The University of Sydney

MATH2902 Vector Spaces

(http://www.maths.usyd.edu.au/u/UG/IM/MATH2902/)

Semester1, 2001 Lecturer: R. Howlett

Tutorial 5

1. In each case decide whether or not the set S is a vector space over the field F, relative to obvious operations of addition and scalar multiplication. If it is, decide whether it has finite dimension, and if so, find the dimension.

(*i*) $S=\mathbb{C}$ (complex numbers), $F=\mathbb{R}$.

(*ii*) $S=\mathbb{C}$, $F=\mathbb{C}$.

(*iii*) $S=\mathbb{R}$, $F=\mathbb{Q}$ (rational numbers).

(*iv*) $S=\mathbb{R}[X]$ (polynomials over $\mathbb{R}$ in the variable X—that is, expressions of the form $a_0+a_1X+\cdots+a_nX^n$ $(a_i\in\mathbb{R})$), $F=\mathbb{R}$.

(*v*) $S=\mathrm{Mat}(n,\mathbb{C})$ ($n\times n$ matrices over $\mathbb{C}$), $F=\mathbb{R}$.

Solution.

(*i*) Yes, $\mathbb{C}$ is a vector space over $\mathbb{R}$. Since every complex number is uniquely expressible in the form $a+b\boldsymbol{i}$ with a, $b\in\mathbb{R}$ we see that $(1,\boldsymbol{i})$ is a basis for $\mathbb{C}$ over $\mathbb{R}$. Thus the dimension is two.

(*ii*) Every field is always a 1-dimensional vector space over itself. The one element sequence (1), where 1 is the multiplicative identity, is a basis. More generally, if $a\neq 0$ then (a) is a basis. (There was a minor omission from the field axioms stated in lectures. The multiplicative identity axiom should have included the requirement that $1\neq 0$. This eliminates the set with just one element, which is not counted as a field.)

(*iii*) $\mathbb{R}$is a vector space over $\mathbb{Q}$. In fact this space is not finite dimensional. (This can be proved by showing that $\mathbb{Q}$ is "countable"—that is, there is a bijective function $\mathbb{Z}\to\mathbb{Q}$—whereas $\mathbb{R}$ is not. But such things are not really part of this course.)

(*iv*) $\mathbb{R}[X]$ is a vector space over $\mathbb{R}$. Since $(1,X,X^2,\dots)$ is an infinite linearly independent sequence in $\mathbb{R}[X]$ it follows that the dimension is infinite.

(*v*) Since

$$S=\left\{\begin{pmatrix} a_{11}+b_{11}\boldsymbol{i} & a_{12}+b_{12}\boldsymbol{i} & \dots & a_{1n}+b_{1n}\boldsymbol{i}\\ a_{21}+b_{21}\boldsymbol{i} & a_{22}+b_{22}\boldsymbol{i} & \dots & a_{2n}+b_{2n}\boldsymbol{i}\\ \vdots & \vdots & & \vdots\\ a_{n1}+b_{n1}\boldsymbol{i} & a_{n2}+b_{n2}\boldsymbol{i} & \dots & a_{nn}+b_{nn}\boldsymbol{i}\end{pmatrix}\middle|\, a_{ij},\, b_{ij}\in\mathbb{R}\right\}$$

it can be seen that S is a $2n^2$-dimensional vector space over $\mathbb{R}$. Indeed the function $f\colon S\to\mathbb{R}^{2n^2}$ such that

$$f\begin{pmatrix} a_{11}+b_{11}\boldsymbol{i} & a_{12}+b_{12}\boldsymbol{i} & \dots & a_{1n}+b_{1n}\boldsymbol{i}\\ a_{21}+b_{21}\boldsymbol{i} & a_{22}+b_{22}\boldsymbol{i} & \dots & a_{2n}+b_{2n}\boldsymbol{i}\\ \vdots & \vdots & & \vdots\\ a_{n1}+b_{n1}\boldsymbol{i} & a_{n2}+b_{n2}\boldsymbol{i} & \dots & a_{nn}+b_{nn}\boldsymbol{i}\end{pmatrix}=\begin{pmatrix} a_{11}\\ b_{11}\\ a_{12}\\ b_{12}\\ \vdots\\ a_{1n}\\ b_{1n}\\ a_{21}\\ \vdots\\ \vdots\\ b_{nn}\end{pmatrix}$$

is a vector space isomorphism.

