second number, etc.

Ex:

- $|S_2| = 2! = 2$.
- $|S_3| = 3! = 6$.
- $|S_4| = 4! = 24$.
- $|S_5| = 5! = 120$.

Cycle Notation

Defn: Say $a_1, \ldots, a_r \in \{1, \ldots, n\}$ distinct. Define the **r-cycle** $\begin{pmatrix} a_1 & a_2 & \cdots & a_r \end{pmatrix}$ as the element of S_n defined by $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_r \mapsto a_1$, and $a_i \mapsto a_i$ for all $a_i \notin \{a_1, \ldots, a_r\}$.

Fact: Every element of S_n can be written as a product of disjoint cycles.
Proof (sketch): Suppose $\sigma \in S_n$. $1 \mapsto \sigma(1), \sigma(1) \mapsto \sigma^2(1), \ldots, \sigma^{r-1}(1) \mapsto 1$.[1] Then successively repeat for the smallest element not already in a cycle.

Ex: $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 2 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 5 \end{pmatrix}$, becuase

$$\begin{gathered} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 5 \\ 4 \mapsto 4 \\ 5 \mapsto 3 \end{gathered}$$

Ex: The elements of S_2 are

- $1 = \text{id}$
- $\begin{pmatrix} 1 & 2 \end{pmatrix}$

Ex: The elements of S_3 are

- $1 = \text{id}$
- $\begin{pmatrix} 1 & 2 \end{pmatrix}$
- $\begin{pmatrix} 1 & 3 \end{pmatrix}$

[1] Note that $\sigma^{r-1}(1)$ cannot map to some $\sigma^k(1)$, because elements of S_n are bijections, and $\sigma^{k-1}(1) \mapsto \sigma^k(1)$.

- $\begin{pmatrix}2 & 3\end{pmatrix}$
- $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$
- $\begin{pmatrix}1 & 3 & 2\end{pmatrix}$

Note that a 2-cycle is just a transposition of two elements.

Fact: The order of an r-cycle is r, because for any σ, $\sigma^r = \mathrm{id}$, and r is minimal.

Defn: For G and H groups, an **isomorphism** between G and H is a bijection $f : G \to H$ s.t. $f(xy) = f(x)f(y)$, $\forall x, y \in G$. We say G and H are **isomorphic**, written $G \cong H$, if such an isomorphism exists.

Ex: In S_5, we consider $G = \left\langle \begin{pmatrix}1 & 2\end{pmatrix} \right\rangle = \left\{\mathrm{id}, \begin{pmatrix}1 & 2\end{pmatrix}\right\}$ and $H = \left\langle \begin{pmatrix}3 & 5\end{pmatrix} \right\rangle = \left\{\mathrm{id}, \begin{pmatrix}3 & 5\end{pmatrix}\right\}$.
$f : G \to H$ where $\begin{pmatrix}1 & 2\end{pmatrix} \mapsto \begin{pmatrix}3 & 5\end{pmatrix}$, $\mathrm{id} \mapsto \mathrm{id}$ is an isomorphism, so $G \cong H$.

Remark:

- If $f : G \to H$ is an isomorphism, $f^{-1} : H \to G$ is an isomorphism. So if $G \cong H$, then $H \cong G$.
- If $f : G \to H$, $g : H \to K$ are isomorphisms, then $g \circ f : G \to K$ is an isomorphism. So if $G \cong H$ and $H \cong K$, then $G \cong K$.

Note: $\mathrm{id} : G \to G$ is an isomorphism, so $G \cong G$. However, there are usually other isomorphisms on G.

Defn: An **automorphism** of G is an isomorphism from G to G. The set of all automorphisms of G is denoted $\mathrm{Aut}(G)$, and is a group under composition.

Ex: G is a group. Consider $\begin{aligned} f : G &\to G \\ x &\mapsto x^{-1} \end{aligned}$. This is a bijection.
$f(xy) = (xy)^{-1} = y^{-1}x^{-1}$, and $f(x)f(y) = x^{-1}y^{-1}$, so they're not equal in general (in fact, they're equal if and only if G is abelian).
So f is an automorphism if and only if G is abelian.

