Presentation on

GALOIS FIELD

Presented To:

A.R.M Mahamudul Hasan Rana

Assistant Professor

Computer Science & Telecommunication Engineering

Presented By:

Mohammad Borhan Uddin

ID: ASH2101008M

Introduction

In mathematics, *Galois theory*, originally introduced by **Évariste Galois**, provides a connection between field theory and group theory.

Évariste Galois (1811 - 1832)
Pronunciation: eh-vah-reest gah-lwah

Évariste Galois Life

Not a brilliant mathematician, but he was also a political activist.

In 1830, the **July Revolution** ***(7 August 1830)*** **overthrew King Charles X**, replacing him with **Louis-Philippe**, the so-called "Citizen King."

At first, Galois believed this change **would bring true democracy** to France, but he soon realized that the new monarchy still f**avored the wealthy and powerful.**

- Galois became a **committed Republican**, advocating for a people's government.
- He joined the revolutionary organization ***Société des Amis du Peuple (Society of the Friends of the People).***
- He was **arrested several times** for his outspoken criticism of the monarchy.
- Galois even **missed one of his mathematics exams** to take part in a political protest!
- **In 1831, he was imprisoned** for allegedly plotting against the government and possessing weapons.

Revolution in France: an eyewitness account - archive, 1830 - theguardian.com
https://www.theguardian.com/world/2020/aug/07/revolution-in-france-eyewitness-account-1830
https://en.wikipedia.org/wiki/July_Revolution

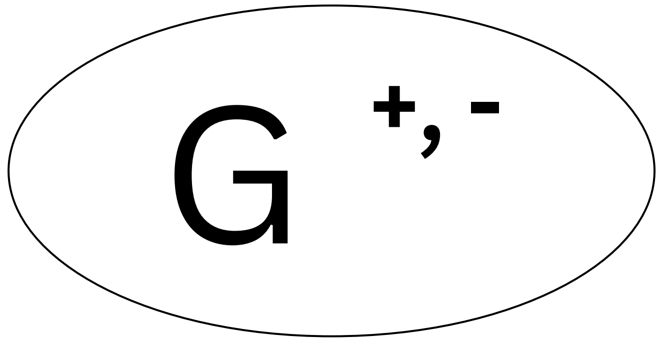
After his release from prison, Galois remained deeply involved in revolutionary circles.

In May 1832, he was killed in a mysterious duel at just 20 years old.

Group → Ring → Field → Galois field

1. Group Theory

A group is a set of elements G together with an operation ◯ which combine two elements of G.

