Possible New Approach Towards This Course!

Monday, November 03, 2014
1:08 PM

In the next lecture, I will talk about a cyclic group.

I will prove:

1

① $K_a := \{n \in \mathbb{Z} \mid a^n = e\}$ is a subgroup of $\mathbb{Z}$.

② Define the order of an element and conclude:

$$K_a = \{0\} \quad \text{or} \quad K_a = o(a)\,\mathbb{Z}$$

③ If a is torsion, then $a^k = e \iff o(a) \mid k$

And $a^{k_1} = a^{k_2} \iff k_1 \equiv k_2 \pmod{o(a)}$

④ If a is torsion, then $\theta : \mathbb{Z}_{o(a)} \longrightarrow \langle a \rangle$,

$$\theta([k]_{o(a)}) := a^k$$

is a well-defined bijection. In particular

$$|\langle a \rangle| = o(a) \quad \text{and}$$

$$\langle a \rangle = \{e, a, \ldots, a^{o(a)-1}\}.$$

⑤ If a is torsion, then $o(a^m) = \dfrac{o(a)}{\gcd(m, o(a))}$.

In particular, any divisor of $\underline{o(a)}$ is the order of an element of $\langle a \rangle$.

⑥ If a, b are torsion and $\gcd(o(a), o(b)) = 1$, then

$$\langle a \rangle \cap \langle b \rangle = \{e\}.$$

Moreover, if $ab = ba$, then

$$o(ab) = o(a)\, o(b).$$

The lecture after that I will talk about the group action.

2

① Define $G \curvearrowright X$.

② Examples left multiplication $H \curvearrowright G$.

Conjugation $G \curvearrowright G$.

Symmetric group of $X \curvearrowright X$.

③ Orbits $\rightsquigarrow$ · a $\underline{\underline{\text{partition}}}$ of X.

· $\underline{\underline{\text{Equivalency relation}}}$ on X.

④ $\underline{\text{Exp}}$. Rotations centered at the origin.

Orbits $\rightsquigarrow$ circles centered at the origin.

<u>Exp.</u> $SL_2(\mathbb{Z}) \curvearrowright \mathbb{Z}^2$

Orbit of $\vec{e}_1 = \left\{ \begin{bmatrix} a \\ b \end{bmatrix} \,\middle|\, \gcd(a,b)=1 \right\}$.

<u>Exp.</u> $S_n \curvearrowright \{1, 2, \dots, n\}$

Orbit of $1 = \{1, 2, \dots, n\}$.

Möbius trans.

<u>Def.</u> Set of all the orbits $:= {}_G\backslash X$

<u>Observation</u>. If X is finite, then

$$|X| = \sum_{O(x) \in {}_G\backslash X} |O(x)| \qquad \circledast$$

3

<u>Lagrange Thm</u> $\left.\begin{array}{l} G : \text{finite group} \\ H \leq G \end{array}\right\} \Rightarrow |G| = |H| \, |{}_H\backslash G|$

In particular $|H| \mid |G|$.

<u>Cor.</u> $|G| < \infty \Rightarrow \forall g \in G, \; g^{|G|} = e$.

$H \curvearrowright G \rightsquigarrow$ any orbit is of the form $\underline{Hg}$ for some $g \in G$. And so the size of any orbit is $|H|$. Hence by $\circledast$ we get the claim.

- $|O(x)| = [G : G_x]$; $\underline{\underline{\text{conj}}}$. ;

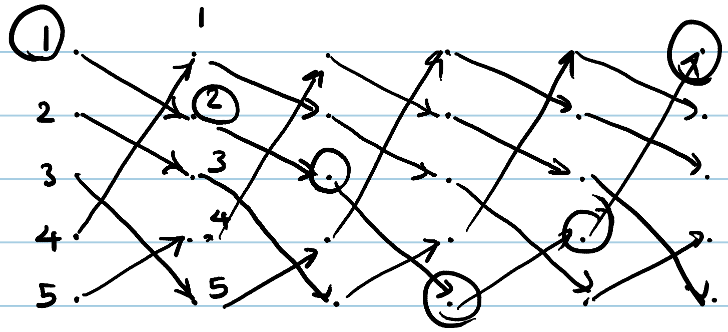
---

4 To have a rich set of examples, let's study the symmetric group S_n.

$$\sigma : \{1, 2, \dots, n\} \longrightarrow \{1, 2, \dots, n\}$$

What are the orbits of $\langle\sigma\rangle \curvearrowright \{1, 2, \cdots, n\}$?

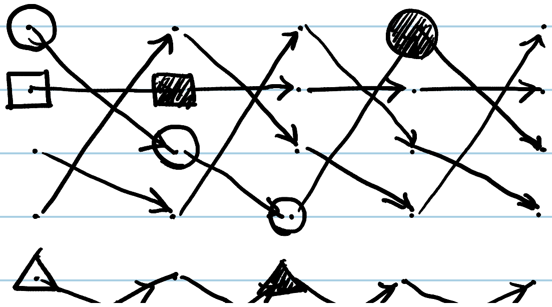
Exp. ①



$$\begin{tikzcd} 1 \arrow[r] & 2 \arrow[r] & 3 \arrow[r] & 5 \arrow[r] & 4 \arrow[llll, bend left] \end{tikzcd}$$

It has only one orbit; and it is a cycle.

