Group Theory
Week #6, Lecture #24

<u>Theorem</u> (Cauchy) Let G be a finite group, and let p be a prime dividing the order of G. Then the number of solutions of the equation $x^p = e$ is a multiple of p.

$$\boxed{p \mid |G| \Rightarrow p \mid \#\{x \in G \mid x^p = e\}} \quad (*)$$

(this will imply a partial converse to Lagrange)

<u>Proof</u> (I) Write $|G| = n$, and put

$$\boxed{S := \{(x_1, \dots, x_p) : x_i \in G \text{ and } x_1 x_2 \cdots x_{p-1} x_p = e\}}$$

any values

$x_p = (x_1 \cdots x_{p-1})^{-1}$

- Note that $|S| = \underbrace{n \cdots n}_{p-1} = n^{p-1}$

in particular, since $p \mid n$:

$$\boxed{|S| \equiv 0 \pmod p} \quad (\dagger)$$

(II) Consider the action of the group $\mathbb{Z}_p \curvearrowright S_p$ on S by cyclic permutation of the elements x_i. That is

$\mathbb{Z}_p = \langle \sigma \rangle$ acts via the p-cycle $\sigma = (1 \cdots p)$ as

$$\boxed{\sigma(x_1, x_2, \dots, x_{p-1}, x_p) = (x_2, \dots, x_p, x_1)}$$

(eg: $\sigma(a,b,c,d,e,f) = (b,c,d,e,f,a)$, also $\sigma(a,b) = (b,a)$)

* Verify that $\sigma : S \to S$:

$$\underbrace{x_1}_{a} \underbrace{x_2 \cdots x_{p-1} \cdot x_p}_{b} = e \Longrightarrow \underbrace{x_2 \cdots x_{p-1} x_p}_{b} \underbrace{x_1}_{a} = e$$

since $ab = e \Rightarrow b = a^{-1} \Rightarrow ba = e$ ✓

* Since σ generates the cyclic group $\mathbb{Z}_p$, the action of σ extends to the whole group $\mathbb{Z}_p$:

$$\sigma^k(x_1,\dots,x_p) = \sigma(\cdots\sigma(x_1\cdots x_p))$$

(III) Analyze the action of $\mathbb{Z}_p$ on S:

Fixed point set: uses p prime!

$$\boxed{S^{\mathbb{Z}_p} = \{(x,\dots,x) : x \in G \;\&\; x^p = e\}}$$

Remains to show: $p \mid |S^{\mathbb{Z}_p}|$.

First notice that $S^{\mathbb{Z}_p} \neq \phi$, since $(e,\dots,e) \in S^{\mathbb{Z}_p}$ $[e^p = e]$ — this justifies formula (*) in the statement

General Theory

Now recall the Class Equation: (for G acting on S)

$$\boxed{|S| = |S^G| + \sum_{|Gx|>1} [G : \underbrace{G_x}_{\text{a proper subgroup of } G}]}$$

In particular, if G is a p-group, then, by Lagrange's theorem, all its proper subgroups have index divisible by p. Hence:

$$\boxed{|S| \equiv |S^G| \pmod p} \quad (*)$$

(IV) Back to our situation, with $G \longrightarrow \mathbb{Z}_p$ (a p-group!) and S as above

$$(*) \longrightarrow \boxed{|S^{\mathbb{Z}_p}| \equiv |S| \pmod p}$$

From (*\) we know $|S| \equiv 0 \pmod p$. And so, $||S|^{\mathbb{Z}_p}| \equiv 0 \pmod p$. Hence, since $|S^{\mathbb{Z}_p}| > 0$:

$|S^{\mathbb{Z}_p}|$ is divisible by p.

QED

As a corollary, we derive the following (partial) converse to Lagrange's theorem (for subgroups of prime order):

Theorem (Cauchy) If $p \mid |G|$, the G has an element of order p, and thus, a subgroup of order p.

Proof. By previous thm, the set $T = \{x \in G : x^p = e\}$ has size divisible by p. Also, $e \in T$. The other elements of T have order p (again, since p is a prime).

(there are $p-1$ of them)

- Take $a \in T$, $a \neq e$. Then:

  * $o(a) = p$
  * $\langle a \rangle$ is a subgroup of G of order p $\square$

Example If $|G| = 60 = 2^2 \cdot 3 \cdot 5$, then G has subgroups of order 2, 3, and 5. As we shall see, it also must have subgroups of order 4 (by Sylow I).

