

# THE HISTORY OF LAGRANGE'S THEOREM

David O Dea, Diarmuid Donnellan, Jonathan Hester and Padraig Lafferty



## Introduction

Our objective for this project is to examine the history of the famous Lagrange's theorem. The theorem as we know it today has evolved greatly since its earliest form in 1771. We hope to tie his initial findings about polynomials to their current applications, and the importance of the theorem to group theory and mathematics in general.

## Joseph-Louis Lagrange

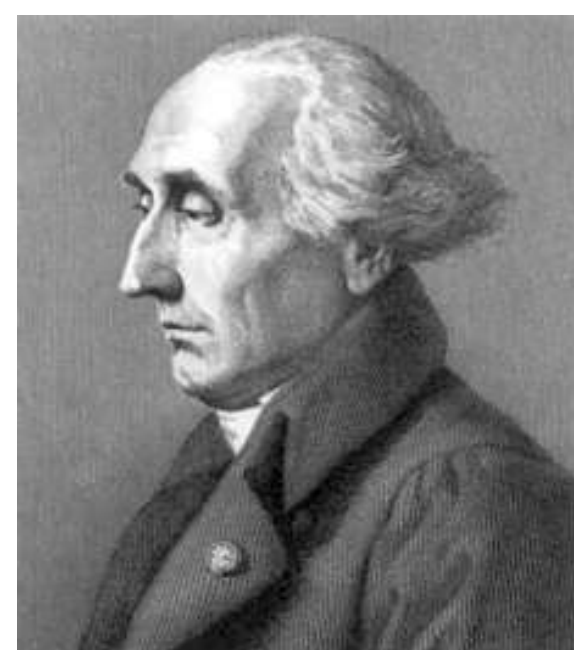


Fig. 1: Lagrange portrait

Born in Turin, Italy on 25th January 1736, Joseph-Louis Lagrange was a brilliant mathematician and astronomer. A major contributor to number theory and analysis, Lagrange also had a significant influence in celestial mechanics. His most important book, *Mécanique Analytique* (1788; "Analytic Mechanics"), was the basis for all later work in this field. In 1766, he succeeded Euler as the director of mathematics at the Prussian Academy of Sciences, Berlin. He moved to France in 1787 to join the French Academy of Sciences where he remained until his death in 1813. Lagrange's influence is obvious in many areas of mathematics, including theorems which carry his name either solely or jointly. Group theory had not been defined at this point in history and only began being studied in later centuries. Not having studied group theory or anything similar, Lagrange was completely unaware of the influence that his findings would subsequently have in that area of study.

## Lagrange's Original Findings

Lagrange initially concerned himself with finding an algebraic formula for the roots of the general 5th degree polynomial and more generally for the nth degree polynomial for  $n > 4$ . The quadratic, cubic, and quartic equations had already been solved, so Lagrange wished to investigate polynomials of degree greater than four. Lagrange observed that the solutions for the cubic and quartic equations involved solving polynomials of lower degree, or "resolvent" polynomials. "For example, the quartic was solved using a cubic resolvent polynomial whose roots could be written as (2):

$$\frac{X_1X_2 + X_3X_4}{2}, \frac{X_1X_3 + X_2X_4}{2}, \frac{X_1X_4 + X_2X_3}{2}$$

Where  $X_1, X_2, X_3$  and  $X_4$  are the roots of the original polynomial". Permute these four roots in the 4!(or 24) possible ways, and three different values are typically outputted. Lagrange reckoned a similar approach was required to solve 5th degree polynomials. He believed that a function had to be found in 5 variables that took on 3 or 4 different typical values, where where the variables are permuted in all 5! (or 120) ways. This would lead to a corresponding resolvent that would be crucial to solving the original equation. Although Lagrange never determined if this was the case, he did however arrive at the following conclusion:

"if a function  $f(X_1, \dots, X_n)$  of  $n$  variables is acted by  $n!$  possible permutations of the variables and these permuted functions take on only  $r$  distinct values, then  $r$  is a divisor of  $n!$ ."

## Timeline

### Evolution of Lagrange's theorem

Lagrange did not originally prove his theorem as we see it today. Although Lagrange was clearly moving towards this idea, he never in fact pinned it down. He received credit for it by many later writers.

