of R on the left, such that for all $a, b \in R$ and $\alpha, \beta \in M$ the following conditions are satisfied:

M_1 : $a\alpha \in M$
M_2 : $a(b\alpha) = (ab)\alpha$
M_3 : $(a + b)\alpha = (a\alpha) + (b\alpha)$ ■
M_4 : $a(\alpha + \beta) = (a\alpha) + (a\beta)$
M_5 : $1\alpha = \alpha$.

A **right R-module** differs from a left R-module simply by multiplying module element by an element of R on the right with the obvious changes in the five conditions for a left module. Here we consider only left R-modules, so we will use the term R-module to mean left R-module.

33.23 Example For any abelian group G, G is a $\mathbb{Z}$-module using the usual notation for an integer times an element of G.

If R is a ring with unity and $I \subseteq R$ is an ideal, then I is an additive abelian group and for any $r \in R$ and $\alpha \in I$, $r\alpha \in I$. The defining properties of a ring with unity give the remaining properties of an R-module. Thus I is an R-module. ▲

33.24 Example Elements of $\mathbb{R}^n$ (written as column vectors) can be multiplied on the left by elements in the ring $M_n(\mathbb{R})$ of $n \times n$ matrices with real number entries. The five properties defining an R-module are all satisfied, which implies $\mathbb{R}^n$ is an $M_n(\mathbb{R})$-module. ▲

The key properties of vector spaces are Corollary 33.17 and Corollary 33.19 (and their generalizations to vector spaces that are not finitely generated). They say any vector space has a basis, and any two bases of a given vector space have the same number of elements. The definitions of independent, spanning, and basis vectors are the same in R-module as in vector spaces. However, in general an R-module need not have a basis, and even if it does, in some cases two bases may have a different number of elements.

33.25 Example The abelian group $\mathbb{Z}_3$ is a $\mathbb{Z}$-module. There is no nonempty subset of $\mathbb{Z}_3$ that is independent since for any $\alpha \in \mathbb{Z}_3$, $3\alpha = 0$ and 3 is a nonzero integer. A similar argument shows that for any finite abelian group G, as a $\mathbb{Z}$-module G has no nonempty independent set. We conclude that as a $\mathbb{Z}$-module a finite abelian group does not have a basis. ▲

EXERCISES 33

Computations

1. Find three bases for $\mathbb{R}^2$ over $\mathbb{R}$, no two of which have a vector in common.

In Exercises 2 and 3, determine whether the given set of vectors is a basis for $\mathbb{R}^3$ over $\mathbb{R}$.

2. $\{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$

3. $\{(-1, 1, 2), (2, -3, 1), (10, -14, 0)\}$

Determine if the indicated vector space is finite dimensional over the field. If it is, find a basis.
In Exercises 4 through 9, give a basis for the indicated vector space over the field.

4. $\mathbb{Z}_{13}$ over $\mathbb{Z}_{13}$

5. $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ over $\mathbb{Q}$

6. $\left\{ \frac{a+b\sqrt{3}}{c+d\sqrt{3}} \mid a, b, c, d \in \mathbb{Q} \text{ and } c + d\sqrt{3} \neq 0 \right\}$ over $\mathbb{Q}$

7. $\mathbb{R}$ over $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

8. $\mathbb{C}$ over $\mathbb{R}$

9. $\mathbb{R}$ over $\mathbb{Q}$

10. There is a field E with 32 elements. Determine which prime field is isomorphic with a subfield of E and determine the dimension of E over its prime field.

Concepts

In Exercises 11 through 14, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

11. The vectors in a subset S of a vector space V over a field F *span* V if and only if each $\beta \in V$ can be expressed uniquely as a linear combination of the vectors in S.

12. The vectors in a subset S of a vector space V over a field F are *linearly independent over* F if and only if the zero vector cannot be expressed as a linear combination of vectors in S.

13. The *dimension over* F of a finite-dimensional vector space V over a field F is the minimum number of vectors required to span V.