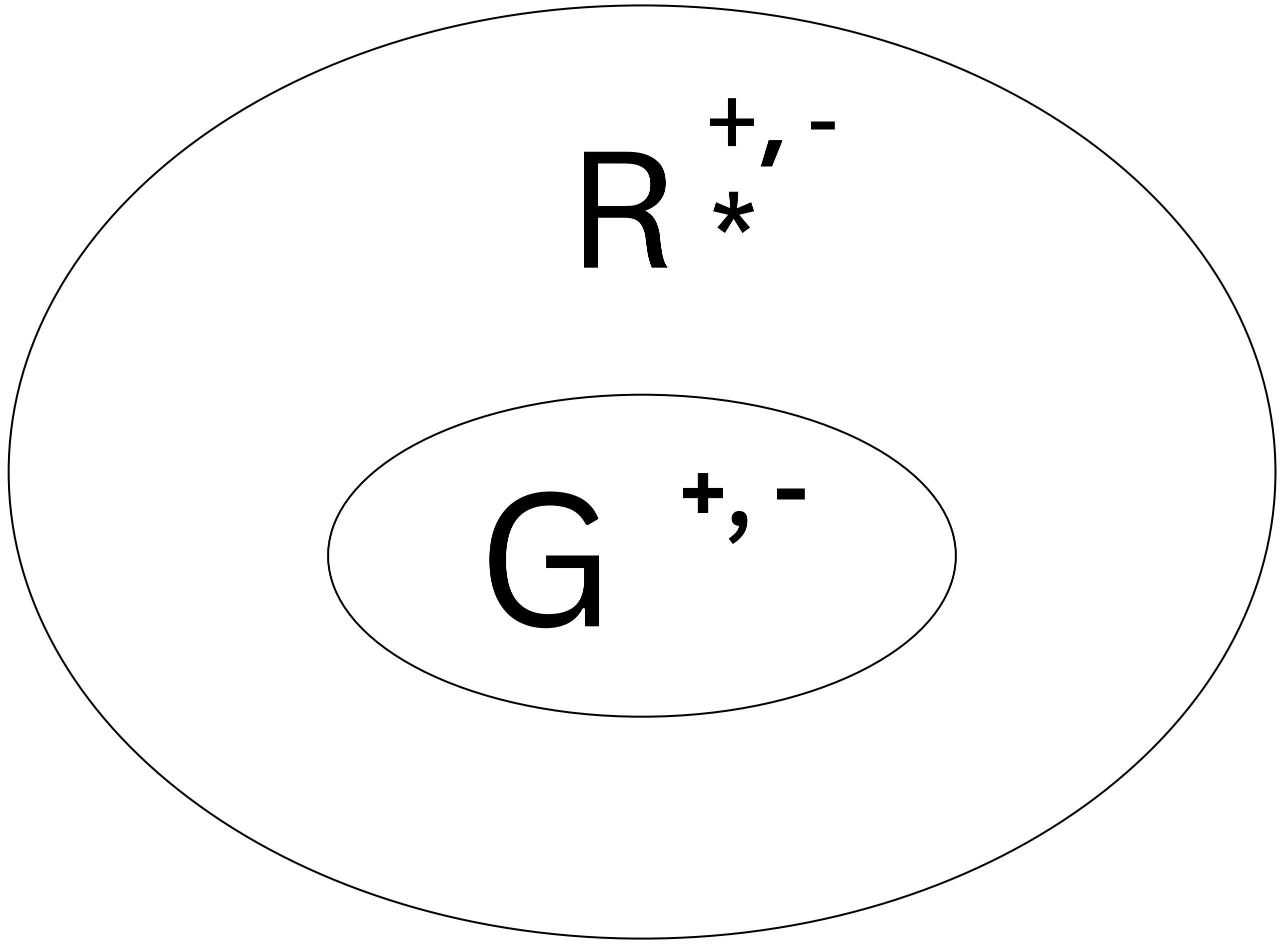


- The group operation ○ is **closed**. That is, for all a, b ∈ G, it holds that a ○ b = c ∈ G.
- The group operation is **associative**. That is, a ○ (b ○ c) = (a ○ b) ○ c for all a, b, c ∈ G.
- There is an element 1 ∈ G, called the **neutral element** (or identity element), such that a ○ 1 = 1 ○ a = a for all a ∈ G.
- For each a ∈ G there exists an element a^{-1} ∈ G, called the **inverse** of a, such that a ○ a^{-1} = a^{-1} ○ a = 1.
- A group G is **abelian (or commutative)** if, furthermore, a ○ b = b ○ a for all a, b ∈ G.

