Lecture 26

In this lecture we are going to use the class equation to prove some nice but non-trivial results.

But first let's see how the class equation reads for a particular group, S_3.

We know that $Z(S_3) = \{\epsilon\}$.

Let's find centralizers of elements of S_3.

$S_3 = \{\epsilon, (12), (13), (23), (123), (132)\}$

$C((12)) = ?$

Clearly ϵ and $(12) \in C((12))$.

$$\left.\begin{aligned}(12)(13) &= (132)\\ (13)(12) &= (123)\end{aligned}\right\} \Rightarrow (13) \notin C((12)).$$

$$\left.\begin{aligned}(12)(23) &= (123)\\ (23)(12) &= (132)\end{aligned}\right\} \Rightarrow (23) \notin C((12))$$

$$\left.\begin{aligned}(12)(123) &= (23)\\ (123)(12) &= (13)\end{aligned}\right\} \Rightarrow (123) \notin C((12))$$

$$\left.\begin{aligned}(12)(132) &= (13)\\ (132)(12) &= (23)\end{aligned}\right\} \Rightarrow (132) \notin C((12))$$

So $C((12)) = \{e, (12)\}$

Note that $(13) = (132)(12)(123)$
$= (132)(12)(132)^{-1}$

$(23) = (123)(12)(132)$
$= (123)(12)(123)^{-1}$

$\Rightarrow$ (13) and $(23) \in O_{(12)}$

And $(132) \in O_{(123)}$

$C((123)) = \{e, (123), (132)\}$

$\Rightarrow$ the class equation for S_3 reads as

$$6 = 1 + \frac{6}{2} + \frac{6}{3} = 1 + 3 + 2$$

Recall from Q.8 A4 that a group of order 9 is abelian. The theorem below generalizes this :-

__Theorem 1__ Let G be a group, $|G| = p^2$ for some prime p. Then G is abelian.

__Proof__ If $|G| = p^2 \Rightarrow$ the possibilities for $|Z(G)| = 1, p$ or p^2. If $|Z(G)| = p^2 \Rightarrow G = Z(G)$ $\Rightarrow$ G is abelian.

If $Z(G) = p \Rightarrow \left|\frac{G}{Z(G)}\right| = \frac{p^2}{p} = p \Rightarrow \frac{G}{Z(G)}$ is cyclic $\Rightarrow$ G is abelian.

So the only case left is can $|Z(G)| = 1$?

Consider the class equation for G

$$|G| = |Z(G)| + \sum \frac{|G|}{|C(a)|}$$

$$\Rightarrow \quad p^2 = |Z(G)| + \sum_{a \notin Z(G)} \frac{p^2}{|C(a)|} \qquad \text{—— } (1)$$

now, $|C(a)| > 1$ for every $a \neq e$

$\Rightarrow \quad \dfrac{p^2}{|C(a)|} = p$ as if $|C(a)| = p^2 \Rightarrow C(a) = G$

$\Rightarrow a \in G$

which is not possible.

Thus $p \,\Big|\, \dfrac{p^2}{|C(a)|}$ and this happens $\forall\, a \notin Z(G)$.

So in (1) p divides the second term on the RHS. p also divides the LHS $\Rightarrow$

p must divide $|Z(G)| \Rightarrow |Z(G)| \neq 1$

and so G is abelian. $\blacksquare$

Proposition 1 Let p be a prime and let G be a group with $|G| = p^n$, $n \geq 1$. Then $Z(G) \neq \{e\}$.

Proof On Assignment 5.

Recall that the converse to Lagrange's Theorem is not true. However, for cyclic groups we saw that $\exists$ a unique subgroup for every divisor of $|G|$. The next theorem says that the same is true for certain groups (which might not be cyclic).

Theorem 2 Let p be a prime and let G be a group with $|G| = p^n$, $n \geq 1$. Then $\forall\, k$, $0 \leq k \leq n$, G has a subgroup of order p^k.

<u>Remark</u> The theorem does not say that the subgroup will be unique. That only happens for cyclic groups.

<u>Proof</u> :- The proof is by induction on n.

$n=1$. Then $|G| = p \Rightarrow G \cong \mathbb{Z}_p$ and hence G has a subgroup of order $1 \; (=p^0)$ $\{e\}$ and $p \; (=p^1)$, G. Thus the theorem is true for $n=1$.

Induction Hypothesis :- Suppose $\forall$ group G w/ $|G| = p^i$, $i<n$, $\exists$ a subgroup of order p^j, $\forall j$, $0 \le j \le i$.

We'll prove the theorem for $|G| = p^n$.

From Prop. 1 above $Z(G) \neq \{e\}$

$\Rightarrow \quad |Z(G)| = p^a \quad , 1 \leq a \leq n.$

Now $Z(G)$ is abelian and $p \mid |Z(G)| \Rightarrow$

by Cauchy's Theorem $\exists \; x \in Z(G)$ s.t. $\operatorname{ord}(x) = p$.

Consider $\langle x \rangle \leq Z(G)$. Since $Z(G) \trianglelefteq G \Rightarrow$

$\langle x \rangle \trianglelefteq G$. So $\dfrac{G}{\langle x \rangle}$ is a group and

$$\left| \frac{G}{\langle x \rangle} \right| = \frac{p^n}{p} = p^{n-1}$$

$\Rightarrow$ by the induction hypothesis $\dfrac{G}{\langle x \rangle}$ has subgr-

-oups $\dfrac{H_k}{\langle x \rangle}$ of order p^k $\forall \, k$, $0 \leq k \leq n-1$.

Now $H_k \leq G$ s.t. $\langle x \rangle \leq H_k$ $\left(\text{as } \dfrac{H_k}{\langle x \rangle} \leq \dfrac{G}{\langle x \rangle} \right)$

Now if $\left| \dfrac{H_k}{\langle x \rangle} \right| = p^k \Rightarrow |H_k| = p^k \cdot |\langle x \rangle|$

$$= p^{k+1}$$

$\because$ H_k is a subgroup of G of order $k+1$

$\Rightarrow$ $H_0, H_1, \ldots, H_{n-1}$ are subgroups of G of order $p, p^2, \ldots, p^n$ respectively, and of course $\{e\} \leq G$ of order p^0. Hence the theorem.

$\boxtimes$