Lecture 16

In this lecture, we'll see more applications of quotient groups.

Converse to Lagrange's Theorem is NOT true.

Let's consider the group A_4. We know that $|A_4|=12$ and $6 \mid 12$. We claim that there isn't a subgroup of A_4 of order 6. If H were such a subgroup, then since $[A_4 : H] = 2$, $H \triangleleft A_4$. So, $\frac{A_4}{H}$ is a group of order 2. Let $\alpha H \in \frac{A_4}{H}$ be the non-identity element.

Since $\mathrm{ord}(\alpha H) = 2 \Rightarrow (\alpha H)^2 = \alpha^2 H = H$ and hence $\alpha^2 \in H$, i.e., for all $\alpha \in A_4$, $\alpha^2 \in H$. However, there are 9 different elements of the form α^2 in A_4 [Check this!] but order of H is 6, so this is impossible. Hence A_4 can't have a subgroup of order 6.

So, we have seen that the converse of Lagrange's theorem is not true. A natural question then arises that, can we atleast say something about the converse of Lagrange's theorem, i.e., can we say that for some special divisors of $|G|$, there do exist a subgroup of that order?

The next two (amazing!) theorems tell us that it is indeed the case.

Cauchy's Theorem

Let G be a finite group and p be a prime number such that $p \mid |G|$. Then G contains an element of order p.

__Remark__ :→ The moment we have an element of order p, say a, we have a subgroup of order p $\langle a \rangle$.

We'll only prove Cauchy's theorem for abelian groups, in this lecture and will prove it for general groups later.

__Proof of Cauchy's Theorem__ (for abelian group)

Let $|G|=n$ and $p|n$. The proof is by strong induction on $|G|$.

If $|G|=2$, then $2\,\big|\,|G|$ and G has an element of order 2.

__Induction Hypothesis__ Suppose for all abelian groups H, with $|H|<|G|$ and $p\,\big|\,|H|$, $\exists$ an element of order p in H.

We'll prove the result for G. First of all, G

has an element of prime order, say q (which might be different from p). Why? Suppose $x \in G$ and $\mathrm{ord}(x) = m$. Then from prime factorization, write $m = qs$ where q is a prime and s is the left-over part. Then $\mathrm{ord}(x^s) = q$.

So let $a \in G$ be the element of some prime power, q. If $q = p$, then a is the desired element. If $q \neq p$, then let's look at $\langle a \rangle$.

Since G is abelian $\Rightarrow \langle a \rangle \triangleleft G$ and hence $\frac{G}{\langle a \rangle}$ is a group. Moreover, $\left|\frac{G}{\langle a \rangle}\right| = \frac{n}{q} < n$.

Also, since $\gcd(p, q) = 1 \Rightarrow p \,\Big|\, \left|\frac{G}{\langle a \rangle}\right|$. So, by the induction hypothesis, $\frac{G}{\langle a \rangle}$ has an element of order p. The theorem now follows from the following result, which you'll prove in Assignment 3.

$\square$

Result [see Assignment 3] Suppose G is a finite group and $H \triangleleft G$. If $\frac{G}{H}$ has an element of order n, show that G has an element of order n.

So, for example, if we have a group whose order is, say, 8633, then you immediately know that it has an element of order 97 and 89.

We now, state another theorem, which guarantees existence of groups of certain order. Again, we'll just prove it for abelian groups, deferring the proof for the general case, till the later part of the course.

Sylow's Theorem

If G is a finite group, p is a prime number such that $p^{\alpha} \mid |G|$, $p^{\alpha+1} \nmid |G|$ (i.e., $p^{\alpha+1}$ doesn't divide $|G|$) then G has a subgroup of order p^{α}.

Proof (for abelian groups only) If $\alpha = 0$ then $\{e\}$ is such a subgroup. So suppose, $\alpha \neq 0$. Then since $p^{\alpha} \mid |G| \Rightarrow p \mid |G|$, so from Cauchy's theorem, G has an element of order p, say $a \in G$. The idea is to consider a special set, prove that it is a subgroup and then prove it's order to be p^{α}.

Consider, the set

$$S = \{ x \in G \mid x^{p^m} = e,\ m \in \mathbb{Z} \}$$

$e \in S$ and $a \in S$, so $S \neq \phi$.

It's very easy to use the subgroup test to see that S is a subgroup.

Claim: $|S| = p^\beta$ for an integer β, $0<\beta\leq\alpha$.

Suppose q is a prime which divides $|S|$. Then by Cauchy's theorem, $\exists$ an element $b\in S$ s.t. $ord(b)=q$. If $q\neq p$, then since $b\in S$, we know $ord(b)=p^s$, $s\in\mathbb{Z}$ $\Rightarrow q=p^s$, which is impossible. So, p is the only prime dividing $|S|$ $\Rightarrow |S|=p^\beta$ for some β.

If $\beta>\alpha$ $\Rightarrow$ by Lagrange's theorem, $|S|\,\big|\,|G|$ $\Rightarrow$ atleast $p^{\alpha+1}\,\big|\,|G|$ which cannot happen, so $\beta\leq\alpha$.

Claim $\beta=\alpha$.

Suppose $\beta<\alpha$. Then since $S\trianglelefteq G$ $\Rightarrow$ $p\,\Big|\,\left|\frac{G}{S}\right|$ $\Rightarrow$ by Cauchy's theorem, $\exists$ an element

$xS\in\frac{G}{S}$, $xS\neq S$, s.t. $ord(xS)=p$.

This means, $\quad x^p S = S \Rightarrow x^p \in S$.

But since $x^p \in S \Rightarrow (x^p)^{p^t} = e$, $t \in \mathbb{Z}$.

So, $(x^p)^{p^t} = e \Rightarrow x^{p^{t+1}} = e \Rightarrow x \in S$

by the definition of S.

This contradicts the fact that $xS = S$.

So $\beta < \alpha$ is not possible.

$\Rightarrow \quad |S| = p^{\alpha}$ and S is the desired subgroup.

In the next lecture, we'll start studying homomor-

-phisms and isomorphisms.