Math 493 Lecture 3

Professor Andrew Snowden

Transcribed by Thomas Cohn

9/11/2019

Ex: Consider $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ ($\mathbb{R}^\times$ is the nonzero real numbers under multiplication).
$\det(AB) = \det(A)\det(B)$, so det is a group homomorphism.
$\ker(\det) = \{A \in \mathrm{GL}_n(\mathbb{R}) | \det(A) = 1\} = \mathrm{SL}_n(\mathbb{R})$, so $\mathrm{SL}_n(\mathbb{R})$ is a normal subgroup of $\mathrm{GL}_n(\mathbb{R})$.

Ex: Given $\sigma \in S_n$, define a linear map $\begin{aligned} A_\sigma : \mathbb{R}^n &\to \mathbb{R}^n \\ e_i &\mapsto e_{\sigma_i} \end{aligned}$.
$A_\sigma \in \mathrm{GL}_n(\mathbb{R})$ – we can check that $A_\sigma A_\tau = A_{\sigma\tau}$.
So we have a group homomorphism $\begin{aligned} A : S_n &\to \mathrm{GL}_n(\mathbb{R}) \\ \sigma &\mapsto A_\sigma \end{aligned}$.
This is clearly injective, so A is an isomorphism between S_n and its image $A(S_n) \subseteq \mathrm{GL}_n(\mathbb{R})$.

Defn: Matrices of the form A_σ for some $\sigma \in S_n$ are called **permutation matrices**.

Defn: $\begin{aligned} \mathrm{sgn} : S_n &\to \{\pm 1\} \\ \sigma &\mapsto \det(A_\sigma) \end{aligned}$.

Ex: $S_2 = \{1, (1 \quad 2)\}$.
$A_1 = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ $\quad \det A_1 = 1 \quad \mathrm{sgn}(1) = 1$.
$A_{(1\ 2)} = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$ $\quad \det A_{(1\ 2)} = -1 \quad \mathrm{sgn}((1 \quad 2)) = -1$.

Ex: $S_3 = \{1, (1 \quad 2), (1 \quad 3), (2 \quad 3), (1 \quad 2 \quad 3), (1 \quad 3 \quad 2)\}$.
$A_1 = \left[\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right]$ $\quad \det A_1 = 1 \quad \mathrm{sgn}(1) = 1$.
$A_{(1\ 2)} = \left[\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right]$ $\quad \det A_{(1\ 2)} = -1 \quad \mathrm{sgn}((1 \quad 2)) = -1$.
$A_{(1\ 3)} = \left[\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{smallmatrix}\right]$ $\quad \det A_{(1\ 3)} = -1 \quad \mathrm{sgn}((1 \quad 3)) = -1$.
$A_{(2\ 3)} = \left[\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right]$ $\quad \det A_{(2\ 3)} = -1 \quad \mathrm{sgn}((2 \quad 3)) = -1$.
$A_{(1\ 2\ 3)} = \left[\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right]$ $\quad \det A_{(1\ 2\ 3)} = 1 \quad \mathrm{sgn}((1 \quad 2 \quad 3)) = 1$.
$A_{(1\ 3\ 2)} = \left[\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right]$ $\quad \det A_{(1\ 3\ 2)} = 1 \quad \mathrm{sgn}((1 \quad 3 \quad 2)) = 1$.

Fact: Transpositions generate S_n.

Fact: For any n and any transposition $\sigma \in S_n$, $\mathrm{sgn}(\sigma) = 1$.
So if $\sigma \in S_n$, write $\sigma = \tau_1 \cdots \tau_m$, where each τ_i is a transposition.
Then $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\tau_1) \cdots \mathrm{sgn}(\tau_m)$.

Defn: $A_n = \ker(\mathrm{sgn} : S_n \to \{\pm 1\})$. A_n is called the **alternating group**, and is a normal subgroup of S_n.

Ex: $A_2 = \{1\}$.
$A_3 = \{1, (1 \quad 2 \quad 3), (1 \quad 3 \quad 2)\}$.
$\# A_n = \frac{1}{2} n!$ for $n \geq 2$.

Defn: Let S be a set. An **equivalence relation** on S is a binary relation $\sim$ s.t.

1. Reflexivity: $\forall x \in S$, $x \sim x$.

2. Symmetry: $\forall x, y \in S$, $x \sim y \Leftrightarrow y \sim x$.

3. Transitivity: $\forall x, y, z \in S$, $x \sim y \wedge y \sim z \Rightarrow x \sim z$.

Ex:

1. Define $x \sim y$ iff $x = y$.

2. Define $x \sim y$, $\forall x, y$.

3. Let $f : S \to T$ is a function. Define $x \sim y$ iff $f(x) = f(y)$.

4. Define an equivalence relation on $\mathbb{Z}$ by $n \sim m$ iff $z \mid n - m$, ie., $n \equiv m \pmod 2$.
   Note: if we define $f : \mathbb{Z} \to \{\text{even}, \text{odd}\}$, where $f(n) = \text{even}$ if n is even and $f(n) = \text{odd}$ if n is odd, then f induces the above equivalence relation.

