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

Homework Assignment 1
Linear Algebra

2020-10-12

1 Question 1

We are required to prove that the set $\mathbb{C}$ of Complex Numbers form a field. under the operations which have been defined.

1.1 Addition Axioms

1. Commutativity :
   We have , $(a+bi)+(c+di) = (a+c)+(b+d)i = (c+a)+(d+b)i$ (As $\mathbb{R}$ is a field) and thus $(a+bi)+(c+di) = (c+di)+(a+bi)$

2. Associativity :
   We have , $(a+bi)+((c+di)+(e+fi)) = (a+bi)+(c+e+(d+f)i) = (a+c+e)+(b+d+f)i = (a+c)+(b+d)i+(e+fi)$ (As $\mathbb{R}$ is a field) and thus $(a+bi)+((c+di)+(e+fi)) = ((a+bi)+(c+di))+(e+fi)$

3. Addition with *0* :
   We have , $(a+bi)+\mathit{0} = \mathit{0}+(a+bi)$ from Commutativity , further $(a+bi)+\mathit{0} = (a+bi)+(\mathit{0}+\mathit{0}i) = (a+\mathit{0})+(b+\mathit{0})i = a+bi$

4. Existence of Inverse :
   We have , $(a+bi)+(-a+(-b)i) = (-a+(-b)i)+(a+bi)$ from Commutativity , further $(a+bi)+(-a+(-b)i) = (a+(-a))+((b+(-b))i = 0+0i = \mathit{0}$

Thus , we see that all the addition axioms hold for C . Now , moving on to multiplication ,

1.2 Multiplication Axioms

1. Commutativity :
   $(a+bi)*(c+di) = (ac-bd)+(bc+ad)i = (ca-db)+(cb+da)i$ As R is a field , we have thus $(ca-db)+(cb+da)i = (c+di)*(a+bi)$

2. Associativity :
   $(a+bi)*((c+di)*(e+fi)) = (a+bi)*((ce-df)+(cf+ed)i) = (a(ce-df)-b(cf+ed)) + (a(cf+ed)+b(ce-df))i = (e(ac-bd)-f(ad+bc))+(e(ad+bc)+f(ac-bd))i$ As R is a field and thus $(e(ac-bd)-f(ad+bc))+(e(ad+bc)+f(ac-bd))i = (e+fi)*((ac-bd)+(ad+bc)i) = (e+fi)*((a+bi)*(c+di)) = ((a+bi)*(c+di))*(e+fi)$ As commutativity holds

3. Multiplication by *1* :
   We have that $(a+bi)*\mathit{1} = \mathit{1}*(a+bi)$ by commutativity and further $(a+bi)*\mathit{1} = (a+bi)*(\mathit{1}+\mathit{0}i) = (a(\mathit{1})-b(\mathit{0}))+(a(\mathit{0})+b(\mathit{1}))i$ Now as $\mathbb{R}$ is a field , we have that : $(a(1)-b(0))+(a(0)+b(1))i = (a+0)+(0+b)i = a+bi$

4. Existence of Inverse :
   Let $z = \frac{a}{a^2+b^2} - (\frac{b}{a^2+b^2})i$ We have that , $(a+bi)*z = z*(a+bi)$ by commutativity and further $(a+bi)*z = (\frac{a(a)+b(b)}{a^2+b^2}) + (\frac{a(b)-b(a)}{a^2+b^2})i = (\frac{a^2+b^2}{a^2+b^2}) + (\frac{\mathit{0}}{a^2+b^2})i$ since $\mathbb{R}$ is a field and this precisely is, $1+0i = \mathit{1}$

1.3 Distributive Property

We have that , $(a+bi)*((c+di)+(e+fi)) = (a+bi)*((c+e)+(d+f)i) = (a(c+e)-b(d+f))+(a(d+f)+b(c+e))i$
But as $\mathbb{R}$ is a field , we have that this is precisely $((ac+ae)-(bd+bf))+(ad+af+bc+be)i = (ac-bd)+(ad+bc)i+(ae-bf)+(af+be)i = (a+bi)*(c+di)+(a+bi)*(e+fi)$
Thus ,$\mathbb{C}$ is a field

2 Question 2

We are given that $\mathbb{F}$ is a field therefore we will assume that all Field axioms hold,

1. To see the uniqueness of 1. Suppose that there are two multiplicative identities 1 and $1^{'}$. Then $1 = 1 * 1^{'} = 1^{'}$ and thus $1 = 1^{'}$
   Similarly , To see the uniqueness of -a , Suppose there exist additive inverses of a -a and $-a^{'}$ then we have ,
   $-a = -a + 0 = -a + a + -a^{'} = 0 + -a^{'}$ by Associativity and thus $-a = -a^{'}$
   Finally , let us assume that $\exists a \in \mathbb{F}$ such that $a \neq 0$ and that it has two inverses a^{-1} and b
   Then we have $a^{-1} = a^{-1} * 1 = a^{-1} * (a * b)$ which by associativity is :
   $(a^{-1} * a) * b = 1 * b = b$

