Assignment 1

MA3.101: Linear Algebra

Spring 2021

Answers

1. The properties to be checked are: (i) V forms an abelian group (V1-5), (ii) F forms a field (F1-11) (iii) V is closed under scalar multiplication, both distributive laws are followed, scalar multiplication is associative and the unit scalar is the identity of scalar multiplication (V6-10).

(a) $V = \mathbb{R}, F = \mathbb{N}$: V does not form a valid vector space over F. This is because $\mathbb{N}$ is *not* a field; in general, elements do not have additive or multiplicative inverses ($\forall x \in \mathbb{N}, -x \notin \mathbb{N}$ and $\frac{1}{x} \notin \mathbb{N}$, in general).

(b) $V = \mathbb{Q}, F = \mathbb{R}$: V does not form a valid vector space over F. This is because $\mathbb{Q}$ is *not* closed under scalar multiplication with $\mathbb{R}$ (one example is $1 \in \mathbb{Q}, \sqrt{2} \in \mathbb{R}$, but $\sqrt{2} \cdot 1 \notin \mathbb{Q}$).

(c) $V = \mathbb{R}, F = \mathbb{Q}$: V forms a valid vector space over F. The proof is as follows:

- $\mathbb{R}$ forms an abelian group. This follows from the fact that the real numbers are closed, associative and commutative under addition. 1 is the identity element. The inverse of $x \in \mathbb{R}$ is $-x \in \mathbb{R}$.
- $\mathbb{Q}$ forms a field. This follows from the fact the rational numbers are closed, associative and commutative under multiplication and addition. The multiplicative and additive identities are 1 and 0 respectively (1 is the scalar unit). All nonzero elements $x \in \mathbb{Q}, x \neq 0$ have a multiplicative inverse $\frac{1}{x} \in \mathbb{Q}$ and all elements $x \in \mathbb{Q}$ have an additive inverse $-x \in \mathbb{Q}$. Further, multiplication distributes over addition in $\mathbb{Q}$.
- Since $\mathbb{Q} \subseteq \mathbb{R}$, the closure, distributivity and associativity of scalar multiplication follow from the corresponding properties of $\mathbb{R}$. Further, the scalar unit 1 is the identity in $\mathbb{R}$ as well.

(d) $V = \mathbb{R}, F = \mathbb{C}$: V does not form a valid vector space over F. This is because $\mathbb{R}$ is *not* closed under scalar multiplication with $\mathbb{C}$ (one example if $1 \in \mathbb{R}, i \in \mathbb{C}$, but $i \cdot 1 \notin \mathbb{R}$).

2. **XOR** is defined as:
$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$

$1 \oplus 1 = 0$,
and **AND** is defined as:
$0 \cdot 0 = 0$
$0 \cdot 1 = 0$
$1 \cdot 0 = 0$
$1 \cdot 1 = 1$.

- $F = \{0, 1\}$ forms an abelian group under **XOR**. Clearly, **XOR** is closed as well as commutative. When we note that it is equivalent to $+_2$, we can conclude that it is associative, since modular addition is always associative. The identity is 0 and the inverse of either element is itself. Hence, F forms an abelian group under **XOR**.

- $F - \{0\}$ is nothing but the singleton set $\{1\}$. This set is a group under multiplication, whose only element is the identity. Since commutativity is not contradicted, we can say that it is an abelian group as well. Hence the nonzero elements of F form an abelian group under **AND**.

- The distributivity can be proved as follows:
  $\forall x, y \in F, 0 \cdot (x \oplus y) = 0$, from the property of fields that $\forall a \in F, 0 \cdot a = 0$.
  But $0 \cdot x \oplus 0 \cdot y = 0 \oplus 0 = 0$, from the same property.
  $\forall x, y \in F, 1 \cdot (x \oplus y) = x \oplus y$, since 1 is the multiplicative identity. But $1 \cdot x \oplus 1 \cdot y = x \oplus y$, for the same reason.
  The above equations prove the dsitributivity of multiplication over addition in F.
  Hence, F is a field under the operations of **XOR** and **AND**.

