WORKSHEET 1.2: MODULES, SUBMODULES, AND QUOTIENTS

Let R be a ring. A *left R-module* is an abelian group $(M,+,0_M)$ together with a scalar multiplication $R\times M\to M$, written $(r,m)\mapsto rm$, satisfying the following axioms:

(i) (Identity) $1_R m = m$ for all $m\in M$,

(ii) (Associativity) $(rs)m = r(sm)$ for all $r,s\in R$ and all $m\in M$,

(iii) (Left Distributivity) $r(m+n) = rm+rn$ for all $r\in R$ and all $m,n\in M$, and

(iv) (Right Distributivity) $(r+s)m = rm+sm$ for all $r,s\in R$ and all $m\in M$.

We write rm for the scalar multiplication of $r\in R$ and $m\in M$, and we write 0 for 0_R or 0_M when the intended identity is clear from context. Unlike a ring, a module need not have a multiplication of its own elements. The associativity axiom describes how multiplication in R interacts with its action on M: acting by s and then by r is the same as acting by rs.

A *right R-module* has its scalars acting on the right, with associativity given by $m(rs) = (mr)s$. Unless we say otherwise, *module* will always mean left module. In a commutative ring the two notions agree by setting $mr = rm$, but in an arbitrary ring it is important to keep track of the side on which scalars act. As in the previous worksheet all rings have a multiplicative identity, but need not be commutative, and the letter $\mathbb{K}$ will denote a field.

The goal of this worksheet is to introduce modules and study their submodules, homomorphisms, and quotients. Modules generalize vector spaces by allowing scalars to come from a ring. You already know several examples, including vector spaces and abelian groups. The definitions let us study these examples together, while retaining differences such as whether a module has a basis.

---

1. **Basic Module Identities.** Throughout this exercise let M be a left R-module.

   (a) Starting from the axioms, prove the following identities:

   (i) $r0_M = 0_M$ for all $r\in R$,

   (ii) $0_R m = 0_M$ for all and $m\in M$, and

   (iii) $(-r)m = -(rm) = r(-m)$ for all $r\in R$ and $m\in M$.

   (b) State in words what each of the three identities above mean.

2. **First Examples of Modules.** Throughout this exercise let R be a ring.

   (a) Compare the module axioms with the vector space axioms, and explain why a $\mathbb{K}$-module is exactly a $\mathbb{K}$-vector space. Do the module axioms require nonzero scalars to be invertible? Do they require multiplication in R to be commutative?

   (b) Check that R itself is a left R-module under its own multiplication. Which module axioms are inherited from which ring axioms?

   (c) If $I \subset R$ is a left ideal, explain why the multiplication on R makes I an R-module.

   (d) Given an example of a ring R and an additive subgroup $A \subset R$, which is not an R-module.

   (e) Let A be an abelian group. Define an action $\mathbb{Z} \times A \to A$ by $(n,a) \mapsto na$ where na means a added to itself n times. Show that this makes A into a $\mathbb{Z}$-module.

   (f) Conversely, show that the axioms force every $\mathbb{Z}$-action on A to be this one. Thus an abelian group has a unique $\mathbb{Z}$-module structure. Compare this with the unique ring homomorphism $\mathbb{Z} \to R$ from Worksheet 1.1.

Let M be an R-module. A *submodule* $N \subset M$ is an additive subgroup which is closed under the R-action, so that the action of R on M restrict to an action of R on N. (There might be some sort of diagram you might draw here.) Equivalently, N is nonempty and $rn + sn' \in N$ whenever $r,s \in R$ and $n,n' \in N$. This is the same closure condition used to recognize subspaces, with the scalars now taken from R.

Let M and N be R-modules, a *module homomorphism*, or *R-linear map*, is a function $\phi : M \to N$ satisfying the following conditions for all $m,m' \in M$ and all $r \in R$:

(i) $\phi(m+m') = \phi(m) + \phi(m')$.

(ii) $\phi(rm) = r\phi(m)$.

Notice the first condition says that ϕ is a homomorphism of the underlying abelian groups. In particular it preserves 0 and additive inverses. The second says that ϕ respects the scalar action. We write $\mathrm{Hom}_R(M,N)$ for the set of such maps. We call a homomorphism from a module to itself a *endomorphism* and so $\mathrm{End}_R(M) := \mathrm{Hom}_R(M,M)$.

A module homomorphism is an *isomorphism* if it has an inverse which is again a module homomorphism. As with groups and rings, this turns out to be equivalent to the set theoretic condition of being a bijection. We write $M \cong N$ when an isomorphism exists. An *automorphism* of M is an isomorphism $\phi : M \to M$. We denote the set of R-linear automorphisms by $\mathrm{Aut}_R(M) \subset \mathrm{End}_R(M)$.

