CMPE 220.02

DISCRETE COMPUTATIONAL STRUCTURES

The Life Story Of A Genius: Évariste Galois

by
Burak Can Koban

Department of Computer Engineering, Bogazici University

Bebek, Istanbul, Turkey

01.12.2021

Contents

1. Life

- Early Life

- Mathematician

- Political Activist

- Final Days

2. Contributions to Mathematics

- Galois Field (Finite Field)

- Galois Theory

Last Words of Galois

"Don't cry, Alfred! I need all my courage to die at twenty!"

1. Life: Early Life

- Galois was French mathematician and genious.
- He was born on 25 October 1811 and unfortunately died on 31 May 1832 at **20 years old**.
- His **father** was a Republican and was a mayor of the village.
- His **mother** was a daughter of a jurist and fluent reader Latin and classical literature. She was responsible for Galois's education for his first twelve years.
- At the age of 14 and 15, he was started reading advanced mathematics papers especially **Joseph-Louis Lagrange's**.

4

Mathematician
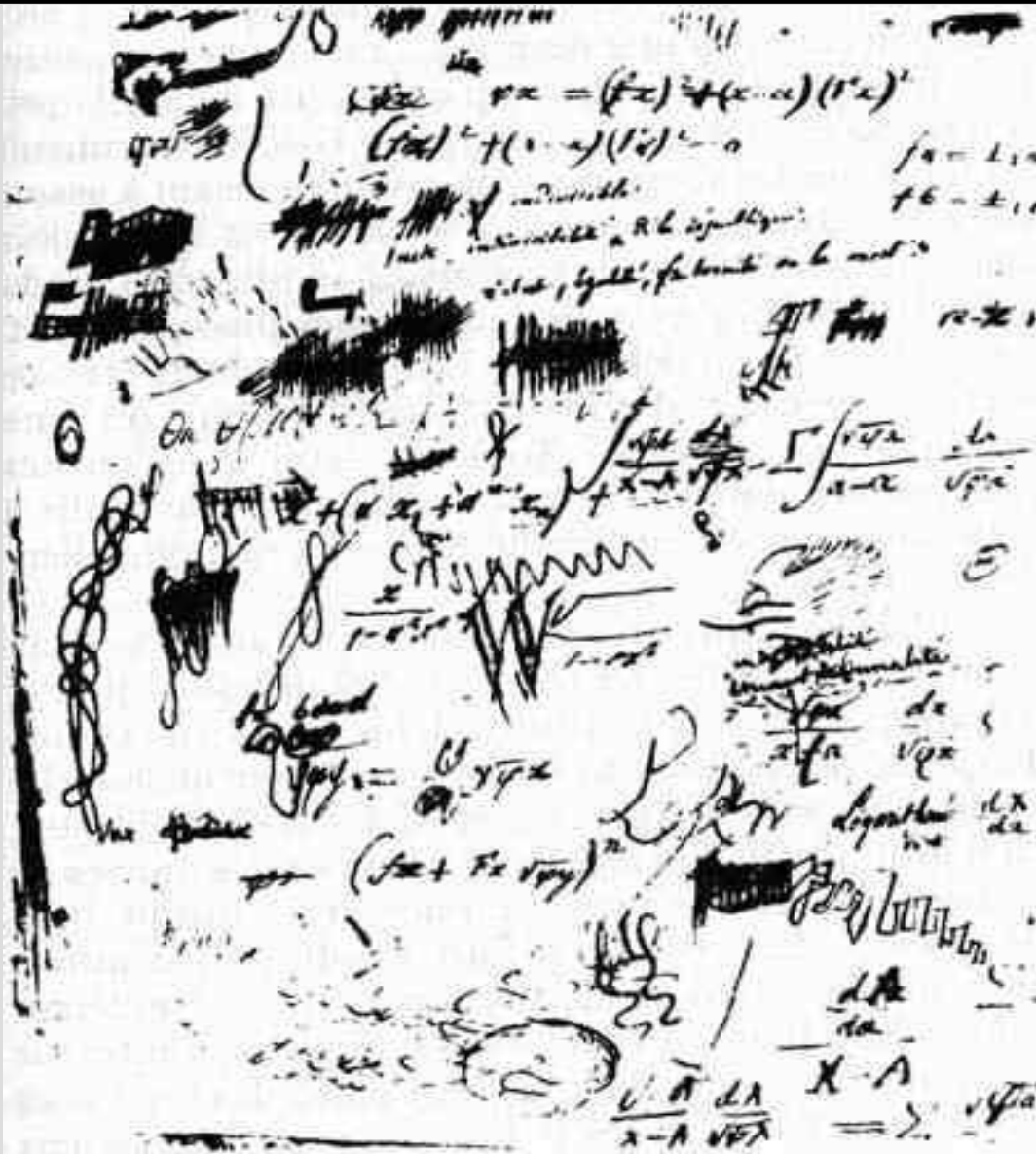
Galois's Handwriting

- In 1828, he attempted the entrance examination for the **École Polytechnique.**
- In 1829, he lost his father by suicide because of political reasons. A couple of days later, Galois made his second and last attempt to enter the **Polytechnique** and failed again.
- Galois had a problem. He was very smart, but his writings were thought as **incomprehensible** and **unclear**.
- After the second failure, Galois decided to enter **École normale**. His examiner is told about Galois that:

"*This pupil is sometimes obscure in expressing his ideas, but he is intelligent and shows a remarkable spirit of research*."

5

