Again by the induction hypothesis all the other coefficients must be 0 as well. **Thus** $\{b_1, b_2, \ldots, b_k, b_{k+1}, a_{k+2}, \ldots, a_n\}$ is a basis for V, and the induction is complete.

Corollary 4.

(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.

Proof: (1) This is a restatement of the last result of Theorem 3 and Corollary 2. (2) This is immediate from (1) since a basis is both a spanning set and a linearly independent set.

Definition. If V is a finitely generated F-module (i.e., has a finite basis) the cardinality of any basis is called the *dimension* of V and is denoted by $\dim_F V$, 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 (written $\dim V = \infty$).

Examples

(1) The dimension of the space of solutions to the differential equation $y'' - 3y' + 2y = 0$ over $\mathbb{C}$ is 2 (with basis e^t, e^{2t}, for example). In general, it is a theorem in differential equations that the space of solutions of an n^{th} order linear, homogeneous, constant coefficient differential equation of degree n over $\mathbb{C}$ form a vector space over $\mathbb{C}$ of dimension n.

(2) The dimension over F of the quotient $F[x]/(f(x))$ by the nonzero polynomial $f(x)$ considered above is $n = \deg f(x)$. The space $F[x]$ and its subspace $(f(x))$ are infinite dimensional vector spaces over F.

Corollary 5. *(Building–Up Lemma)* If A is a set of linearly independent vectors in the finite dimensional space V then there exists a basis of V containing A.

Proof: This is also immediate from Theorem 3, since we can use the elements of A to successively replace the elements of any given basis for V (which exists by the assumption that V is finite dimensional).

Theorem 6. If V is an n dimensional vector space over F, then $V \cong F^n$. 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

$$\varphi : F^n \to V \qquad \text{by} \qquad \varphi(\alpha_1, \alpha_2, \ldots, \alpha_n) = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n.$$

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.

Examples

(1) Let $\mathbb{F}$ be a finite field with q elements and let W be a k-dimensional vector space over $\mathbb{F}$. We show that the number of distinct bases of W is

$$(q^k - 1)(q^k - q)(q^k - q^2)\dots(q^k - q^{k-1}).$$

Every basis of W can be built up as follows. Any nonzero vector w_1 can be the first element of a basis. Since W is isomorphic to $\mathbb{F}^k$, $|W| = q^k$, so there are $q^k - 1$ choices for w_1. Any vector not in the 1-dimensional space spanned by w_1 is linearly independent from w_1 and so may be chosen for the second basis element, w_2. A 1-dimensional space is isomorphic to $\mathbb{F}$ and so has q elements. Thus there are $q^k - q$ choices for w_2. Proceeding in this way one sees that at the i^{th} stage any vector not in the $(i-1)$-dimensional space spanned by $w_1, w_2, \dots, w_{i-1}$ will be linearly independent from $w_1, w_2, \dots, w_{i-1}$ and so may be chosen for the i^{th} basis vector w_i. An $(i-1)$-dimensional space is isomorphic to $\mathbb{F}^{i-1}$ and so has q^{i-1} elements. Thus there are $q^k - q^{i-1}$ choices for w_i. The process terminates when w_k is chosen, for then we have k linear independent vectors in a k-dimensional space, hence a basis.

(2) Let $\mathbb{F}$ be a finite field with q elements and let V be an n-dimensional vector space over $\mathbb{F}$. For each $k \in \{1, 2, \dots, n\}$ we show that the number of subspaces of V of dimension k is

$$\frac{(q^n - 1)(q^n - q)\dots(q^n - q^{k-1})}{(q^k - 1)(q^k - q)\dots(q^k - q^{k-1})}.$$

Any k-dimensional space is spanned by k independent vectors. By arguing as in the preceding example the numerator of the above expression is the number of ways of picking k independent vectors from an n-dimensional space. Two sets of k independent vectors span the same space W if and only if they are both bases of the k-dimensional space W. In order to obtain the formula for the number of distinct subspaces of dimension k we must divide by the number of repetitions, i.e., the number of bases of a fixed k-dimensional space. This factor which appears in the denominator is precisely the number computed in Example 1.

Next, we prove an important relation between the dimension of a subspace, the dimension of its associated quotient space and the dimension of the whole space:

Theorem 7. Let V be a vector space over F and let W be a subspace of V. Then V/W is a vector space with $\dim V = \dim W + \dim V/W$ (where if one side is infinite then both are).

Proof: Suppose W has dimension m and V has dimension n over F and let $w_1, w_2, \dots, w_m$ be a basis for W. By Corollary 5, these linearly independent elements of V can be extended to a basis $w_1, w_2, \dots, w_m, v_{m+1}, \dots, v_n$ of V. The natural surjective projection map of V into V/W maps each w_i to 0. No linear combination of the v_i is mapped to 0, since this would imply this linear combination is an element of W, contrary to the choice of the v_i. Hence, the image V/W of this projection map is isomorphic to the subspace of V spanned by the v_i, hence $\dim V/W = n - m$, which is the theorem when the dimensions are finite. If either side is infinite it is an easy exercise to produce an infinite number of linearly independent vectors showing the other side is also infinite.

Corollary 8. 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 $\dim V = \dim \ker \varphi + \dim \varphi(V)$.

Proof: This follows immediately from Theorem 7. Note that the proof of Theorem 7 is in fact the special case of Corollary 8 where U is the quotient V/W and φ is the natural projection homomorphism.

Corollary 9. Let $\varphi : V \to W$ 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, i.e., $\varphi(V) = W$
(4) φ sends a basis of V to a basis of W.

Proof: The equivalence of these conditions follows from Corollary 8 by counting dimensions.

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 $\ker \varphi = 0$, the transformation is said to be *nonsingular.*

Example

Let F be a finite field with q elements and let V be an n-dimensional vector space over F. Recall that the *general linear group* $GL(V)$ is the group of all nonsingular linear transformations from V to V (the group operation being composition). We show that the order of this group is

$$|GL(V)| = (q^n - 1)(q^n - q)(q^n - q^2)\dots(q^n - q^{n-1}).$$

To see this, fix a basis $v_1, \dots, v_n$ of V. A linear transformation is nonsingular if and only if it sends this basis to another basis of V. Moreover, if $w_1 \dots, w_n$ is any basis of V, by Theorem 6 in Section 10.3 there is a unique linear transformation which sends v_i to w_i, $1 \le i \le n$. Thus the number of nonsingular linear transformations from V to itself equals the number of distinct bases of V. This number, which was computed in Example 1 above (with $k = n$), is the order of $GL(V)$.

EXERCISES

1. Let $V = \mathbb{R}^n$ and let $(a_1, a_2, \dots, a_n)$ be a fixed vector in V. Prove that the collection of elements $(x_1, x_2, \dots, x_n)$ of V with $a_1x_1 + a_2x_2 + \dots + a_nx_n = 0$ is a subspace of V. Determine the dimension of this subspace and find a basis.
2. Let V be the collection of polynomials with coefficients in $\mathbb{Q}$ in the variable x of degree at most 5. Prove that V is a vector space over $\mathbb{Q}$ of dimension 6, with $1, x, x^2, \dots, x^5$ as basis. Prove that $1, 1+x, 1+x+x^2, \dots, 1+x+x^2+x^3+x^4+x^5$ is also a basis for V.