Vector Spaces

Definition. If F is an field and V is an F-module, then V is called a *vector space over F*.

Definition.

1. A subset S of V is called a set of ***linearly independent*** vectors if an equation $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$ with $\alpha_1, \ldots \alpha_n \in F$ and $v_1, \ldots, v_n \in S$ implies $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$. (Note: an infinite set is linearly independent if this condition holds for any finite subset.)
2. A *basis* of a vector space V is an ***ordered set*** of linearly independent vectors which span V. In particular, two bases sill be considered different even if one is simply a rearrangement of the other. This is sometimes referred to as an *ordered basis*.

Proposition. Assume that $\mathcal{A} = \{v_1, v_2, \ldots, v_n\}$ spans the vector space V but no proper subset of $\mathcal{A}$ spans V. Then $\mathcal{A}$ is a basis of V. In particular, any finitely generated vector space over F is a free F-module.

Theorem 0.1. *(A Replacement Theorem)* Assume $\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$ is a basis for V containing n elements and $\{b_1, b_2, \ldots, b_m\}$ is a set of linearly independent vectors in V. Then there is an ordering $a_1, a_2, \ldots, a_n$ such that for each $k \in \{1, 2, \ldots, m\}$ the set $\{b_1, \ldots, b_k, a_{k+1}, \ldots, a_n\}$ is a basis of V. In other words, the elements of $b_1, b_2, \ldots, b_m$ can be used to successively replace the elements of the basis $\mathcal{A}$, still retaining a basis. In particular $n \geq m$

Corollary.

1. Suppose V has a finite basis with n elements. Any set of linearly independent vectors has $\leq n$ elements. Any spanning set has $\geq n$ elements.
2. If V has some finite basis, then any two bases of V have the same cardinality.

Definition. If V is a finitely generated F-module the cardinality of any basis is called the *dimension* of V and is denoted $\dim_F(V)$, or just $\dim(V)$ when F is clear from the context, and V is said to be *finite dimensional over F*. If V is not finitely generated, V is said to be infinite dimensional.

Corollary. If A is a set of linearly independent vectors in the finite dimensional vector space V, then there exists a basis of V containing A

Theorem 0.2. If V is an n dimensional vector space over F, the $V \cong F^n$. In particular, any two finite dimensional vector spaces over F of the same dimension are isomorphic.

Proof. Let $v_1, v_2, \ldots, v_n$ be a basis for V. Define the map

$$\varphi : F^n \to V : (\alpha_1, \alpha_2, \ldots, \alpha_n) \mapsto \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n.$$

The map φ is clearly F-linear, is surjective since the v_i span V, and is injective since the v_i are linearly independent, hence is an isomorphism. □

Theorem 0.3. Let V be a vector space over F and let W be a subspace of V. Then $V/W$is a vector space with $\dim(V) = \dim(W) + \dim(V/W)$.

Corollary. Let $\varphi : V \to U$ be a linear transformation of vector spaces over F. Then $\ker(\varphi)$ is a subspace of V, $\varphi(V)$ is a subspace of U, and $\dim(V) = \dim(\ker(\varphi)) + \dim(\varphi(V))$.

Corollary. Let $\varphi : V \to U$ be a linear transformation of vector spaces of the same finite dimension. Then the following are equivalent

1. φ is an isomorphism
2. φ is injective, i.e., $\ker(\varphi) = 0$
3. φ is surjective
4. φ sends a basis of V to a basis of W.

Definition. If $\varphi : V \to U$ is a linear transformation of vector spaces over F, $\ker(\varphi)$ is sometimes called the ***null space*** of φ. and the dimension of $\ker(\varphi)$ is called the ***nullity*** of φ. The dimension of $\varphi(V)$ is called the ***rank*** of φ. If $\ker(\varphi) = 0$, then the transformation is said to be ***nonsingular***.

Definition. The $m \times m$ matrix $A = (a_{ij})$ associated to the linear transformation φ is said to *represent* the linear transformation φ with respect to the bases $\mathcal{B}, \mathcal{E}$. Similarly, φ is the linear transformation represented by A with respect to the bases $\mathcal{B}, \mathcal{E}$.

Theorem 0.4. Let B be a vector space over F of dimension n and let W be a vector space over F of dimension m, with bases $\mathcal{B}, \mathcal{E}$ respectively. Then the map $\mathrm{Hom}_F(V, W) \to M_{m \times n}(F)$ from the space of linear transformations from v to W to the space of $m \times n$ matrices with coefficients in F defined by $\varphi \mapsto M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$ is a vector space isomorphism. In particular, there is a bijective correspondence between linear transformations and their associated matrices with respect to a fixed choice of bases.

Corollary. The dimension of $\mathrm{Hom}_F(V, W)$ is $(\dim(V))(\dim(W))$.

Definition. An $m \times n$ matrix A is called ***nonsingular*** if $Ax = 0$ with $x \in F^n$ implies $x = 0$.