Ex: $G = \left\langle \begin{pmatrix}1 & 2 & 3\end{pmatrix} \right\rangle \subseteq S_3$. That is, $G = \left\{1, \begin{pmatrix}1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\end{pmatrix}\right\}$.
$\begin{aligned} f : G &\to G \\ x &\mapsto x^{-1} \end{aligned}$. So $1 \mapsto 1$, $\begin{pmatrix}1 & 2 & 3\end{pmatrix} \mapsto \begin{pmatrix}1 & 3 & 2\end{pmatrix}$, and $\begin{pmatrix}1 & 3 & 2\end{pmatrix} \mapsto \begin{pmatrix}1 & 2 & 3\end{pmatrix}$.

Ex: $\sigma \in S_3$. Define $f : S_3 \to S_3$, where
$\begin{pmatrix}1 & 2\end{pmatrix} \mapsto \big(\sigma(1), \sigma(2)\big)$
$\begin{pmatrix}1 & 3\end{pmatrix} \mapsto \big(\sigma(1), \sigma(3)\big)$
$\begin{pmatrix}2 & 3\end{pmatrix} \mapsto \big(\sigma(2), \sigma(3)\big)$
$\begin{pmatrix}1 & 2 & 3\end{pmatrix} \mapsto \big(\sigma(1), \sigma(2), \sigma(3)\big)$
$\begin{pmatrix}1 & 3 & 2\end{pmatrix} \mapsto \big(\sigma(1), \sigma(3), \sigma(2)\big)$
This is an automorphism.

Defn: Let G be a group, and $g \in G$. Define $\begin{aligned} \gamma_g : G &\to G \\ x &\mapsto gxg^{-1} \end{aligned}$.
This is called the **conjugate** of x by g.

Claim: $\gamma_g \in \mathrm{Aut}(G)$. Proof: $\gamma_g(\gamma_{g^{-1}}(x)) = g\gamma_{g^{-1}}(x)g^{-1} = gg^{-1}x(g^{-1})^{-1}g = x$.
So $\gamma_g \circ \gamma_g^{-1} = \mathrm{id}$ and $\gamma_{g^{-1}} \circ \gamma_g = \mathrm{id}$, so γ_g is a bijection, and $\gamma_g^{-1} = \gamma_{g^{-1}}$.
$\gamma_g(xy) = gxyg^{-1} = gx(g^{-1}g)yg^{-1} = (gxg^{-1})(gyg^{-1}) = \gamma_g(x)\gamma_g(y)$.
Thus, γ_g is an isomorphism, so $\gamma_g \in \mathrm{Aut}(G)$. $\square$

Lemma: If $\sigma \in S_n$, $a_1, \ldots, a_r \in \{1, \ldots, n\}$ distinct, then $\sigma \begin{pmatrix}a_1 & \cdots & a_r\end{pmatrix} \sigma^{-1} = \begin{pmatrix}\sigma(a_1) & \cdots & \sigma(a_r)\end{pmatrix}$.

If G is abelian, then $\gamma_g = \mathrm{id}$, $\forall g \in G$.

Ex: $G = \mathbb{R}^2$ under addition. A is an invertible 2×2 real matrix. So $\begin{aligned} f : G &\to G \\ x &\mapsto Ax \end{aligned}$ is an automorphism, because $f(x + y) = A(x + y) = Ax + Ay = f(x) + f(y)$, and because A is invertible, so f is indeed a bijection.

Defn: automorphisms defined by conjugation are called **inner automorphisms**.

Ex: $\mathrm{SL}_n(\mathbb{R})$ is the subgroup of $\mathrm{GL}_n(\mathbb{R})$ consisting of matrices with determinant 1.
$\begin{aligned} f : \mathrm{SL}_n(\mathbb{R}) &\to \mathrm{SL}_n(\mathbb{R}) \\ x &\mapsto {}^T x^{-1} = (x^T)^{-1} \end{aligned}$ is an automorphism.

If f were inner, then $\exists g \in \mathrm{SL}_n(\mathbb{R})$ s.t. $f = \gamma_g$, i.e., ${}^T x^{-1} = gxg^{-1}$, $\forall x$.
So f is inner if and only if $n \leq 2$.

Defn: Let G and H be groups. A (**group**) **homomorphism** from G to H is a function $f : G \to H$ s.t. $f(xy) = f(x)f(y)$, $\forall x, y \in G$.