Defn: Let S be a set with an equivalence relation $\sim$. Let $x \in S$.
The **equivalence class** of x is $C_x = \{y \in S | x \sim y\}$.
Ex: $S = \mathbb{Z}$, $n \sim m$ iff $n \equiv m \pmod 2$.
$C_1 = \{\ldots, -3, -1, 1, 3, \ldots\}$
$C_2 = \{\ldots, -2, 0, 2, \ldots\}$
$C_3 = \{\ldots, -3, -1, 1, 3, \ldots\}$
$C_4 = \{\ldots, -2, 0, 2, \ldots\}$

Prop: If two equivalence classes have any common element, they're equal.
Proof: Suppose $z \in C_x \cap C_y$. Let $w \in C_x$. Then $w \sim x \sim z \sim y$. So $w \sim y$, so $w \in C_y$. Thus, $C_x \subseteq C_y$. A similar argument gives us $C_y \subseteq C_x$, so $C_x = C_y$. $\square$

Defn: Let S be a set. A **partition** of S is a collection $\mathcal{P}$ of non-empty subsets of S s.t. every element of S belongs to a unique member of $\mathcal{P}$.

From the previous proposition, we know that a collection of equivalence classes form a partition.
We can reverse this: suppose $\mathcal{P}$ is a partition. Define an equivalence relation on S by $x \sim y$ if x and y are in the same element of $\mathcal{P}$.

Defn: Let S be a set with an equivalence relation. Define $\overline{S}$ to be the set of equivalence classes. For $x \in S$, we'll write $\overline{x} = C_x \in \overline{S}$.
$\overline{x} = \overline{y} \Leftrightarrow x \sim y$.
So we can define a function $\begin{aligned} \pi : S &\to \overline{S} \\ x &\mapsto \overline{x} \end{aligned}$. $x \sim y$ iff $\pi(x) = \pi(y)$, so $\sim$ is induced by π.

Ex: $S = \mathbb{Z}$, with $n \sim m$ iff $n \equiv m \pmod 2$. Then $\overline{S} = \{\overline{0}, \overline{1}\}$.

Ex: Let G be a group, $H \subset G$ a subgroup. Define an equivalence relation on G by $g \equiv g' \pmod H$ if $g = g'h$ for some $h \in H$ (so $(g')^{-1}g \in H$).
Check:

1. Reflexivity: $g = g \cdot 1$, and $1 \in H$, So $g \equiv g \pmod H$.

2. Symmetry: if $g \equiv g' \pmod H$, then $g = g'h$ for some $h \in H$. So $g' = gh^{-1}$.
   Since $h^{-1} \in H$, $g' \equiv g \pmod H$.

3. Transitivity: if $g \equiv g' \pmod H$ and $g' \equiv g'' \pmod H$, then $g = gh'$ and $g' = g''h'$, for some $h, h' \in H$. So $g = (g''h')h = g''(h'h)$. $h'h \in H$, so $g \equiv g'' \pmod H$.

Ex: $G = \mathbb{Z}$, $H = d\mathbb{Z}$ $(d > 0)$. $n, m \in \mathbb{Z}$, $n \equiv m \pmod H$, according to this definition, iff $n - m \in H \Leftrightarrow n \equiv m \pmod d$.

What is $\overline{g} = C_g$? Well,

$$\begin{aligned}\overline{g} &= \{g' \in G | g' \equiv g \pmod H\} \\ &= \{g' | \exists h \in H \text{ st } g' = gh\} \\ &= \{gh | h \in H\} \\ &= gH\end{aligned}$$

Defn: gH is the **left coset** of H defined by g.

By our previous considerations the left cosets of H form a partition of G.

Defn: The **index** of H in G is the number of left cosets, denoted $[G : H]$.

Prop: $[G : H]$ is the number of right cosets.
Proof: $\begin{array}{c}\{\text{left cosets}\} \to \{\text{right cosets}\} \\ gH \mapsto Hg^{-1}\end{array}$.

Observe: For any element $g \in G$, $\#(gH) = \#H$.

Thm: $\#G = \#H \cdot [G : H]$.

Cor: (Lagrange's Theorem) If $\#G$ is finite, then $\#H | \#G$.

Cor: If G is finite $g \in G$, then $\text{ord}(g) | \#G$.

Suppose G is a group, N is a normal subgroup. Then for any $g \in G$, we have $gN = Ng$, because for $n \in N$, $gn = \underbrace{(gng^{-1})}_{\in N} g \in Ng$, so $gN \subseteq Ng$. (The other direction follows similarly.)

Defn: The **quotient group** G/N is the set of cosets of N, where $(gN)(g'N) = (gg')N$.