

# Some prehistory of Lagrange's Theorem in group theory:

“The number of values of a function”

The Mathematical Association,

Royal Holloway College, Saturday 8 April 2017

Peter M. Neumann (The Queen's College, Oxford)

A fundamental fact of modern group theory, that the order of a subgroup of a finite group divides the order of the group, is called Lagrange's Theorem.

There is nothing like that in Lagrange's writings. I shall explain the insight of Lagrange (1770/71) that took a century to evolve into this modern theorem.

- The number of values of a function
- Lagrange's Theorem 1770 and 1870
- Those hundred years of evolution

## A brain flexercise

Think of functions  $f(x,y,z)$  of three variables: we call the various functions like  $f(y,x,z)$  obtained by permuting the variables the **values** of  $f$ .

Are there functions that have 1 value?

2 values?

3 values?

4 values?

5 values?

6 values?

7 values or more?

# The values of functions of three variables

## Examples

If  $f(x,y,z) = x + y + z$  then  $m = 1$

If  $f(x,y,z) = x + y^2 + z^3$  then  $m = 6$

If  $f(x,y,z) = x + y + z^2$  then  $m = 3$

Are there functions  $f$  for which  $m = 2$  or  $m = 4$  or  $m = 5$ ?

## Functions of three variables continued

If  $f(x,y,z) = xy^2 + yz^2 + zx^2$  then  $f$  has just one other value, namely  $x^2y + y^2z + z^2x$ : so this function has precisely 2 values.

Can a function  $f(x,y,z)$  have 4 or 5 values?

## Another exercise

Do we have time (and inclination) to try the same problem for functions  $f(w,x,y,z)$  of four variables?

## The general case

**Notation:**  $n$  a positive integer;  
 $x_1, x_2, x_3, \dots, x_n$   $n$  variables;  
 $f(x_1, x_2, x_3, \dots, x_n)$  a function of these variables;  
 $m$  the number of different functions obtained by  
permuting  $x_1, x_2, x_3, \dots, x_n$  in all possible ways;  
these are the **'values'** of  $f$ .

**Lagrange (1770/71):** Given  $n$ , what are the possibilities for  $m$ ?

## Number of values of a function

**First observation:** Certainly  $m \leq n!$

**Let's tabulate:**

n	possibilities for the number m of values . . . . .
1	1
2	1, 2
3	
4	
5	

## Number of values of a function

**First observation:** Certainly  $m \leq n!$

**Let's tabulate:**

n	possibilities for the number m of values . . . . .
1	1
2	1, 2
3	1, 2, 3, 6
4	
5	



## Number of values of a function

**First observation:** Certainly  $m \leq n!$

**Let's tabulate:**

n	possibilities for the number m of values . . . . .
1	1
2	1, 2
3	1, 2, 3, 6
4	1, 2, 3, 4, 6, 8, 12, 24
5	

## Number of values of a function

**First observation:** Certainly  $m \leq n!$

**Let's tabulate:**

n	possibilities for the number m of values . . . . .
1	1
2	1, 2
3	1, 2, 3, 6
4	1, 2, 3, 4, 6, 8, 12, 24
5	<b>What about this row? Any values? Any conjectures?</b>

## Functions of 5 variables: Ruffini 1799, Cauchy 1815

**Paolo Ruffini** showed in 1799 that if  $n = 5$  then  $m$  cannot be 3, 4, or 8

Inspired by Ruffini's work, **A.-L. Cauchy** showed in 1815 that if  $n$  is prime then  $m = 1$  or  $m = 2$  or  $m \geq n$ ;  
he conjectured that if  $n \geq 5$  then  $m = 1$  or  $m = 2$  or  $m \geq n$

**Joseph Bertrand** proved Cauchy's conjecture in 1845 subject to the truth of his celebrated Hypothesis about prime numbers; stimulated by this, in 1845 **Cauchy** found a complete proof (for which he introduced his version of groups)

## The content of Section 97 of Lagrange's "Réflexions"

Section 97 of Lagrange's "Réflexions sur la résolution algébrique des équations" [Berlin 1770/71] suggests the wonderful insight:

The number  $m$  of values of  $f$  divides  $n$ !

