The History of Lagrange's Theorem

Thomas Maher † Shane Lawless † Noel Finan
Groups Poster

NUI Galway
OÉ Gaillimh

Introduction

In this poster we will uncover the whole timeline of Lagrange's Theorem from his original theorem on polynomials to the real world applications that we have 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"

The Theorem was named after the prolific Italian mathematician Joseph-Louis Lagrange who's polynomial theorem paved the way for the groups theorem above.

Lagrange's Original Theorem

The initial work that Lagrange did on polynomials bore little resemblance to the theorem that we have today. Group theory was not defined at this point of time (1770) and he was more so focused on the theory of equations.

He stated, in his article "Réflexions sur la résolution algébrique des équations", 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!

RÉFLEXIONS

SUR LA

RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS (*).

[Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin, années 1770 et 1771 (**).]

La théorie des équations est de toutes les parties de l'Analyse celle qu'on eût cru devoir acquérir les plus grands degrés de perfection et par son importance et par la rapidité des progrès que les premiers inventeurs y ont faits; mais quoique les Géomètres qui sont venus depuis n'aient cessé de s'y appliquer, il s'en faut beaucoup que leurs efforts aient eu le succès qu'on pouvait désirer. On a à la vérité épuisé presque tout ce qui concerne la nature des équations, leur transformation, les conditions nécessaires pour que deux ou plusieurs racines deviennent égales, ou aient entre elles un relation donnée, et la manière de trouver ces racines, la forme des racines imaginaires, et la méthode de trouver la valeur de celles qui, quoique réelles, se présentent sous une forme imaginaire, etc. On a aussi découvert des règles générales pour reconnaître si toutes les racines d'une équation sont réelles ou non, et pour savoir dans le premier cas combien il doit y en avoir de positives et de négatives; mais on n'a jusqu'à présent aucune règle générale pour connaître

(*) Ce Mémoire a été lu à l'Académie dans le courant de l'année 1771.

(**) Les deux premières Sections de ce Mémoire ont été insérées dans le volume de 1770, les suivantes dans le volume de 1771. (Note de l'Éditeur.)

Fig. 1: Réflexions sur la résolution algébrique des équations

Further Developments of Lagranges Work

Other Mathematicians came along in the following decades to further Lagrange's work. In 1799, Ruffini showed that the converse of the original theorem is false (there does not exist any function of 5 variables that takes on 3 or 4 variables). Basically that the group S_5 has no subgroup of 30 or 40. Therefore a group doesn't necessarily have subgroups of order that divide the original groups order.

Abatti, his friend and mathematical collaborator from the same university (University of Modena) gave a proof of Lagranges original theorem.

Cauchy and Permutation Group Theory

The French mathematician Augustin Louis Cauchy had an important role in developing Lagrange's theorem as we know today. While he did some work on it in 1815, such as proving Lagrange's original (polynomial) theorem in a similar way to Abatti. The bulk of his contribution came nearly 30 years later. In 1844, Cauchy wrote a paper on permutation group theory where he proved that the order the order of a subgroup of the symmetric group S_n is a divisor of n! This is essentially a proof of Lagrange's theorem in the case of symmetric groups.

In a series of papers in the following years, Cauchy would show the link between his theorem and Lagrange's polynomial by showing that the set of permutations fixing functions values from a subgroup S_n.

Another French mathematician Camille Jordan, proved that Lagrange's theorem held for any finite permutation group. He published this in his thesis in 1861. This proof would go on to be used in a number of influential books in the following decade.

Fig. 2: Augustin Louis Cauchy

Lagrange's Theorem Until Now

The abstract idea of groups emerged in the 1880's and with it came the proof of Lagrange's Theorem with regards to group theory. Although it is difficult to pinpoint exactly who proved the first proof, there is an example from German mathematician Otto Hölder in 1889. There is still ambiguity and debate to this day with respect to this.

It was likely that the first person to give a proof in the language of cosets was Heinreich Weber in "Lehrbuch der Algebra"

Lagrange wasn't credited for around half a century after the abstract proof. He was referenced in many books such as "Moderne Algebra" by Van der Waerden but it took until 1941 before his name was firmly attached to the proof. It was in the book "A survey of Modern Algebra" that gave the proof that we still use today with Lagranges name on it.

