ALGEBRA II (VECTOR SPACES) (1982)

Paul Taylor (Trinity)

A thorough understanding of Linear Algebra is essential for almost any branch of Mathematics. Many students will already be familiar with vectors and matrices, but this course emphasises a coordinate-free approach: one eventually realises that the subject is easier if one treats vectors as abstract "point" entities rather than as lists of numbers.

A vector space over a field K (which you may always in this course assume to be $\mathbb{R}$ or $\mathbb{C}$, although you will gain in understanding if you experiment with, say, $K=\{0,1\}$ and addition and multiplication modulo 2) is an Abelian group $(V,+,0)$ (where 0 is the zero vector and $+$ is vector-parallelogram-addition) with an operation $\cdot : F\times V \to V$ called scalar multiplication (don't confuse this with the so-called "scalar product" in the Michaelmas Vector Calculus course) such that $\lambda.(\underline{x}+\underline{y}) = \lambda.\underline{x} + \lambda.\underline{y}$, $(\lambda+\mu).\underline{x} = \lambda\underline{x}+\mu.\underline{x}$ and $(\lambda\mu).\underline{x} = \lambda.(\mu.\underline{x})$.

By a subspace we mean a subset closed under addition and scalar multiplication by elements of K (including 0, so it always contains the zero vector). Given an arbitrary subset, the subspace spanned by it is the smallest subspace containing it, consisting of those vectors which may be expressed as (finite) linear combinations of the given elements. The empty set spans the zero subspace, $\{0\} \leq V$.

If the subspace spanned by a subset is the whole space we call it a spanning set. A subset which is such that no proper subset of it spans the whole of the subspace which it does is said to be linearly independent; equivalently, any relation of the form $a_1\underline{x}_1 + a_2\underline{x}_2 + \ldots + a_n\underline{x}_n = 0$ with $\underline{x}_i$ distinct elements of the given set must have $0=a_1=a_2=\cdots=a_n$. A linearly independent spanning set is called a basis (or base).

A vector-space with a finite spanning set is said to be finitely-generated or of finite dimension; in this case we may choose a subset which is also linearly independent, ie a basis. Moreover any two bases have the same number of elements, this number being called the dimension of the space. One frequently wants to extend a given linearly independent set to a basis by choosing vectors from a particular spanning set; this and the fact that a linearly independent set is at most as large as a spanning set (from which the invariance of dimension follows immediately) are called the exchange lemma.

We define a linear map or vector-space homomorphism in the same way as we did with groups, namely as a function preserving addition and scalar multiplication:

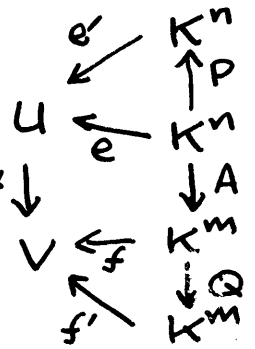
$$(\lambda \underline{x} + \mu \underline{y})\alpha = \lambda(\underline{x}\alpha) + \mu(\underline{y}\alpha)$$

A bijective linear map has an inverse linear map and is called an isomorphism. The image of a linear map is a subspace, as is its kernel (the set of elements mapping to zero). When you solve a homogeneous linear differential equation (in Linear Systems), you're finding the kernel of a linear map from an infinite-dimensional vector-space to itself. An important difference between vector-spaces and groups is that in the former case every subspace is the kernel of some homomorphism, and this fact makes the theory much simpler.

One may define a base as a particular isomorphism between K^n (for some n, being the dimension) and V, by $(1,0,\ldots 0) \mapsto e_1$, $(0,1,\ldots) \mapsto e_2$, etc. The coordinates of a vector wrt a basis are then essentially the inverse image of the vector under this isomorphism. Given a linear map $\alpha: U \to V$ between two vector spaces, with bases $e: K^n \cong U$ and $f: K^m \cong V$, we have a linear map $A: K^n \to K^m$ completing the square, so $A = e\alpha f^{-1}$, which is called the matrix of the linear map wrt the bases e, f.

$$\begin{array}{ccc} U & \xleftarrow{e} & K^n \\ {\scriptstyle\alpha}\downarrow & & \vdots{\scriptstyle A} \\ V & \xleftarrow[f]{} & K^m \end{array}$$

If we now change to bases e', f' we have isomorphisms (invertible matrices) $P = ee'^{-1} : K^n \cong K^n$ and $Q = f f'^{-1} : K^m \cong K^m$ and the matrix of α wrt (e', f') is now $P^{-1}AQ$.



