

15 Finite Galois Field

Finite Field

Definition 15.1. Galois field, is a field with a finite number of elements. A finite field with q elements is denoted as \mathbb{F}_q (or GF(q)).

Prime Field

Theorem 15.1. If p is prime number, Then \mathbb{Z}_p prime field \mathbb{F}_p .

For example $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \dots, \mathbb{Z}_p = \mathbb{F}_p$ are field.

Remark 15.1. If the positive integer n is composite, \mathbb{Z}_n is not a field.

For example \mathbb{Z}_4 , \mathbb{Z}_6 , \mathbb{Z}_8 , \mathbb{Z}_9 , ... are not field.

Order of a Finite Field

Definition 15.2. The **order** of a finite field \mathbb{F}_q is the number of distinct elements in \mathbb{F}_q (denoted by $|\mathbb{F}_q|$).

For example $|\mathbb{F}_p| = p$, where $\mathbb{F}_p = \{0, 1, 2, \dots p-1\}$.

If p = 7, $|\mathbb{F}_7| = 7$, where $\mathbb{F}_p = \{0, 1, 2, 3, 4, 5, 6\}$

Order of a Finite Field

Definition 15.3. The field \mathbb{F}_{p^n} , also denoted as $GF(p^n)$, is a **finite field** with p^n elements, where:

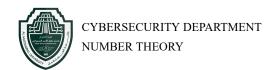
- p is a prime number (the **characteristic** of the field).
- n is a positive integer (the **degree** of the field extension).

It is an extension field of \mathbb{F}_p , meaning it contains \mathbb{F}_p as a subfield.

Construction

The field \mathbb{F}_{p^n} is constructed as follows:

1. Consider the prime field $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}.$



- 2. Choose an irreducible polynomial f(x) of degree n over \mathbb{F}_p .
- 3. Define \mathbb{F}_{p^n} as the set of all polynomials in x of degree less than n with coefficients in \mathbb{F}_p , where arithmetic is performed modulo f(x).

Properties

- The multiplicative group $\mathbb{F}_{p^n}^{\times} = \mathbb{F}_{p^n} \setminus \{0\}$ of order $p^n 1$, meaning there exists a **primitive** element g such that every nonzero element can be written as g^k for some k.
- Every element of \mathbb{F}_{p^n} satisfies the equation:

$$x^{p^n} = x$$

which characterizes the field.

Example: \mathbb{F}_{2^3}

Consider p=2 and n=3. The field \mathbb{F}_{2^3} has $2^3=8$ elements.

To construct it:

- Start with $\mathbb{F}_2 = \{0, 1\}$.
- Choose an irreducible polynomial of degree 3 over \mathbb{F}_2 , such as $f(x) = x^3 + x + 1$.
- The elements of \mathbb{F}_{2^3} are represented as:

$$\{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$$

where α is a root of f(x) and a primitive element.