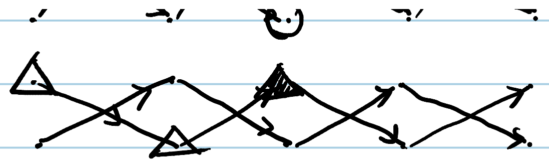
We denote it by $(1, 2, 3, 5, 4)$



$$\begin{tikzcd} 1 \arrow[r] & 3 \arrow[r] & 4 \arrow[ll, bend left] \end{tikzcd}$$

$$\begin{tikzcd} 2 \arrow[loop below] \end{tikzcd}$$

$$5 \longrightarrow 6$$



$$\begin{tikzcd} 5 \arrow[r] & 6 \arrow[l, bend left] \end{tikzcd}$$

$(1,3,4)(2)(5,6)$

Any permutation can be written as composite of disjoint cycles. And if we drop cycles of length 1, then, up to permutation, this decomposition is unique.

Examples of multiplication in S_n;

Order of a cycle of length k;

Order of $\sigma \in S_n$;

* Transposition

* Parity of a permutation ⇝ A_n.

---

5 Homomorphism: definition

6 · $\mathbb{Z} \to \mathbb{Z}_n$. $S_n \to \{\pm 1\}$

· $\mathbb{Z}_n \to \{\zeta_n^i \mid 0 \le i \le n-1\}$. . $\det: GL_n(\mathbb{R}) \to \mathbb{R}^\times$.

· $G \curvearrowright X$ via θ $\iff$ $\rho_\theta : G \to S_X$ is a homomorphism

- $G \curvearrowright G \rightsquigarrow \rho: G \hookrightarrow S_G$ Cayley's theorem.
- kernel and image.
- Isomorphism.

---

7 8

Can any subgp be <u>kernel</u> of a homo. $\rightsquigarrow$ normal subgroup

$\rightsquigarrow$ ${}_{N}\backslash^{G}$ with <u>natural operation</u> is a group.

It is called a factor group

<u>First isomorphism theorem</u> $\mathrm{Im}\, f \simeq G/_{\ker f}$.

<u>Second isomorphism theorem</u> $\left.\begin{matrix} N \trianglelefteq G \\ H \leq G \end{matrix}\right\} \Rightarrow HN \leq G$ & $HN/_{N} \simeq H/_{H\cap N}$.

<u>Third isomorphism theorem</u> $\dfrac{G/N}{H/N} \simeq G/_{H}$

if $N, H \triangleleft G$ and $N \subseteq H$.

9

$G \curvearrowright X$;

$O(x) \longleftrightarrow {}_{G_x}\backslash^{G}$ where $G_x = \{g \in G \mid g\cdot x = x\}$

So $|X| = \sum_{[x]\in {}_{G}\backslash X} [G:G_x] = |X^G| + \sum_{[x]\in {}_{G}\backslash X} [G:G_x]$

fixed points x not

fixed points　　x not fixed

$G \curvearrowright G$ by conjugation.

$G_g := C(g)$ the centralizer of g

fixed points $= Z(G)$: the center of G.

Each orbit is called a <u>conjugacy class</u>.

$$|G| = |Z(G)| + \sum_{\substack{[g] \text{ a conj. class} \\ g \notin Z(G)}} [G : C(g)] .$$ (Class equation)

$G \curvearrowright \{\text{subgroups of } G\}$

$H \longmapsto gHg^{-1}$

- gHg^{-1} is called a <u>conjugate</u> of H.
- Stab. of $H = \{g \in G \mid gHg^{-1} = H\} =: N_G(H)$ is called <u>the normalizer of H</u>.

$\Rightarrow$ # of conj. of $H = [G : N_G(H)]$.

<u>Remark</u>. H is a fixed point of this action $\Leftrightarrow H \trianglelefteq G$.

---

10 P: finite p-group $\curvearrowright X$ (finite set)

10 P: finite p-group $\curvearrowright X$ (finite set)

$\Rightarrow \quad |X| \equiv |X^P| \pmod{p}$

Cor. $\quad |G| \overset{p}{\equiv} |Z(G)| \Rightarrow p \mid |Z(G)|$

$\Rightarrow Z(G) \neq \{e\}$.

Cor.

$\mathbb{Z}_p \curvearrowright \{(g_1, \dots, g_p) \mid g_1 \cdot \dots \cdot g_p = 1\}$

$\Rightarrow \quad |G|^p \equiv |\{g \in G \mid g^p = 1\}| \pmod{p}$.

$\Rightarrow$ if $p \mid |G|$, then $p \mid |\{g \in G \mid g^p = 1\}|$

So $\exists\, g \in G$ s.t. $o(g) = p$ (Cauchy's theorem).