3. A set $A \subseteq V$ is a subspace of V if $\forall x, y \in A, \forall a, b \in F, ax + by \in A$, *i.e.*, it is closed under linear combination.

(a) A is not a subspace of V.
Suppose X and Y are both invertible $n \times n$ matrices, *i.e.*, $X, Y \in A$. Then, $aX + bY$ is not necessarily invertible for all $a, b \in F$. One counterexample is if $X = I_n$ and $Y = -I_n$; then $1 \cdot X + 1 \cdot Y = I^n - I^n = 0_n$, the null matrix, which is not invertible.

(b) A is not a subspace of V.
Suppose X and Y are both non-invertible $n \times n$ matrices, *i.e.*, $X, Y \in A$. Then, $aX + bY$ is not necessarily non-invertible for all $a, b \in F$. One counterexample is if $X = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 0 & 1 & 0 \end{bmatrix}$ and $Y = \begin{bmatrix} 0 & 1 & 0 \\ 3 & 2 & 1 \\ 3 & 2 & 1 \end{bmatrix}$, both of which are clearly singular and therefore non-invertible. However,

$1 \cdot X + 1 \cdot Y = X + Y = \begin{bmatrix} 1 & 3 & 3 \\ 4 & 4 & 4 \\ 3 & 3 & 1 \end{bmatrix}$, which has a determinant of 16 and is therefore invertible.

(c) A is a subspace of V.
Suppose that X and Y are both such that $XB = BX$ and $YB = BY$. Then, for arbitrary $a, b \in F$,
$(aX + bY) \cdot B = aXB + bYB$ (distributivity of matrix multiplication over addition) $= aBX + bBY$ (by assumption). This is equal to $B(aX) + B(bY)$ (proved below), and by distributivity of matrix multiplication over addition, to $B \cdot (aX + bY)$. Hence $aX + bY \in A$, and A is indeed a subspace.
We need to prove that $aPQ = P(aQ)$ for any $a \in F$ and $P, Q \in V$. We know that

$$[PQ]_{ij} = (\sum_{k=1}^{k=n} p_{ik} q_{kj}).$$

Hence,

$$[aPQ]_{ij} = a \cdot (\sum_{k=1}^{k=n} p_{ik} q_{kj}) = (\sum_{k=1}^{k=n} a p_{ik} q_{kj}) = (\sum_{k=1}^{k=n} p_{ik} (a q_{kj})) = [P(aQ)]_{ij}.$$

Therefore, $aPQ = P(aQ)$.

(d) A is not a subspace of V.
Suppose that X and Y are idempotent, *i.e.*, $X, Y \in A$. Then, $aX + bY$ is not necessarily idempotent for all $a, b \in F$. One counter example is if $X = Y = I_n$. Then, $1 \cdot X + 1 \cdot Y = I_n + I_n = 2I_n$. But $(2I_n)^2 = 4I_n \neq 2I_n$, which means $aX + bY$ is not idempotent.

4. (a) Let this set be C. C is a subspace of V.
Suppose $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ are two continuous functions, *i.e.*, $f, g \in C$. Then, consider the function $af + bg$ for arbitrary $a, b \in \mathbb{R}$ (assuming $\mathbb{R}$ is the scalar field). For all $c \in \mathbb{R}$,

$$\lim_{x \to c}(af + bg) = \lim_{x \to c} af + \lim_{x \to c} bg = a \lim_{x \to c} f + b \lim_{x \to c} g = af(c) + bg(c) = (af + bg)(c),$$

by the properties of limits. Therefore, $af + bg$ is also continuous and belongs to C; hence C is indeed a subspace.

(b) Let this set by S. S is not a subspace of V. One counterexample is if $f(x) = x$, the identity function, and $g(x) = 1$, the constant function with value 1. Then $1 \cdot f(x) + 1 \cdot g(x) = x + 1$. But, in general, $(x + 1)^2 \neq x + 1$. Hence S is not a subspace.