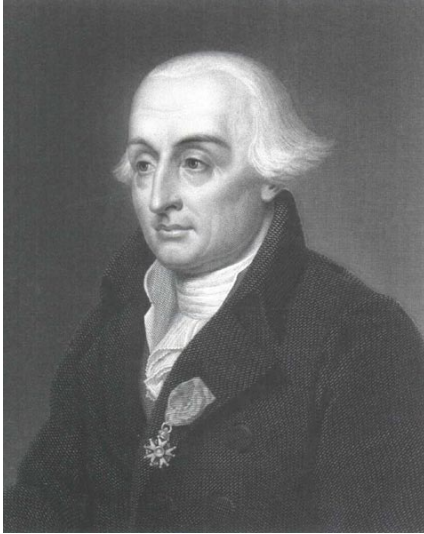
**BUT**, although Lagrange was clearly moving via special cases towards this idea, he did not pin it down—it was imputed to him by many later writers

**Moreover**, his argument is based only on an example

**Furthermore**, that example is incorrect

**Nevertheless**, Lagrange's ideas inspired much great mathematics

# Lagrange's "Réflexions", 1770



## Réflexions sur la résolution algébrique des équations (1770/71) by J.-L. Lagrange

### Lagrange's theorem in §97 (from Œuvres)

97. Quoique l'équation  $\Theta = 0$  doive être, en général, du degré  $1.2.3\dots\mu = \varpi$ , qui est égal au nombre des permutations dont les  $\mu$  racines  $x', x'', x''', \dots$  sont susceptibles, cependant s'il arrive que la fonction soit telle, qu'elle ne reçoive aucun changement par quelque-une ou quelques-unes de ces permutations, alors l'équation dont il s'agit s'abaissera nécessairement à un degré moindre.

Car supposons, par exemple, que la fonction  $f[(x')(x'')(x''')(x^{iv})\dots]$  soit telle, qu'elle conserve la même valeur en échangeant  $x'$  en  $x''$ ,  $x''$  en  $x'''$ , et  $x'''$  en  $x^{iv}$ , en sorte que l'on ait

$$f[(x')(x'')(x''')(x^{iv})\dots] = f[(x'')(x''')(x^{iv})(x')\dots],$$

il est clair que l'équation  $\Theta = 0$  aura déjà deux racines égales; mais je vais prouver que dans cette hypothèse toutes les autres racines seront aussi égales deux à deux. En effet, considérons une racine quelconque de la même équation, laquelle soit représentée par la fonction

$$f[(x^{iv})(x''')(x')(x'')\dots],$$

comme celle-ci dérive de la fonction

$$f[(x')(x'')(x''')(x^{iv})\dots],$$

en échangeant  $x'$  en  $x^{iv}$ ,  $x''$  en  $x'''$ ,  $x'''$  en  $x'$ ,  $x^{iv}$  en  $x''$ , il s'ensuit qu'elle devra garder aussi la même valeur en y changeant  $x^{iv}$  en  $x'''$ ,  $x'''$  en  $x''$  et  $x'$  en  $x^{iv}$ ; de sorte qu'on aura aussi

$$f[(x^{iv})(x''')(x')(x'')\dots] = f[(x''')(x')(x^{iv})(x'')\dots].$$

Done, dans ce cas, la quantité  $\Theta$  sera égale à un carré  $\theta^2$ , et par conséquent l'équation  $\Theta = 0$  se réduira à celle-ci  $\theta = 0$ , dont la dimension sera  $\frac{\varpi}{2}$ .

## Proofs of Lagrange's Theorem

Clear formulations and proofs of Lagrange's Theorem (as the assertion that  $m$  divides  $n!$ ) were given by **Pietro Abbati** (a student and colleague of **Ruffini**) in 1802, by **Cauchy** in 1815, and by many others thereafter.

Let's see if we can work out our own proof  
in the spirit of those times  
before groups were invented.

## Lagrange's Theorem 1770 and 1870

**Lagrange's Theorem 1770:** The number  $m$  of 'values' of a function of  $n$  variables divides  $n!$

**Lagrange's Theorem 1870:** Si le groupe  $H$  est contenu dans le groupe  $G$ , son ordre  $n$  est un diviseur de  $N$ , ordre de  $G$ .

[Camille Jordan, *Traité des Substitutions et des Équations Algébriques* (1870), p. 25—the origin of the name; the theorem occurs earlier in this form, but in Cauchy's language, in a text by Serret (1866)]

---

**Lagrange's Theorem 2017:** The order of a subgroup  $H$  of a finite group  $G$  divides the order of  $G$ .

**Questions:** How are these theorems related?  
What is the path from there to here?

## Groups, subgroups, cosets

**Galois (1829–32, 1846), Cauchy (1845):** A **group** is a [non-empty] closed collection of substitutions (permutations) of  $\{1, 2, \dots, n\}$

**Discuss!**

A **subgroup**  $H$  of a group  $G$  is a [non-empty] closed collection of some of the members of  $G$

