II. Vector spaces

II.A. Vector spaces and subspaces

I'll begin by discussing some of the basic objects of abstract algebra that are relevant to matrices, and arrive at the definition of vector spaces, rather than throwing one lengthy definition at you.

First off, there is a name for the algebraic structure comprising the $m \times m$ matrices $M_m(\mathbb{R})$ with (matrix) multiplication. (Recall that this product is associative but not commutative.)

II.A.1. DEFINITION. A *semigroup* $(S, \cdot, 1)$ consists of a set S, an associative binary operation (product) "$\cdot$", and an identity element $1 \in S$ such that $s \cdot 1 = s = 1 \cdot s$ for every $s \in S$.

Whenever the binary operation is commutative we call the algebraic structure *abelian*, after Abel. The *units* in a semigroup are its invertible elements.[1]

What if we look only at the invertible matrices $GL_m(\mathbb{R})$ (the "general linear group")?

II.A.2. DEFINITION. A *group* $(G, \cdot, 1)$ is just a semigroup consisting entirely of units. The *center* $Z(G)$ is the "subgroup" of elements that commute with every other element. For instance, $Z(GL_m(\mathbb{R})) =$ matrices of the form $a\mathbb{I}_m$ (with $a \in \mathbb{R}$).

Now you can *add* matrices (in fact, $m \times n$ matrices), and obviously $M_1 + M_2 = M_2 + M_1$. This gives an abelian group $(G, +, 0)$. (While "$\cdot$" can be commutative or not, "$+$" always denotes a commutative binary operation. For such "additive" groups, the inverses are written "$-g$" rather than "g^{-1}".)

[1] That is, elements $x \in S$ for which there exists a $y \in S$ with $xy = yx = 1$.

Let's put the two structures on $M_m(\mathbb{R})$ together.

II.A.3. DEFINITION. A *ring* $(R, +, \cdot, 0, 1)$ is a set with two binary operations (and corresponding identity elements) such that

(i) $(R, +, 0)$ is an abelian group,
(ii) $(R, \cdot, 1)$ is a semigroup, and
(iii) the distributive laws hold (on both sides).

We can combine the operations in a ring to define the *commutator* of two elements

$$[r, s] := r \cdot s - s \cdot r = r \cdot s + \{-(s \cdot r)\}.$$

These are important in quantum mechanics: they tell when two quantities (eigenvalues of their respective operator matrices) are not simultanously determinable. Clearly $M_m(\mathbb{R})$ is a ring, but a non-commutative one. One can construct some commutative examples via "modular arithmetic": declaring $0 \equiv n$ for $n > 1$ some fixed positive integer gives the ring $\mathbb{Z}/n\mathbb{Z}$. For example, in $\mathbb{Z}/6\mathbb{Z}$, $2 \cdot 3 \equiv 0$ and $3 + 4 \equiv 1$.

Just as a group is a nice kind of semigroup, we have:

II.A.4. DEFINITION. A *field* $(F, \cdot, +, 0, 1)$ is a nice type of ring, in which

(i) "$\cdot$" is commutative and
(ii) every element *but* 0 is multiplicatively invertible.

We write $F^* = F \setminus \{0\}$ for those elements, and rewrite (i) and (ii) by saying that $(F, +, 0)$ and $(F^*, \cdot, 1)$ are both abelian groups. $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields, and so is $\mathbb{Z}/n\mathbb{Z}$ if $n > 1$ is prime!

II.A.5. REMARK. Dropping (i) from Definition II.A.4 yields an algebraic structure somewhere between a ring and a field, called a *division ring*. You might wonder if the invertible matrices $GL_m(\mathbb{R})$ (together with the zero matrix) constitute a division ring. But they do

not, as they fail to be closed under addition:

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ are invertible}$$

$$\text{but } \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

is not. An actual example of a division ring that is not a field is given in Exercise (3).

