Finite Field

AK Bhateja

Ring

- Definition: A ring is a set R together with two binary operations, '+' and '·', called addition and multiplication, such that:
  – (R, +) is an abelian group
  – the product $r \cdot s$ of any two elements $r, s \in R$ is in R
  – Multiplication is associative
  – for all $r, s, t \in$ R: $r \cdot (s + t) = r \cdot s + r \cdot t$ and

  $$(r + s) \cdot t = r \cdot t + s \cdot t$$

  (multiplication is distributive over addition).

Ring

- Commutative Ring: Ring R is said to be commutative if multiplication is commutative.

  Example: Z set of integers and nZ are commutative rings
- Ring with unity: If there is an element 1 in R such that $r \cdot 1 = 1 \cdot r = r$ for any $r \in R$, then 1 is called an identity (or unit) element. As for groups the identity is unique if it exists.
- Zero divisors: If in a ring R there exists r and s in R s.t. $rs = 0$ when $r \neq 0$, $s \neq 0$, then r is called a left zero divisor and s a right zero divisor.
- Ring without zero divisors: A ring R is without zero divisors if $rs = 0 \Rightarrow r = 0$ or $s = 0$ for all $r, s \in R$, then R is called ring without zero divisors.

Integral Domain & Division Ring

- Integral domain: A ring is called integral domain if it
  - (i) is commutative
  - (ii) has unit element
  - (iii) is without zero divisors.

  Example: Z set of integers is integral domain
- Skew field or a division ring: A ring R is called division ring or skew field if it
  - (i) has unity
  - (ii) is such that each non-zero element possesses multiplicative inverse

  Example. Skew field: Set of matrices of the form

$$\begin{pmatrix} a & \bar{b} \\ -b & \bar{a} \end{pmatrix}$$

Field

- Field: A ring is called a field if it
  (i) is commutative
  (ii) has unity
  (iii) is such that every non-zero element possesses multiplicative inverse

  Example: Q, R, and C are fields.

  Let p be prime. Z_p is a field.

  $Z_p = \{0, 1, 2, 3, \ldots, p - 1\}$

Theorem: Every field is an integral domain

Proof: Let $(F, +, \cdot)$ be a field

Let $a, b \in F$, with $a \neq 0$

Since $a \in F$, therefore a^{-1} exists.

Let $ab = 0 \Rightarrow a^{-1}ab = a^{-1}0 \Rightarrow b = 0$

Similarly let $b \neq 0$ but $ab = 0 \Rightarrow ab\, b^{-1} = 0\, b^{-1} \Rightarrow a = 0$

Thus F is without zero divisors. Hence F is an integral domain

Converse of this is not true.

Example: Z set of integers is integral domain but not a field.

Let p be prime. Z_p is a field. $Z_p = \{0, 1, 2, 3, \dots, p-1\}$

Theorem: The integer ring $(Z_n, +, .)$ is a field if and only if n is prime.
Proof: Let n be prime & $m \in \{0, 1, \ldots, n-1\}$ and suppose that m has no inverse in Z_n.
Then none of the n numbers $0m, 1m, 2m, \ldots, (n-1)m$ under mod n can be equal to 1.
So this list must contain two numbers which are equal in Z_n.
Hence we have $im \equiv jm \pmod{n}$ or $(i-j)m \equiv 0 \pmod{n}$ for some i, j with $0 < i - j < n$.
Since p is prime one of the numbers $i - j$ or m must be a multiple of n and considering their ranges the only possibility is $m = 0$
Hence 0 is the only element with no inverse and so Z_n is a field
To complete the proof we show that if n is not prime, then Z_n is not a field.
If $n \geq 2$ is not prime then we can write $n = qr$ for some $q, r \geq 2$. But now we have two nonzero elements q and r whose product is the zero element of Z_n.
Since this is not possible in a field it follows that Z_n is not a field.