2.RING

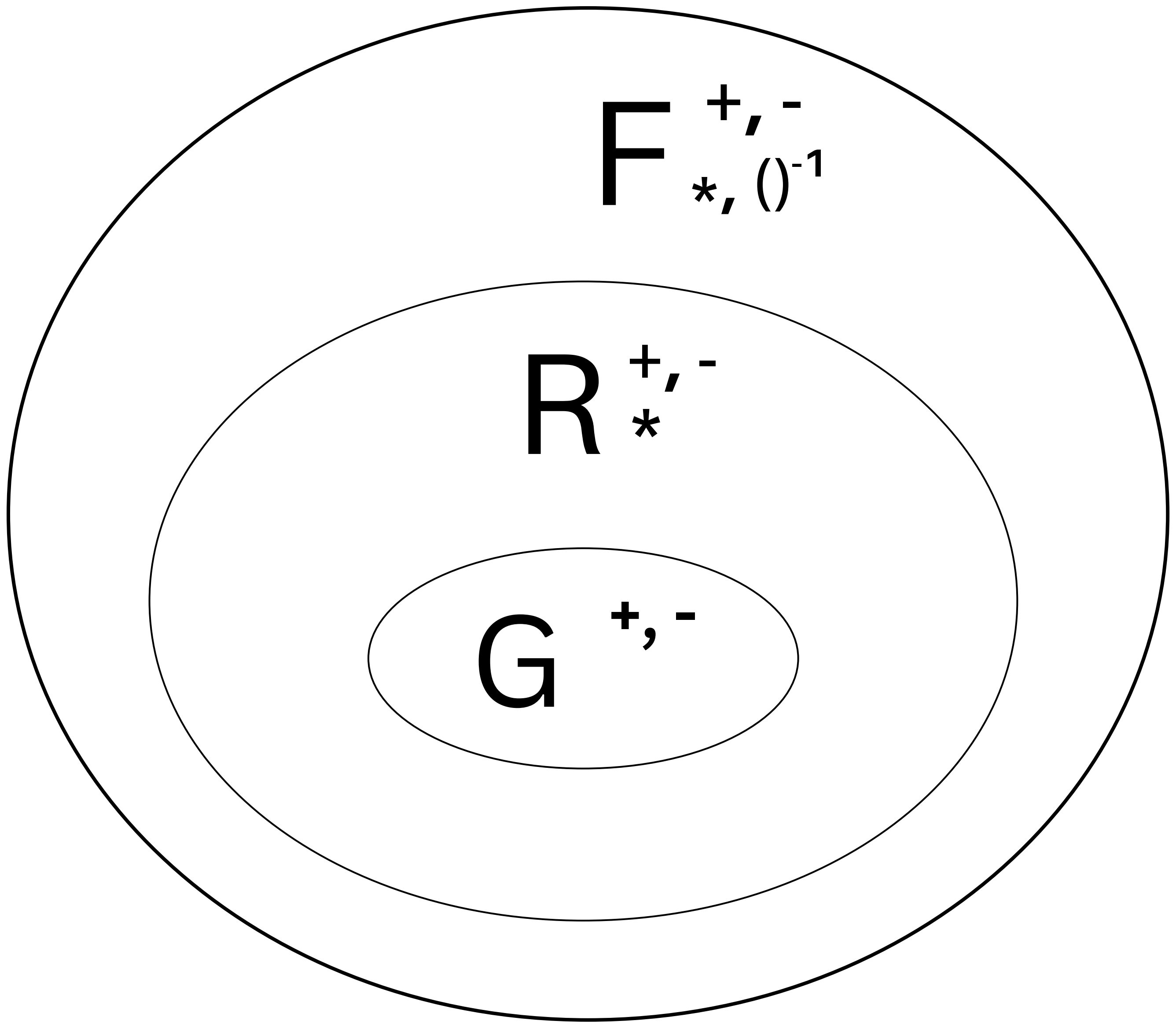
A ring is a set that has two operations, usually written as:

- addition (+)
- multiplication (·)



3.FIELD

In order to have all four basic arithmetic operations (i.e.. addition, subtraction, multiplication, division) in one structure, we need a set which contains an additive and a multiplicative group. This is what we call a field.



A field is a set of numbers in which we can add, subtract, multiply and divide.

Field Types

INFINITE

$\mathbb{R}$

FINITE
/GALOIS FILED

Finite Field

A finite field is a field with a finite field order also called a *Galois field.*

<u>The Existence Theorem</u>

A finite field of order q exists if and only if $q = p^n$ for some prime number p and positive integer n.

Example:

(1) There is a Galois field with 13 elements : $GF\left(13^1\right)$

(2) There is a finite field with 81 elements : $GF\left(3^4\right)$

(3) There is a finite field with 256 elements : $GF\left(2^8\right)$

(4) There is not a finite field with 12 elements : $GF\left(2^2 \times 3\right) \neq p^n$

$$\begin{tikzcd}
 & GF\left(p^m\right) \arrow[dl, "m=1"'] \arrow[dr, "m>1"] & \\
GF\left(p\right) & & GF\left(p^m\right)
\end{tikzcd}$$

Prime field — Extension Field

Prime Field

The elements of prime field of GF(p) are the

$$GF(p) = \{0, 1, \ldots, P - 1\}$$

Example:

$GF(2) = \{0,1\}$

$GF(7) = \{0,1, 2, 3, 4, 5, 6\}$

1. **Addition & Substraction**

$GF(7) = \{0,1, 2, 3, 4, 5, 6\}$

$$c = 5 + 6 = 11 \equiv 4 \ \ mod7$$

2. Multiplication

$$c = 5 \times 6 = 30 \equiv 2 \ \ mod7$$

3. Inversion

$a \in GF(p)$

The inverse a^{-1} must satisfy

$$a \cdot a^{-1} \equiv 1 \bmod p$$

(Using Extended Euclidian Algorithm)

