Finite Fields

Areas for Discussion

- Fundamentals
  - Finite Field
  - Fields - Abstraction of Real Number System
  - Subsets of \( \mathbb{R} \)
  - Four Operations to Two Operations
- Algebraic Structures
  - Groups, Abelian Groups, Rings, Commutative Rings, Integral Domains and Fields

Fundamentals

- Finite Field – a Field with a finite number of elements
  - For example \( \mathbb{Z}_p = \{0, 1, 2, \ldots, \ldots p-1\} \)
  - Field an abstraction of our Real Number System
- Subsets of \( \mathbb{R} \) - See next slide
- Four Operators to Two Operators
  - Addition = addition and subtraction
  - Multiplication = multiplication and division
Fundamentals

- Subsets of Real Numbers

\[ \mathbb{N}^+ = \{1, 2, 3, 4, 5, 6, 7, \ldots\} \]
\[ \mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, 7, \ldots\} \]
\[ \mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\} \]
\[ \mathbb{Q} = \left\{ \frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N}^+ \right\} \]

Algebraic Structures

1. Closure under Addition
2. Associativity of Addition
3. Additive Identity
4. Additive Inverse
5. Commutativity of Addition
6. Closure under Multiplication
7. Associativity of Multiplication
8. Distributive Laws (left and right)
9. Commutativity of Multiplication
10. Multiplicative Identity
11. No Zero Divisors
12. Multiplicative Inverse

Fields – Finite and Infinite

Order – finite and infinite

Let \( G \) be a group
\( \alpha \in G \Rightarrow \alpha^\prime \in G \)

If there is a positive integer \( n \) for which
\( \alpha^\prime = e \) the identity then the least such integer
\( n \) is said to be the order of \( \alpha \).

If no such \( n \) exists then \( \alpha \) is of infinite order
and \( G \) is said to be of infinite order.

Characteristic - finite and infinite

Let \( F \) be a Field (or Ring)
\( \alpha \in F \Rightarrow \sum \alpha \in F \)

In particular \( 1 \in F \Rightarrow \sum 1 \in F \)

If there is a least positive integer \( j \) for which
\( \sum 1 = 0 \) then the field is said to have characteristic \( j \)

If no such \( j \) exists then field is said to have characteristic \( \infty \) (or 0 in older texts)
Polynomial Arithmetic

Polynomials are of the form:

\[ f(x) = \sum_{i=0}^{n} a_i x^i = a_0 x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \]

A Monic Polynomial has coefficient \( a_n = 1 \)

The degree of a polynomial (denoted by \( \deg f(x) \)) is the highest power of \( x \) in the polynomial.

Addition and Subtraction

These are defined in terms of addition only:

Let \( f(x) = \sum_{i=0}^{n} a_i x^i \) and \( g(x) = \sum_{i=0}^{m} b_i x^i \) then we define

\[ f(x) + g(x) = \sum_{i=0}^{\max(n, m)} (a_i + b_i) x^i \]

Multiplication

These are defined as follows:

Let \( f(x) = \sum_{i=0}^{n} a_i x^i \) and \( g(x) = \sum_{j=0}^{m} b_j x^j \) then we define

\[ f(x) \cdot g(x) = \sum_{i=0}^{n+m} (\sum_{j=0}^{i} a_j b_{i-j}) x^i \]

Division

Division between two polynomials \( f(x) \) and \( g(x) \) with \( f(x)/g(x) \) is described in terms of two additional polynomials \( h(x) \) and a remainder \( r(x) \) such that

\[ \text{Deg } h(x) = \deg \{ f(x) - g(x) \} \]

and

\[ 0 < r(x) < \deg g(x) \]

Example

\( f(x) = 3x^4 - 7x^3 + 2x - 1 \)

\( g(x) = x^2 - 3x + 2 \)

\( h(x) = 3x^2 + 2x \)

\( r(x) = -2x - 1 \)

Note (in checking calculations)

\[ f(x) = g(x) \cdot h(x) + r(x) \iff \frac{f(x)}{g(x)} = \frac{h(x)}{g(x)} + \frac{r(x)}{g(x)} \]
Finite Fields

The finite field \( F_p \) is also known as the Galois Field GF(p) after Evariste Galois. For \( q = 1 \), we have \( F_p = \mathbb{Z}_p \). We note that this is a field iff \( p \) is a prime number. For \( q > 1 \), a natural number we construct the field \( \mathbb{Z}_p[x] / f(x) \) with \( f(x) \) an irreducible Polynomial. Note \( p^q = \) number of elements in the Finite (Galois) Field.

Example

- We consider the finite field with \( p = q = 2 \)
- We are looking for a finite field with 4 elements
- This is given by an irreducible polynomial \( f(x) \) of degree \( q = 2 \) over \( \mathbb{Z}_2[x] \)
  - A quadratic polynomial with coefficients 0 or 1
- The elements can already be stated as
  - 0, 1, \( x \), \( x + 1 \)

Example

- We require \( f(x) \) and \( \mathbb{Z}_2[x] / f(x) \) to aid us in calculating the products (multiplication)
- We first consider addition and construct an addition table
- We next consider multiplication and construct a multiplication table
- We then consider inverses of non zero elements

Summary

- Fundamentals
  - Finite Field
  - Fields - Abstraction of Real Number System
  - Subsets of \( \mathbb{R} \)
  - Four Operations to Two Operations
- Algebraic Structures
  - Groups, Abelian Groups, Rings, Commutative Rings, Integral Domains and Fields

Summary

- Fields – Finite and Infinite
  - Finite Order and Infinite Order
  - Characteristic of a Field
- Polynomial Arithmetic
  - Polynomials, Polynomials and Sigma Notation, Monic, Degree
  - Addition, subtraction, Multiplication and Division
- Finite Fields – GF(p) and GF(p^q)