- Definitions. A subset U of a field F is called a subfield of F, in symbols $U \leq F$, if U is a subset of F and U is a field with respect to the operations in F.

  Field $(F, +, \cdot)$ is called an extension field (or extension) of the field $(U, +, \cdot)$
- U is a subfield of F, and $U \neq F$, then $(U, +, \cdot)$ is called a proper subfield of $(F, +, \cdot)$, in symbols $U < F$.
- Prime field: A field P is called a prime field if it has no proper sub fields.

  Example: Q is a prime, R is not prime.

  The field Z_p is prime field.

Characteristics

- Definition. Characteristic of a ring/field: The characteristic of R is the smallest natural number k with $k\,r = r + \cdot\cdot\cdot + r$ (k-times) equal to 0 $\forall\ r \in R$. Then we write char $R = k$.
- Characteristic is order under addition
- If no such k exists, then R is said to be of characteristic zero or infinite.
- Z has characteristic 0, because 1 has infinite order under addition.
- Z_n has characteristic n
- If $Z_6 = \{0, 1, 2, 3, 4, 5\}$, characteristic of the ring $(Z_6, +_6, \times_6)$ is 6 since $6x = 0\ \forall\ x \in \mathrm{R}$
- So if k = char R, all elements in the group (R, +) have an order dividing k.

Theorem: The characteristic of an integral domain D is either 0 or a prime number.

Proof; (By contradiction): Suppose that it is not true that the characteristic is either 0 or prime.

Then the characteristic is a +ve non-prime number. Let it be mn.

Then $mn\,(r) = 0$, $\forall\ r \in R$, by definition of characteristic. Therefore

$0 = r + r + r + \dots + r$ (mn times)

$0 = (r + r + \dots + r) + (r + r + \dots + r) + \dots + (r + r + \dots + r)$ (m groups of n r's)

$0 = n\,r + n\,r + \dots + n\,r$ (m times) $= n\,mr = (n)(m\,r)$ or $m(n\,r)$

But neither nr nor mr is 0

This means D has zero divisors, contradicting the fact that D is an integral domain.

This contradiction proves the theorem.

Characteristic of a field

- Every field is an integral domain, therefore the characteristic of any field is either 0 or a prime number.
- A field of non-zero characteristic is called a field of finite characteristic or positive characteristic or prime characteristic.

Vector Space

- Definition. Let $(F, +, \cdot)$ be a field. A nonempty set V is said to be a vector space over the field F if
  1. Set V is an abelian group under '+'
  2. For every $a \in F$, $\alpha \in V$; $a\alpha \in V$ i.e. V is closed under '·' (scalar multiplication)
  3. The two compositions '+' (vector addition) and '·' (scalar multiplication) satisfy the following:

     (i) $a \cdot (\alpha + \beta) = a \cdot \alpha + a \cdot \beta \;\; \forall\, a \in F, \;\; \forall\, \alpha, \beta \in V$

     (ii) $(a + b) \cdot \alpha = a \cdot \alpha + b \cdot \alpha \;\; \forall\, a, b \in F, \;\; \forall\, \alpha \in V$

     (iii) $(a\,b) \cdot \alpha = a \cdot (b \cdot \alpha) \;\; \forall\, a, b \in F, \;\; \forall\, \alpha \in V$

     (iv) $1 \cdot \alpha = \alpha \;\; \forall\, \alpha \in V$ & 1 is the unity element of the field F.

The elements of field F are called scalars and the elements of elements of the vector space are called vectors.

Vector space V over F is denoted by $V(F)$

Example 1: Let F be a field and let K be a field which contains F as a subfield i.e. $F \leq K$. We consider K as a vector space over F.

Justification: K is a field, therefore $(K, +)$ is an abelian group.

$F \leq K$, therefore $a\alpha \in K$ for every $a \in F$, $\alpha \in K$

1 is the unity element of K, then 1 is also unity element of the subfield F.

The following conditions will also be true.