2. Next for $a \in \mathbb{F}$ we have that $a * 0 = a * (0 + 0) = a * 0 + a * 0$
   But we know that $a * 0 + 0 = a * 0$ and thus we have
   $a * 0 + 0 = a * 0 + a * 0$ and the conclusion follows :

3. Next we have that $-a + a = 0$ and thus $-a + a * 1 + a * -1 = a * -1$ and finally by the distributive property
   $-a + a * (1 + -1) = a * -1$
   $-a + a * 0 = a * -1$ which from the first part implies that $-a + 0 = a * -1$ and the conclusion follows

4. We have that -1^{2} is by definition $-1 * -1$ which by the previous proof is precisely $-(-1)$ which by definition is 1

5. Given that $ab = 0$ where $a, b \in \mathbb{F}$
   The case that both are *0* is trivially verified thus we shall consider the case when either is 0
   Suppose that $a \neq 0$ then we have that $a^{-1} \in \mathbb{F}$ and thus , $a^{-1} * (ab) = 1.b$ which is 0 therefore $b = 0$
   similarly if $b \neq 0$ we can show that $a = 0$

3 Question 3

By definition $char(\mathbb{F})$ is the smallest natural number n such that $(1_{\mathbb{F}} + 1_{\mathbb{F}}....)_{ntimes} = 0_{\mathbb{F}}$ if no such number exists then $char(\mathbb{F}) = 0$. If $char(\mathbb{F}) = 0$ then there is nothing to prove. Thus assume , that $char(\mathbb{F}) \neq 0$

We now have that $\exists n \in \mathbb{N}$ such that $(1_{\mathbb{F}} + 1_{\mathbb{F}}....)_{ntimes} = 0_{\mathbb{F}}$. Assume that n is composite we shall derive a contradiction from this assumption;

Clearly if n is composite by definition it can be written in the form ab where $a, b \in \mathbb{N}$ such that $a \neq 1$ and $b \neq 1$ and $a < n$ and $b < n$
Let $(1_{\mathbb{F}} + 1_{\mathbb{F}}....)_{btimes}$ be termed as $p \in \mathbb{F}$. Since $\mathbb{F}$ is a field we have that :

$$(1_{\mathbb{F}} + 1_{\mathbb{F}}....)_{ntimes} = (p + p....)_{atimes} \tag{1}$$

Let $(1_{\mathbb{F}} + 1_{\mathbb{F}}....)_{atimes}$ be termed as $q \in \mathbb{F}$. We have that ;

$$(p + p....)_{atimes} = (p * 1_{\mathbb{F}} + p * 1_{\mathbb{F}}....)_{atimes} = p * (1_{\mathbb{F}} + 1_{\mathbb{F}}...)_{atimes} = p * q \tag{2}$$

But by definition $(1_{\mathbb{F}} + 1_{\mathbb{F}}....)_{ntimes} = 0_{\mathbb{F}}$ From (1) and (2) , we have that $p * q = 0_{\mathbb{F}}$.
From the last part of the previous question we have that either $p = 0_{\mathbb{F}}$ or $q = 0_{\mathbb{F}}$ either way we get a contradiction since the minimality of n is violated ! ■

4 Question 4

We are given that $\mathbb{F}$ is a finite field such that $||\mathbb{F}|| = n$ for some $n \in \mathbb{N}$ We are to show that $(1_{\mathbb{F}}+1_{\mathbb{F}}....)_{ntimes} = 0_{\mathbb{F}}$
.
Clearly $\mathbb{F}$ cannot have $char(\mathbb{F}) = 0$ for otherwise the process of adding $1_{\mathbb{F}}$ can generate infinitely many distinct elements contradicting the finiteness of $\mathbb{F}$

Thus $char(\mathbb{F}) \neq 0$ and in particular $char(\mathbb{F}) = p$ for some prime p from the previous answer.
We shall show that $p|n$

Because if it were to be that p *does not divide* n . Then by the euclidean algorithm we have the existence of $q, r \in \mathbb{N}$ with $0 < r < p-1$ such that