Political Activist

- Galois is lived in the times when France had many politacally problems.

- In 1830, **July Revolution** also known as **Second French Revolution** was happenning. Although Galois was very motivated to attend movements, he and his friends are locked in the school by the director of École Normale.

- Later, Galois wrote a letter about him and published in the school's newspaper. He was dismissed from the school becaue of his criticisms he wrote about the diretor.

- He joined to the Republican artillery unit of the National Guard.

- The unit was disbanded, soon after Galois became a member, because of the fear fear that they might destabilize the government.

- Galois was **arrested twice** because of political reasons.

Final Days

Illustration of the Duel

- On 30 May 1832, Galois lost a duel against his opponent and lost his life.

- The reason behind the duel still is not certain. However, there are strong evidences shows that it was about a woman Galois was attracted.

Final Days

- Day before the duel, Galois assembled his all-mathematical studies and sent them to his friend Chevalier with a letter attached.

- Galois wanted from his friend to pass his studies to the best mathematicians of these days:

  Gauss and **Jacobi**.

- "*Ask Jacobi or Gauss publicly to give their opinion, not as to the truth, but as to the importance of these theorems. Later there will be, I hope, some people who will find it to their advantage to decipher* all this mess.* "

- Finally, in 1843, 11 years after his death, **Joseph Liouville** reviewed his manuscript and make it possible to publish them in an important mathematical journal.