2. Let $\mathbb{Z}_2$ be the field which has just the two elements 0 and 1. (See §1d#10 of the book.) How many elements will there be in a four dimensional vector space over $\mathbb{Z}_2$?

Solution.

Let V be a four dimensional vector space over $\mathbb{Z}_2$, and let (v_1,v_2,v_3,v_4) be a basis of V. Then every element of V is uniquely expressible in the form $\lambda_1v_1+\lambda_2v_2+\lambda_3v_3+\lambda_4v_4$ with each λ_i in $\mathbb{Z}_2$, and since there two choices (0 or 1) for each of the four λ_i we have $2^4=16$ choices altogether. Thus V has 16 elements.

3. (*i*) Let V be a vector space over a field F and let S be any set. Convince yourself that that the set of all functions from S to V becomes a vector space over F if addition and scalar multiplication of functions are defined in the usual way.

(Hint: To do this in detail requires checking that all the vector space axioms are satisfied. However, the proof in §3b#6 of the book is almost word for word the same as the proof required here.)

(*ii*) Use part (*i*) to show that if V and W are both vector spaces then the set of all linear transformations from V to W is a vector space (with the usual definitions of addition and scalar multiplication of functions).

Solution.

(*i*) Let $\mathcal{F}$ be the set of all functions from S to V. If f, $g\in\mathcal{F}$ and $\lambda\in F$ then $f+g$ and λf are the functions defined by $(f+g)(s)=f(s)+g(s)$ and $(\lambda f)(s)=\lambda(f(s))$ for all $s\in S$. We must check that, with addition and scalar multiplication defined in this way, $\mathcal{F}$ satisfies the vector space axioms (listed in Definition 2.3). In each case, the proof that $\mathcal{F}$ satisfies a given axiom makes use of the fact that V satisfies that axiom.

Let f, g and h be arbitrary elements of $\mathcal{F}$ and λ, μ arbitrary scalars. Since addition in V is associative ($(x+y)+z = x+(y+z)$ for all x, y, $z \in V$) we find that for all $s \in S$

$$((f+g)+h)(s) = (f+g)(s)+h(s) = (f(s)+g(s))+h(s)$$
$$= f(s)+(g(s)+h(s)) = f(s)+(g+h)(s) = (f+(g+h))(s),$$

and so $(f+g)+h = f+(g+h)$. Similarly since $(\lambda+\mu)x = \lambda x+\mu x$ for all $x \in V$, we have, for all $s \in S$,

$$((\lambda+\mu)f)(s) = (\lambda+\mu)(f(s)) = \lambda(f(s))+\mu(f(s))$$
$$= (\lambda f)(s)+(\mu f)(s) = (\lambda f+\mu f)(s)$$

and so $(\lambda+\mu)f = \lambda f+\mu f$. Similar proofs show that $f+g = g+f$, $\lambda(f+g) = \lambda f+\lambda g$, $(\lambda\mu)f = \lambda(\mu f)$ and $1f = f$. This takes care of six of the eight axioms; it remains to show that $\mathcal{F}$ has a zero element, and that all elements of $\mathcal{F}$ have negatives. Define $z: S \to V$ by $z(s) = \underset{\sim}{0}$ for all $s \in S$, where $\underset{\sim}{0}$ is the zero of V. Then z is a zero for $\mathcal{F}$, since for all $f \in \mathcal{F}$ and all $s \in S$

