Lecture 24 Sep 30, 2022

Ex $GL_n(\mathbb{R})$ contains a subgroup isomorphic to S_n.

$n=3$: $S_3 = \{(1), (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$.

Consider the identity matrix $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

For $\sigma \in S_3$, we define $\sigma(I_3)$ to be the matrix obtained by permuting the columns of I_3 according to σ. For example, $\sigma(I_3) = I_3$ if $\sigma = (1)$,

$\sigma(I_3) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ if $\sigma = (1\,2)$, $\ldots$, $\sigma(I_3) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ if $\sigma = (1\,3\,2)$.

Thus, $\{\sigma(I_3) \mid \sigma \in S_3\}$ is the set of all the 3×3 permutation matrices.

In general, $\{\sigma(I_n) \mid \sigma \in S_n\} \leq GL_n(\mathbb{R})$

group of all the $n \times n$ permutation matrices.

Clearly, $\{\sigma(I_n) \mid \sigma \in S_n\} \cong S_n$.

---

§ <u>Converse of Lagrange theorem:</u>

Let G be a finite group, and let $|G| = n$. If $H \leq G$, then Lagrange theorem says that $|H| \mid |G|$.

Question (Converse of Lagange thm): If $m \mid |G|$, does there exist a subgroup H of G s.t. $|H| = m$?

In general, the converse of Lagrange theorem is <u>not</u> true.

For example, A_4 has no subgroup of order 6 (but $6 \mid |A_4|$).

The converse of Lagrange theorem is true for (finite) cyclic groups:

<u>Theorem 1</u>: Let G be a finite cyclic group of order n. Then, for each divisor m of n, G has a <u>unique</u> subgroup of order m, namely, $\langle a^{\frac{n}{m}} \rangle$, where a is a generator of the cyclic group G.

<u>Proof</u>: Let $G = \langle a \rangle$. Then, clearly $o(a^{\frac{n}{m}}) = m$ (since $o(a) = n$).

$\therefore \langle a^{\frac{n}{m}} \rangle$ is a subgroup of G of order m.

We now prove that $\langle a^{\frac{n}{m}} \rangle$ is the only subgroup of G of order m.

Let K be a subgroup of G of order m.

<u>Claim:</u> $K = \langle a^{\frac{n}{m}} \rangle$.

Since $K \leq G$ and G is cyclic, so K is also cyclic.

Let $K = \langle a^k \rangle$ and hence $o(a^k) = |K| = m$.

Let $d = \frac{n}{m}$. Now, $m = o(a^k) = \frac{o(a)}{\gcd(o(a), k)} = \frac{n}{\gcd(n,k)}$

$\Rightarrow \gcd(n,k) = \frac{n}{m} = d$

$\Rightarrow d \mid k \Rightarrow k = d \cdot s$ for some integer s.

Now, $a^k = a^{d.s} = (a^d)^s \in \langle a^d \rangle = \langle a^{\frac{n}{m}} \rangle$

$\therefore \langle a^k \rangle \subseteq \langle a^{\frac{n}{m}} \rangle$.

But $|\langle a^k \rangle| = |\langle a^{\frac{n}{m}} \rangle| = m$, and hence

$K = \langle a^k \rangle = \langle a^{\frac{n}{m}} \rangle$.

This completes the proof.

———x———

Ex: Let G be a cyclic group of order 10.

Then, G has a unique subgroup for each divisor $m = 1, 2, 5, 10$

Let $G = \langle a \rangle$. Then:

the unique subgroup of order 1 $= \langle a^{\frac{10}{1}} \rangle = \langle a^{10} \rangle = \{e\}$.

" " " " 2 $= \langle a^{\frac{10}{2}} \rangle = \langle a^{5} \rangle = \{e, a^{5}\}$.

" " " " 5 $= \langle a^{\frac{10}{5}} \rangle = \langle a^{2} \rangle = \{e, a^{2}, a^{4}, a^{6}, a^{8}\}$

" " " " 10 $= \langle a^{\frac{10}{10}} \rangle = \langle a \rangle = G$.

#

Theorem 2: Let G be a cyclic group of order n. Let m be a divisor of n. Then, G has $\varphi(m)$ number of elements of order m.

Proof: Let m/n. Let $H = \langle a^{\frac{n}{m}} \rangle$ be the unique subgroup of G of order m.

Let $b \in G$ be an element of order m.

Then, $\langle b \rangle$ is a subgroup of G of order m.

$\therefore H = \langle b \rangle \Rightarrow b \in H$.

This proves that H contains all the elements of G of order m.

Since $H = \langle a^{\frac{n}{m}} \rangle$ is a cyclic group of order m, so H contains exactly $\varphi(m)$ number of elements of order m.

Hence, there are exactly $\varphi(m)$ number of elements of order m in the group G.

This completes the proof.

<u>Ex:</u> In $\mathbb{Z}_{10}$, there are $4 = \varphi(5)$ elements of order 5. There is only 1 element of order 2. Also, there are $4 = \varphi(10)$ elements of order 10.

#

The converse of Theorem 1 is also true. We have:

<u>Theorem 3 (Converse of Theorem 1):</u> Let G be a finite group. If to each divisor m of $|G|$, there exists a unique subgroup of order m, then G is cyclic.

(We will prove this theorem later using some number theory concepts).

#