(i) $a(\alpha + \beta) = a\alpha + a\beta \;\; \forall\, a \in F, \;\; \forall\, \alpha, \beta \in V$

(ii) $(a + b)\,\alpha = a\alpha + b\alpha \;\; \forall\, a, b \in F, \;\; \forall\, \alpha \in V$

(iii) $(a\,b)\,\alpha = a\,(b\alpha) \;\; \forall\, a, b \in F, \;\; \forall\, \alpha \in V$

(iv) $1\alpha = \alpha \;\; \forall\, \alpha \in V$ and 1 is the unity element of the field F.

Example 2: C is a vector space over R.

Note: If F is any field, then F itself is a vector space over the field F.

Basis of a Vector Space

- Definition. A subset S of a vector space $V(F)$ is said to be a basis of $V(F)$ if
  (i) S consists of linearly independent vectors.
  (ii) S generates $V(F)$ i.e. $L(S) = V$ i.e. each vector in V is a linear combination of a finite number of elements of S.

Example: A set S consisting of n vectors

$e_1 = (1, 0, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, … , $e_n = (0, 0, 0, \ldots, 1)$ is a basis of $V_n(F)$

- The number of elements in the basis S is called Dimension of the vector space.

  e.g. Dimension of $V_n(F)$ is n.

Polynomial over a field

- Let F be a field and let x (called an indeterminate) be any symbol not an element of F. Expression

  $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots$ where $a_0, a_1, a_2 \ldots$ are elements of F and only finite number of them are non-zero elements of F.

- Set of all polynomials over a Field F:

  $F[x] = \{a_0 + a_1 x + a_2 x^2 + \ldots \mid a_i \in F$ and only finite number of them are non-zero$\}$

Theorem: If F is a field, then the set $F[x]$ of all polynomials over F is an integral domain, not a field.

Proof: It is easy to prove that $F[x]$ is integral domain.

To prove $F[x]$ is not a field:

Let $f(x)$ be a non-zero polynomial.

Unity element of $F[x]$ is $1 + 0\,x + 0\,x^2 + \ldots$

deg[unit polynomial] = 0

Suppose $g(x)$ be a non-zero polynomial, which is inverse of $f(x)$.

$\deg\,[f(x).\ g(x)] = \deg f(x) + \deg g(x) > 0$,

while deg[unit polynomial] = 0

Thus $f(x)$ does not possess multiplicative inverse.

Therefore $F[x]$ is not a field.

Irreducible Polynomial

- Definition. Let $p, q \in R[x]$. We say that p divides q (denoted by $p \mid q$) if $q = p \cdot r$ for some $r \in R[x]$.

  If deg $q >$ *deg* $p > 0$, then p is called a proper divisor of q.
- Definition. **Irreducible polynomial**: A polynomial q with deg $q \geq 1$ which has no proper divisors is called irreducible.
- Every polynomial of degree 1 is, irreducible.
- A monic irreducible polynomial is called a **prime polynomial**
- In $Z_3[x]$, $x^2 + 2x$ has non-trivial divisors x, $x + 2$ and is not irreducible

- Definition. **(Mobius function):**

  The mapping $\mu : \mathrm{N} \to \{0, 1, -1\}$ defined by

  $\mu(1) = 1,$

  $\mu(p_1 \cdots p_t) = (-1)^t$ if p_i are distinct primes,

  $\mu(n) = 0,$ if $p^2 \mid n$ for some prime p

  is called the **Mobius function** or μ-function.

- The number of monic irreducible polynomials of degree m over Z_p is given by

$$N_p(m) = \frac{1}{m} \sum_{d/m} \mu(d) p^{m/d}$$

- The probability of a random monic polynomial of degree m in $Z_p[x]$ being irreducible over Z_p is

$$\frac{N_p(m)}{p^m} \approx \frac{1}{m}$$

- Euclidean Division: Let F be a field and $f, g \in F[x]$ with $g \neq 0$. Then there exist uniquely determined $q, r \in R[x]$ s.t.

  $$f = gq + r \quad \text{and} \quad deg\, r < \deg g.$$

- Greatest common divisor of two polynomials:

  Let f and $g \in F[x]$ with $f \neq 0$ *or* $g \neq 0$, then there exists a monic polynomial of greatest degree d in $F[x]$ s.t.