$$(z+f)(s) = z(s)+f(s) = \underset{\sim}{0}+f(s) = f(s).$$

Finally, if $f \in \mathcal{F}$ then $-f$ defined by $(-f)(s) = -(f(s))$ satisfies $f+(-f) = z$, since

$$(f+(-f))(s) = f(s)+(-f)(s) = f(s)+(-f(s)) = 0 = z(s).$$

(ii) Let $\mathcal{L}$ be the set of all linear functions from V to W and $\mathcal{F}$ the set of all functions from V to W. Clearly $\mathcal{L} \subseteq \mathcal{F}$, and $\mathcal{F}$ is a vector space by the first part. We must show that $\mathcal{L}$ is nonempty and closed under addition and scalar multiplication.

The zero function z is clearly linear: for all u, $v \in V$ and λ, $\mu \in F$ we have

$$z(\lambda u+\mu v) = 0 = \lambda 0+\mu 0 = \lambda z(u)+\mu z(v).$$

Thus $\mathcal{L}$ contains at least the element z, and is therefore nonempty.

Let f, $g \in \mathcal{L}$ and $\alpha \in F$. For all u, $v \in V$ and λ, $\mu \in F$ we have

$$(f+g)(\lambda u+\mu v) = f(\lambda u+\mu v)+g(\lambda u+\mu v)$$
$$= (\lambda f(u)+\mu f(v))+(\lambda g(u)+\mu g(v))$$
$$= \lambda(f(u)+g(u))+\mu(f(v)+g(v))$$
$$= \lambda(f+g)(u)+\mu(f+g)(v),$$

the first line and last equalities by the definition of addition of functions, the second by the fact that f and g are linear, and the third by use of associative, commutative and distributive laws in the vector space W. Thus we see that $f+g$ is linear, and we have shown that the sum of two elements of $\mathcal{L}$ is necessarily in $\mathcal{L}$. Similarly,

$$(\alpha f)(\lambda u+\mu v) = \alpha(f(\lambda u+\mu v)$$
$$= \alpha(\lambda f(u)+\mu f(v))$$
$$= \lambda(\alpha f(u))+\mu(\alpha f(v))$$
$$= \lambda((\alpha f)(v))+\mu((\alpha f)(v))$$

showing that αf is linear, and hence showing that $\mathcal{L}$ is closed under scalar multiplication.

4. Let U and V be vector spaces over a field F. A function $f: V \to W$ is called a *vector space isomorphism* if f is a bijective linear transformation. Prove that if $f: U \to V$ is a vector space isomorphism then the inverse function $f^{-1}: V \to U$ (defined by the rule that $f^{-1}(v) = u$ if and only if $f(u) = v$) is also a vector space isomorphism.

Solution.

It is a general fact about functions that if $f: U \to V$ is bijective then there exists an inverse function $f^{-1}: V \to U$ which is also bijective. Let us prove this first.

We must show that

$$f^{-1}(v) = u \text{ if and only if } f(u) = v$$

is a well defined rule assigning a uniquely determined element of U to each element of V. So, let $v \in V$ (arbitrary). Since f is surjective there exists $u \in U$ with $f(u) = v$. Since f is injective there is no other element of U with this property: if $f(u') = v = f(u)$ then $u' = u$. So the stated rule does indeed assign a unique element of U to each element of V. Suppose that $f^{-1}(v_1) = f^{-1}(v_2)$ for some v_1 $v_2 \in V$. Let $u = f^{-1}(v_1) = f^{-1}(v_2)$. Then by definition of f^{-1}, $f(u) = v_1$ and $f(u) = v_2$. So $v_1 = v_2$. Hence f^{-1} is injective. Let u be an arbitrary element of U. Let $v = f(u) \in V$. Then $f^{-1}(v) = u$. Hence f^{-1} is surjective.

