$F[x]$-submodule for this T.

21. Let $n \in \mathbb{Z}^+$, $n > 1$ and let R be the ring of $n \times n$ matrices with entries from a field F. Let M be the set of $n \times n$ matrices with arbitrary elements of F in the first column and zeros elsewhere. Show that M is a submodule of R when R is considered as a left module over itself, but M is not a submodule of R when R is considered as a right R-module.

22. Suppose that A is a ring with identity 1_A 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 $a, b \in A$. Prove that the map $f : R \to A$ defined by $f(r) = r \cdot 1_A$ is a ring homomorphism mapping 1_R to 1_A and that $f(R)$ is contained in the center of A. Conclude that A is an R-algebra and that the R-module structure on A induced by its algebra structure is precisely the original R-module structure.

23. Let A be the direct product ring $\mathbb{C} \times \mathbb{C}$ (cf. Section 7.6). Let τ_1 denote the identity map on $\mathbb{C}$ and let τ_2 denote complex conjugation. For any pair $p, q \in \{1, 2\}$ (not necessarily distinct) define

$$f_{p,q} : \mathbb{C} \to \mathbb{C} \times \mathbb{C} \qquad \text{by} \qquad f_{p,q}(z) = (\tau_p(z), \tau_q(z)).$$

So, for example, $f_{2,1} : z \mapsto (\bar{z}, z)$, where $\bar{z}$ is the complex conjugate of z, i.e., $\tau_2(z)$.

(a) Prove that each $f_{p,q}$ is an injective ring homomorphism, and that they all agree on the subfield $\mathbb{R}$ of $\mathbb{C}$. Deduce that A has four distinct $\mathbb{C}$-algebra structures. Explicitly give the action $z \cdot (u, v)$ of a complex number z on an ordered pair in A in each case.

(b) Prove that if $f_{p,q} \neq f_{p',q'}$ then the identity map on A is *not* a $\mathbb{C}$-algebra homomorphism from A considered as a $\mathbb{C}$-algebra via $f_{p,q}$ to A considered a $\mathbb{C}$-algebra via $f_{p',q'}$ (although the identity is an $\mathbb{R}$-algebra isomorphism).

(c) Prove that for any pair p, q there is some ring isomorphism from A to itself such that A is isomorphic as a $\mathbb{C}$-algebra via $f_{p,q}$ to A considered as $\mathbb{C}$-algebra via $f_{1,1}$ (the "natural" $\mathbb{C}$-algebra structure on A).

Remark: In the preceding exercise $A = \mathbb{C} \times \mathbb{C}$ is not a $\mathbb{C}$-algebra over either of the direct factor component copies of $\mathbb{C}$ (for example the subring $\mathbb{C} \times 0 \cong \mathbb{C}$) since it is not a unital module over these copies of $\mathbb{C}$ (the 1 of these subrings is not the same as the 1 of A).

10.2 QUOTIENT MODULES AND MODULE HOMOMORPHISMS

This section contains the basic theory of quotient modules and module homomorphisms.

Definition. Let R be a ring and let M and N be R-modules.

(1) A map $\varphi : M \to N$ is an *R-module homomorphism* if it respects the R-module structures of M and N, i.e.,

  (a) $\varphi(x + y) = \varphi(x) + \varphi(y)$, for all $x, y \in M$ and

  (b) $\varphi(rx) = r\varphi(x)$, for all $r \in R$, $x \in M$.

(2) An R-module homomorphism is an *isomorphism (of R-modules)* if it is both injective and surjective. The modules M and N are said to be *isomorphic*, denoted $M \cong N$, if there is some R-module isomorphism $\varphi : M \to N$.

(3) If $\varphi : M \to N$ is an R-module homomorphism, let $\ker \varphi = \{m \in M \mid \varphi(m) = 0\}$ (the *kernel* of φ) and let $\varphi(M) = \{n \in N \mid n = \varphi(m) \text{ for some } m \in M\}$ (the *image* of φ, as usual).

(4) Let M and N be R-modules and define $\mathrm{Hom}_R(M, N)$ to be the set of all R-module homomorphisms from M into N.

Any R-module homomorphism is also a homomorphism of the additive groups, but not every group homomorphism need be a module homomorphism (because condition (b) may not be satisfied). The unqualified term "isomorphism" when applied to R-modules will always mean R-module isomorphism. When the symbol $\cong$ is used without qualification it will denote an isomorphism of the respective structures (which will be evident from the context).

It is an easy exercise using the submodule criterion (Proposition 1) to show that kernels and images of R-module homomorphisms are submodules.

Examples

(1) If R is a ring and $M = R$ is a module over itself, then R-module homomorphisms (even from R to itself) need not be ring homomorphisms and ring homomorphisms need not be R-module homomorphisms. For example, when $R = \mathbb{Z}$ the $\mathbb{Z}$-module homomorphism $x \mapsto 2x$ is not a ring homomorphism (1 does not map to 1). When $R = F[x]$ the ring homomorphism $\varphi : f(x) \mapsto f(x^2)$ is not an $F[x]$-module homomorphism (if it were, we would have $x^2 = \varphi(x) = \varphi(x \cdot 1) = x\varphi(1) = x$).

(2) Let R be a ring, let $n \in \mathbb{Z}^+$ and let $M = R^n$. One easily checks that for each $i \in \{1, \ldots, n\}$ the projection map

$$\pi_i : R^n \to R \quad \text{by} \quad \pi_i(x_1, \ldots, x_n) = x_i$$

is a surjective R-module homomorphism with kernel equal to the submodule of n-tuples which have a zero in position i.