We come to our last pair of algebraic structures:

II.A.6. DEFINITION. A *module* M over a ring R is an abelian group $(M, +, 0)$ together with a "left-action" $R \times M \to M$ of the ring R on M. This associates $(r, m) \mapsto rm$ in such a way that

(i) $r(m_1 + m_2) = rm_1 + rm_2$,
(ii) $(r_1 + r_2)m = r_1 m + r_2 m$,
(iii) $(r_1 \cdot r_2)m = r_1(r_2 m)$, and
(iv) $1m = m$.

A simple example: $\mathbb{R}^m$ is a module over $M_m(\mathbb{R})$ (the map $M_m(\mathbb{R}) \times \mathbb{R}^m \to \mathbb{R}^m$ is just the action of $m \times m$ matrices on vectors). Finally:

II.A.7. DEFINITION. A module over a field is called a *vector space* V/F. For instance, one has $\mathbb{R}^m/\mathbb{R}$ where the map $\mathbb{R} \times \mathbb{R}^m \to \mathbb{R}^m$ sending $(a, \vec{v}) \mapsto a\vec{v}$ is just scalar multiplication (which obeys (i)-(iv) in II.A.6 above).

Vector subspaces. For the sake of concreteness let's pass back to the case $F = \mathbb{R}$ (though what follows works for any field).

II.A.8. DEFINITION. A subset $W \subseteq V/\mathbb{R}$ is called a *subspace* if it is itself a vector space $/\mathbb{R}$, under the "$\cdot$" and "$+$" inherited from V.

Obviously there's a lot to check in the definition, so the following is welcome:

II.A.9. PROPOSITION. *$W \subseteq V$ is a subspace if it contains all linear combinations $a\vec{w}_1 + b\vec{w}_2$ of its own elements.*

Now we give some examples of how to construct subspaces. Suppose we already have two, W_1 and W_2. Then $W_1 \cap W_2$ is one but $W_1 \cup W_2$ is *not*! (Think of the union of the two coordinate axes in $\mathbb{R}^2$: it contains $\hat{e}_1$ and $\hat{e}_2$ but not their sum.) To fix this, define

$$W_1 + W_2 = \{\vec{w}_1 + \vec{w}_2 \,|\, \forall\, \vec{w}_1 \in W_1,\, \vec{w}_2 \in W_2\}\,,$$

which *is* a subspace (the smallest one containing $W_1 \cup W_2$). Solutions of $A\vec{x} = 0$ are subspaces, but the same does not go for $A\vec{x} = \vec{y}$ ($\vec{y} \neq 0$): in particular, the $\mathcal{W}_i$ from §I.A aren't subspaces of $\mathbb{R}^n$.

In the same spirit as $W_1 + W_2$, we can also construct a subspace of V if we have some vectors $\vec{v}_1, \ldots, \vec{v}_m \in V$. Define

$$span\{\vec{v}_1, \ldots, \vec{v}_m\} = \{a_1\vec{v}_1 + \ldots + a_m\vec{v}_m \,|\, \forall\, a_i \in \mathbb{R}.\}$$

If $span\{\vec{v}_i\}_{i=1}^m = V$ then the $\{\vec{v}_i\}_{i=1}^m$ "span V".

Linear (In)dependence.

II.A.10. DEFINITION. The (finite) collection[2] of vectors $\{\vec{v}_1, \ldots, \vec{v}_m\}$ is said to be linearly *dependent* iff there is a relation

$$x_1\vec{v}_1 + \ldots + x_m\vec{v}_m = 0, \text{ where not all } x_i = 0.$$

Otherwise, it is linearly *independent*.

