Thus the vectors in $\{\alpha_i \mid i \in I\}$ are linearly independent over F if the only way the 0-vector can be expressed as a linear combination of the vectors α_i is to have all scalar coefficients equal to 0. If the vectors are linearly dependent over F, then there exist $a_j \in F$ for $j = 1, \cdots, n$ such that $\sum_{j=1}^{n} a_j\alpha_{i_j} = 0$, where not all $a_j = 0$.

33.11 Example Observe that the vectors spanning the space $\mathbb{R}^n$ that are given in Example 33.7 are linearly independent over $\mathbb{R}$. Likewise, the vectors in $\{x^m \mid m \geq 0\}$ are linearly independent vectors of $F[x]$ over F. Note that (1, −1), (2, 1), and (−3, 2) are linearly dependent in $\mathbb{R}^2$ over $\mathbb{R}$, since

$$7(1, -1) + (2, 1) + 3(-3, 2) = (0, 0) = 0.$$ ▲

33.12 Definition If V is a vector space over a field F, the vectors in a subset $B = \{\beta_i \mid i \in I\}$ of V form a **basis for** V **over** F if they span V and are linearly independent. ■

33.13 Example As seen from Examples 33.7 and 33.11,

$$\{(1, 0, 0, \ldots, 0), (0, 1, 0, 0, \ldots, 0), \ldots, (0, 0, \ldots, 0, 1)\}$$

is a basis for $\mathbb{R}^n$ and

$$\{1, x, x^2, \ldots\}$$

is a basis for $F[x]$ where F is a field. ▲

33.14 Example Let F be a field and $p(x) \in F[x]$ be a degree $n \geq 1$ irreducible polynomial over F. Theorems 31.9 and 31.25 imply that the factor ring

$$E = F[x]/\langle p(x)\rangle$$

is a field. We can think of F as a subfield of E by identifying $a \in F$ with $a + \langle p(x)\rangle \in E$. Example 33.4 shows that E is a vector space over F. The vectors

$$\alpha_j = x^j + \langle p(x)\rangle \quad \text{for} \quad 0 \leq j \leq n - 1$$

are linearly independent since if

$$a_0\alpha_0 + a_1\alpha_1 + a_2\alpha_2 + \cdots + a_{n-1}\alpha_{n-1} = 0 \in F[X]/\langle p(x)\rangle,$$

then

$$a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} \in \langle p(x)\rangle.$$

Every polynomial in $\langle p(x)\rangle$ except the zero polynomial has degree at least n. Thus each coefficient a_j is zero and the vectors $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ form an independent set. On the other hand, given any polynomial $f(x) \in F[x]$, the division algorithm implies that $f(x) + \langle p(x)\rangle = g(x) + \langle p(x)\rangle$ for some polynomial $g(x)$ where either $g(x) = 0$ or the degree of $g(x)$ is less than n. It follows that the vectors

$$\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$$

span E and therefore form a basis for E.

Looking back at this example, it is not necessary for $p(x)$ to be an irreducible polynomial. The field F can be thought of as a subring of the commutative ring with unity $E = F[x]/\langle p(x)\rangle$ and all the axioms of a vector space follow from the properties of a ring and the fact that the unity in F and the unity in E are the same. ▲

Dimension

The only other results we wish to prove about vector spaces are that every finite-dimensional vector space has a basis, and that any two bases of a finite-dimensional vector space have the same number of elements. Both these facts are true without the assumption that the vector space is finite dimensional, but the proofs require more knowledge of set theory than we are assuming, and the finite-dimensional case is all we need. First we give an easy lemma.

33.15 Lemma Let V be a vector space over a field F, and let $\alpha \in V$. If α is a linear combination of vectors β_i in V for $i = 1, \cdots, m$ and each β_i is a linear combination of vectors γ_j in V for $j = 1, \cdots, n$, then α is a linear combination of the γ_j.

Proof Let $\alpha = \sum_{i=1}^{m} a_i\beta_i$, and let $\beta_i = \sum_{j=1}^{n} b_{ij}\gamma_j$, where a_i and b_{ij} are in F. Then

$$\alpha = \sum_{i=1}^{m} a_i\Big(\sum_{j=1}^{n} b_{ij}\gamma_j\Big) = \sum_{j=1}^{n}\Big(\sum_{i=1}^{m} a_i b_{ij}\Big)\gamma_j,$$

and $(\sum_{i=1}^{m} a_i b_{ij}) \in F$. ◆

33.16 Theorem In a finite-dimensional vector space, every finite set of vectors spanning the space contains a subset that is a basis.

Proof Let V be finite dimensional over F, and let vectors $\alpha_1, \cdots, \alpha_n$ in V span V. Let us list the α_i in a row. Examine each α_i in succession, starting at the left with $i = 1$, and discard the first α_j that is some linear combination of the preceding α_i for $i < j$. Then continue, starting with the following α_{j+1}, and discard the next α_k that is some linear combination of its remaining predecessors, and so on. When we reach α_n after a finite number of steps, those α_i remaining in our list are such that none is a linear combination of the preceding α_i in this reduced list. Lemma 33.15 shows that any vector that is a linear combination of the original collection of α_i is still a linear combination of our reduced, and possibly smaller, set in which no α_i is a linear combination of its predecessors. Thus the vectors in the reduced set of α_i again span V.

