Linear Algebra I
Exercise Sheet 1: Vector Spaces
Sample Solutions

For each of the following determine whether V is a vector space. Standard addition and scaling is to be assumed unless otherwise stated. If V is a vector space then determine a basis.

Question 2. $V = \mathbb{R}$.

Recall the axiomatic definition of a vector space.

Definition. Let k be a field, let V be a set, let + be a binary operation on V, and let $\cdot : k \times V \to V$ be a function. We call V a *vector space* if the following eight axioms are satisfied: for all u, v, and $w \in V$ and ρ, $\lambda \in k$,

- $v + w = w + v$;
- $(u + v) + w = u + (v + w)$;
- there exists $0 \in V$ such that $v + 0 = v$;
- there exists $-v$ such that $v + (-v) = 0$;
- $\lambda(\rho v) = (\lambda\rho)v$;
- $(\lambda + \rho)v = \lambda v + \rho v$;
- $\lambda(v + w) = \lambda v + \lambda w$;
- $1v = v$.

Solution. The base field is $\mathbb{R}$. Addition is standard addition of numbers and scaling is standard multiplication. As such we inherit the commutativity of addition (1) and associativity of both addition (2) and multiplication (5). Distributivity of real numbers provides (6) and (7). The existence of 0 (3) and additive inverses (4) also follow from $\mathbb{R}$ being a field, as is the standard multiplication by 1 (8). Hence $\mathbb{R}$ is a vector space over $\mathbb{R}$.

Every real number is a linear combination of 1 (any real number is written $1 \cdot \alpha = \alpha \in \mathbb{R}$). Hence a basis for $\mathbb{R}$ is $\{1\}$. In fact, any set containing a single non zero real number is a basis for $\mathbb{R}$.

Question 6. *Let k be composite (not prime).*

$$V = \mathbb{Z}_k = \big\{\{nk \,|\, n \in \mathbb{Z}\}, \{nk+1 \,|\, n \in \mathbb{Z}\}, \ldots, \{nk+k-1 \,|\, n \in \mathbb{Z}\}\big\},$$

where

$$\{n_1k + p\} + \{n_2k + q\} = \{(n_1 + n_2)k + p + q\}$$

for all $p, q \in \mathbb{Z}_k$ and

$$\lambda \cdot \{nk + p\} = \{\lambda nk + \lambda p\}$$

for all $\lambda \in \mathbb{Z}_k$.

Recall our working definition of a field for this course:

Definition.
- A *binary operation* $*$ on a set S is a function $* : S \times S \to S$.
- A *field* is a set with two binary operations + and $\cdot$ with the same properties as $\mathbb{R}$, that is, commutativity of addition, associativity of addition and multiplication, standard distribution, and existence of both additive and multiplicative inverses (necessitating the existence of both additive and multiplicative identities).

Solution. We do not have multiplicative inverses in $\mathbb{Z}_n$ if n is composite: say $n = ab$ with $a \neq 0$ and $b \neq 0$, or, more precisely, $a \not\equiv 0 \mod n$ and $b \not\equiv 0 \mod n$. Then $a \cdot b \equiv 0 \mod n$. Hence $\mathbb{Z}_n$ is not a field. However we may still check the axioms: say a^{-1} exists. Then

$$0 \equiv a^{-1} \cdot 0 \equiv a^{-1}(ab) \equiv (a^{-1}a)b \equiv b \mod n.$$

This is a contradiction as we assumed $b \not\equiv 0 \mod n$.

Question 8. *$V = \{a_0 + a_1x + \ldots + a_ix^i \mid i \leq n\}$, for some fixed $n \in \mathbb{N}$, where $a_i \in \mathbb{R}$ for all i. Addition and scaling are standard for polynomials with real coefficients.*

Solution. Every polynomial is written $f(x) = f_0 + \ldots + f_nx^n$ where $f_i \in \mathbb{R}$ can be zero. Let us check the first four axioms. Let $f(x)$, $g(x)$, and $h(x)$ be such polynomials with coefficients f_i, g_i, and h_i respectively. Let λ and ρ be real numbers.

(1)
$$\begin{aligned} f(x) + g(x) &= f_0 + \ldots f_nx^n + g_0 + \ldots g_nx^n \\ &= (f_0 + g_0) + (f_1 + g_1)x + \ldots (f_n + g_n)x^n \\ &= (g_0 + f_0) + (g_1 + f_1)x + \ldots (g_n + f_n)x^n \\ &= g_0 + \ldots g_nx^n + f_0 + \ldots f_nx^n \\ &= g(x) + f(x). \end{aligned}$$

The second equality follows from the commutative property of real polynomials and the third follows from commutativity of real numbers.

(2)
$$\begin{aligned} f(x) + \big(g(x) + h(x)\big) &= f_0 + \ldots f_nx^n + (g_0 + \ldots g_nx^n + h_0 + \ldots h_nx^n) \\ &= f_0 + \ldots f_nx^n + \big((g_0 + h_0) + \ldots (g_nx^n + h_nx^n)\big) \\ &= f_0 + (g_0 + h_0) + \ldots f_nx^n + (g_nx^n + h_nx^n) \\ &= (f_0 + g_0) + h_0 + \ldots (f_nx^n + g_nx^n) + h_nx^n \\ &= (f_0 + \ldots f_nx^n + g_0 + \ldots g_nx^n) + h_0 + \ldots h_nx^n \\ &= \big(f(x) + g(x)\big) + h(x). \end{aligned}$$

The second inequality follows from commutativity of real polynomials and the third from associativity of real numbers.

(3) The additive identity is the polynomial whose coefficients are all 0:

$$\begin{gathered} a_0 + \ldots + a_nx^n + 0 + 0 \cdot x + \ldots + 0 \cdot x^n = (a_0 + 0) + \ldots + (a_n + 0)x^n \\ a_0 + \ldots a_nx^n. \end{gathered}$$

We typically denote this polynomial by 0, although this is an abuse of notation, as 0 now refers to both a real number and a polynomial whose coefficients are all 0.

(4) The additive identity of a polynomial $f(x) = f_0 + \ldots + f_nx^n$ is polynomial formed by taking the additive inverse of every coefficient $-f(x) := (-f_0) + \ldots + (-f_n)x^n$:

$$\begin{aligned} f(x) + \big(-f(x)\big) &= f_0 + \ldots + f_nx^n + (-f_0) + \ldots + (-f_n)x^n \\ &= (f_0 - f_0) + \ldots + (f_n - f_n)x^n \\ &= 0. \end{aligned}$$

The second inequality follows from commutativity of real polynomials.

A basis for degree-n polynomials can be inferred directly from their definition:

$$f(x) = f_0 + f_1x + f_2x^2 + \ldots + f_nx^n$$

is already a linear combination of $X = \{1, x, x^2, \ldots, x^n\}$. It remains to show that X is linearly independent, i.e. that only linear combination

$$a_0 + a_1x + \ldots a_nx^n = 0 + 0 \cdot x + \ldots 0 \cdot x^n$$

if and only if $a_i = 0$ for all $i = 1, \ldots, n$. Recall that two polynomials $f(x) = f_0 + \ldots f_nx^n$ and $g(x) = g_0 + \ldots g_nx^n$ are equal if and only if $f_i = g_i$ for all i. Hence

$$a_0 + a_1x + \ldots a_nx^n = 0 + 0 \cdot x + \ldots 0 \cdot x^n$$

if and only if a_i=0 for all i, and so X is linearly independent, and must be a basis.