Applications

This can be used to prove Fermat's little theorem and its generalization, Euler's theorem. These special cases were known long before the general theorem was proved. Helps compute powers of integers modulo prime numbers which is used in cryptography. Therefore, we can say that a modern application of Lagrange's theorem is crypto-currencies and cyber-security.

Lagrange's theorem can also be used to show that there are infinitely many primes: if there were a largest prime p, then a prime divisor q of the Mersenne number

Joseph-Louis Lagrange

Joseph-Louis Lagrange was an Italian mathematician, born in 25 January 1736 (Turin, Piedmont-Sardinia). He made significant contributions to the fields of analysis, number theory, and both classical and celestial mechanics. He passed away in Paris 1813, aged 77. In his early life he did not have a great passion for mathematics. He studied at the University of Turin where his favourite subject was classical Latin. It wasn't until he came across a paper by Edmond Halley that his enthusiasm for mathematics grew. He moved to Berlin in 1766 where he started work on what became known as Lagrange's theorem.

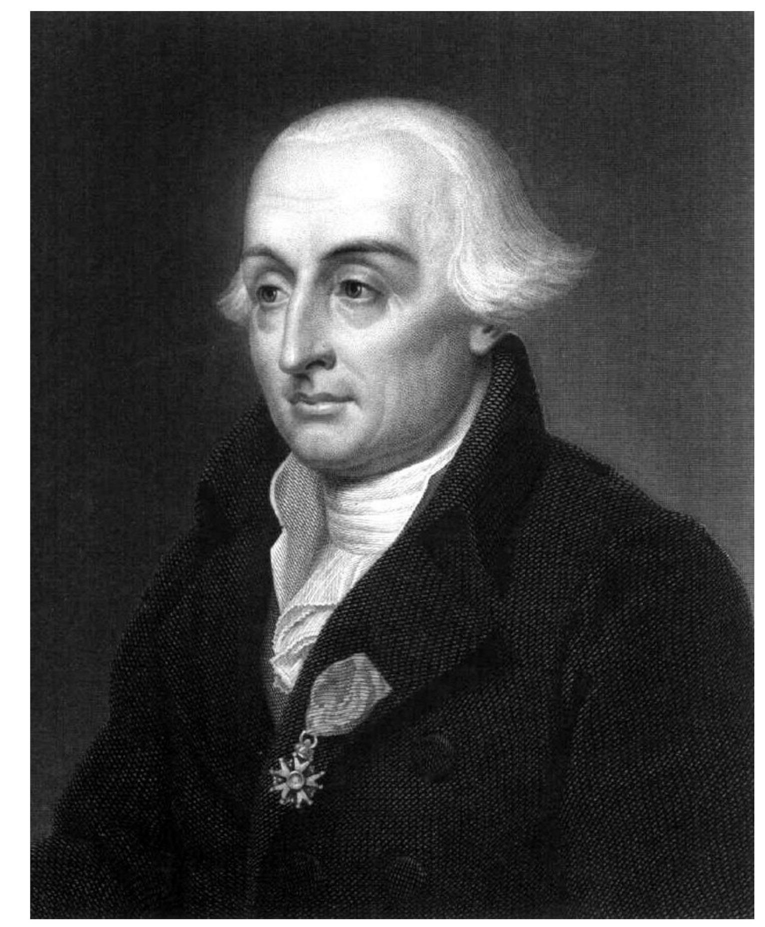

Fig. 3: Joeseph-Louis Lagrange

Lagrange Fun Facts

He was largely self-taught and did not obtain a university degree.

Lagrange is one of the 72 prominent French scientists who were commemorated on plaques at the first stage of the Eiffel Tower when it first opened.

He always thought out the subject of his papers before he began to compose them, and usually wrote them straight off without a single erasure or correction.

In character he was nervous and timid, he detested controversy, and to avoid it willingly allowed others to take the credit for what he had himself done.

References

• Roth, R. (2001). A History of Lagrange's Theorem on Groups. Mathematics Magazine, 74(2), 99-108. doi:10.2307/2690624
• O'Connor, J., Robertson, E. (1999). Joseph-Louis Lagrange (1736-1813). Retrieved from https://www-history.mcs.st-andrews.ac.uk/Biographies/Lagrange.html
• Lagrange's theorem (group theory). (2019). Retrieved 4 November 2019, from https://en.wikipedia.org/wiki/Lagrange