$$n = q * p + r$$

Then from above , we have that

$(1_{\mathbb{F}} + 1_{\mathbb{F}}....)_{ntimes} = (1_{\mathbb{F}} + 1_{\mathbb{F}}....)_{q*p+rtimes}$
Let $(1_{\mathbb{F}} + 1_{\mathbb{F}}....)_{qtimes} = i$ and $1_{\mathbb{F}} + 1_{\mathbb{F}}....)_{rtimes} = j$
Then we have that ,
$(1_{\mathbb{F}} + 1_{\mathbb{F}}....)_{ntimes} = i * 0_{\mathbb{F}} + j$ as $char(\mathbb{F}) = p$
Implying that, $(1_{\mathbb{F}} + 1_{\mathbb{F}}....)_{ntimes} = j$
as $r < p$ we have that $j \neq 0_{\mathbb{F}}$
Thus as long as $p|n$ we are done,since $j = 0_{\mathbb{F}}$
In fact we shall show the stronger statement that $\|\mathbb{F}\| = p^m$ for some $m > 0, m \in \mathbb{N}$.
To see this , Consider the subfield of $\mathbb{F}$ formed by the elements $1_{\mathbb{F}}, (1_{\mathbb{F}} + 1_{\mathbb{F}}....)_{2times}.....(1_{\mathbb{F}} + 1_{\mathbb{F}}....)_{ptimes}$. This is a valid subfield since $0_{\mathbb{F}}$ and $1_{\mathbb{F}}$ are in this subfield and a quick check reveals that all field axioms are satisfied (we can use the euclidean algorithm to reduce any $(1_{\mathbb{F}} + 1_{\mathbb{F}}....)_{ktimes}$ where $k > p$ to $(1_{\mathbb{F}} + 1_{\mathbb{F}}....)_{utimes}$ where $k = mp + u$ for some m and $0 \leq u \leq p-1$)

Now , we state that $\mathbb{F}$ is a vector space over this subfield with the operations of Vector Addition and Scalar Multiplication defined as follows :

1. Vector Addition : This is simply the addition of any two elements in $\mathbb{F}$
2. Scalar Multiplication : In this case if q is an element of the subfield and $v \in \mathbb{F}$ as $q \in \mathbb{F}$ $q * v$ is well defined with respect to the multiplication in $\mathbb{F}$ and thus we chose this to be our scalar multiplication

Using the field axioms , it is easy to see that our definition of $\mathbb{F}$ as a vector space is valid .
Clearly then , $\|\mathbb{F}\| = p^m$ for $m > 0$ where m is in fact the *dimension* of this Vector Space.
This is easy to see as if m is the dimension of this vector space then there are exactly p^m distinct possible combinations of m linearly independent basis vectors (since each can have p choices in total)
■

5 Question 5

Lemma : **0** is unique
Proof : Suppose that $\exists \mathbf{0}, \mathbf{0}'$. We have that $\mathbf{0} + \mathbf{0}' = \mathbf{0}$ considering $\mathbf{0}'$ to be the zero vector but then considering that $\mathbf{0}$ is the zero vector $\mathbf{0} + \mathbf{0}' = \mathbf{0}'$ and thus $\mathbf{0} = \mathbf{0}'$ □

Given that V is a vector space over a field $\mathbb{F}$ and that $c \in F$ and $v \in V$.
Now $\mathbf{0} + \mathbf{0} = \mathbf{0}$ Implies that $c.\mathbf{0} = \mathbf{c}.(\mathbf{0} + \mathbf{0}) = \mathbf{c}.\mathbf{0} + \mathbf{c}.\mathbf{0}$ Thus if $u = c.\mathbf{0}$ then $u + c.\mathbf{0} = \mathbf{u}$ which implies that u is **0** which is uniquely determined from the lemma
Now , suppose that $0_{\mathbb{F}}.v = \mathbf{a}$ for some $\mathbf{a} \in \mathbf{V}$ then we have that for $c \in \mathbb{F}$
$c.v = (c + 0_{\mathbb{F}}).v = c.v + \mathbf{a}$
Once again we have that , a is uniquely determined to be **0**
■

6 Question 6

Given that $A \in \mathbb{F}^{m \times n}$ and $B \in \mathbb{F}^{n \times m}$ We are to show that :
$trace(AB) = trace(BA)$

Let $A = [a_{ij}]$ for $1 \leq i \leq m$ and $1 \leq j \leq n$
Similarly let Let $B = [b_{ij}]$ for $1 \leq i \leq n$ and $1 \leq j \leq m$
Diagonal elements of AB are of the form $[AB]_{ii}$ where $1 \leq i \leq m$ and of BA are of the form $[BA]_{ii}$ where $1 \leq i \leq n$
Using the properties of matrix multiplication

$$[AB]_{ii} = \sum_{j=1}^{j=n} a_{ij} b_{ji}$$

$$[BA]_{ii} = \sum_{j=1}^{j=m} a_{ij} b_{ji}$$

Thus we have ,

$$trace(AB) = \sum_{i=1}^{i=m} [AB]_{ii} = \sum_{i=1}^{i=m} (\sum_{j=1}^{j=n} a_{ij} b_{ji})$$

Exchanging summation the right hand side gives ,

$$\sum_{i=1}^{i=m} (\sum_{j=1}^{j=n} a_{ij} b_{ji}) = \sum_{j=1}^{j=n} (\sum_{i=1}^{i=m} a_{ij} b_{ji}) = \sum_{i=1}^{i=n} (\sum_{j=1}^{j=m} a_{ij} b_{ji}) = \sum_{i=1}^{i=n} [BA]_{ii} = trace(BA)$$

■