A **(right) coset** of a subgroup  $H$  of a group  $G$  is the collection  $Ha$  of members of  $G$ , where  $a$  is a member of  $G$  (each coset will usually have several different representatives  $a$ )

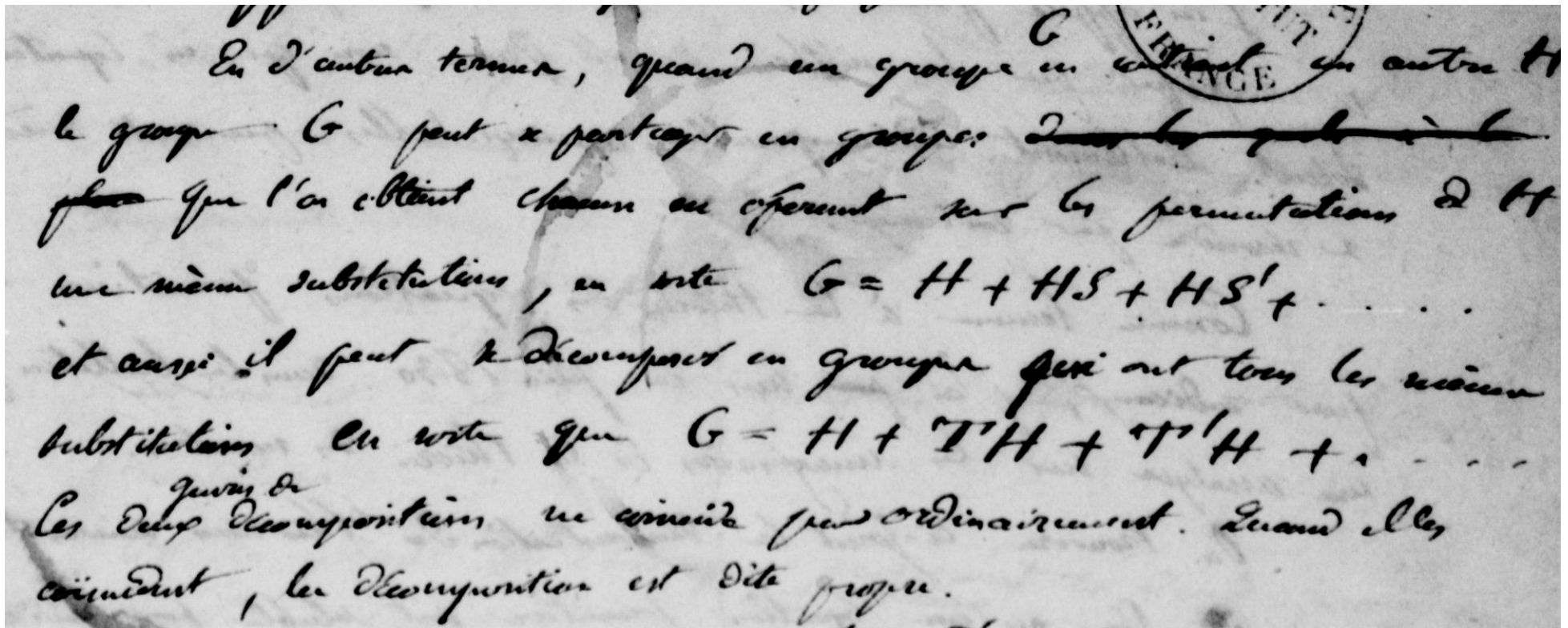
**Note.** Galois calls these ‘groupes’; he has both left and right cosets **[see next screen]**

They are implicit in Cauchy’s work of 1845, but not explicit



## Groups, subgroups and cosets: Galois 1832

Évariste Galois: his **Lettre Testamentaire** written 29 May 1832, published September 1832:



