Linear Algebra and Applications

Sartaj Ul Hasan

विद्याधनं सर्वधन प्रधानम्

Department of Mathematics
Indian Institute of Technology Jammu
Jammu, India - 181221

Email: sartaj.hasan@iitjammu.ac.in

Lecture 12

(Aug 21, 2019)

Introduction to Fields

Fields

- **Informal Definition:** A field is a system with universal addition, subtraction, multiplication, division (except by zero).
- **Formal Definition:** A field $\mathbb{F}$ is a non-empty set together with two operations $+$ (known as addition) and . (known as multiplication) which satisfies the following properties (axioms):

  (a). $< \mathbb{F}, + >$ satisfies the following properties w. r. t. addition

  1. **Closure property:** For every $x, y \in \mathbb{F}$, we have $x + y \in \mathbb{F}$.
  2. **Associative property:** $x + (y + z) = (x + y) + z$ for all $x, y, z \in \mathbb{F}$.
  3. **Existence of Identity Element:** There exist a unique element 0 (zero) in $\mathbb{F}$ such that $x + 0 = x = 0 + x$ for every $x \in \mathbb{F}$.
  4. **Existence of Inverse:** For each $x \in \mathbb{F}$, there exists a unique element $-x \in \mathbb{F}$ such that $x + (-x) = 0 = (-x) + x$.
  5. Commutative Property: $x + y = y + x$ for all $x, y \in \mathbb{F}$.

  Remark: With the properties as described in (a), $\mathbb{F}$ is abelian group w. r. t. addition.

Fields (Conti . . .)

(b). $< \mathbb{F}, . >$ satisfies the following properties w. r. t. multiplication.

1. **Closure property:** For every $x, y \in \mathbb{F}$, we have $x.y \in \mathbb{F}$.
2. **Associative property:** $x.(y.z) = (x.y).z$ for all $x, y, z \in \mathbb{F}$.
3. **Existence of Identity Element:** There exist a unique non-zero element $1 \neq 0$ (unity) in $\mathbb{F}$ such that $x.1 = x = 1.x$ for every $x \in \mathbb{F}$.
4. **Existence of Inverse:** For each non-zero $x \in \mathbb{F}$, there exists a unique element $x^{-1} \in \mathbb{F}$ such that $x.x^{-1} = 1 = x^{-1}.x$.
5. Commutative Property: $x.y = y.x$ for all $x, y \in \mathbb{F}$.

Remark: With the properties as described in (b), $\mathbb{F}^\star = \mathbb{F} - \{0\}$ is abelian group w. r. t. multiplication.

(c). **Distribution Law:** Multiplication is distributive over addition.

$$x.(y+z) = x.y + x.z, \qquad \forall \;\; x, y, z \in \mathbb{F}$$

$$(x+y).z = x.z + y.z, \qquad \forall \;\; x, y, z \in \mathbb{F}$$

Fields (Conti...)

Note: The unity element $1 \in \mathbb{F}$ is different from the zero element $0 \in \mathbb{F}$. Hence, every field must have at least two elements, 0 and 1.

- **Examples:** The well-known examples of fields are:

  The set $\mathbb{Q}$ of rational numbers is a Field, known as Rational Field,

  The set $\mathbb{R}$ of real numbers is a Field, known as Real Field,

  The set $\mathbb{C}$ of complex numbers is a Field, known as Complex Field.

- **Examples of non-empty sets which are not Fields:**

  The set $\mathbb{N}$ of natural numbers is NOT a field as it does not have additive identity, additive inverse property fails, multiplicative inverse property fails.

  The set $\mathbb{Z}$ of integers is NOT a field as multiplicative inverse property fails.

  The set $\mathcal{M}_{2\times2}(\mathbb{R})$ (or $\mathbb{R}^{2\times2}$) of all matrices over real field $\mathbb{R}$ is not a field as the multiplicative commutative property and multiplicative inverse property both fail.

Fields (Conti . . .)

Are there other examples?