Note that if U and V are the same space we have $e = f$, $e' = f'$ and $P = Q$ so the base-change for an <u>endomorphism</u> $\alpha : U \to U$ is $P^{-1}AP$.

The dimensions of the image and kernel spaces of a linear map are called its <u>rank</u> and <u>nullity</u> respectively. The sum of these is the dimension of the domain space. This may be shown by extending the inverse image of a basis for the image to a basis for the domain, or else as an immediate consequence of the isomorphism theorem that $\text{im}\,\alpha \cong \text{dom}\,\alpha / \ker\alpha$ where we define the quotient space as the set of cosets in the same way as for groups.

Given two vector-spaces, we may put a vector-space structure on their cartesian product in the same way as we did with groups. Then if $\alpha : W \to U$, $\beta : W \to V$ are linear maps there is a linear map $(\alpha, \beta) : W \to U \times V$ by $\underline{w} \mapsto (\underline{w}\alpha, \underline{w}\beta)$ so that $U \times V$ is a "product". On the other hand, given $\gamma : U \to X$ and $\delta : V \to X$ we also have $\gamma + \delta : U \times V \to X$ by $(\underline{u}, \underline{v}) \mapsto \underline{u}\gamma + \underline{v}\delta$ so $U \times V$ is also a sum, and it's usually written $U \oplus V$ since $\dim U \oplus V = \dim U + \dim V$ [It's clear that $K^n \oplus K^m \cong K^{n+m}$ and you can prove it in general using these properties of sums and products and the definition of a base as an isomorphism $V \cong K^n$.] $U \oplus V$ is then called the <u>direct sum</u> of U and V.

If a vector-space can be expressed as the direct sum of two subspaces then they intersect in the zero subspace and their set-theoretic union spans the space. In this case they are said to be <u>complementary</u>; the converse also holds. However beware that the complement of a subspace is <u>not</u> unique (consider lines in the plane, $\mathbb{R}^2$) and the converse is not true for three or more subspaces. A complement to a subspace is isomorphic to the quotient space, a fact which is often useful.

Given any two vector-spaces over a given field K, the collection of linear maps from one to the other has the structure of a vector space by pointwise addition and scaling, so for $\alpha,\beta: X\to Y$ and $\lambda,\mu\in K$, $\underline{x}\in X$ we have $\underline{x}(\lambda\alpha+\mu\beta)=\lambda(\underline{x}\alpha)+\mu(\underline{x}\beta)$. If $X\cong K^n$ and $Y\cong K^m$, α and β are $n\times m$ matrices, so its easy to see that the matrices with "1" in exactly one place and "0" elsewhere form a basis, so the dimension of this space (which we shall call $[X\to Y]$ although you will find othernames such as $\mathcal{L}(X,Y)$ and $\mathrm{Hom}(X,Y)$) is $\dim X.\dim Y$

In the special case where $Y=K$ (considered as a one-dimensional vector-space) we call $X^*=[X\to K]$ the <u>dual space</u>. If X is finite-dimensional then $\dim X^*=\dim X$, for given a basis $(e_1,\dots,e_n)$ for X we define one $(\varepsilon_1,\dots,\varepsilon_n)$ for X^* by $e_i\varepsilon_j=\delta_{ij}$; however if we change the basis for X by a matrix A, then the basis for X^* will change by X^{-1} so the isomorphism is not natural. For example if $X\cong\mathbb{R}^3$ gives the weights of apples, bananas and cherries which we might buy then X^* represents their price per pound, so $X^*\cong\mathbb{R}^3$ but they're clearly not "naturally" isomorphic.