(c) Let this set be D. D is not a subspace of V. Suppose $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ are two functions such that $f(3) - f(-5) = g(3) - g(-5)$, *i.e.*, $f, g \in C$. Then, consider the function $af + bg$ for $a = 2, b = 3$.
$(2f + 3g)(3) - (2f + 3g)(-5) = 2\{f(3) - f(-5)\} + 3\{g(3) - g(-5)\} = 2 + 3 = 5 \neq 1$, which means $(2f + 3g) \notin D$. Therefore D is not a subspace.

5. We know that V is a vector space. Suppose $S_2 \subseteq V$ and S_2 is linearly independent. We will assume $S_1 \subseteq S_2$ is linearly dependent and derive a contradiction.
If S_1 is linearly dependent, there are vectors $v_1, v_2, \cdots, v_k \in S_1$ which have a linear combination equal to 0. But since $S_1 \subseteq S_2$, all of $v_1, v_2, \cdots, v_k$ belong to S_2 as well. This means that there are vectors in S_2 which have a linear combination equal to 0. This contradicts the assumption that S_2 is linearly independent. Hence, S_1 must also be linearly independent, QED.

6. In order to show that Z forms a vector space over F, we need to prove that (i) Z forms an abelian group (V1-5), (ii) F is a field (F1-11) and (iii) Z is closed under scalar multiplication, both distributive laws are followed, scalar multiplication is associative and the unit scalar is the identity of scalar multiplication (V6-10).

(i) Since V and W are vector spaces over F, they are also abelian groups. Hence, we can prove the various axioms for Z to be an abelian group as follows:

- **Closure** Let $(v_1, w_1), (v_2, w_2) \in Z$. Then, $v_1 + v_2 \in V$ by closure of V, and $w_1 + w_2 \in W$ by closure of W.
Hence, $(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2) \in Z$. Therefore Z is also closed.

- **Associativity** Let $(v_1, w_1), (v_2, w_2), (v_3, w_3) \in Z$. Then, $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$, by associativity of V, and $(w_1 + w_2) + w_3 = w_1 + (w_2 + w_3)$, by associativity of W.
Then, $((v_1, w_1) + (v_2, w_2)) + (v_3, w_3) = (v_1 + v_2, w_1 + w_2) + (v_3 + w_3) = ((v_1 + v_2) + v_3), (w_1 + w_2) + w_3) = (v_1 + (v_2 + v_3), w_1 + (w_2 + w_3))$, by the associativity of V and W.
Now, this is equal to $(v_1, w_1) + (v_2 + v_3, w_2 + w_3) = (v_1, v_2) + ((v_2, w_2) + (v_3, w_3))$; hence Z is also associative.

- **Commutativity** Let $(v_1, w_1), (v_2, w_2) \in Z$. Then, $v_1 + v_2 = v_2 + v_1$ by commutativity of V, and $w_1 + w_2 = w_2 + w_1$ by commutativity of W.
Hence, $(v_1, w_1) + (v_2 + w_2) = (v_1 + v_2, w_1 + w_2) = (v_2 + v_1, w_2 + w_1)$, by the commutativity of V and W.
This is equal to $(v_2, w_2) + (v_1, w_1)$. Therefore Z is also commutative.

- **Existence of Identity** Let $e_V \in V$ and $e_W \in W$ be the identities of V and

W. Then $e_Z = (e_V, e_W) \in Z$ is the identity of Z, since $(v, w) + (e_V, e_W) = (e_V, e_W) + (v, w) = (v + e_V, w + e_W) = (v, w)$. Therefore Z also has an identity element.

- **Existence of Inverse** Let $v \in V$ and $w \in W$ be arbitrary elements of V and W. Then, if $-v \in V$ and $-w \in W$ are their respective inverses, the inverse of $(v, w) \in Z$ is $(-v, -w) \in Z$.
  This is because $(v, w) + (-v, -w) = (v + (-v), w + (-w)) = (e_V, e_W) = e_Z$.
  Therefore all elements of Z have inverses.
  By the above properties (V1-5), Z is an abelian group under addition.