(3) If R is a field, R-module homomorphisms are called *linear transformations*. These will be studied extensively in Chapter 11.

(4) For the ring $R = \mathbb{Z}$ the action of ring elements (integers) on any $\mathbb{Z}$-module amounts to just adding and subtracting within the (additive) abelian group structure of the module so that in this case condition (b) of a homomorphism is implied by condition (a). For example, $\varphi(2x) = \varphi(x + x) = \varphi(x) + \varphi(x) = 2\varphi(x)$, etc. It follows that

$\mathbb{Z}$-module homomorphisms are the same as abelian group homomorphisms.

(5) Let R be a ring, let I be a 2-sided ideal of R and suppose M and N are R-modules annihilated by I (i.e., $am = 0$ and $an = 0$ for all $a \in I$, $n \in N$ and $m \in M$). Any R-module homomorphism from N to M is then automatically a homomorphism of (R/I)-modules (see Example 5 of Section 1). In particular, if A is an additive abelian group such that for some prime p, $px = 0$ for all $x \in A$, then any group homomorphism from A to itself is a $\mathbb{Z}/p\mathbb{Z}$-module homomorphism, i.e., is a linear transformation over the field $\mathbb{F}_p$. In particular, the group of all (group) automorphisms of A is the group of invertible linear transformations from A to itself: $GL(A)$.

Proposition 2. Let M, N and L be R-modules.

(1) A map $\varphi : M \to N$ is an R-module homomorphism if and only if $\varphi(rx + y) = r\varphi(x) + \varphi(y)$ for all $x, y \in M$ and all $r \in R$.

(2) Let φ, ψ be elements of $\mathrm{Hom}_R(M, N)$. Define $\varphi + \psi$ by

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m) \qquad \text{for all } m \in M.$$

Then $\varphi + \psi \in \mathrm{Hom}_R(M, N)$ and with this operation $\mathrm{Hom}_R(M, N)$ is an abelian group. If R is a commutative ring then for $r \in R$ define $r\varphi$ by

$$(r\varphi)(m) = r(\varphi(m)) \qquad \text{for all } m \in M.$$

Then $r\varphi \in \mathrm{Hom}_R(M, N)$ and with this action of the commutative ring R the abelian group $\mathrm{Hom}_R(M, N)$ is an R-module.

(3) If $\varphi \in \mathrm{Hom}_R(L, M)$ and $\psi \in \mathrm{Hom}_R(M, N)$ then $\psi \circ \varphi \in \mathrm{Hom}_R(L, N)$.

(4) With addition as above and multiplication defined as function composition, $\mathrm{Hom}_R(M, M)$ is a ring with 1. When R is commutative $\mathrm{Hom}_R(M, M)$ is an R-algebra.

Proof: (1) Certainly $\varphi(rx+y) = r\varphi(x)+\varphi(y)$ if φ is an R-module homomorphism. Conversely, if $\varphi(rx + y) = r\varphi(x) + \varphi(y)$, take $r = 1$ to see that φ is additive and take $y = 0$ to see that φ commutes with the action of R on M (i.e., is *homogeneous*).

(2) It is straightforward to check that all the abelian group and R-module axioms hold with these definitions — the details are left as an exercise. We note that the commutativity of R is used to show that $r\varphi$ satisfies the second axiom of an R-module homomorphism, namely,

$$\begin{aligned}(r_1\varphi)(r_2m) &= r_1\varphi(r_2m) && \text{(by definition of } r_1\varphi)\\ &= r_1r_2(\varphi(m)) && \text{(since } \varphi \text{ is a homomorphism)}\\ &= r_2r_1\varphi(m) && \text{(since } R \text{ is commutative)}\\ &= r_2(r_1\varphi)(m) && \text{(by definition of } r_1\varphi).\end{aligned}$$

Verification of the axioms relies ultimately on the hypothesis that N is an R-module. The domain M could in fact be any set — it does not have to be an R-module nor an abelian group.

(3) Let φ and ψ be as given and let $r \in R$, $x, y \in L$. Then

$$\begin{aligned}(\psi \circ \varphi)(rx + y) &= \psi(\varphi(rx + y))\\ &= \psi(r\varphi(x) + \varphi(y)) && \text{(by (1) applied to } \varphi)\\ &= r\psi(\varphi(x)) + \psi(\varphi(y)) && \text{(by (1) applied to } \psi)\\ &= r(\psi \circ \varphi)(x) + (\psi \circ \varphi)(y)\end{aligned}$$

so, by (1), $\psi \circ \varphi$ is an R-module homomorphism.

(4) Note that since the domain and codomain of the elements of $\mathrm{Hom}_R(M, M)$ are the same, function composition is defined. By (3), it is a binary operation on $\mathrm{Hom}_R(M, M)$. As usual, function composition is associative. The remaining ring axioms are straightforward to check — the details are left as an exercise. The identity function, I, (as usual, $I(x) = x$, for all $x \in M$) is seen to be the multiplicative identity of $\mathrm{Hom}_R(M, M)$. If R is commutative, then (2) shows that the ring $\mathrm{Hom}_R(M, M)$ is a left R-module and defining $\varphi r = r\varphi$ for all $\varphi \in \mathrm{Hom}_R(M, M)$ and $r \in R$ makes $\mathrm{Hom}_R(M, M)$ into an R-algebra.

Definition. The ring $\mathrm{Hom}_R(M, M)$ is called the *endomorphism ring of* M and will often be denoted by $\mathrm{End}_R(M)$, or just $\mathrm{End}(M)$ when the ring R is clear from the context. Elements of $\mathrm{End}(M)$ are called *endomorphisms*.