Corollary: A finite group is a p-group if and only if every element has order a power of p:

$$\boxed{|G| = p^n \text{ (for some } n \geq 1) \iff (\forall g \in G,\ o(g) = p^k, \text{ for some } k,\ 0 \leq k \leq n)}$$

Proof ($\Longrightarrow$) By Lagrange, $o(g) \mid |G| = p^n \Rightarrow o(g) = p^k$ $(0 \leq k \leq n)$

($\Longleftarrow$) Suppose $q \mid |G|$ for some prime $q \neq p$. Then, by Cauchy, G has an element of order q, which is not a power of p. — Contradiction $\square$

Remark The notion of p-group can be generalized to infinite groups, by requiring that all elements in that group have order a power of p.

Interlude: Correspondence Theorem

Theorem Let $N \trianglelefteq G$ and let $\pi: G \longrightarrow G/N$ be the canonical projection. Then π induces a 1-to-1 correspondence

$$\boxed{\left\{\begin{array}{c}\text{subgroups of } G\\ \text{containing } N\end{array}\right\} \longleftrightarrow \left\{\text{subgroups of } G/N\right\}}$$

$$N \subseteq H \leq G \longrightarrow \pi(H)$$

$$\pi^{-1}(K) \longleftarrow K \leq G/N$$

Moreover:

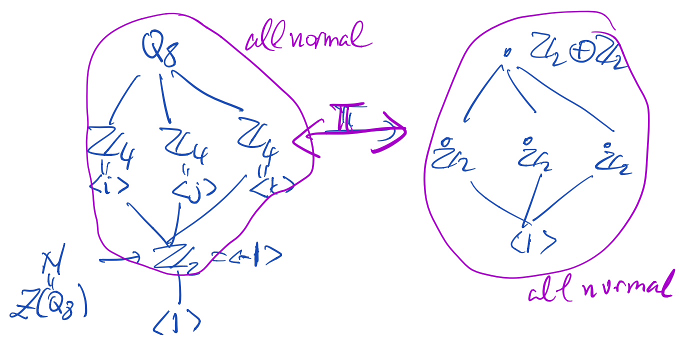
* $N \leq H \trianglelefteq G \iff K \trianglelefteq G/N$
* If G is finite, then $\boxed{|H| = |K| \cdot |N|}$ Exercise!

Examples

(1) $G = Q_8$, $N = \{\pm 1\}$
$\{\pm 1, \pm i, \pm j, \pm k\}$

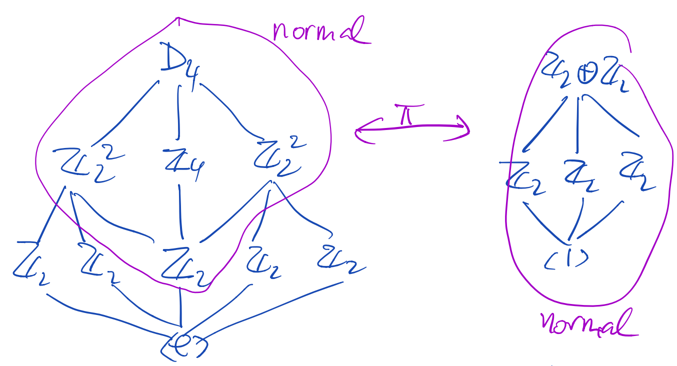
$Q_8/N = \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$\pi(i) = (1,0)$
$\pi(j) = (0,1)$
$\pi(k) = (1,1)$



(2) $G = D_4$, $N = Z(D_4) \cong \mathbb{Z}_2$

$D_4/Z(D_4) = \mathbb{Z}_2 \oplus \mathbb{Z}_2$



Next topic: $\boxed{\text{Sylow's Theorems}}$
(due to Peter Ludwig Sylow ~1872)

(Sylow I)
<u>Theorem</u> If $p^k \mid |G|$ for some prime p and $k>0$ then there is a subgroup H with $|H|=p^k$:

$$\boxed{p^k \mid |G| \implies \exists\, H \leq G,\ |H|=p^k}$$

We will prove this theorem using Cauchy's Theorem (for $k=1$) and induction on $|G|$, via the correspondence theorem from above.

Aside: If $|G|=n$, then $G \leq S_n$ (Cayley)

Question: what is smallest r for which $G \leq S_r$?

eg: $D_4 \leq S_4$ (use symmetries of square)

but $Q_8 \not\leq S_5$! (use Sylow Theorems)