(ii) We know that F is a field, since V and W form vector spaces over it.

(iii) We can prove that Z has the relevant properties from the corresponding properties of V and W, as follows:

- **Closure under scalar multiplication** V and W are both closed under scalar multiplication, *i.e.*, $\forall c \in F, v \in V, w \in W$, we have $cv \in V, cw \in W$. Hence, if $(v, w) \in Z$, then $c(v, w) = (cv, cw) \in Z$ as well, for all $c \in F$. Therefore Z is also closed under scalar multiplication.

- **Distributive laws** We know the distributive laws hold in V and W. Let $(v_1, w_1), (v_2, w_2) \in Z$, and $c_1, c_2 \in F$.
  Then $c_1 \cdot ((v_1, w_1) + (v_2, w_2)) = c_1(v_1 + v_2, w_1 + w_2) = (c_1 \cdot (v_1 + v_2), c_1 \cdot (w_1 + w_2)) = (c_1v_1 + c_1v_2, c_1w_1 + c_1w_2)$, by the first distributive law in V and W.
  This is equal to $(c_1v_1, c_1w_1) + (c_1v_2, c_1w_2) = c_1(v_1, w_1) + c_1(v_2, w_2)$. This proves the first distributive law.
  Also, $(c_1 + c_2) \cdot (v_1, w_1) = ((c_1 + c_2) \cdot v_1, (c_1 + c_2) \cdot w_1) = (c_1v_1 + c_2v_1, c_1w_1 + c_2w_1)$, by the second distributive law in V and W.
  This is equal to $(c_1v_1, c_1w_1) + (c_2v_1, c_2w_1) = c_1(v_1, w_1) + c_2(v_1, w_1)$. This proves the second distributive law.

- **Associativity of scalar multiplication** We know that scalar multiplication is associative in V and W. Let $c_1, c_2 \in F$, and $(v, w) \in F$; then we know that $(c_1c_2)v = c_1(c_2v)$ and $(c_1c_2)w = c_1(c_2w)$.
  Then $(c_1c_2)(v, w) = ((c_1c_2)v, (c_1c_2)w) = (c_1(c_2v), c_1(c_2w))$, from the associativity of scalar multiplication in V and W.
  This is equal to $c_1(c_2v, c_2w) = c_1(c_2(v, w))$. Therefore scalar multiplication is associative in Z.

- **Unit scalar is identity** Let $e \in F$ be the unit scalar. We know it is the identity of scalar multiplication in V and W. If $(v, w) \in Z$, then $e(v, w) = (ev, ew) = (v, w)$, which proves that e is the identity of scalar multiplication in Z as well.
  From the above properties, we can conclude that Z also forms a vector

space over the field F with the given operations, QED.

7. Let $B = \{u, v, w\}$. If B is a basis for V, then it is a linearly independent set and $L(B) = V$. We will prove these properties for $C = \{u+v+w, v+w, w\}$ also.

(i) C is linearly independent. To prove this, let us assume the contrary, *i.e.*, C is linearly dependent. This means that there exist scalars c_i, not all zero, such that $c_1(u + v + w) + c_2(v + w) + c_3(w) = 0$. Rearranging, we see that $(c_1)u + (c_1 + c_2)v + (c_1 + c_2 + c_3)w = 0$. Since the c_i are not all zero, the coefficients in this equation are not all zero either, which means that B is linearly dependent. This is a contradiction; hence C is indeed linearly independent.

(ii) $L(C) = V$. Given an arbitrary vector $a \in V$, we know $a \in L(B)$, *i.e.*, it is possible to write it as $a = c_1u + c_2v + c_3w$. From this equation, we obtain $a = c_1(u + v + w) + (c_2 - c_1)(v + w) + (c_3 - c_2)w$. This means that $a \in L(C)$. Thus we conclude that $V = L(B) \subseteq L(C)$. However, by closure of vector addition, $L(C) \subseteq V$. This implies that $L(C) = V$.
From the above properties, we see that C is also a basis of V, QED.