Theorem 0.5. With notation as above $M_{\mathcal{B}}^{\mathcal{E}}(\varphi \circ \psi) = M_{\mathcal{B}}^{\mathcal{E}}(\varphi) M_{\mathcal{B}}^{\mathcal{E}}(\psi)$.

Corollary. Matrix multiplication is associative and distributive. An $n \times n$ matrix A is nonsingular if and only if it is invertible.

Corollary.

1. If $\mathcal{B}$ is a basis of the n-dimensional space V, the map $\varphi \mapsto M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$ is a ring and a vector space isomorphism of $\mathrm{Hom}_F(V, V)$ onto the space $M_n(F)$ of $n \times n$ matrices with coefficients in F.
2. $GL(V) \cong GL_n(F)$ where $\dim(V) = n$.

Definition. If A is any $m \times n$ matrix with entries of F, the ***row rank*** of A is the maximal number of linearly independent rows of A.

Definition. Two $n \times n$ matrices A and B are said to be ***similar*** if the is an invertible $n \times n$ matrix P such that $P^{-1}AP = B$. Two linear transformations φ and ψ from a vector space V to itself are said to be *similar* if the is a nonsingular linear transformation ξ

Definition. 1. For V any vector space over F let $V^* = \mathrm{Hom}_F(V, F)$ be the space of linear transformations from V to F, called the ***dual space*** of V. Elements of V^* are called ***linear functionals***.

2. If $\mathcal{B} = \{v_1, v_2, \ldots, v_n\}$ is a basis of the finite dimensional space V, define $v_i^* \in V^*$ for each $i = 1..n$ by its action on the basis $\mathcal{B}$:

$$v_i^*(v_j) = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases} \qquad 1 \leq j \leq n.$$

Proposition. With notations as above, $\{v_1^*, v_2^*, \ldots, v_n^*\}$ is a basis of V^*. In particular, if V is finite dimensional then V^* has the same dimension as V.

Proof. (Copied from D&F) Observe that since V is finite dimensional, $\dim(V^*) = \dim(\mathrm{Hom}_F(V, F)) = \dim(V) = n$ (Corollary 11.11), so since there are n of the v_i^*'s it suffices to prove that they are linearly independent. If

$$\alpha_1 v_1^* + \alpha_2 v_2^* + \cdots + \alpha_n v^n = 0 \quad \text{in } \mathrm{Hom}_F(V, F),$$

then applying this element to v_i and using th equation above gives us that $\alpha_i = 0$. Since i is arbitrary these elements are linearly independent. □

Definition. The basis $\{v_1^*, v_2^*, \ldots, v_n^*\}$ of V^* is called the ***dual basis*** to $\{v_1, v_2, \ldots, v_n\}$.

Theorem 0.6. There is a natural injective linear transformation from V to V^{**}. If V is finite dimensional then this linear transformation is an isomorphism.

Sketch of proof. Let $v \in V$ and define the evaluation map $E_v : V^* \to F : f \mapsto f(v)$. This is a linear transformation from V^* to F, and so is an element of $\mathrm{Hom}_F(V^*, F) = V^{**}$. This defines a natural map $\varphi : V \to V^{**} : v \mapsto E_v$. This map is injective for all V and φ is an isomorphism if V is finite dimensional.

Theorem 0.7. Let V, W be finite dimensional vector spaces over F with bases $\mathcal{B}, \mathcal{E}$, respectively and let $\mathcal{B}^*, \mathcal{E}^*$ be the dual bases . Fix some $\varphi \in \mathrm{Hom}(V, W)$. Then for each $f \in W^*$, the composite $f \circ \varphi$ is a linear transformation from V to F, that is $f \circ \varphi \in V^*$. Thus, we can define a map $\varphi^* : W^* \to V^* : f \mapsto f \circ \varphi$ (called the ***pullback*** of f) and the matrix $M_{\mathcal{E}^*}^{\mathcal{B}^*}(\varphi^*)$ is the transpose of th matrix $M_{\mathcal{B}}^{\mathcal{E}}(\varphi)$.

Corollary. For any matrix A, the row rank of A equals the column rank of A.

Definition.

1. A map $\varphi : V_1 \times V_2 \times \cdots \times V_n \to W$ is called ***multilinear*** if for each fixed i and fixed i and fixed elements $v_j \in V_j$, $j \neq i$, the map

$$V_i \to W \qquad \text{defined by} \qquad x \mapsto \varphi(v_1, \ldots, v_{i-1}, x, v_{i+1}, \ldots, v_n)$$

is an R-module homomorphism. If $V_i = V$, $i = 1, 2, \ldots, n$, then φ is called an *n-multilinear function on V*, and if in addition $W = R$, φ is called an *n-multilinear form on V*.

2. An n-multilinear function φ on V is called *alternating* if $\varphi(v_1, v_2, \ldots, v_n) = 0$ whenever $v_i = v_{i+1}$ for some $i \in \{1, 2, \ldots, n-1\}$. The function φ is called *symmetric* if interchanging v_i and v_j for any i and j in $(V_1, v_2, \ldots, v_n)$ does not alter the value of φ on this n-tuple.