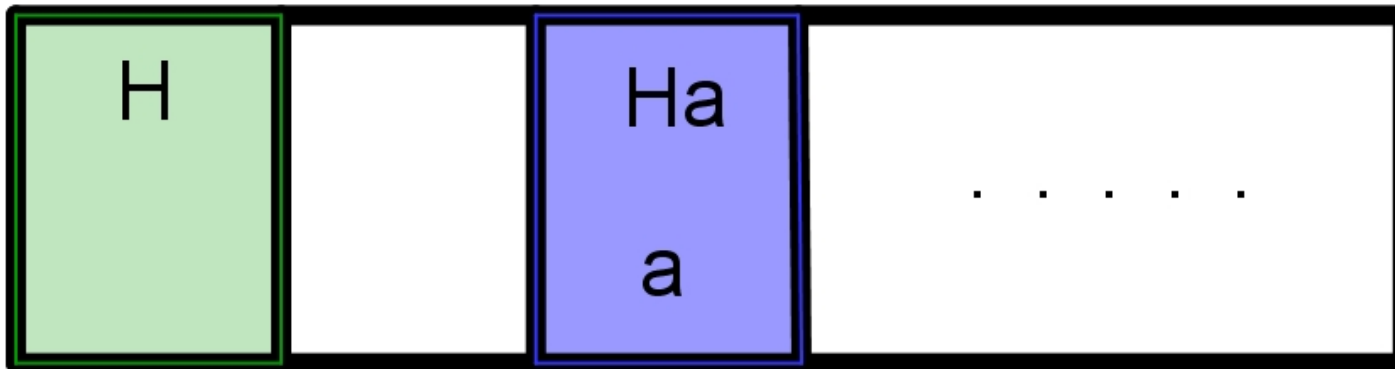
En d'autres termes, quand un groupe  $G$  est contenu en un autre  $H$  le groupe  $G$  peut se partager en groupes: ~~sur les quels~~ ~~pour~~ que l'on obtient chacun en opérant sur les permutations de  $H$  une même substitution, en sorte  $G = H + HS + HS' + \dots$  et aussi il peut se décomposer en groupes qui ont tous les mêmes substitutaires en sorte que  $G = H + TH + T'H + \dots$  Ces deux décompositions ne coïncident pas ordinairement. Quand elles coïncident, la décomposition est dite propre.

## Lagrange's Theorem 1866–2017

**Lagrange's Theorem (modern version):** If  $H$  is a subgroup of a group  $G$  then:

- every coset  $Ha$  has the same number of members as  $H$ ;
- the cosets of  $H$  partition  $G$ ; that is, every member of  $G$  lies in one and only one of the cosets.

**Note.** This holds for any kind of group, infinite as well as finite



Portrait of a group  $G$  partitioned  
by the cosets of a subgroup  $H$

## Return to 1770 version of Lagrange's Theorem

**Lagrange's Theorem 1770:** The number  $m$  of 'values' of a function of  $n$  variables divides  $n!$

**Using groups to prove it:**

Let  $G :=$  group of all permutations of  $\{x_1, x_2, \dots, x_n\}$

For  $f(x_1, x_2, \dots, x_n)$  and  $g \in G$ , let  $f^g$  be the function obtained by applying the permutation  $g$  to the variables in  $f$

Let  $H :=$  collection of all permutations  $h$  in  $G$  such that  $f^h = f$

Then  $H$  is a subgroup of  $G$  and two 'values'  $f^{g_1}$ ,  $f^{g_2}$  are equal if and only if  $g_1$  and  $g_2$  lie in the same coset of  $H$

So the number of 'values' of  $f$  is the number of cosets of  $H$  in  $G$ , and therefore divides  $n!$

## Further influence of Lagrange's ideas, I

Académie des Sciences, Paris, Grand Prix de mathématiques  
1860, Announcement (1857):

Quels peuvent être les nombres de valeurs des fonctions bien définies qui contiennent un nombre donné de lettres, et comment peut-on former les fonctions pour lesquelles il existe un nombre donné de valeurs?

English translation on next page

[C. R. Acad. Sci. Paris, 44 (1857), p. 794: Séance du lundi 13 avril 1857; Commissaires, MM. Liouville, Lamé, Cauchy, Serret, Bertrand rapporteur]

Taken almost verbatim from Cauchy, 15 September 1845

## Further influence of Lagrange's ideas, II

What are the possibilities for the numbers of values of well defined functions that contain a given number of letters, and how may one form the functions for which there exists a given number of values?

Led to great activity in group theory by **Émile Mathieu**, **Camille Jordan**, **Revd T. P. Kirkman** (the competitors) and, a little later, by many others.

## Conclusion: a 1921 homily on eponymy

“In this case we have attributed to Lagrange a theorem which he probably never knew or conjectured, on the ground (it would seem) that he knew a certain special case of it. In Hardy’s paper we have a theorem [the four-squares theorem] referred to Lagrange apparently on the ground that he first published a proof of it though it had been in the literature long before. Somewhere between these two extremes lies the golden mean of proper practice in attaching the names of mathematicians to specific theorems; and this mean, in the opinion of the reviewer, is rather far removed from each of the extremes indicated.”

**R. D. Carmichael**, in **Bull. Amer. Math. Soc. 1921**