EXTENSION FIELD (2^m)

The element of $GF(2^m)$ are polynomials

$$a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \ldots + a_1 x + a_0 = A(x) \in GF(2^m)$$

$$a_i \in GF(2) = \{0, 1\}$$

Example:

$GF(2^3), m = 3$

$A(x) = a_2 x^2 + a_1 x + a_0$

$$GF(2^3) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$$

a2	**a1**	**a0**
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

Extension Field (2^m)

1. Addition and Substraction

$$A(x), B(x) \in GF(2^m)$$

$$C(x) = A(x) + B(x) = \sum_{i=0}^{m-1} c_i x^i \qquad c_i = (a_i + b_i) \bmod 2$$

$$C(x) = A(x) - B(x) = \sum_{i=0}^{m-1} c_i x^i \qquad c_i = a_i - b_i = (a_i + b_i) \bmod 2$$

$$\text{Addition } mod\ 2 = \text{Substraction } mod\ 2$$

Extension Field (2^m)

Example

$$A(x) = x^2 + x + 1, B(x) = x^2 + 1$$

$$C(x) = A(x) + B(x) = (2x^2 + x + 2)\ mod\ 2 = x$$

2. Multiplication

$$C(x) = A(x) \times B(x) \text{ modulo } 2 = C'(x)$$

Reduce $C'(x)$ modulo a polynomial that "behaves like a prime".

Which is called irreducible polynomial $P(x)$

$$P(x) = \sum_{i=0}^{m} P_i x^i,\ P_i \in GF(2)$$

$$C(x) = A(x) \cdot B(x)\ mod\ P(x)$$

Extension Field (2^m)

$$A(x) = x^2 + x + 1, B(x) = x + 1 \quad \in GF(2^3)$$

$$C(x) = A(x) \cdot B(x) \text{ modulo } 2 = x^4 + x^3 + x + 1 = C'(x)$$

$$P(x) = \sum_{i=0}^{m} Pix^i = P_0x^0 + P_1x^1 + P_2x^2 + P_3x^3,\ P_i \in GF(2)$$

$$= x^3 + x + 1$$

Divide $C'(x)$ by $P(x)$ and find the remainder

$$C(x) = x^2 + x = A(x) \cdot B(x)\ mod\ P(x)$$

Extension Field (2^m)

$$A(x) = x^2 + x + 1, B(x) = x + 1 \quad \in GF(2^3)$$

$$C(x) = A(x) \cdot B(x) \text{ modulo } 2 = x^4 + x^3 + x + 1 = C'(x)$$

$$P(x) = \sum_{i=0}^{m} Pix^i = P_0x^0 + P_1x^1 + P_2x^2 + P_3x^3,\ P_i \in GF(2)$$

$$= x^3 + x + 1$$

Divide $C'(x)$ by $P(x)$ and find the remainder

$$C(x) = \ x^2 + x \ = A(x) \cdot B(x)\, mod\, P(x)$$

Galois field in AES

SubBytes (Substitution Step)

- SubBytes is the first step in each AES round.
- It replaces each byte in the 4×4 matrix with a new byte using an S-box (Substitution box).
- The S-box is a fixed table that gives one output byte for each input byte.
- This makes the data non-linear and adds confusion, which means the relationship between the key and ciphertext becomes harder to guess.

S-Box

- How it's created: The values are carefully constructed using mathematical operations in the finite field GF(2^8) including:
  - Taking the multiplicative inverse of each byte (except 0, which maps to 0).
  - Applying an affine transformation over GF(2) (simple bitwise operations).

byte → GF(2^8) inverse → affine → S-box

Galois field in AES

MixColumn

MixColumn is a crucial part of the Diffusion Layer in AES.

To provide diffusion by mixing the data within each column of the state matrix. A change in a single input bit will affect all output bits after this operation.

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \times \begin{pmatrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{pmatrix}$$

B_0...B_3 are the 4 bytes of the input column.
C_0...C_3 are the 4 bytes of the transformed output column.
01, 02, 03 are hexadecimal values representing elements in GF(2^8).

Calculate : A3 * 02

$$A3(hex) = 10100011(binary) = x^7 + x^5 + x + 1$$

$$02(hex) = 00000010 = x^1$$

THANK YOU!