Writing

$$A = \begin{pmatrix} \uparrow & & \uparrow \\ \vec{v}_1 & \ldots & \vec{v}_m \\ \downarrow & & \downarrow \end{pmatrix},$$

this means that $\{\vec{v}_i\}_{i=1}^m$ are independent iff $A\vec{x} = 0$ has only the trivial solution. Equivalently, $rref(A)$ has a leading 1 in every column:

[2]Warning: by "collection", we mean an unordered list, not a set. After all, the definition is sensitive to repetition: if (say) $\vec{v}_1 = \vec{v}_2$, taking $x_1 = 1 = -x_2$ (and the remaining x_i zero) yields a dependence relation.

e.g., if

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = rref \begin{pmatrix} \uparrow & \uparrow & \uparrow \\ \vec{v}_1 & \vec{v}_2 & \vec{v}_3 \\ \downarrow & \downarrow & \downarrow \end{pmatrix}$$

for three vectors in $\mathbb{R}^5$, they are linearly independent. On the other hand, if some column of $rref(A)$ lacks a leading 1 you can freely plug in some nonzero value for the corresponding variable and solve $rref(A)\vec{x} = 0$ (hence $A\vec{x} = 0$) for a nontrivial dependence relation.

Exercises

(1) Let V be the set of all pairs (x, y) of real numbers, and let $\mathbb{R}$ as usual denote the field of real numbers. (a) Is V, with the operations

$$(x, y) + (x_1, y_1) = (x + x_1, y + y_1) \quad \text{and} \quad c(x, y) = (cx, y),$$

a vector space over the field of real numbers? (b) What if we replace the operations by

$$(x, y) + (x_1, y_1) = (x + x_1, 0) \quad \text{and} \quad c(x, y) = (cx, 0)?$$

(2) Let F be a field and let n be a positive integer ($n \geq 2$). Let V be the vector space of all $n \times n$ matrices over F. Which of the following sets of matrices A in V are subspaces of V?
(a) all invertible A;
(b) all non-invertible A;
(c) all A such that $AB = BA$, where B is some fixed matrix in V;
(d) all A such that $A^2 = A$.

(3) The subset $\mathbb{H} \subseteq M_2(\mathbb{C})$ defined in Exercise (I.C.6), since it is closed under addition and multiplication, is in fact a *subring*.

(a) Find a matrix for the inverse of x in Exercise (I.C.6), writing for convenience $|x|^2 := a_0^2 + a_1^2 + a_2^2 + a_3^2$. It should not look complicated. (This shows that every nonzero element of $\mathbb{H}$ is invertible, making $\mathbb{H}$ a division ring.)

(b) Next, writing

$$\mathbf{i} = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \ \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \mathbf{k} = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix},$$

so that all $x \in \mathbb{H}$ can be written $x = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$ (where a_0 means $a_0\mathbb{I}_2$), what is x^{-1} in these terms?

(c) Derive a multiplication table for $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ (e.g., what is $\mathbf{j}^2$, $\mathbf{i} \cdot \mathbf{k}$, etc., in terms of linear combinations of $1 = \mathbb{I}_2$, $\mathbf{i}$, $\mathbf{j}$, and $\mathbf{k}$ with real coefficients). For example, $\mathbf{i}^2 = -1$ and so via $a_0 + a_1\mathbf{i}$ you can think of $\mathbb{C}$ as lying inside of $\mathbb{H}$. (Congratulations! It took Hamilton 10 years to produce this multiplication table, extending the complex numbers.)

(4) Are the vectors

$$\vec{v}_1 = \begin{pmatrix} 1 \\ 1 \\ 2 \\ 4 \end{pmatrix}, \ \vec{v}_2 = \begin{pmatrix} 2 \\ -1 \\ -5 \\ 2 \end{pmatrix}, \ \vec{v}_3 = \begin{pmatrix} 1 \\ -1 \\ -4 \\ 0 \end{pmatrix}, \ \vec{v}_4 = \begin{pmatrix} 2 \\ 1 \\ 1 \\ 6 \end{pmatrix}$$

linearly independent in $\mathbb{R}^4$?

(5) Does

$$\vec{b} = \begin{pmatrix} 2 \\ 5 \\ -4 \end{pmatrix}$$

belong to the span of

$$\vec{v}_1 = \begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix} \text{ and } \vec{v}_2 = \begin{pmatrix} -4 \\ 3 \\ 8 \end{pmatrix}?$$