*decipher: to decode or decrypt
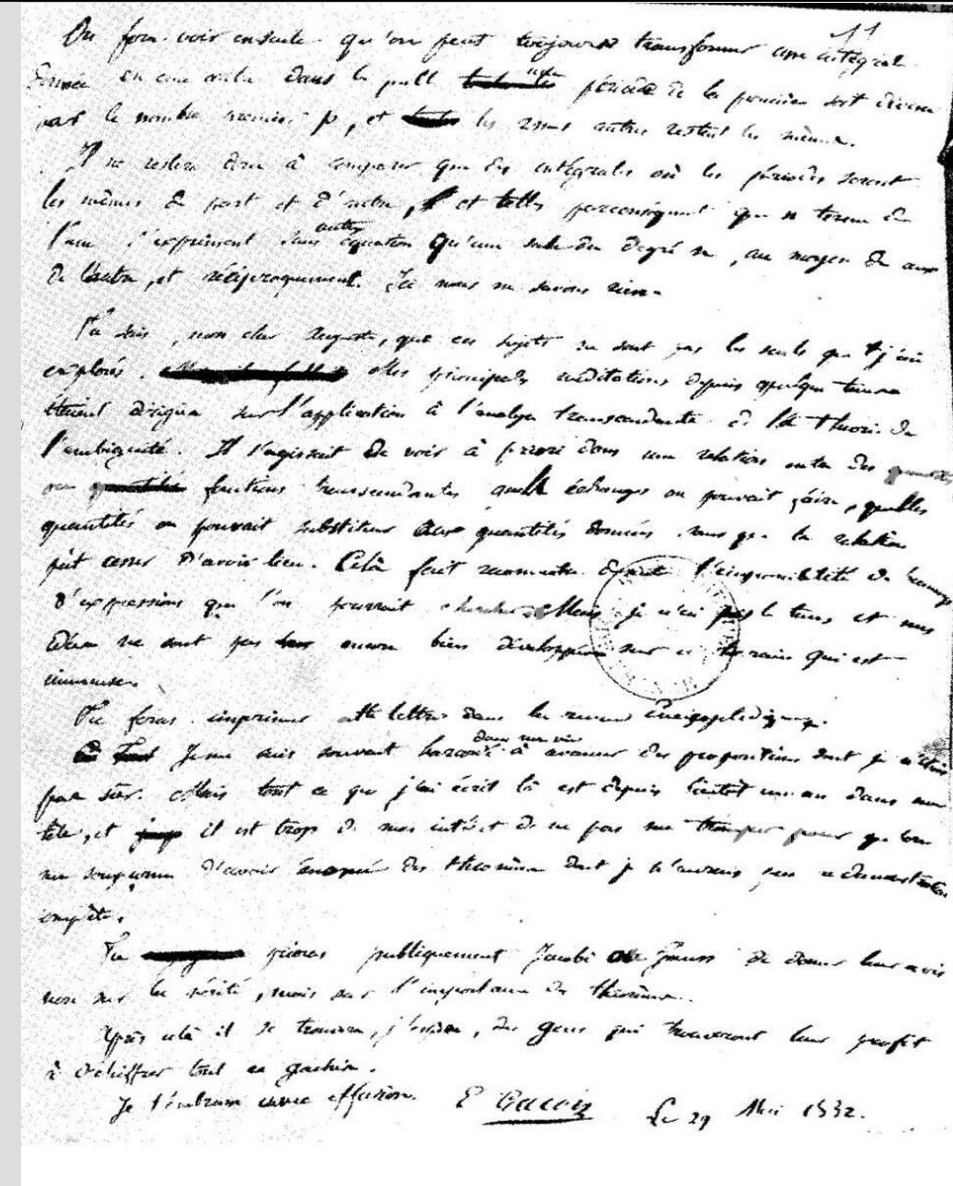
The final page of Galois's mathematical testament

8

2. Contributions to Mathematics: Named After

- Absolute Galois group
- Differential Galois theory
- Galois closure
- Galois cohomology
- Galois connection
- Galois/Counter Mode
- Galois covering
- Galois (crater)
- Galois deformation

- Galois descent
- Galois extension
- **Galois field**
- Galois geometry
- Galois group
- Galois LFSRs
- Galois module
- Galois representation
- **Galois theory**
- Inverse Galois problem

Recall

Single Binary Operation [A,+]

- Binary Operation

- Semigroup

- Monoid

- Group

- Abelian Group

Two Binary Operation [A,+,x]

- Ring

- Field

Galois Field (Finite Field)

- Definition: A is field, [A, +, x], is a ring such that [A\{0}, x] is an abelian group. If A is finite, A is called finite field.

- How many elements?

3, 4, 6 or 7 etc.?

- The answer is p^k where p is a prime number and k is a positive integer.
- GF$\left(p^k\right)$
- Therefore, a finite field can have elements like:

- 3, 4 or 7 but not 6.

- The theory of Finite Fields was developed by Galois in his work addressing the problem of the solutions of polynomial equations (Galois Theory).

Galois Theory

The **Abel**–Ruffini theorem provides a counterexample proving that there are polynomial equations for which such a formula cannot exist.

Galois Theory provides a much more complete answer to this question, by explaining:
- Why it is possible to solve some equations, including all those of **degree four or lower.**
- Why it is not possible to solve in radicals for **most** equations of **degree five or higher**.

Galois theory implies also that
$$x^5 - x - 1 = 0$$

is the simplest equation that cannot be solved in radicals.

The central idea of Galois' theory is to consider permutations (or rearrangements) of the roots such that any algebraic equation satisfied by the roots is still satisfied after the roots have been permuted.

The END

Thank you

Questions?

References

- https://en.wikipedia.org/wiki/%C3%89variste_Galois
- https://en.wikipedia.org/wiki/Galois_theory#Galois'_writings
- https://www.math3ma.com/blog/what-is-galois-theory-anyway
- https://www.youtube.com/watch?v=Mc0bvea6G3I&t=29s&ab_channel=Socratica
- https://mathshistory.standrews.ac.uk/Biographies/Galois/#:~:text=%C3%89variste%20Galois%20was%20a%20French,young%20after%20fighting%20a%20duel.
- https://www.britannica.com/biography/Evariste-Galois
- Handouts