  $d \mid f$ and $d \mid g$ then $\gcd(f, g) = d$.

- The polynomials f and g are called relatively prime (or coprime) if $\gcd(f, g) = 1$.
- An element r of a field F is a root of the polynomial $p \in F[x]$ iff $x - r$ divides p.

Extension Field

- K is vector space over F. Suppose F is a field. Then a field K is called an extension of F if F is a subfield of K.
- If K is extension field of F then K is vector space over F.
- Degree of extension field: Dimension of vector space $K(F)$ is the degree of K. Degree of extension field is denoted by $[K : F]$.
- Finite field extension: Let K be an extension field of F. Then K is said to be a finite extension of F if the degree of K over F is finite.

Extension Field: Examples

- If F is any field then F can be regarded as a subfield of F. Therefore F can be thought of as an extension of F.
- The field C of complex numbers is a finite extension of the field R of real numbers.
- $[C : R] = 2$, because $\{1, i\}$ is basis of the vector space $C(R)$.

  The set $\{1, i\}$ generates the elements of C.

  Set $C = \{a + bi : a, b \in R\}$

Theorem. Let L be a finite extension of K and let K be a finite extension of F. Then

$$[L : K][K : F] = [L : F].$$

Proof: Let $\{\alpha_i \mid i \in \mathrm{I}\}$ be a basis of L over K and let $\{\beta_j \mid j \in \mathrm{J}\}$ be a basis of K over F.

It is not hard to verify that the $|I|\cdot|J|$ elements $\{\alpha_i \beta_j \mid i \in I, j \in J\}$ form a basis of L over F.

Theorem. Let F be a finite field of characteristic p. Then F contains p^n elements, where $n = [F : Z_p]$.

Proof: The field F, considered as a vector space over its prime field Z_p, contains a finite basis of n elements. Each element of F can be expressed as a unique linear combination of the n basis elements with coefficients in Z_p. Therefore there are p^n elements in F.

Let basis of F be $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ and α be any element of F, then $\alpha = a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n$ where $a_i \in Z_p$

Primitive elements

- Let F be a finite field with q elements. The multiplicative group $(F^*, \cdot)$ of the nonzero elements of F is cyclic of order $q - 1$.

$$F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}, \text{ where } \alpha^{q-1} = 1$$

- Such an element α is called a primitive root modulo q.
- A generator of the cyclic group of a finite field F is called a primitive element.

Constructing field extensions by adjoining elements

Example 1: Consider the field Q($\sqrt{2}$).

$$Q(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in Q\}$$

Multiplication works by

$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$.

$[Q(\sqrt{2}) : Q] = 2$, The set $\{1, \sqrt{2}\}$ is a basis of $Q(\sqrt{2})$.

Example 2: The field $Q(\sqrt{2}, \sqrt{3})$ is a finite extension of Q.

$Q(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} : a, b, c, d \in Q\}$

$[Q(\sqrt{2}, \sqrt{3}) : Q] = 4$.

Basis of $Q(\sqrt{2}, \sqrt{3})$ is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$

Algebraic & Transcendental elements

- Algebraic element: Let K be an extension field of F. An element $\alpha \in K$ is said to be algebraic over F, if there exists a non-zero polynomial $f(x) \in F[x]$ for which $f(\alpha) = 0$

  i.e. $\alpha \in K$ is algebraic over F if $\exists$ elements $a_0, a_1, \dots, a_n$ in F, not all 0, such that $a_0 + a_1 \alpha + \dots + a_n \alpha^n = 0$
- The degree of the minimal polynomial $f(x) \in F[x]$ for which $f(\alpha) = 0$ is called degree of an algebraic element α.
- Transcendental element: Let K be an extension field of F. An element $\alpha \in K$ is said to be transcendental over F if it is not algebraic over F.
- Example:

  $\alpha_1 = \sqrt{2}$, $\alpha_2 = \sqrt[3]{7}$ are algebraic over Q.