14. A *basis* for a vector space V over a field F is a set of vectors in V that span V and are linearly dependent.

15. Determine whether each of the following is true or false.

- **a.** The sum of two vectors is a vector.
- **b.** The sum of two scalars is a vector.
- **c.** The product of two scalars is a scalar.
- **d.** The product of a scalar and a vector is a vector.
- **e.** Every vector space has a finite basis.
- **f.** The vectors in a basis are linearly dependent.
- **g.** The 0-vector may be part of a basis.
- **h.** A vector space over a field F is an F-module.
- **i.** If R is a commutative ring with unity and M is an R module, then M has a basis over R.
- **j.** Every vector space has a basis.

Exercises 16–27 deal with the further study of vector spaces. In many cases, we are asked to define for vector spaces some concept that is analogous to one we have studied for other algebraic structures. These exercises should improve our ability to recognize parallel and related situations in algebra. Any of these exercises may assume knowledge of concepts defined in the preceding exercises.

16. Let V be a vector space over a field F.

- **a.** Define a *subspace of the vector space* V *over* F.
- **b.** Prove that an intersection of subspaces of V is again a subspace of V over F.

17. Let V be a vector space over a field F, and let $S = \{\alpha_i \mid i \in I\}$ be a nonempty collection of vectors in V.

- **a.** Using Exercise 16(b), define the *subspace of* V *generated by* S.
- **b.** Prove that the vectors in the subspace of V generated by S are precisely the (finite) linear combinations of vectors in S. (Compare with Theorem 7.7.)

18. Let $V_1, \cdots, V_n$ be vector spaces over the same field F. Define the *direct sum* $V_1 \oplus \cdots \oplus V_n$ *of the vector spaces* V_i for $i = 1, \cdots, n$, and show that the direct sum is again a vector space over F.

19. Generalize Example 33.2 to obtain the vector space F^n of ordered n-tuples of elements of F over the field F, for any field F. What is a basis for F^n?

20. Define an *isomorphism* of a vector space V over a field F with a vector space V' over the same field F.

Theory

21. Prove that if V is a finite-dimensional vector space over a field F, then a subset $\{\beta_i, \beta_2, \cdots, \beta_n\}$ of V is a basis for V over F if and only if every vector in V can be expressed *uniquely* as a linear combination of the β_i.

22. Let F be any field. Consider the "system of m simultaneous linear equations in n unknowns"

$$\begin{aligned} a_{11}X_1 + a_{12}X_2 + \cdots + a_{1n}X_n &= b_1, \\ a_{21}X_1 + a_{22}X_2 + \cdots + a_{2n}X_n &= b_2, \\ &\vdots \\ a_{m1}X_1 + a_{m2}X_2 + \cdots + a_{mn}X_n &= b_m, \end{aligned}$$

where $a_{ij}, b_i \in F$.

a. Show that the "system has a solution," that is, there exist $X_1, \cdots, X_n \in F$ that satisfy all m equations, if and only if the vector $\beta = (b_1, \cdots, b_m)$ of F^m is a linear combination of the vectors $\alpha_j = (a_{1j}, \cdots, a_{mj})$. (This result is straightforward to prove, being practically the definition of a solution, but should really be regarded as the *fundamental existence theorem for a simultaneous solution of a system of linear equations*.)

b. From part (a), show that if $n = m$ and $\{\alpha_j \mid j = 1, \cdots, n\}$ is a basis for F^n, then the system always has a unique solution.

23. Prove that every finite-dimensional vector space V of dimension n over a field F is isomorphic to the vector space F^n of Exercise 19.

24. Let V and V' be vector spaces over the same field F. A function $\phi : V \to V'$ is a **linear transformation of** V **into** V' if the following conditions are satisfied for all $\alpha, \beta \in V$, and $a \in F$:

$$\phi(\alpha + \beta) = \phi(\alpha) + \phi(\beta).$$
$$\phi(a\alpha) = a(\phi(\alpha)).$$

a. If $\{\beta_i \mid i \in I\}$ is a basis for V over F, show that a linear transformation $\phi : V \to V'$ is completely determined by the vectors $\phi(\beta_i) \in V'$.

b. Let $\{\beta_i \mid i \in I\}$ be a basis for V, and let $\{\beta_i' \mid i \in I\}$ be any set of vectors, not necessarily distinct, of V'. Show that there exists exactly one linear transformation $\phi : V \to V'$ such that $\phi(\beta_i) = \beta_i'$.

