Lecture 22:

Last time: Cayley's theorem:

Theorem: Every finite group G (embeds into) is isomorphic to a subgroup of an S_n for some n.

G as a set here not a group.

Proof: Let $\varphi: G \to S_G$ be defined by

$$\varphi(g): G \to G$$

$$\varphi(g)(g_i) = gg_i$$

- $\varphi(g)$ is a permutation since it has an inverse: $\varphi(g)^{-1} = \varphi(g^{-1})$ since

$$(\varphi(g^{-1}) \circ \varphi(g))(h) = g^{-1}gh = h \text{ for all } h.$$

similarly

$$\varphi(g) \circ \varphi(g^{-1}) = id_G.$$

- φ is a homomorphism.

We want to see that $\varphi(g) \circ \varphi(h) = \varphi(g \cdot h)$

$$(\varphi(g) \circ \varphi(h))(g_i) = \varphi(g)(hg_i) = ghg_i = \varphi(gh)(g_i) \checkmark$$

- φ is injective.

Assume $\varphi(g) = \varphi(h)$, then $\varphi(g)(e) = \varphi(h)(e)$

$$g = h.$$

We are done by the following lemma.

Lemma: If $\varphi: G \to K$ is a group homomorphism, then, for every subgroup H of G, $\varphi(H)$ is a subgroup of K.

proof: We have:

- $\varphi(e) = e \in \varphi(H)$
- $\varphi(H)$ is closed under the group operation since $\varphi(h_1)\cdot\varphi(h_2) = \varphi(h_1 h_2) \in \varphi(H)$
- $\varphi(H)$ is closed under taking inverses since $\underbrace{\varphi(h^{-1})}_{\in \varphi(H)} = \varphi(h)^{-1}$.

Hence $\varphi(H)$ is a subgroup. $\square$

Example:

$$D_6 = \{\overset{1}{1}, \overset{2}{r}, \overset{3}{r^2}, \overset{4}{s}, \overset{5}{sr}, \overset{6}{sr^2}\}$$

$\varphi: D_6 \hookrightarrow S_{D_6}$

$$\varphi(1) = \begin{pmatrix} 1 & r & r^2 & s & sr & sr^2 \\ 1 & r & r^2 & s & sr & sr^2 \end{pmatrix}$$

$$\varphi(r) = \begin{pmatrix} 1 & r & r^2 & s & sr & sr^2 \\ r & r^2 & 1 & rs & rsr & rsr^2 \end{pmatrix}$$

$$\begin{array}{ccc} rs & rsr & rsr^2 \\ \shortparallel & \shortparallel & \shortparallel \\ sr^2 & s & sr \\ 6 & 4 & 5 \end{array}$$

$$\varphi(s) = \begin{pmatrix} 1 & r & \cdots \\ & \cdots & \end{pmatrix}$$

similarly fill it.

(note this is different from our embedding into S_3; this works for any group!)

in terms of numbers. $S_{D_6} \cong S_6$

$$\varphi(r) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 4 & 5 \end{pmatrix}.$$

Cosets:

* Let G be a group and let H be a subgroup. Define an (equivalence) relation on G by: $\forall a,b \in G$

$$a \sim_H b \iff \exists h \in H \text{ s.t } ah = b$$

* Let's check that it's an equivalence relation.

- reflexivity: $\forall a \in G$, $a \cdot \underset{e \in H}{1} = a$ ✓. so $a \sim_H a$.

- symmetry: Assume $a \sim_H b$, then $\exists \underset{\in H}{h}$ s t $ah = b$.

  Then $ahh^{-1} = bh^{-1}$, so $a = bh^{-1}$.

  So $\exists h^{-1} \in H$ s.t $bh^{-1} = a$, so $b \sim_H a$.

- transitivity: Assume $a \sim_H b$ and $b \sim_H c$

  so: $ah_1 = b$ and $bh_2 = c$.

  then $a h_1 h_2 = c$ so $a \sim_H c$.

* What are the equivalence classes:

$$[e] = \{a \in G \mid \exists h \in H \text{ s.t } \underset{\overset{\shortparallel}{h}}{e.h} = a\} = H$$

equivalence class of e

$$[a] = \{b \in G \mid \exists h \in H \text{ s.t } ah = b\} =: aH$$

definition

"set of all multiples ah".

<u>Def</u>: aH is called the left coset of H containing a.

Ha " " " right coset of H containing a.

<u>Rmk</u>: Ha is the equivalence class of a under a similar relation

$$a \underset{H}{\sim} b \iff \exists h \in H \text{ s.t. } ha = b.$$

<u>Ex</u>: $G = \mathbb{Z}$. $H = 3\mathbb{Z}$.

$0 + 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

$1 + 3\mathbb{Z} = \{\ldots, -5, -2, 1, 4, \ldots\}$

$2 + 3\mathbb{Z} = \{\ldots, -4, -1, 2, 5, \ldots\}$