MAT301H5Y

Week 8 Lecture 1: Cosets revised and continued

Tuesday Jul 11th, 2023

3-5pm instructed by Marcu-Antone Orsoni

Overview

In this lecture we went over lagrange's theorem, its proof, propositions and examples of its application. Assume that $\epsilon \in G$ is the identity element of G unless specified otherwise.

Recap of fundamental theorem of cyclic groups.

Below we recap on the fundamental theorem of cyclic subgroups, more specifically 2 key points that possibly connect to lagrange's theorem.

Fundamental theorem of cyclic subgroups

Suppose G is a cyclic group and $H \preceq G$, then the following holds true:

1. $|H| \Big| |G|$
2. If $k \in \mathbb{Z}$ such that $k|n = |G|$ then there exists subgroup of order $\frac{n}{k}$

Lagrange's theorem takes general finite groups which may not be cyclic in nature. It also gives us a relation between the order of the subgroup $H \preceq G$ and $|G|$ given as below

Lagrange's theorem

Suppose $|G|$ is finite and $H \preceq G$ then $|H| \Big| |G|$, more precisely

$$[G : H] = |G/H| = \frac{|G|}{|H|}$$

Proof:

Assume that $H \preceq G$ and suppose $[G : H] = |G/H| = r$. From this we can say that all the left cosets of H in G be $a_1H, a_2H, a_3H, \ldots, a_rH$. We realize that cosets form a partition of G with H which is equivalent to forming a disjoint union which can be described as below:

$$G = \bigsqcup_{i=1}^{r} a_iH$$

Which implies that:

$$|G| = \sum_{i=1}^{r} |a_iH| = \sum_{i=1}^{r} |H| [\because |aH| = |H|, \text{ from previous lecture}]$$

$$= |H| \sum_{i=1}^{r} = |H|r$$

$$\implies |G| = |H|r \implies [G : H] = r = \frac{|G|}{|H|}$$

Which is what we needed to show lagrange's theorem.

■

Remark: the converse of lagrange's theorem is not true necessarily. That is, it is not necessary that there must exist a subgroup of order which divides the order of the group. A counterexample is studied in the textbook.

Corollary: element orders divide group order

Let G be a finite group, $a \in G \implies |a| \Big| |G|$

Proof:

Let $a \in G$ such that G is finite. Observe that $|a| = |\langle a \rangle|$ which is a subgroup and thus by lagrange's theorem we conclude that $|a| = |\langle a \rangle| \Big| |G|$.

■

Corollary

Suppose $|G| = N$ then for all $a \in G$, $a^N = \epsilon$.

Proof:

By previous corollary is it trivial

■

Corollary

If $|G| = p$ with p prime then G is cyclic.

Proof:

By one of the previous corollaries, if $a \in G$ then $|a| \Big| |G|$. By this, the only possible valus of $|a|$ are 1 and p. Since the only possible element of order one is unique to the identity, the non-trivial elements must have order p and therefore that makes G cyclic.

■

We did an exercise in class. It is as below with the solution.

Exercise: applying lagrange's theorem

Let $a, b \in G$ such that $a \neq \epsilon \neq b$. Suppose $|G| = 155$ Show that the only subgroup containing a and b is G.

Solution:

Consider some cases, if $|a| = 155$(or same for b respectively) then G is cyclic thus the statement holds true in this case.

Suppose $|a|, |b| \neq 155$. We can apply lagrange's theorem to realize that since $155 = 5 \times 31$ we can take without loss of generality that $|a| = 5$ and $|b| = 31$. Suppose $H \preceq G$ such that $a, b \in H$. We can then apply the corollary of lagrange's theorem and obtain that $|a| \Big| |H|$ and $|b| \Big| |H|$. This implies that $\operatorname{lcm}(|a|, |b|) = \operatorname{lcm}(5, 31) = 155 \Big| |H|$. However, the only subgroup with order which 155 can divide is G itself thus $H = G$.

■

Exercise: prime factors

Suppose $|G| = 21$, show that all proper subgroups of G are cyclic.

Solution:

We see that $|G| = 21 = 3 \times 7$ and therefore the proper subgroups of $|G|$ must be non-equal factors of 21 which are 1,3,7. $|H| = 1$ is the trivial subgroup which is cyclic. If $|H| = 3$ then we know from earlier corollary that since $|H|$ is prime it must be cyclic, same logic applies for $|H| = 7$, completing the proof.

$\blacksquare$

Corollary: Euler's theorem

If $\gcd(k, n) = 1$ then $k\phi(n) \equiv 1 \mod n$.

Proof

If $\gcd(k, n) = 1$ then $[k] \in U(n)$. Using a corrollary from earlier we see that $k^{|U(n)|} = k^{\phi}(n) \equiv 1 \mod n$ which is what we needed to show.

$\blacksquare$

Remark: Fermat's little theorem is a consequence of a special case for Euler's theorem where $n = p$ for prime p. It is left as an exercise to the reader to show that if p is prime and $a \in \mathbb{Z}$ then $x^p \equiv x \mod p$.

Theorem: Product of subgroups

Let $H, K \preceq G$. and consider the subgroup product defined by $HK = \{hk : h \in H, k \in K\}$.

1. If $|H| = \infty$ or $|K| = \infty$ then $|HK| = \infty$
2. If both are finite subgroups then :

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Proof was long and thus not covered in class. We however covered an exercise that applies this theorem to reach interesting conclusions.

Exercise: previous theorem application.

Let $|G| = 242$. Show there is at most subgroup of order 121.

Solution:

Suppose by contradiction we had two subgroups of order 121 which are distinct. We can call them $H, K \preceq G$. We know that $H \cup K$ is a subgroup of H, K and thus by lagranges theorem its orders must divide H, K. The factors of $|H| = |K| = 121$ are 1,11,121. Note thatt $|H \cup K| \neq 121$ as that makes them non-distinct. If $|H \cup K| = 1$. This gives us the product computation as

$$|HK| = \frac{|H||K|}{|H \cup K|} = \frac{11^2 \times 11^2}{1} > |G| = 242$$

Which is not possible as the number of elements of G is bounded by 242. We see similarly that if $|H \cup K| = 11$ that $|HK|$ again exceeds the order of the group which is another contradiction. Therefore it must be the case that $H = K$ and thus existing at most one subgroup of order 121.

∎

We have a resultant theorem that emerges from lagrange's theorem as below

Theorem: Group classification

Groups of order $2p$ with p prime are either isomorphic to $\mathbb{Z}_{2p}$ or r D_p

Remark: The proof of the given theorem is long and in the textbook. One can also realize that if $|G| = 2p$ and it is non abelian then it must be isomorphic to D_p immediately.