

Lagrange's Theorem

If G is a finite group, then the order of any subgroup divides the order of G .

BACKGROUND:

It has been said that Lagrange's Theorem, discovered about 1770 in the context of permutation groups, is the most important theorem in group theory. Not the deepest theorem...usually the Sylow theorems are collectively given this title based on the stunning advance they represented considering the time and state of knowledge when they were introduced. In turn, there are also more recent specialized results that one could argue represent the solution of a greater intellectual puzzle than the Sylow theorems, but this is a bit like arguing who the best baseball player of all time was. It is certainly true that Lagrange's Theorem insinuates itself either directly or indirectly into just about every important result in group theory, and for that reason we should know its proof in detail.

The first general proof, presumably still in the context of permutation groups, was given about 1800 by Pietro Abbati. It was not uncommon prior to the Age of Rigor (roughly the last half of the nineteenth century) in mathematics that a great mathematician like Lagrange would discover a theorem, become intuitively convinced of its truth, and not feel the need to provide a detailed proof even according to the standards of the day, much less those of the modern era. Exhibit A in this regard is the Fundamental Theorem of Calculus, dating from perhaps 1670, which could not be said to have been really "proved" until Riemann introduced his definite integral in 1854.

NOTATION:

(1) Algebraists like to use capital letters to stand for wild cards when they write various expressions. For example, if A and B are sets and it makes sense to operate from the left any element of A on any element of B , they will write AB to indicate the set $\{ab : a \in A, b \in B\}$. Typically, A and B are both subgroups of some given group. Also, computer scientists write things like AB to mean any word in the language A followed by (concatenated with) any word from the language B , so the usage transcends algebra proper. The idea is to simply let the set symbol stand for any of its elements whenever the context is appropriate.

(2) Even if a set is not a group, we will extend the "absolute value bars" notation for order of a group to mean simply the cardinality of a set. So $|S|$ counts the elements of S , no matter what structure, if any, S has.

KEY DEFINITIONS:

1) A *subgroup* H of a group G is a subset of elements of G that, using the operation induced by G , constitute a group by themselves.

2) If G is a group, $g \in G$ an arbitrary element, and $H \leq G$ an arbitrary subgroup, the set $\{gh : h \in H\}$, abbreviated gH , is called the *left coset* (of H by g). The *right coset* Hg is defined analogously. The element g is called the *coset representative* of either gH or Hg . Note the left or right designation agrees with the side on which the coset representative is applied.

3) A *partition* of a set S is a family of subsets (called *blocks*) of S that satisfies three properties: (i) each subset is nonvoid, (ii) any two subsets are disjoint, and (iii) the union over the family of subsets is all of S .

4) If G is a finite group and $H \leq G$, the *index* of H in G is the number of distinct cosets of H in

G . This index is written $[G : H]$.

KEY FACTS:

- 1) If $H \leq G$, then for $x, y \in G$, either $xH = yH$ or $xH \cap yH = \emptyset$
- 2) If $H \leq G$, then for $x, y \in G$, $|xH| = |yH|$
- 3) If $H \leq G$, then $xH = H$ if and only if $x \in H$

PROOF STRATEGY:

We consider the cosets of a subgroup $H \leq G$, show that they partition the group, and establish that each coset has the same number of elements. This leads to a simple arithmetic formula...the number of cosets times the common number of elements per coset must equal the number of elements in the group. Since H itself is a coset (with coset representative being any of its elements per key fact #3), the order of H will be seen to divide the order of G .

PROOF:

Given the finite group G and $H \leq G$, form the collection of all cosets $\{gH : g \in G\}$ and cull any duplicates using key fact #1 to form the collection $\mathcal{C}$ of distinct cosets of H in G . I claim $\mathcal{C}$ is a partition of the elements of G . No coset is void and all distinct cosets are mutually disjoint by construction of the family $\mathcal{C}$. Moreover, every element $g \in G$ is in some member of $\mathcal{C}$, since $g \in gH$ and gH must appear as one of the distinct cosets of H (perhaps with a different coset representative). These three properties are enough to ensure that $\mathcal{C}$ is a partition of the elements of G . We may write $G = \bigcup \{xH : x \in R\}$, where R is a set of coset representatives for the partition $\mathcal{C}$. We then have $|G| = \sum |\{xH : x \in R\}|$ and since key fact #2 assures us that all cosets have the identical number of elements in them, we may write this sum as $[G : H] \cdot |\{xH : x \in R\}|$, where $[G : H]$ is the index, or number of distinct cosets, of H in G . Finally, we may write $[G : H] \cdot |\{xH : x \in R\}| = [G : H] \cdot |H|$, since one of the distinct cosets must be H itself, and $|H|$ is therefore the common value for $|\{xH : x \in R\}|$. Putting it all together, we see that $|G| = [G : H] \cdot |H|$, and it follows immediately that the order of H divides the order of G .

DANGER ZONE:

Lagrange's Theorem does not have a general converse, although by making some further assumptions a "weak" converse can be stated and shown to be valid. Just because a factor divides the order of a group, it does not mean that there is a subgroup with that factor as its order. Paolo Ruffini was the first to provide a counterexample to the converse of Lagrange's Theorem, namely the group A_4 , which has order 12 (it is the alternating group of permutations on four symbols, hence has order $\frac{4!}{2} = 12$). And yet although 6 divides 12, A_4 has no subgroup of order 6. You can demonstrate this by considering the 8 elements of order 3 in A_4 , all of which must be in the subgroup of order 6...bit of a tight fit.