In the finite-dimensional case the double dual, X^{**}, <u>is</u> naturally isomorphic to the original space, X. Define $\varphi: X\to X^{**}$ by $\underline{x}\mapsto\tilde{\underline{x}}$, where $\tilde{\underline{x}}: X^*\to K$ by $\alpha\longmapsto\underline{x}\alpha$. [It's easy to get confused by these convoluted definitions, and the best way to understand it is to go through it with diagrams several times, remembering that we've put no new structure into the space: we've just turned it inside-out twice!] In general this gives $X\hookrightarrow X^{**}$ as a subspace, but if the dimensions are finite we know they're equal, so it's an isomorphism.

Giving an isomorphism $\varphi: X\to X^*$ is precisely equivalent to giving a <u>bilinear form</u> $\tilde{\varphi}: X\times X\to K$ on X, where $(\lambda\underline{x}_1+\mu\underline{x}_2,\underline{y})\tilde{\varphi}=\lambda(\underline{x}_1,\underline{y})\tilde{\varphi}+\mu(\underline{x}_2,\underline{y})\tilde{\varphi}$ and similarly for the second argument. [You may have met such a thing in coordinate geometry for specifying conic sections]. φ being iso is equivalent to nonsingularity of $\tilde{\varphi}$:

$$(\underline{x},\underline{y})\tilde{\varphi}=0 \text{ for all } \underline{y} \Rightarrow \underline{x}=0$$

For we define $(\underline{x},\underline{y})\tilde{\varphi}=\underline{x}(\underline{y}\varphi)$.

The space of bilinear maps $X \times Y \to K$ (or $\to W$) is a vector-space in the obvious way, and (if $\dim X, \dim Y < \infty$) its dimension is $\dim X . \dim Y$. Since it's a space of maps into the ground field K (or $\mathbb{R}$) we might expect it to be the dual space of something, and indeed it is, namely of the <u>tensor product</u>, $X \otimes Y$. This will be constructed in general in the IB Rings and Modules course, but for the finite dimensional case (since $V^{**} \cong V$) it is $[X \times Y \to K]^*$ or, since we've not formally defined $[X \times Y \to K]$, it's $[[X \to [Y \to K]] \to K]$. The dimension is $\dim X . \dim Y$, hence the $\otimes$ symbol. We also have $[X \to Y] \cong X^* \otimes Y$: can you construct the natural isomorphism?

$[X \to X]$ has more structure than just a vector-space: the composition operation ($\varphi * \psi : \underline{x} \mapsto (\underline{x}\varphi)\psi$) makes it a <u>ring</u> or <u>algebra</u>. The multiplication is obviously associative (but not commutative) and distributes over (ie is linear over) addition and scalar multiplication. $[X \to X]$ is the <u>ring of endomorphisms</u> of X and may be written $\mathrm{End}(X)$. It corresponds precisely (with a given choice of basis) to matrix multiplication and addition. The centre of this ring consists of the scalar matrices, $\lambda . 1$ with $\lambda \in K$. The invertible elements form the <u>general linear group</u>, $GL(X)$, under composition.

Given a map $\alpha : U \to V$ there is a dual map $\alpha^* : V^* \to U^*$ by $v' \mapsto \alpha v'$ where $v' : V \to K$ and $\alpha v' : U \to V \to K$. Wrt particular bases, the matrix of α^* is the transpose of that of α. Any theorem about vector-spaces may be translated into another by reversing the arrows and putting stars on things (at least, suitably interpreted). The rank of α^* is equal to that of α.

The solution to a system of <u>simultaneous linear equations</u> is exactly equivalent to asking whether a given point in the range of a linear map is in its image, and if so how many inverse images it has. Let us deal firstly with uniqueness on the assumption that a solution exists. Clearly if $\underline{x} \in U$ satisfies $\underline{x}\alpha = \underline{b} \in V$ where $\alpha : U \to V$ and $\underline{u} \in \ker \alpha$ (ie $\underline{u}\alpha = 0$) then $\underline{x} = \underline{x}_0 + \underline{u}$ also satisfies the equation.

Thus uniqueness is equivalent to $\ker\alpha = 0$, so $n(\alpha) = \dim\ker\alpha = 0$ and $r(\alpha) = \dim\operatorname{im}\alpha = \dim U$.

