R SAINIRANJAN
SR : 15543
rsainiranjan@iisc.ac.in

MA 219 : Linear Algebra
Lecture 1

2020-11-07

1 Introduction

Given a system of linear equations we may represent it through matrix operations. Given , knowledge of the underlying field to which the coefficients belong, we may perform some operations to obtain solutions if they exist.

It is essential to understand that a general field $\mathbb{F}$ has its own advantages as compared to being restricted to $\mathbb{R}$

2 What is a Field ?

We define a field $\mathbb{F}$ as a tuple of the form $(\mathbb{F}, +, 0, -(), \times, 1, ()^{-1})$

where $\mathbb{F}$ is a set of at-least two elements , $0, 1 \in \mathbb{F}$

$+ : \mathbb{F} \times \mathbb{F} \mapsto \mathbb{F}$
$\times : \mathbb{F} \times \mathbb{F} \mapsto \mathbb{F}$
$-() : \mathbb{F} \mapsto \mathbb{F}$
$()^{-1} : \mathbb{F} \mapsto \mathbb{F}$ satisfying the following axioms :

Addition 1: $+$ is commutative

Addition 2 : $+$ is associative

Addition 3 : 0 is the identity of $+$ in $\mathbb{F}$

Addition 4 : $-()$ gives the unique *additive inverse* of any element in this field.

Multiplication 1 : $\times$ is commutative

Multiplication 2 : $\times$ is associative

Multiplication 3 : 1 is the identity of $\times$

Multiplication 4 : $()^{-1}$ gives the unique inverse for any element in $\mathbb{F} \setminus \{0\}$

Distributivity : $+$ distributes over $\times$

Note : There is an implicit assumption that $0 \neq 1$. For otherwise , we can look at the *singleton* field but in this case the multiplicative inverse axiom is vacuous. Such single element fields are irrelevant for the considerations that follow throughout this course and thus we shall choose to continue forward with this assumption.

Examples of Fields :

1. $\mathbb{R}$ is a field under standard operations
2. $\mathbb{Q}$ is a field under standard operations
3. $\mathbb{C}$ forms a field under the standard operations
4. $\mathbb{F}_2 = \{0, 1\}$ forms a field with the familiar operations if we treat this as analogous to modular arithmetic with base 2 i.e 0 corresponds to any 'even' natural number and 1 corresponds to any 'odd' natural number. $\mathbb{F}_2$ is the smallest possible field.
5. More generally define $\mathbb{F}_p$ for p , prime as $\{0, 1, ...p-1\}$ and with the operations in modular arithmetic base p. This forms a field.

Lemma 1 :

1. If $b, c, a \in \mathbb{F}$ then if $a(b+c) = ab + ac$ from distributivity we have $(b+c)a = ba + bc$
2. $0_{\mathbb{F}}$ (0 in the field $\mathbb{F}$) is unique

Proof :

1. From commutativity $(b+c)a = a(b+c)$ but from distributivity $a(b+c) = ab + ac$ and once again using commutativity the conclusion follows □

2. Suppose to the contrary $\exists\, 0_{\mathbb{F}}, 0_{\mathbb{F}}^{'}$. Since $0_{\mathbb{F}}$ is an additive identity , we have $0_{\mathbb{F}} + 0_{\mathbb{F}}^{'} = 0_{\mathbb{F}}^{'}$ but again as $0_{\mathbb{F}}^{'}$ is also an additive identity we have $0_{\mathbb{F}} + 0_{\mathbb{F}}^{'} = 0_{\mathbb{F}}$ and the result follows □

Some other proofs related to general properties of fields are given as Homework problems.

3 How to identify fields - by characteristics !

Characteristic of a Field :
$char(\mathbb{F})$ or the Characteristic of a field $\mathbb{F}$ is the smallest $n \in \mathbb{N}$ such that adding $1_{\mathbb{F}}$ to itself n times yields $0_{\mathbb{F}}$ and we term $char(\mathbb{F}) = n$. If no such n exists , $char(\mathbb{F}) = 0$

Examples of characteristic values :

1. $char(\mathbb{F}_p) = p$
2. $char(\mathbb{R}) = char(\mathbb{Q}) = 0$

Theorem 1 : Characteristic of a field is uniquely either 0 or a prime number

Proof : Solved in Homework

Lemma 2 : Every field $\mathbb{F}$ contains a $smallest$ subfield (A non-empty subset of $\mathbb{F}$ that satisfies all field axioms with the same operations as $\mathbb{F}$). This smallest subfield is termed as the *prime subfield* of $\mathbb{F}$

Proof : Let $Z_{\mathbb{F}} \in \mathbb{F}$ be the subset defined as $\{(1_{\mathbb{F}} + 1_{\mathbb{F}}...)_{n\ times} \forall n \in \mathbb{N}\} \cup \{0_{\mathbb{F}}\} \cup \{(-1_{\mathbb{F}} + -1_{\mathbb{F}}...)_{n\ times} \forall n \in \mathbb{N}\}$

If $char(\mathbb{F}) = p > 0$ then quite clearly $Z_{\mathbb{F}}$ is an analogue to $\mathbb{F}_p$

Let $Q_{\mathbb{F}} = \{pq^{-1} | p, q \in Z_{\mathbb{F}}, q \neq 0_{\mathbb{F}}\}$

If $char(\mathbb{F}) = p > 0$ then $Q_{\mathbb{F}} = Z_{\mathbb{F}}$

Now , we claim that $Q_{\mathbb{F}}$ is the requisite subfield.

Clearly $0_{\mathbb{F}}, 1_{\mathbb{F}} \in Q_{\mathbb{F}}$. Note that since all the elements of $Q_{\mathbb{F}}$ are contained in $\mathbb{F}$ most of the properties follow trivially. Thus, it suffices to check for closure of $Q_{\mathbb{F}}$ under the field operations. We can treat each element of $Q_{\mathbb{F}}$ analogous to a 'rational number' and thus closure of addition and multiplication follows and since $0_{\mathbb{F}}, 1_{\mathbb{F}} \in Q_{\mathbb{F}}$ closure of inverses follows as well and therefore $Q_{\mathbb{F}}$ is a subfield

Next , we show that if E is any other subfield then $Q_{\mathbb{F}} \subseteq E$

Clearly, if E is a subfield then $0_{\mathbb{F}}, 1_{\mathbb{F}} \in E$ and therefore by closure we have that $(1_{\mathbb{F}} + 1_{\mathbb{F}}...)_{n\ times} \in E\, \forall\, n \in \mathbb{N}$ and then by closure of additive inverses we have that $Z_{\mathbb{F}} \subseteq E$. Finally , for any $q \neq 0_{\mathbb{F}} \in Z_{\mathbb{F}}, q^{-1} \in E$ as E is closed under multiplicative inverses. Thus again we have that $pq^{-1} \in E\, \forall p \in Z_{\mathbb{F}}, q \in Z_{\mathbb{F}} \setminus \{0_{\mathbb{F}}\}$ which means that $Q_{\mathbb{F}} \subseteq E$ as claimed ■

Note : If $char(\mathbb{F}) = p > 0$ then the prime subfield is an analogue to $\mathbb{F}_p$ otherwise the prime subfield is an analogue of $\mathbb{Q}$