To show that f^{-1} is an isomorphism it remains to show that it is linear. So, let v_1, $v_2 \in V$, $\lambda \in F$. Let $u_1 = f^{-1}(v_1)$, $u_2 = f^{-1}(v_2)$. Then since f is linear,

$$f(u_1+u_2) = f(u_1)+f(u_2) = v_1+v_2$$

and

$$f(\lambda u_1) = \lambda f(u_1) = \lambda v_1$$

and therefore

$$f^{-1}(v_1 + v_2) = u_1 + u_2 = f^{-1}(v_1) + f^{-1}(v_2)$$

and

$$f^{-1}(\lambda v_1) = \lambda u_1 = \lambda f^{-1}(v_1).$$

Hence f^{-1} is linear, as required.

5. (*i*) Prove that if $v_1,\ v_2,\ \ldots,v_n$ are linearly independent elements of a vector space V and $v_{n+1} \in V$ is not contained in $\mathrm{Span}(v_1, v_2, \ldots, v_n)$ then $v_1,\ v_2,\ \ldots,v_{n+1}$ are linearly independent.

(*ii*) If $v_1,\ v_2,\ \ldots,v_n$ are linearly independent elements of V and V is spanned by elements $w_1,\ w_2,\ \ldots,w_m$ then $n \le m$. (This is Theorem 4.14 of the book, the proof of which was relatively hard.) Use this result and the first part to prove that if $v_1,\ v_2,\ \ldots,v_n$ are linearly independent then there exist $v_{n+1},\ v_{n+2},\ \ldots,\ v_d \in V$ such that $v_1,\ v_2,\ \ldots,v_d$ form a basis of V.

Solution.

(*i*) Since "if p and q then r" is logically equivalent to "if p and not r then not q" the question can be rephrased as follows: if $v_1,\ v_2,\ \ldots,v_n$ are linearly independent and $v_1,\ \ldots,v_n,\ v_{n+1}$ are not linearly independent then v_{n+1} is in $\mathrm{Span}(v_1, v_2, \ldots, v_n)$. This is proved in the book, and was proved in lectures (Lemma 4.4).

There is no harm in proving it again. Assume that $v_1, v_2, \ldots,\ v_n$ are linearly independent and $v_{n+1} \notin \mathrm{Span}(v_1, \ldots, v_n)$. Suppose now that $\lambda_1,\ \lambda_2,\ \ldots,\lambda_{n+1}$ are scalars such that

$$(*) \qquad \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_{n+1} v_{n+1} = 0$$

If $\lambda_{n+1} \neq 0$ then $(*)$ gives $v_{n+1} = -\lambda_{n+1}^{-1} \sum_{i=1}^{n} \lambda_i v_i \in \mathrm{Span}(v_1, \ldots, v_n)$, a contradiction. So $\lambda_{n+1} = 0$, and $(*)$ becomes

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0.$$

Linear independence of $v_1,\ v_2, \ldots, v_n$ gives $\lambda_i = 0$ for $i = 1, 2, \ldots, n$. So the only solution to $(*)$ is given by

$$\lambda_1 = \lambda_2 = \cdots = \lambda_{n+1} = 0.$$

Hence $v_1,\ v_2,\ \ldots,v_{n+1}$ are linearly independent.

(*ii*) If $v_1,\ v_2, \ldots, v_n$ span V then they form a basis of V, and the claim is vacuously true (with $d = n$). Otherwise there must be at least one element of V not in $\mathrm{Span}(v_1, v_2, \ldots, v_n)$. Let v_{n+1} be any such element.

By the first part we know that $v_1,\ v_2, \ldots, v_{n+1}$ are linearly independent. If they also span V then they form a basis, and we are finished (taking $d = n + 1$). If they do not span then we can repeat the argument, choosing v_{n+2} to be outside the subspace they span, thereby obtaining a longer linearly independent sequence of elements. Either this lot will be a basis, or we can choose another independent element and increase the length again. But the number of terms in a linearly independent sequence can not exceed m, the number of terms in the spanning sequence. So in at most m steps a situation will be reached in which the length of our linearly independent sequence of elements cannot be increased further, and this can only happen when they span the whole space V.