For existence, $\underline{b} \in \operatorname{im}\alpha$ iff the subspace of V spanned by $\operatorname{im}\alpha$ and $\underline{b}$ together is the same as that spanned by $\operatorname{im}\alpha$ (namely $\operatorname{im}\alpha$ itself). In this we may replace $\operatorname{im}\alpha$ by a spanning set, such as the image of a basis of U; in coordinate terms this is given by the set of row vectors of the matrix $\underline{\underline{A}}$ of α. Moving entirely to a matrix description, this says that the rank of $(\underline{\underline{A}}|\underline{b})$ (a temporary notation for the matrix obtained by adjoining $\underline{b}$ as an extra row to $\underline{\underline{A}}$), which is the dimension of the space spanned by its rows, is the same as that of $\underline{\underline{A}}$ alone.

If the domain and range space have the same dimension (ie there are the same number of unknowns and equations), a solution exists for all values in the image iff it is unique, ie the map is invertible. Thus if you know the inverse matrix (found using "minor" determinants or, much more efficiently, Gaussian elimination) the unique solution may be found. We are left with the problem of defining determinants.

Intuitively, the <u>determinant of an endomorphism</u> is the factor by which it changes the volume of a hyper-parallelopiped spanned by any set of n vectors (where n is the dimension). We shall, in effect, show that this is equivalent to an alternating form, which is the definition we use in general since our motivation is restricted to vector-spaces over $\mathbb{R}$ (see Rings & Modules).

It is immediately clear that $\det 1 = 1$ and $\det\alpha\beta = \det\alpha.\det\beta$ and it's not difficult to see that $\det\alpha \neq 0$ iff α is an automorphism (ie nonsingular). Thus we have only to derive the usual formula [although we've cheated on showing it's well-defined].

Let's choose a particular hyperparallelopiped with nonzero volume (ie a basis) and fix the images of all but one of the vectors, varying the remainining one. In terms of matrices, we shall consider the determinant as a function of one row, the others being fixed. The

images of our hyperparallelopiped under two endom.s from this family then differ only in their "length" and when placed end-to-end give us the image under the sum. Thus the determinant is linear in <u>each</u> row <u>separately</u> (and we say it's <u>multilinear</u> in the n rows).

Now if we choose our variable image to coincide with one of the fixed ones, the determinant vanishes. Thus writing the row vectors as $\underline{r}_1, \ldots, \underline{r}_n$, we have

$$\det(\underline{r}_1, \underline{r}_1, \underline{r}_3, \ldots) = 0 = \det(\underline{r}_2, \underline{r}_2, \underline{r}_3, \ldots)$$

and so since we have this for any $(\underline{r}_i)$ and using linearity,

$$0 = \det(\underline{r}_1+\underline{r}_2, \underline{r}_1+\underline{r}_2, \underline{r}_3, \ldots) = \det(r_1, r_1, r_3, \ldots) + \det(r_1, r_2, r_3, \ldots) + \det(r_2, r_1, r_3, \ldots) + \det(r_2, r_2, r_3, \ldots)$$

thus $\det(\underline{r}_1, \underline{r}_2, \underline{r}_3, \ldots) = -\det(\underline{r}_2, \underline{r}_1, \underline{r}_3, \ldots)$

showing that we must consider <u>signed</u> volumes and <u>ordered</u> n-tuples of vectors. Thus the determinant is <u>alternating</u>.

Now one may easily show that there are just $\binom{n}{k}$ linearly independent alternating k-linear forms in n dimensions, and in particular only one n-linear one. Thus we have prescribed the determinant uniquely since we want $\det 1 = 1$. One may then calculate it in the usual way.

When restricted to nonsingular endomorphisms, the determinant is a group homomorphism $GL(V) \to K^*$ whose kernel, consisting of the endomorphisms (or matrices) of unit determinant, is called $SL(V)$, the <u>special linear group</u>. As previously remarked, the centre of $GL(V)$ (and also of $SL(V)$) consists of scalar matrices, and the quotients of $GL(V)$ and $SL(V)$ by their centres are of interest in group theory and projective geometry, being called the <u>projective general</u> (respectively <u>special</u>) <u>linear groups</u>, $PGL(V)$ and $PSL(V)$. Like A_n, $PSL(V)$ is usually simple (has no nontrivial normal subgroups), giving an independent reason for studying the determinant.