Ex: $\begin{aligned} \gamma : G &\to \mathrm{Aut}(G) \\ g &\mapsto \gamma_g \end{aligned}$ is a group homomorphism.

Proof:

$$\begin{aligned} \gamma_g(\gamma_h(x)) &= g\gamma_h(x)g^{-1} \\ &= g(hxh^{-1})g^{-1} \\ &= (gh)x(h^{-1}g^{-1}) \\ &= (gh)x(gh)^{-1} \\ &= \gamma_{gh}(x) \end{aligned}$$

So $\gamma_{gh} = \gamma_g \circ \gamma_h$. $\square$

Remark: Is $\gamma : S_n \to \mathrm{Aut}(S_n)$ an isomorphism? Sometimes, but the conditions are weird.

Ex: G is a group, $g \in G$. $\begin{aligned} f : \mathbb{Z} &\to G \\ n &\mapsto g^n \end{aligned}$ is a homomorphism.

$f(n + m) = g^{n+m} = \underbrace{g \cdots g}_{n+m} = \underbrace{g \cdots g}_{n} \underbrace{g \cdots g}_{m} = g^n g^m = f(n)f(m)$.

Note:

- f is injective $\Leftrightarrow \mathrm{ord}(g) = \infty$. More generally, $f(i) = f(j) \Leftrightarrow \mathrm{ord}(g) \mid i - j$.
- f is surjective $\Leftrightarrow g$ generates G.

Defn: Let $f : G \to H$ be a group homomorphism. The **image** of f is $im(f) = \{y \in H | \exists x \in G \text{ s.t. } y = f(x)\}$.

Fact: $\mathrm{im}(f)$ is a subgroup.

Proof:

- $1 \in \mathrm{im}(f)$, because $1 = f(1)$.
- If $y \in \mathrm{im}(f)$, then $y = f(x)$, so $y^{-1} = f(x^{-1}) \in \mathrm{im}(f)$.
- $y, y' \in \mathrm{im}(f) \Rightarrow y = f(x), y' = f(x') \Rightarrow yy' = f(xx') \in \mathrm{im}(f)$.

$\square$

Lemma: If f is a homomorphism, then

- $f(1) = 1$. Proof: $1 \cdot 1 = 1$, so $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$. Thus, $f(1) = 1$. $\square$
- $f(x^{-1}) = f(x)^{-1}$. Proof: $x \cdot x^{-1} = 1$, so $f(x)f(x^{-1}) = f(xx^{-1}) = f(1) = 1$. $\square$

Defn: The **kernel** of f is $\ker(f) = \{x \in G | f(x) = 1\}$.

Fact: $\ker(f)$ is a subgroup of G.
Proof:

- $f(1) = 1$, so $1 \in \ker(f)$.
- If $x \in \ker(f)$, Then $f(x) = 1$, so $f(x^{-1}) = f(x)^{-1} = 1^{-1} = 1$. Thus, $x^{-1} \in \ker(f)$.
- If $x, x' \in \ker(f)$, Then $f(xx') = f(x)f(x') = 1 \cdot 1 = 1$, so $xx' \in \ker(f)$.

$\square$

Defn: A subgroup K of G is called **normal** if $\forall g \in G, x \in K$, $gxg^{-1} \in K$.

Fact: $\ker(f)$ is normal.
Proof: Let $x \in \ker(f)$, $g \in G$. Then $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g) \cdot 1 \cdot f(g)^{-1} = 1$.
So $gxg^{-1} \in \ker(f)$. $\square$

Ex: G is a group, $g \in G$. Consider $\begin{array}{c} f : \mathbb{Z} \to G \\ n \mapsto g^n \end{array}$. $\ker(f) = \{n \in \mathbb{Z} | g^n = 1\}$.
This is equal to $d\mathbb{Z}$, where $d = \text{ord}(g)$.

Prop: Let $f : G \to H$ be a group homomorphism. Then f is injective $\Leftrightarrow \ker(f) = \{1\}$.
Proof: If f is injective, then $\ker(f) = \{1\}$.
If $\ker(f) = \{1\}$, let $f(x) = f(y)$. Then $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = 1$. So $xy^{-1} \in \ker(f)$, so $xy^{-1} = 1$, so $x = y$. $\square$