MTH100A **Math 1 (Linear Algebra)** **Monsoon Semester – 2023-24**

Tutorial Exercise for Tuesday 20230912

1. Let V be a vector space. Prove the following (see Proposition 7):
   A. The additive inverse vector of any vector **u** is unique; we use the notation $-\mathbf{u}$ for the inverse vector.
   B. $0\mathbf{u} = \mathbf{0}$ for every vector **u**
   C. $c\mathbf{0} = \mathbf{0}$ for every scalar c
   D. Cancellation Law, i.e. show that if $\mathbf{u} + \mathbf{v} = \mathbf{u} + \mathbf{w}$, for $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$, then $\mathbf{v} = \mathbf{w}$.

2. Give an example of a set X and an operation involving elements of X, which does not satisfy the cancellation law. Briefly justify your answer.

3. Verify the properties of a vector space for the space C[0,1] of continuous real-valued functions defined on the closed interval [0,1] using the field of real numbers as the underlying field of scalars. *You may assume that the sum of continuous functions and scalar multiples of continuous functions are also continuous functions.*

4. Show that the set $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a,b \in \mathbb{Q}\}$ is a field. **Remark**: Note that $\mathbb{Q}[\sqrt{2}]$ is a subset of $\mathbb{R}$; the wording for this situation is: $\mathbb{Q}[\sqrt{2}]$ is a ***subfield*** of $\mathbb{R}$. (***Hint: The key step is to show that nonzero elements of $\mathbb{Q}[\sqrt{2}]$ have multiplicative inverses in $\mathbb{Q}[\sqrt{2}]$.***)

5. a) Is $\mathbb{R}$ a vector space over $\mathbb{Q}$? Justify your answer in brief.
   b) Is $\mathbb{C}$ a vector space over $\mathbb{R}$? Justify your answer in brief.
   c) Can you generalize the answers to a) and b) above to a statement about fields and vector spaces ? Explain briefly.

6. *Modular arithmetic and fields*: Let n be a fixed but arbitrary positive integer, $n \geq 2$. Put $\mathbb{Z}_n = \{0,1,2,\ldots,n-1\}$. Define the operations of modular addition and modular multiplication on $\mathbb{Z}_n$ by: $x \oplus y = (x+y) \pmod n$ and $x \otimes y = (xy) \pmod n$. **NB**: Recall that $z \pmod n$ = **remainder** after division of z by n for all $z \in \mathbb{Z}$. Note that we have $0 \leq$ remainder $< n$, i.e. $z \pmod n \in \mathbb{Z}_n$ for all $z \in \mathbb{Z}$.
   a) Show that if $x \in \mathbb{Z}_n$, then x has an inverse in $\mathbb{Z}_n$ with regard to the operation $\oplus$ (i.e. additive inverse)..
   b) ***We have already shown in class that $\mathbb{Z}_2$ is a field.*** Now show that $\mathbb{Z}_3$ and $\mathbb{Z}_5$ are fields. (***Hint: You may assume that $\oplus$ and $\otimes$ satisfy closure, associativity, commutativity and distributivity on $\mathbb{Z}_n$. This is straightforward but a ittle lengthy. Also see the hint for Q4.***)
   c) Are $\mathbb{Z}_4$ and $\mathbb{Z}_6$ fields ? Justify your answer briefly.
   d) Can you generalize the above to state a condition for $\mathbb{Z}_n$ **not to be a field**? Briefly justify your statement.

[SOLUTIONS FOLLOW: MAY NOT BE IN SAME ORDER.]

1.A. Suppose u_1 & u_2 are two inverse vectors of u

Then,

$$u_1 + u_2 = \bar{0} \quad \text{(By property of additive inverse)}$$

Adding u_2 on both sides

$$u_1 + u + u_2 = u_2 + \bar{0}$$
$$u_1 + \bar{0} = u_2 + \bar{0}$$
$$\Rightarrow \quad u_1 = u_2$$

Hence additive inverse of any vector is unique

B. c) $0(u) = (0+0)u$

$$= 0u + 0u \quad \forall \quad u \in V$$

Let v be additive inverse of $0 \cdot u$.

