We emphasize that an abelian group M may have many different R-module structures, even if the ring R does not vary (in the same way that a given group G may act in many ways as a permutation group on some fixed set Ω). We shall see that the structure of an R-module is reflected by the ideal structure of R. When R is a field (the subject of the next chapter) all R-modules will be seen to be products of copies of R (as in Example 3 above).

We shall see in Chapter 12 that the relatively simple ideal structure of the ring $F[x]$ (recall that $F[x]$ is a Principal Ideal Domain) forces the $F[x]$-module structure of V to be correspondingly uncomplicated, and this in turn provides a great deal of information about the linear transformation T (in particular, gives some nice matrix representations for T: its *rational canonical form* and its *Jordan canonical form*). Moreover, the same arguments which *classify* finitely generated $F[x]$-modules apply to any Principal Ideal Domain R, and when these are invoked for $R = \mathbb{Z}$, we obtain the Fundamental Theorem of Finitely Generated Abelian Groups. These results generalize the theorem that every finite dimensional vector space has a basis.

In Part VI of the book we shall study modules over certain noncommutative rings (group rings) and see that this theory in some sense generalizes both the study of $F[x]$-modules in Chapter 12 and the notion of a permutation representation of a finite group.

We establish a submodule criterion analogous to that for subgroups of a group in Section 2.1.

Proposition 1. *(The Submodule Criterion)* Let R be a ring and let M be an R-module. A subset N of M is a submodule of M if and only if

(1) $N \neq \emptyset$, and

(2) $x + ry \in N$ for all $r \in R$ and for all $x, y \in N$.

Proof: If N is a submodule, then $0 \in N$ so $N \neq \emptyset$. Also N is closed under addition and is sent to itself under the action of elements of R. Conversely, suppose (1) and (2) hold. Let $r = -1$ and apply the subgroup criterion (in additive form) to see that N is a subgroup of M. In particular, $0 \in N$. Now let $x = 0$ and apply hypothesis (2) to see that N is sent to itself under the action of R. This establishes the proposition.

We end this section with an important definition and some examples.

Definition. Let R be a commutative ring with identity. An R-*algebra* is a ring A with identity together with a ring homomorphism $f : R \to A$ mapping 1_R to 1_A such that the subring $f(R)$ of A is contained in the center of A.

If A is an R-algebra then it is easy to check that A has a natural left and right (unital) R-module structure defined by $r \cdot a = a \cdot r = f(r)a$ where $f(r)a$ is just the multiplication in the ring A (and this is the same as $af(r)$ since by assumption $f(r)$ lies in the center of A). In general it is possible for an R-algebra A to have other left (or right) R-module structures, but unless otherwise stated, this natural module structure on an algebra will be assumed.

Definition. If A and B are two R-algebras, an *R-algebra homomorphism* (or isomorphism) is a ring homomorphism (isomorphism, respectively) $\varphi : A \to B$ mapping 1_A to 1_B such that $\varphi(r \cdot a) = r \cdot \varphi(a)$ for all $r \in R$ and $a \in A$.

Examples

Let R be a commutative ring with 1.

(1) Any ring with identity is a $\mathbb{Z}$-algebra.

(2) For any ring A with identity, if R is a subring of the center of A containing the identity of A then A is an R-algebra. In particular, a commutative ring A containing 1 is an R-algebra for any subring R of A containing 1. For example, the polynomial ring $R[x]$ is an R-algebra, the polynomial ring over R in any number of variables is an R-algebra, and the group ring RG for a finite group G is an R-algebra (cf. Section 7.2).

(3) If A is an R-algebra then the R-module structure of A depends only on the subring $f(R)$ contained in the center of A as in the previous example. If we replace R by its image $f(R)$ we see that "up to a ring homomorphism" every algebra A arises from a subring of the center of A that contains 1_A.

(4) A special case of the previous example occurs when $R = F$ is a *field*. In this case F is *isomorphic* to its image under f, so we can identify F itself as a subring of A. Hence, saying that A is an algebra over a field F is the same as saying that the ring A contains the field F in its center and the identity of A and of F are the same (this last condition is necessary, cf. Exercise 23).

Suppose that A is an R-algebra. Then A is a ring with identity that is a (unital) left R-module satisfying $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$ for all $r \in R$ and $a, b \in A$ (these are all equal to the product $f(r)ab$ in the ring A—recall that $f(R)$ is contained in the center of A). Conversely, these conditions on a ring A define an R-algebra, and are sometimes used as the definition of an R-algebra (cf. Exercise 22).

EXERCISES

In these exercises R is a ring with 1 and M is a left R-module.

