LAGRANGE'S THEOREM

Sharon Donohoe and Ciara Hamilton†
†National University of Galway

INTRODUCTION

This poster will discuss one of the Lagrange's lasting legacies;
Lagrange's theorem on groups, as well as the developments it underwent to become the theorem we recognise today.

Lagrange's theorem is a well known result which is used in group theory and other fields in mathematics, it is defined as followed:
"Let G be a group of order n and H a subgroup of order m. Then m is a divisor for n"

WHO WAS LAGRANGE?

Joseph-Louis Lagrange was an Italian mathematician born in Turin in 1736.
By age 19, Lagrange had become a professor of mathematics Royal Artillery School in Turin.
Due to his prolific contributions to mathematics and physics, he soon became known as one of the greatest mathematicians in Europe.
Lagrange was born into a changing world in 18th century Italy.
Growing up he was surrounded by great developments in medicine, physics, and the natural sciences, pioneered by his fellow Italian scholars.
There is no doubt that Lagrange soon went on to become one of the defining academics of the age of enlightenment in Italy.

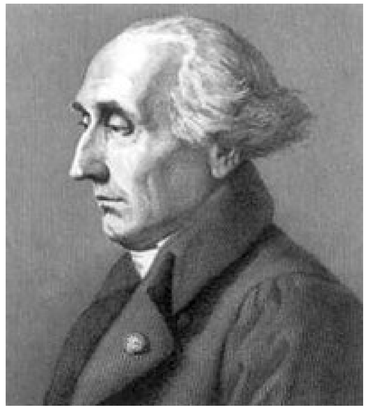

Fig. 1: Joseph-Louis Lagrange.

SOME IMPORTANT DEFINITIONS

GROUP: a non-empty set equipped with a binary operation that together satisfy the properties of closure, associativity, the identity property, and the inverse property.

SUBGROUP: Suppose G is a group under the operation *, and let H be a subset of G. Then H is a subgroup of G if H satisfies the four properties of a group under the operation of G.

ORDER: the order of a group is the number of elements in its set.

ORIGINAL THEOREM OF LAGRANGE

When Lagrange first proposed his theorem, group theory had not yet been defined.
The theorem was first developed in 1770 when Lagrange published workings on the theory of equations.
In this he aimed to derive a formula that could be used to solve a polynomial of 5 degrees or higher.
He reasoned that if solving the quadratic and cubic polynomials involved solving supplementary polynomials of a lower degree then the same might stand for a polynomial of the 5th degree.
This led to the original theorem which stated: If a function F(x1, x2, . . . , xn) of n variables is acted on by all n! possible permutations of the variables and these permuted functions take on only r distinct values then r is a division of n.
This original theorem is vastly different from the one we know today. As the study of group theory developed and changed so too did the theorem originally propose by Lagrange back in 1770.

DEVELOPMENTS ON HIS WORK

Many later developments were made on Lagrange's original work.
In 1799, Paolo Ruffini published a book in which he provided proof that the converse of Lagrange's Theorem does not hold.
In 1815, a paper by Cauchy tied together the prior developments made on Lagrange's Theorem. Cauchy provided a proof of the original theorem as well as a generalised version of Ruffini's theorem.
Cauchy later went on to prove that order of a subgroup Sn is a divisor of n!.
This was the first solid proof of Lagrange's theorem in the case of symmetric groups.
It wasn't until the twentieth century that the language of cosets was used to prove Lagrange's theorem.
Though it is hard to accredit anyone in particular with the first formal proof of the theorem, the coset approach is said to have been inspired by Galois.

Fig. 2: Austin Louis Cauchy

PROVING LAGRANGE'S THEOREM

In order to proof Lagrange's theorem we start with a subgroup H of the finite group G.
If we find that H = G then the theorem holds.But if H G then we choose an element x of G with x not being an element of H (xH).
Then the coset xH is disjoint from H and has |H| elements. If H xH = G then |G| = 2|H| and we are done.
If not, choose y 6 H 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|.

THE THEOREM EXPLAINED

In this case the term "divides" tells us that the order of subgroup H is a factor of the order of group G.
An example of the theorem in practice is the group S4. S4 has 4! (or 24) elements.
A subgroup of S4 could possibly have 1,2,3,4,6,8,12, or 24 elements as these are all factors of 24 (the order of S4).
The subgroup could not have, for example, 9 or 11 elements as these do not divide 24.
The converse of the theorem is not true.

APPLICATIONS OF LAGRANGE

Lagrange Theorem can be widely applied in mathematics's to prove other theorems.
This can be used to prove Euler's theorem and Fermat Theorem (an integer raised to a prime power leaves the same remainder as the integer itself when divided by the prime) and its generalization.
In addition to this we can use Lagrange to illustrate that there are infinitely many primes.
Lagrange's Theorems can be seen today used in the modern world of the digital payments system namely Cyptocurrencies (eg.Bitcoin).

THE FUTURE OF LAGRANGE

The Future of Lagrange lies in the hands of two very capable students of the School of Mathematics at NUI Galway.

References

Moravia, Sergio., 'An Outline of the Italian Enlightenment', in Comparative Literature Studies, vol. 6, no. 4 (1969), pp.380-409.

Roth, Richard L., 'The History of Lagrange's Theorem on Groups', in Mathematics Magazine, vol. 74, no. 2 (April 2001), pp. 99-108.

'Joseph-Louis Lagrange',Physics Today, (January 2017), https://physicstoday.scitation.org/do/10.1063/PT.5.031404/full/, accessed