  π and e (both irrational numbers) are transcendental over Q but algebraic over the field of real numbers R.

Algebraic Field Extension

- A field extension $[K : F]$ is called **algebraic** if every element of K is algebraic over F.

  i.e. if every element of K is a root of some non-zero polynomial with coefficients in F.
- Field extensions that are not algebraic, i.e. which contain transcendental elements, are called **transcendental field extension**.
- For example, the field extension $[R : Q]$, that is the field of real numbers as an extension of the field of rational numbers, is transcendental, while the field extensions $[C : R]$ and $[Q(\sqrt{2}) : Q]$ are algebraic.

Splitting Field

- A polynomial $f(x) \in F[x]$ is said to *split* in an extension K *of* F if $f(x)$ factors completely into linear factors in $K[x]$.
- The field K is called a splitting field of $f(x)$ over F if $f(x)$ splits in K, but does not split in any proper subfield of K containing F.
- Degree of this extension field K is n (degree of the polynomial $f(x)$).
- Examples: C is splitting field of $x^2 + 1$ over R

Definition: Let K be a field and let $f(x) \in K[x]$ be a monic irreducible polynomial (prime polynomial) of degree n. Then

$$K[x]/(f) = \{a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \text{ where } a_0, a_1, \dots, a_{n-1} \in K\}$$

Theorem: Let K be a field and let $f \in K[x]$ be a monic irreducible polynomial (prime polynomial). Then $K[x]/(f)$ is a field.

Proof: $K[x]/(f)$ is a ring.

Let $g \in K[x]$ as a polynomial of degree less than f .

Since f is irreducible, and deg $g <$ deg f

By the Euclidean algorithm for polynomials

we obtain some $h, k \in K[x]$ with $gh + f\,k = 1$ as elements of $K[x]$.

$\Rightarrow$ $gh - 1 = -f\,k$ in $K[x]$

$\Rightarrow$ $gh = 1 \bmod f(x)$

$\Rightarrow$ Polynomial h is inverse of g under modulo $f(x)$.

Hence $K[x]/(f)$ is a field.

Note: For a prime p and positive integer n, there is an irreducible polynomial $f(x)$ of degree n in $Z_p[x]$, and $Z_p[x]/(f(x))$ is a field of order p^n.

Example: Consider field $Z_2 = \{0, 1\}$, then $Z_2[x]/(x^2 + x + 1)$ is a field of order 4.

The polynomial $x^2 + x + 1$ is irreducible in Z_2, because it has no root in Z_2.

Therefore $Z_2[x]/(x^2 + x + 1)$ is a field of order 4.

$Z_2[x]/(x^2 + x + 1) = \{a + b\alpha : a, b \in \mathrm{Z}_2$, where α satisfies $f(x)\}$

i.e., $\alpha^2 + \alpha + 1 = 0$,

which means that $\alpha^2 = \alpha + 1$.

Hence $Z_2[x]/(x^2 + x + 1)$ is a field with four elements:

$Z_2[x]/(x^2 + x + 1) = \{0, 1, \alpha, 1 + \alpha\}$.

For instance, $\alpha(1 + \alpha) = \alpha + \alpha^2 = \alpha + \alpha + 1 = 1$.

Addition & Multiplication tables of $Z_2[x]/(x^2 + x + 1)$

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

References

- Rudolf Lidl & Gunter Pilz, “Applied Abstract Algebra”, Springer
- I.N. Herstein, “Topics in Algebra”, Wiley
- Alfred J. Menezes, Pall C. van Oorschot, Scott A. Vanstone, “Handbook of Applied Cryptography”, CRC Press