Shannon Wood MAT 380

Lagrange's Theorem is used in group theory to find a list of possible orders of the subgroups of a group. Lagrange stated his theorem in 1770, before group theory itself came about. The theorem identifies candidates for the orders of subgroups of a group and the index of a group, which is the number of distinct left cosets of a subgroup in a group, denoted by $|G: H|$.

Coset:

$Let\ G\ be\ a\ group\ and\ H\ be\ a\ subset\ of\ G. For\ a \in G, define\ aH = \{ah: h \in H\}.$
$If\ H\ is\ a\ subgroup\ of\ G, then\ aH\ is\ a\ left\ (right) coset\ of\ H\ in\ G\ containing\ a,$
$where\ a\ is\ the\ coset\ representative\ of\ aH.$

Lemma: Properties of Cosets

$Let\ H\ be\ a\ subgroup\ of\ G\ and\ let\ a\ and\ b\ belong\ to\ G. Then,$

1. $a \in aH$
2. $aH = H\ if\ and\ only\ if\ a \in H,$
3. $aH = bH\ if\ and\ only\ if\ a \in bH$
4. $aH = bH\ or\ aH \cap bH = \emptyset,$
5. $aH = bH\ if\ and\ only\ if\ a^{-1}b \in H,$
6. $|aH| = |bH|,$
7. $aH = Ha\ if\ and\ only\ if\ H = aHa^{-1},$
8. $aH\ is\ a\ subgroup\ of\ G\ if\ and\ only\ if\ a \in H.$

Lagrange's Theorem: $|H|\ divides\ |G|$

$If\ G\ is\ a\ finite\ group\ and\ H\ is\ a\ subgroup\ of\ G, then\ |H|\ divides\ |G|. Also,$
$the\ number\ of\ distinct\ left\ (right) cosets\ of\ H\ is |G|/|H|.$

Corollary 1 $|G: H| = |G|/|H|.$

$$If\ G\ is\ a\ finite\ group\ and\ H\ is\ a\ subgroup\ of\ G, then |G: H| = |G|/|H|.$$

Corollary 2 $|a|\ divides\ |G|$

$$For\ G\ finite\ group, a \in G\ then\ |a|\big||G|.$$

Corollary 3 Groups of Prime Order are Cyclic

$$If\ |G| = prime, then\ G\ cyclic.$$

Corollary 4 $a^{|G|} = e$

$$Let\ G\ be\ afinite\ group, and\ let\ a \in G. Then\ a^{|G|} = e.$$

Corollary 5 Fermat's Little Theorem

$$If a \in \mathbb{Z}, p\ prime, then\ a^p mod\ p = a\ mod\ p.$$