For the reduced set, suppose that

$$a_1\alpha_{i_1} + \cdots + a_r\alpha_{i_r} = 0$$

for $i_1 < i_2 < \cdots < i_r$ and that some $a_j \neq 0$. We may assume from Theorem 33.5 that $a_r \neq 0$, or we could drop $a_r\alpha_{i_r}$ from the left side of the equation. Then, using Theorem 33.5 again, we obtain

$$\alpha_{i_r} = \Big(-\frac{a_1}{a_r}\Big)\alpha_{i_1} + \cdots + \Big(-\frac{a_{r-1}}{a_r}\Big)\alpha_{i_{r-1}},$$

which shows that α_{i_r} is a linear combination of its predecessors, contradicting our construction. Thus the vectors α_i in the reduced set both span V and are linearly independent, so they form a basis for V over F. ◆

33.17 Corollary A finite-dimensional vector space has a finite basis.

Proof By definition, a finite-dimensional vector space has a finite set of vectors that span the space. Theorem 33.16 completes the proof. ◆

The next theorem is the culmination of our work on vector spaces.

33.18 Theorem Let $S = \{\alpha_1, \cdots, \alpha_r\}$ be a finite set of linearly independent vectors of a finite-dimensional vector space V over a field F. Then S can be enlarged to a basis for V over F. Furthermore, if $B = \{\beta_1, \cdots, \beta_n\}$ is any basis for V over F, then $r \leq n$.

Proof By Corollary 33.17, there is a basis $B = \{\beta_1, \cdots, \beta_n\}$ for V over F. Consider the finite sequence of vectors

$$\alpha_1, \cdots, \alpha_r, \beta_1, \cdots, \beta_n.$$

These vectors span V, since B is a basis. Following the technique, used in Theorem 33.16, of discarding in turn each vector that is a linear combination of its remaining predecessors, working from left to right, we arrive at a basis for V. Observe that no α_i is cast out, since the α_i are linearly independent. Thus S can be enlarged to a basis for V over F.

For the second part of the conclusion, consider the sequence

$$\alpha_1, \beta_1, \cdots, \beta_n.$$

These vectors are not linearly independent over F, because α_1 is a linear combination

$$\alpha_1 = b_1\beta_1 + \cdots + b_n\beta_n,$$

since the β_i form a basis. Thus

$$\alpha_1 + (-b_1)\beta_1 + \cdots + (-b_n)\beta_n = 0.$$

The vectors in the sequence do span V, and if we form a basis by the technique of working from left to right and casting out in turn each vector that is a linear combination of its remaining predecessors, at least one β_i must be cast out, giving a basis

$$\{\alpha_1, \beta_1^{(1)}, \cdots, \beta_m^{(1)}\},$$

where $m \leq n - 1$. Applying the same technique to the sequence of vectors

$$\alpha_1, \alpha_2, \beta_1^{(1)}, \cdots, \beta_m^{(1)},$$

we arrive at a new basis

$$\{\alpha_1, \alpha_2, \beta_1^{(2)}, \cdots, \beta_s^{(2)}\},$$

with $s \leq n - 2$. Continuing, we arrive finally at a basis

$$\{\alpha_1, \cdots, \alpha_r, \beta_1^{(r)}, \cdots, \beta_t^{(r)}\},$$

where $0 \leq t \leq n - r$. Thus $r \leq n$. ◆

33.19 Corollary Any two bases of a finite-dimensional vector space V over F have the same number of elements.

Proof Let $B = \{\beta_1, \cdots, \beta_n\}$ and $B' = \{\beta_1', \cdots, \beta_m'\}$ be two bases. Then by Theorem 33.18, regarding B as an independent set of vectors and B' as a basis, we see that $n \leq m$. A symmetric argument gives $m \leq n$, so $m = n$. ◆

33.20 Definition If V is a finite-dimensional vector space over a field F, the number of elements in a basis (independent of the choice of basis, as just shown) is the **dimension of V over F**. ■

33.21 Example Let F be a field and $V \subseteq F[x]$ be the set of all polynomials of degree less than n including 0. The monomials $1, x, x^2, \ldots, x^{n-1}$ span V and they are independent. Consequently, the dimension of V over F is n. From this we can conclude that any set of fewer than n polynomials in V does not span V and any set of more than n polynomials in V is not an independent set. Of course, an arbitrary set of n polynomials in V may or may not form a basis. ▲

Modules over a Ring

When studying abelian groups using additive notation we defined what it means to multiply an integer times an element in a group. For example, if g is an element of an abelian group, then $2g = g + g$. The table at the beginning of Section 4 looks similar to the definition of a vector space. The difference is that instead of a field, in the case of abelian groups we used the ring of integers.

33.22 Definition Let R be a ring with unity. A **left R-module** is an abelian group M under addition together with an operation of scalar multiplication of each element of M by each element