**1771**

He stated that that if a polynomial in  $n$  variables has its variables permuted in all  $n!$  ways, the number of different polynomials that are obtained is always a factor of  $n!$ .

**1799**

Paolo Ruffini showed in 1799 that if  $n = 5$  then  $m$  cannot be 3, 4, or 8. Inspired by Ruffini's work.

**1801**

Carl Friedrich Gauss proved Lagrange's theorem for the special case of  $(\mathbb{Z}/p\mathbb{Z})$ , the multiplicative group of nonzero integers modulo  $p$ , where  $p$  is a prime.



Fig. 2: Lagrange Findings 1771

**1815**

Augustin-Louis Cauchy showed in 1815 that if  $n$  is prime then  $m = 1$  or  $m = 2$  or  $m > n$ ; he conjectured that if  $n > 5$  then  $m = 1$  or  $m = 2$  or  $m > n$

**1845**

Joseph Bertrand proved Cauchy's conjecture in 1845 subject to the truth of his celebrated Hypothesis about prime numbers Stimulated by this, Cauchy also proved Lagrange's theorem for the symmetric group  $S_n$ .

**1861**

Camille Jordan finally proved Lagrange's theorem for the case of any permutation group

## Lagrange's Theorem As We Know It

Let  $G$  be a finite group with a subgroup  $H$ . Then the order of  $H$  divides the order of  $G$ .

Lagrange's Theorem says that a subgroup of  $S_4$  which has  $4! = 24$  elements, could possibly have 1, 2, 3, 4, 6, 8, 12 or 24 elements, but couldn't have (for example) 11 or 17 elements.

The converse of Lagrange's Theorem is not true if  $n$  and  $k$  are integers and  $k|n$ , it is not true that every group of order  $n$  has a subgroup of order  $k$ .

## Proof Mechanism

Start with the subgroup  $H$  of the finite group  $G$ .

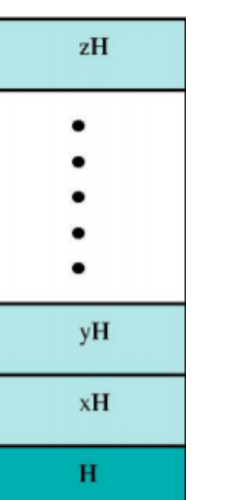
If  $H = G$  the theorem holds

If not, choose an element  $x$  of  $G$  with  $x \notin H$ . Then the coset  $xH$  is disjoint from  $H$  and has  $|H|$  elements.

If  $H \cup xH = G$  then  $|G| = 2|H|$  and we are done.

If not, choose  $y \notin H \cup xH$  and add the coset  $yH$ .

Eventually we find that  $G$  is the union of  $k$  disjoint left cosets of  $H$ , and  $|G| = k|H|$ .



## Real Life Application of Lagrange's Theorem



Fig. 3: Speed Gun

There exists certain police equipment used in Italy that detects speed limit violations by motorists. It does this by snapping a pair of separate pictures of vehicles that are taken a couple of kilometres apart. If the time elapsed between the pictures is less than the time it should take to travel the distance then the vehicle is deemed to have broken the speed limit and the driver will receive a ticket. The average speed is higher than the limit. Lagrange's theorem guarantees that there existed a point on the stretch of road between the cameras where the instantaneous speed of the car was equal to the average speed, which was established by the cameras to be in excess of the speed limit.

## References

1. Newman, P., (2017): Some prehistory of Lagrange's Theorem. "The number of values of a function, <https://www.m-a.org.uk/resources/downloads/3H-Peter-Neumann-Lagrange-Theorem.pdf>
2. Roth, Richard L. "A History of Lagrange's Theorem on Groups." *Mathematics Magazine*, vol. 74, no. 2, 2001, pp. 99–108. JSTOR, [www.jstor.org/stable/2690624](http://www.jstor.org/stable/2690624).
3. Maths.nuigalway.ie. 2020. NUI Galway MA3343: Groups, 2020/21. [online] Available at: <http://www.maths.nuigalway.ie/~rquinlan/groups/> [Accessed 17 December 2020].