Proposition. Let φ be an n-multilinear alternating function on V. Then

1. $\varphi(v_1, \ldots, v_{i-1}, v_{i+1}, v_i, v_{i+2}, \ldots, v_n) = -\varphi(v_1, v_2, \ldots, v_n)$ for any $i \in \{1, 2, \ldots, n-1\}$.
2. For each $\sigma \in S_n$, $\varphi(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(n)}) = sgn(\sigma)\varphi(v_1, v_2, \ldots, v_n)$.
3. If $v_i = v_j$ for any pair of distinct $i, j \in \{1, 2, \ldots, v_n\}$ then $\varphi(v_1, v_2, \ldots, v_n) = 0$.
4. If v_i is replaced by $v_i + \alpha v_j$ in $(v_1, v_2, \ldots, v_n)$ for any $j \neq i$ and any $\alpha \in R$, the value ofφ on this n-tuple is not changed.

Proposition. Assume φ is an n-multilinear alternating function on V and that for some $v_1, v_2, \ldots, v_n$ and $w_1, w_2, \ldots, w_n \in V$ and some $\alpha_{ij} \in R$ we have

$$\begin{aligned}
w_1 &= \alpha_{11}v_1 + \alpha_{21}v_2 + \cdots + \alpha_{n1}v_n \\
w_2 &= \alpha_{12}v_1 + \alpha_{22}v_2 + \cdots + \alpha_{n2}v_n \\
&\vdots \\
w_n &= \alpha_{1n}v_1 + \alpha_{2n}v_2 + \cdots + \alpha_{nn}v_n.
\end{aligned}$$

Then

$$\varphi(w_1, w_2, \dots, w_n) = \sum_{\sigma \in S_n} sgn(\sigma)\alpha_{\sigma(1)1}\alpha_{\sigma(2)2}\cdots\alpha_{\sigma(n)n}\varphi(v_1, v_2, \dots, v_n).$$

Definition. An $n \times n$ ***determinant function*** on R is any function

$$\det : M_{n\times n}(R) \to R$$

that satisfies the following two axioms:

1. det is an n-multilinear alternating form on $R^n (= V)$, where the n-tuples are the n columns of the matrices in $M_{n\times n}(R)$.
2. $\det(I) = 1$.

Theorem 0.8. There is a unique $n \times n$ determinant function on R and it can be computed for any $n \times n$ matrix (α_{ij}) by the formula:

$$det(\alpha_{ij}) = \sum_{\sigma \in S_n} sgn(\sigma)\alpha_{\sigma(1)1}\alpha_{\sigma(2)2}\cdots\alpha_{\sigma(n)n}$$

Corollary. The determinant is an n-multilinear function of the rows of $M_{n\times n}(R)$ and for any $n \times n$ matrix A, $\det(A) = \det(A^t)$.

Theorem 0.9. *(Cramer's Rule)* If $A_)1, A_23, \dots, A_n$ are the columns of an $n \times n$ matrix A and $B = \beta_1 A_1 + \beta_2 A_2 + \cdots + \beta_n A_n$, for some $\beta_1, \dots, \beta_n \in R$, then

$$\beta_i \det(A) = \det(A_1, \dots, A_{i-1}, B, A_{i+1}, \dots, A_n).$$

Corollary. If R is an integral domain, then $\det(R) = 0$ for $A \in M_n(R)$ if and only if the columns of A are R-linearly dependent as elements of the free R-module of rank n. Also $\det(A) = 0$ if and only if the rows of A are R-linearly dependent.

Theorem 0.10. For matrices $A, B \in M_{n\times n}(R)$, $\det(A, B) = \det(A)\det(B)$.

Definition. Let $A = (\alpha_{ij})$ be an $n \times n$ matrix. For each $i,\ j$, let A_{ij} be the $n-1 \times n-1$ matrix obtained from A by deleting its i^{th} row and j^{th} column. Then $(-1)^{i+j}\det(A_{ij})$ is called the ij ***cofactor of** A.*

Theorem 0.11. *(The Cofactor Expansion Formula along the i^{th} row)* If $A = (\alpha_{ij})$ is an $n \times n$ matrix, then for each fixed $i \in \{1, 2, \ldots n\}$ the determinant of A can be computed from the formula

$$\det(A) = (-1)^{i+1}\alpha_{i1}\det(A_{i1}) + (-1)^{i+2}\alpha_{i2}\det(A_{i2}) + \cdots + (-1)^{i+n}\alpha_{in}\det(A_{in}).$$

Theorem 0.12. *(Cofactor Formula for the Inverse of a Matrix)* Let $A = (\alpha_{ij})$ be an $n \times n$ matrix and let B be the transpose of is matrix of cofactors, i.e., $B = (\beta_{ij})$, where $\beta_{ij} = (-01)^{i+j}\det(A_{ji})$, $1 \leq ii, j \leq n$. Then $AB = BA = \det(A)I$. Moreover, $\det(A)$ is a unit in R if and only if A is a unit in $M_{n\times n}(R)$; in this case the matrix $\frac{1}{\det(A)}B$ is the inverse of A.