25. Let V and V' be vector spaces over the same field F, and let $\phi : V \to V'$ be a linear transformation.

a. To what concept that we have studied for the algebraic structures of groups and rings does the concept of a *linear transformation* correspond?

b. Define the *kernel* (or *nullspace*) of ϕ, and show that it is a subspace of V.

c. Describe when ϕ is an isomorphism of V with V'.

26. Let V be a vector space over a field F, and let S be a subspace of V. Define the *quotient space* V/S, and show that it is a vector space over F.

27. Let V and V' be vector spaces over the same field F, and let V be finite dimensional over F. Let $\dim(V)$ be the dimension of the vector space V over F. Let $\phi : V \to V'$ be a linear transformation.

a. Show that $\phi[V]$ is a subspace of V'.

b. Show that $\dim(\phi[V]) = \dim(V) - \dim(\text{Ker}(\phi))$. [*Hint:* Choose a convenient basis for V, using Theorem 33.18. For example, enlarge a basis for $\text{Ker}(\phi)$ to a basis for V.]

28. Let R be a commutative ring with unity and F a subring of R that is a field. Think of F as the scalars and R as the set of vectors with scalar multiplication given by multiplication in the ring R.

a. Give an example to show that R need not be a vector space over F.

b. Show that if the unity of R and the unity of F are the same, then R is a vector space over F.

SECTION 34 UNIQUE FACTORIZATION DOMAINS

The integral domain $\mathbb{Z}$ is our standard example of an integral domain in which there is unique factorization into primes (irreducibles). Section 28 showed that for a field F, $F[x]$ is also such an integral domain with unique factorization. In order to discuss analogous

ideas in an arbitrary integral domain, we shall give several definitions, some of which are repetitions of earlier ones. It is nice to have them all in one place for reference.

34.1 Definition Let R be a commutative ring with unity and let $a, b \in R$. If there exists $c \in R$ such that $b = ac$, then a **divides** b (or a **is a factor of** b), denoted by $a \mid b$. We read $a \nmid b$ as "a does not divide b." ■

34.2 Definition An element u of a commutative ring with unity R is a **unit of** R if u divides 1, that is, if u has a multiplicative inverse in R. Two elements $a, b \in R$ are **associates in** R if $a = bu$, where u is a unit in R.

Exercise 27 asks us to show that this criterion for a and b to be associates is an equivalence relation on R. ■

34.3 Example The only units in $\mathbb{Z}$ are 1 and -1. Thus the only associates of 26 in $\mathbb{Z}$ are 26 and -26. ▲

34.4 Definition A nonzero element p that is not a unit of an integral domain D is an **irreducible of** D if every factorization $p = ab$ in D has the property that either a or b is a unit. ■

Note that an associate of an irreducible p is again an irreducible, for if $p = uc$ for a unit u, then any factorization of c provides a factorization of p.

34.5 Definition An integral domain D is a **unique factorization domain** (abbreviated UFD) if the following conditions are satisfied:

1. Every element of D that is neither 0 nor a unit can be factored into a product of a finite number of irreducibles.
2. If $p_1 \cdots p_r$ and $q_1 \cdots q_s$ are two factorizations of the same element of D into irreducibles, then $r = s$ and the q_j can be renumbered so that p_i and q_i are associates. ■

34.6 Example Theorem 28.21 shows that for a field F, $F[x]$ is a UFD. Also we know that $\mathbb{Z}$ is a UFD; we have made frequent use of this fact, although we have never proved it. For example, in $\mathbb{Z}$ we have

$$24 = (2)(2)(3)(2) = (-2)(-3)(2)(2).$$

Here 2 and -2 are associates, as are 3 and -3. Thus except for order and associates, the irreducible factors in these two factorizations of 24 are the same. ▲

Recall that the *principal ideal* $\langle a \rangle$ of D consists of all multiples of the element a. After just one more definition we can describe what we wish to achieve in this section.

34.7 Definition An integral domain D is a **principal ideal domain** (abbreviated PID) if every ideal in D is a principal ideal. ■

We know that $\mathbb{Z}$ is a PID because every ideal is of the form $n\mathbb{Z}$, generated by some integer n. Theorem 31.24 shows that if F is a field, then $F[x]$ is a PID. Our purpose in this section is to prove two exceedingly important theorems:

1. Every PID is a UFD. (Theorem 34.18)
2. If D is a UFD, then $D[x]$ is a UFD. (Theorem 34.30)