Adding v to both sides

$$v + 0(u) = v + 0 \cdot u + 0 \cdot u$$
$$\Rightarrow \quad \bar{0} = 0 \cdot u$$

C. $c(\bar{0}) = c(\bar{0} + \bar{0})$

$$= c \cdot \bar{0} + c \cdot \bar{0}$$

Adding inverse of $c \cdot \bar{0}$ (say v) to both the sides

$$c(\bar{0}) + v = v + c \cdot \bar{0} + c \cdot \bar{0}$$
$$\bar{0} = c \cdot \bar{0}$$

D. If $u + v = u + w \quad \forall \quad u, v, w \in V$

from existence of additive inverse of each vector of V, adding inverse of u (say $-u$) to both the sides:

$$-u + u + v = -u + u + w$$
$$(-u + u) + v = (-u + u) + w$$
$$\bar{0} + v = \bar{0} + w$$
$$\Rightarrow \quad v + w$$

(2)

Solution 2 Suitable example is $X = \mathbb{R}^{n \times n}$ and the operation be matrix multiplication. So, for any matrix A being non-invertible

$$AB = AC \not\Rightarrow B = C$$

Example:

$$X = \mathbb{R}^{2\times 2}, \quad A = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$AB = AC = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

but $B \neq C$

Q5.

(a) Is $\mathbb{R}$ a vector space over $\mathbb{Q}$? Justify.

Ans: Yes. If $x, y \in \mathbb{R}$, then $x+y \in \mathbb{R}$ is well-defined. Also, if $q \in \mathbb{Q}$ and $x \in \mathbb{R}$, the scalar product $qx \in \mathbb{R}$ is the usual product in $\mathbb{R}$ (since $\mathbb{Q} \subseteq \mathbb{R}$). Furthermore, all the vector space axioms are satisfied, since $\mathbb{R}$ satisfies all the field axioms, which are stronger than vector space axioms.

(b) Is $\mathbb{C}$ a vector space over $\mathbb{R}$? Justify.

Ans. Yes. The reasoning is the same as for a). If $z_1 = a+bi$ and $z_2 = c+di \in \mathbb{C}$, then $z_1+z_2 = (a+c)+(b+d)i \in \mathbb{C}$ is well defined, and if $x \in \mathbb{R}$, then $xz_1 = xa + xbi \in \mathbb{C}$ is well-defined since $\mathbb{R} \subseteq \mathbb{C}$. Again, all V-S axioms are satisfied.

(c) Generalization:

We can generalize as follows: if F, K are fields with $F \subseteq K$, i.e. F is a subfield of K, then K is a vector space over F, with the natural definitions of addition and scalar multiplication as above.

Remark: this idea plays a major role in field theory (an important part of algebra).

Q3. Verify that $C[0,1]$ is a vector space over $\mathbb{R}$.

Ans: Preliminary Remarks:-

1. We use the standard definitions for the sum function and the scalar multiple function: If $f, g \in C[0,1]$ and $\alpha \in \mathbb{R}$ then:
   - $f+g$ is the function defined by $(f+g)(x) = f(x) + g(x) \quad \forall x \in [0,1]$
   and
   - αf is the function defined by $(\alpha f)(x) = \alpha f(x) \quad \forall x \in [0,1]$.

2. Many of the vector space axioms state the equality of two mathematical objects. In the case of $C[0,1]$, these objects are functions. So we need to apply the definition of equality of functions:-
   Two functions f and g defined on the same domain X are said to be equal if $f(x) = g(x)$ for all $x \in X$. (1)

Any answer to Q3 which does not use (1) would be incorrect.

Q3- cont'd

We consider the axioms for a vector space under the subheadings A, B, C.