1. Prove that $0m = 0$ and $(-1)m = -m$ for all $m \in M$.

2. Prove that $R^\times$ and M satisfy the two axioms in Section 1.7 for a *group action* of the multiplicative group $R^\times$ on the set M.

3. Assume that $rm = 0$ for some $r \in R$ and some $m \in M$ with $m \neq 0$. Prove that r does not have a left inverse (i.e., there is no $s \in R$ such that $sr = 1$).

4. Let M be the module R^n described in Example 3 and let $I_1, I_2, \dots, I_n$ be left ideals of R. Prove that the following are submodules of M:

(a) $\{(x_1, x_2, \dots, x_n) \mid x_i \in I_i\}$

(b) $\{(x_1, x_2, \dots, x_n) \mid x_i \in R \text{ and } x_1 + x_2 + \cdots + x_n = 0\}$.

5. For any left ideal I of R define

$$IM = \{\sum_{\text{finite}} a_i m_i \mid a_i \in I,\ m_i \in M\}$$

to be the collection of all finite sums of elements of the form am where $a \in I$ and $m \in M$. Prove that IM is a submodule of M.

6. Show that the intersection of any nonempty collection of submodules of an R-module is a submodule.

7. Let $N_1 \subseteq N_2 \subseteq \cdots$ be an ascending chain of submodules of M. Prove that $\cup_{i=1}^{\infty} N_i$ is a submodule of M.

8. An element m of the R-module M is called a *torsion element* if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is denoted

$$\mathrm{Tor}(M) = \{m \in M \mid rm = 0 \text{ for some nonzero } r \in R\}.$$

(a) Prove that if R is an integral domain then $\mathrm{Tor}(M)$ is a submodule of M (called the *torsion* submodule of M).
(b) Give an example of a ring R and an R-module M such that $\mathrm{Tor}(M)$ is not a submodule. [Consider the torsion elements in the R-module R.]
(c) If R has zero divisors show that every nonzero R-module has nonzero torsion elements.

9. If N is a submodule of M, the *annihilator of N in R* is defined to be $\{r \in R \mid rn = 0 \text{ for all } n \in N\}$. Prove that the annihilator of N in R is a 2-sided ideal of R.

10. If I is a right ideal of R, the *annihilator of I in M* is defined to be $\{m \in M \mid am = 0 \text{ for all } a \in I\}$. Prove that the annihilator of I in M is a submodule of M.

11. Let M be the abelian group (i.e., $\mathbb{Z}$-module) $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$.
(a) Find the annihilator of M in $\mathbb{Z}$ (i.e., a generator for this principal ideal).
(b) Let $I = 2\mathbb{Z}$. Describe the annihilator of I in M as a direct product of cyclic groups.

12. In the notation of the preceding exercises prove the following facts about annihilators.
(a) Let N be a submodule of M and let I be its annihilator in R. Prove that the annihilator of I in M contains N. Give an example where the annihilator of I in M does not equal N.
(b) Let I be a right ideal of R and let N be its annihilator in M. Prove that the annihilator of N in R contains I. Give an example where the annihilator of N in R does not equal I.

13. Let I be an ideal of R. Let M' be the subset of elements a of M that are annihilated by some power, I^k, of the ideal I, where the power may depend on a. Prove that M' is a submodule of M. [Use Exercise 7.]

14. Let z be an element of the center of R, i.e., $zr = rz$ for all $r \in R$. Prove that zM is a submodule of M, where $zM = \{zm \mid m \in M\}$. Show that if R is the ring of 2×2 matrices over a field and e is the matrix with a 1 in position 1,1 and zeros elsewhere then eR is *not* a left R-submodule (where $M = R$ is considered as a left R-module as in Example 1) — in this case the matrix e is not in the center of R.

15. If M is a finite abelian group then M is naturally a $\mathbb{Z}$-module. Can this action be extended to make M into a $\mathbb{Q}$-module?

16. Prove that the submodules U_k described in the example of $F[x]$-modules are all of the $F[x]$-submodules for the shift operator.

17. Let T be the shift operator on the vector space V and let $e_1, \ldots, e_n$ be the usual basis vectors described in the example of $F[x]$-modules. If $m \geq n$ find $(a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0) e_n$.

18. Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is rotation clockwise about the origin by $\pi/2$ radians. Show that V and 0 are the only $F[x]$-submodules for this T.

19. Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is projection onto the y-axis. Show that V, 0, the x-axis and the y-axis are the only $F[x]$-submodules for this T.

20. Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is rotation clockwise about the origin by π radians. Show that *every* subspace of V is an