8. We can prove this by contradiction. Let us assume that f and g are linearly dependent, *i.e.* there exists some $c_1, c_2 \in \mathbb{R}$, not both 0, such that $c_1f + c_2g = 0$.
Now, if either $c_1 = 0$ or $c_2 = 0$, then one of f and g must be identically equal to 0. Both being exponential functions, this is not possible; therefore both c_1 and c_2 are nonzero.
Hence we can write $f(t) = -\frac{c_2}{c_1}g(t)$, *i.e.*, $e^{rt} = ce^{st}$ for some constant $c = -\frac{c_1}{c_2}$.
e^{st} is always nonzero, so we divide both sides by it to get $e^{(r-s)t} = c$, for all $t \in \mathbb{R}$. Since no exponential function can have a constant value, this is a contradiction; hence f and g are in fact linearly independent, QED.

9. The set S does generate $\mathbb{R}^3$ and is linearly independent. The proof is as follows:

(i) S generates $\mathbb{R}^3$. Consider an arbitrary element $(x, y, z) \in \mathbb{R}^3$. Clearly,

$$(x, y, z) = (\frac{x + y - z}{2})(1, 1, 0)+(\frac{x - y + z}{2})(1, 0, 1)+(\frac{-x + y + z}{2})(0, 1, 1),$$

where all the coefficients are real numbers. This proves that $L(S) = \mathbb{R}^3$.

(ii) S is linearly independent. Assume that $c_1(1, 1, 0)+c_2(1, 0, 1)+c_3(0, 1, 1) = (0, 0, 0)$ for some $c_1, c_2, c_3 \in \mathbb{R}$. From this, we get the equations

$$c_1 + c_2 = 0,$$

$$c_2 + c_3 = 0,$$

and

$$c_3 + c_1 = 0.$$

The only solution to this system of equation is $c_1 = c_2 = c_3 = 0$, which means that S is in fact linearly independent.

10. Consider the vector space $\mathbb{R}^2$ over the field $\mathbb{R}$. Two of its subspaces are the sets $X = \{(x, 0)|x \in \mathbb{R}\}$ and $Y = \{(0, y)|y \in \mathbb{R}\}$, *i.e.*, the X and Y axes (proved below). The union of these two subspaces is not a subspace, as it is not closed under vector addition. For example, $(0, 3) + (4, 0) = (4, 3)$ which does not lie on either axis. This proves that the union of two subspaces of a vector space may not be a subspace.
To prove that X is a subspace, it is sufficient to show that $a(x_1, 0) + b(x_2, 0) \in X$ for all $x_1, x_2, a, b \in \mathbb{R}$, since by the definition of X, $(x_1, 0), (x_2, 0) \in X$ for all $x_1, x_2 \in \mathbb{R}$.
Now, $a(x_1, 0) + b(x_2, 0) = (ax_1, a \cdot 0) + (bx_2, b \cdot 0) = (ax_1 + bx_2, 0)$ since $x \cdot 0 = 0$ for all $x \in \mathbb{R}$. But $(ax_1 + bx_2, 0) \in X$ because $ax_1 + bx_2 \in \mathbb{R}$; hence X is a subspace.
Similarly, to prove that Y is a subspace, it is sufficient to show that $a(0, y_1) + b(0, y_2) \in Y$ for all $y_1, y_2, a, b \in \mathbb{R}$, since by the definition of Y, $(0, y_1), (0, y_2) \in X$ for all $y_1, y_2 \in \mathbb{R}$.
Now, $a(0, y_1) + b(0, y_2) = (a \cdot 0, ay_1) + (b \cdot 0, by_2) = (0, ay_1 + by_2)$ since $y \cdot 0 = 0$ for all $y \in \mathbb{R}$. But $(0, ay_1 + by_2) \in Y$ because $ay_1 + by_2 \in \mathbb{R}$; hence Y is a subspace.