A. Closure under addition and scalar multiplication - this has been given and doesn't need to be proved.

B. For B and C, we assume $f, g, h \in C[0,1]$, $c, d \in \mathbb{R}$. Let x be any arbitrary element of $[0,1]$.

B. a) Associativity :-

$$[(f+g)+h]x = (f+g)(x) + h(x) \text{ - by defn.}$$
$$= (f(x)+g(x)) + h(x) \text{ - by defn.}$$
$$= f(x) + (g(x)+h(x)) \text{ - Asso. property in } \mathbb{R}$$
$$= f(x) + (g+h)(x) \text{ - by defn.}$$
$$= [f+(g+h)](x) \text{ - by defn.}$$

→ i.e. we have proved (1) for this axiom.

b) Identity property: Consider the function $\overline{0}: [0,1] \longrightarrow \mathbb{R}$ defined by $\overline{0}(x) = 0 \quad \forall x \in [0,1]$

Q3 – cont'd

Then: $(f+\bar{0})(x) = f(x) + \bar{0}(x)$

$= f(x) + 0 = f(x)$.

Similarly, $(\bar{0}+f)(x) = f(x)$.

$\Rightarrow (f+\bar{0}) = (\bar{0}+f) = f$

So $\bar{0}$ is an (additive) identity function.

c) Additive Inverse function. For $f \in C[0,1]$, define $\bar{f}$ by $\bar{f}(x) = (-1) f(x)$ for all x. $\bar{f} \in C[0,1]$ by assumption.

But $(f+\bar{f})(x) = f(x) + (-1) f(x) = 0$

(Distributive Property for $\mathbb{R}$)

$= \bar{0}(x)$.

Similarly, $(\bar{f}+f)(x) = \bar{0}(x)$

$\Rightarrow f+\bar{f} = \bar{f}+f = \bar{0}$

$\therefore \bar{f}$ is an additive identity.

d) Commutativity.

$(f+g)(x) = f(x) + g(x)$ – defn.

$= g(x) + f(x)$ – commutativity for $\mathbb{R}$

$= (g+f)(x)$. $\Rightarrow f+g = g+f$

C. (a) $[c(f+g)](x) = c(f+g)(x)$ – defn.

$= c(f(x)+g(x))$ – defn.

$= cf(x) + cg(x)$ – Distributivity for $\mathbb{R}$

$= (cf + cg)(x)$ by defn

$\Rightarrow c(f+g) = cf + cg$

Q3 – cont'd

b) $[(c+d)f](x) = (c+d)f(x)$ – defn.
$= cf(x) + df(x)$ – Distributivity for $\mathbb{R}$
$= (cf)(x) + (df)(x)$ – defn.
$= (cf + df)(x)$ – defn.
$\Rightarrow (c+d)f = cf + df$

c) $[c(df)](x) = c[(df)(x)]$ – defn.
$= c(df(x))$ – defn.
$= (cd)f(x)$ – Assoc. for $\mathbb{R}$
$= ((cd)f)(x)$ – defn.
$\Rightarrow c(df) = (cd)f$

d). $(1 \cdot f)(x) = 1 \cdot f(x)$ – defn.
$= f(x)$ – since 1 is a unity element in $\mathbb{R}$
$\Rightarrow 1 \cdot f = f$

Remark: The above verification steps are somewhat repetitive. However, you should observe that in many places we have used the fact that certain properties hold in $\mathbb{R}$, since it is a field. This indicates that if X is a set of functions with codomain F, a field, then X is a likely candidate to be a vector space over F.

~~(4)~~

Q4. Show that $\mathbb{Q}[\sqrt{2}]$ is a field, where $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$. (4a)

Ans: Note that $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R}$; hence axioms such as associativity, commutativity and distributivity are automatically satisfied by $\mathbb{Q}[\sqrt{2}]$.

The remaining properties which need to be verified are:

A. Closure under $+$ and $\cdot$.

B. Existence of zero element and

B. (i) Zero property and unity property

AND

(ii) Additive and multiplicative inverse property.

We verify these as follows:

A: Suppose $a+b\sqrt{2}$ and $c+d\sqrt{2} \in \mathbb{Q}[\sqrt{2}] = F$ (for convenience, only).

Then: $(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + (b+d)\sqrt{2} \in F$

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

(PTO)

Q4 - cont'd (4h)

B. (i) Clearly $0 = 0 + 0\sqrt{2}$ and $1 = 1 + 0\sqrt{2}$ are in F.

(ii) Suppose $a + b\sqrt{2} \in F$.