1. There are fields $\mathbb{F}$ which lie between $\mathbb{Q}$ and $\mathbb{R}$, i.e., $\mathbb{Q} \subsetneq \mathbb{F} \subsetneq \mathbb{R}$. For example, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}$ is a field. Verify it !!
2. We can construct example via modular arithmetic.
   Recall: Let n be a +ve integer. Then for any integer x, $x \pmod{n}$ is defined to be the remainder after division by n. Note that the remainder r must satisfy $0 \leq r < n$. For example, $11 \pmod 3 = 2$, $11 \pmod 4 = 3$, $10 \pmod 5 = 0$ etc.
   - **Notation:** For any integer $n > 0$, we define
     $$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$
     We see that $|\mathbb{Z}_n| = n$.
   - Let $n > 0$ be fixed. Define two operations $+_n$ (modular addition or simply addition) and $\times_n$ (modular multiplication or multiplication) by:
     $$a +_n b = (a + b) \pmod n \quad \text{for all} \quad a, b \in \mathbb{Z}_n$$
     $$a \times_n b = (ab) \pmod n \quad \text{for all} \quad a, b \in \mathbb{Z}_n$$

Fields (Conti . . .)

Modular Arithmetic Operations

- [(a mod n) + (b mod n)] mod n= $(a + b)$ mod n.
- [(a mod n) − (b mod n)] mod n= $(a - b)$ mod n.
- [(a mod n) × (b mod n)] mod n= $(a \times b)$ mod n.

Extended Euclidean Algorithm

If $\gcd(a, b) = d$, then there are $X, Y \in \mathbb{Z}$ such that $aX + bY = d$.

Fields (Conti . . .)

- We can easily verify all the properties of a field for $\mathbb{Z}_n$–with the exception of multiplicative inverse property.
- Let us consider a few cases.
  1. $\mathbb{Z}_2 = \{0, 1\}$.
     The only nonzero element is 1, and its inverse is 1 (this holds always for unity element). Hence $\mathbb{Z}_2$ is a field. So we can construct various vector spaces over the field $\mathbb{Z}_2$. For example, $\mathbb{Z}_2^n$ is the vector space of all ordered n-tuple with entries 0 and 1. Subspaces of $\mathbb{Z}_2^n$ play an essential role in coding theory (part of both CSE and ECE).
  2. $\mathbb{Z}_3 = \{0, 1, 2\}$.
     Here we only need to consider the element 2 (since 1 has an inverse). But $2 \times_3 2 = 1$ i.e. 2 has an inverse. Therefore $\mathbb{Z}_3$ is a field.
  3. $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.
     Now it happens that $\mathbb{Z}_4$ is NOT a field.
     Reason: A field can not have zero-divisors.

Fields (Conti . . .)

- **Definition:** A zero-divisor is an element $a, a \neq 0$, for which there is an element $b, b \neq 0$ such that $ab = 0$.
- **Why does a field $\mathbb{F}$ have no zero divisors?**

  Suppose by way of contradiction (BWOC) that $a \in \mathbb{F}$ is a zero divisor. Then $a \neq 0$ and there is an element $b \neq 0$ such that $a.b = 0$. Multiplying by a^{-1}, we get:

  $$a^{-1}.(a.b) = a^{-1}.0 \quad \text{or} \quad 1.b = 0 \quad \text{or} \quad b = 0.$$

  But this is a contradiction, since $b \neq 0$.
- Now, consider $\mathbb{Z}_4$. We have $2 \times_4 2 = 4 \pmod 4) = 0$, i.e. 2 is a zero divisor. Therefore, $\mathbb{Z}_4$ can not be a field.

Fields (Conti . . .)

- **Proposition:** $\mathbb{Z}_n$ is a field if and only if n a prime number.

  Proof: [$\Longrightarrow$] Suppose $\mathbb{Z}_n$ is a field. We have to show n is a prime. Suppose BWOC that n is not a prime. Then $n = mk$, where $1 < m < n$, and $1 < k < n$. Therefore $m, k \in \mathbb{Z}_n$. But, in $\mathbb{Z}_n$, $m \times_n k = n \pmod{n} = 0$ and so m, k are zero divisors, which is a contradiction.

  [$\Longleftarrow$] Given n is prime, to show that $\mathbb{Z}_n$ is a field. It is enough to show that every non-zero element $a \in \mathbb{Z}_n$ has an inverse. Clearly $\gcd(a, n) = 1$. Thus by **extended Euclidean algorithm**, there are integers x and y such that $ax + yn = 1$. Thus, $ax = 1 \pmod{n}$, which shows that a in invertible.

- The field $\mathbb{Z}_p$ plays a very big role in cryptography and coding theory.