Then: $(-a) + (-b)\sqrt{2} \in F$ also,

and $(a + b\sqrt{2}) + [(-a) + (-b)\sqrt{2}] = 0$.

So additive inverse property holds.

Finally, suppose $r = a + b\sqrt{2} \in F$, ~~[illegible]~~.

~~If [illegible]~~ $r \neq 0$. If $b = 0$,

$r = a$, and $\frac{1}{r} = \frac{1}{a} = \frac{1}{a} + 0\cdot\sqrt{2} \in F$.

(since $r \neq 0$)

So, we may assume $b \neq 0$.

Now, $\frac{1}{r} \in \mathbb{R}$. We need to show $\frac{1}{r} \in F$. (1)

But $\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}}$

$= \frac{a}{a^2-2b^2} - \frac{b\sqrt{2}}{a^2-2b^2} \in F$

provided $a^2 - 2b^2 \neq 0$. But $a^2 - 2b^2 = 0$

$\Rightarrow \sqrt{2} = \pm \frac{a}{b} \in \mathbb{Q} \Rightarrow\Leftarrow$. This proves (1)

Remark: Clearly, there is nothing special about $\sqrt{2}$: we could have used $\sqrt{3}, \sqrt{5}, \sqrt[3]{2}$, etc. Fields like this F are called algebraic extension fields and play a ~~[illegible]~~ major [illegible] in NUMBER THEORY

Q6: Modular Arithmetic in $\mathbb{Z}_n$.

Remark: As we have seen in Q3 and Q4, ~~many field and~~ verification of field or vector space axioms are frequently straightforward and repetitive. Difficulties typically arise only in: closure, zero and unity, and inverse axioms. In this question, closure follows directly from the definition of $\oplus$ and $\otimes$, and other axioms may be assumed. Clearly 0 and 1 are elements of $\mathbb{Z}_n$ and are the zero and unity elements respectively. So, in Q6, we have to deal with the inverse axioms only.

(a) Let $x \in \mathbb{Z}_n$. Then $n-x \in \mathbb{Z}_n$ also and $x \oplus (n-x) = [x+(n-x)] \pmod n$

$= n \pmod n = 0$.

$\therefore$ $n-x$ is the additive inverse of x.

(b) We are left with only the multiplicative inverse property. Here are the $\otimes$ tables for $\mathbb{Z}_3$ and $\mathbb{Z}_5$ respectively (0 has been excluded).

$\mathbb{Z}_3$

$\otimes$	1	2
1	1	2
2	2	1

So $2 = 2^{-1}$ in $\mathbb{Z}_3$

$\mathbb{Z}_5$

$\otimes$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

So: $3 = 2^{-1}$; $2 = 3^{-1}$; $4 = 4^{-1}$ in $\mathbb{Z}_5$ - every ~~elem~~ (non-zero) element has an inverse.

(C) In $\mathbb{Z}_4$, $2 \otimes 2 = 4 \pmod 4 = 0$, i.e. 2 is a zero-divisor in $\mathbb{Z}_4$. However, fields cannot have zero-divisor (see the Slide: Fields - What You Need to Know in LII-MON on 20230904), YOU were asked to prove these.

Q6 – cont'd

* Beyond our scope in MTH100

6(c) Similarly, in $\mathbb{Z}_6$, $2 \otimes 3 = 6 \pmod 6 = 0$ – so $\mathbb{Z}_6$ also has zero-divisors and cannot be a field.

6(d) Looking to 6(c), we can say:

If m is composite, then $\mathbb{Z}_m$ is not a field. (1)

Proof: let $m = pq$, $p, q > 1$.
Then, $p, q \in \mathbb{Z}_m$ and $p \otimes q = pq \pmod m = m \pmod m = 0$. ∴ $\mathbb{Z}_m$ has zero-divisors, and is not a field

Remark: The contra-positive of (1) is:
If $\mathbb{Z}_m$ is a field, then m is a prime (2)
We have verified (2) for $m = 2, 3, 5$.
In fact, (2) holds in general. *
The fields $\mathbb{Z}_p$, p a prime, play a major role in finite field theory.
In recent years, they have become a major topic of research because of applications in cryptography.