As with ring homomorphisms, a module homomorphism $\phi : M \to N$ comes with a *kernel* and an *image*:

$$\ker(\phi) := \{m \in M \mid \phi(m) = 0_N\} \subset M \qquad \text{and} \qquad \mathrm{img}(\phi) := \{\phi(m) \mid m \in M\} \subset N.$$

A homomorphism is surjective exactly when its image is the whole target, while its kernel measures its failure to be injective. Whether an additive subgroup is a submodule depends on the ring action. For example, a subspace of $\mathbb{K}^2$ need not be preserved by every matrix in $\mathrm{Mat}_2(\mathbb{K})$. We will see this distinction in the following exercise.

---

3. **Submodules and Module Homomorphisms.** Throughout this exercise let M and N be R-modules.

   (a) Prove that $N \subset M$ is a non-empty R-submodule if and only if N is non-empty and $rn + sn' \in N$ whenever $r, s \in R$ and $n, n' \in N$.

   (b) Show that $\mathbb{K}$-module maps are exactly the linear maps of vector spaces.

   (c) Show that $\mathbb{Z}$-module maps are exactly the homomorphisms of abelian groups.

   (d) Let $\phi : M \to N$ be an R-linear map. Prove that $\ker(\phi)$ is a submodule of M and that $\mathrm{img}(\phi)$ is a submodule of N

   (e) Prove that ϕ is injective if and only if $\ker(\phi) = \{0\}$, and surjective if and only if $\mathrm{img}(\phi) = P$.

   (f) Show that compositions of R-linear maps and identity maps are R-linear. If ϕ is a bijective R-linear map, prove that ϕ^{-1} is R-linear, so that ϕ is an isomorphism. Hint: write two elements of the target as $\phi(m)$ and $\phi(m')$.

   (g) Let $R = \mathrm{Mat}_2(\mathbb{K})$ act on the column space $\mathbb{K}^2$ by matrix multiplication. Verify the module axioms. Show that any nonzero column can be carried to any other column by a suitable matrix, and deduce that this module has exactly two submodules. In particular, is the line $\mathbb{K}e_1$ an R-submodule? Compare this with the left ideal of $\mathrm{Mat}_2(\mathbb{K})$ consisting of matrices whose second column is zero, which you studied in Worksheet 1.1.

Modules over the polynomial ring $\mathbb{K}[x]$ give a useful dictionary between module theory and linear algebra. Let V be a $\mathbb{K}$-vector space and let $T : V \to V$ be a linear operator. Substituting T for x defines an action of $\mathbb{K}[x]$ on V by the rule

$$\left(a_0 + a_1 x + \cdots + a_d x^d\right) v := a_0 v + a_1 T(v) + \cdots + a_d T^d(v), \qquad T^0 := \mathrm{Id}_V .$$

We write V_T for the resulting module. Constant polynomials act by the original scalar multiplication on V, and the variable x acts by T. Conversely, a $\mathbb{K}[x]$-module becomes a vector space once we restrict the scalars to the constant polynomials, and multiplication by x is then a linear operator on that vector space. A $\mathbb{K}[x]$-module is therefore the same thing as a vector space together with a choice of linear operator. The variable x is still a formal symbol; it is the module structure which specifies how it acts.

This dictionary also translates submodules and homomorphisms. Let W be a $\mathbb{K}$-vector space with a linear operator $S : W \to W$. A $\mathbb{K}$-linear map $\phi : V \to W$ is a module homomorphism $V_T \to W_S$ if and only if $\phi \circ T = S \circ \phi$, in which case we call ϕ an *intertwining map*. Similarly, a subspace $U \subset V$ is a submodule of V_T if and only if $T(U) \subset U$, in which case we call U a *T-invariant subspace*. These translations let us study a linear operator by studying its module, a point of view we will return to when we discuss canonical forms. We check the dictionary in the following exercise.

---

4. **Modules over $\mathbb{K}[x]$ and Linear Operators.** Throughout this exercise let V and W be $\mathbb{K}$-vector spaces equipped with linear operators T and S respectively.

   (a) Verify that the displayed formula makes V into a $\mathbb{K}[x]$-module. For the associativity axiom, first check that $T^i T^j = T^{i+j}$, and then expand a product of two polynomials.

   (b) Conversely, let M be a $\mathbb{K}[x]$-module. Use the constant polynomials to regard M as a $\mathbb{K}$-vector space, and set $T(m) \coloneqq xm$. Prove that T is $\mathbb{K}$-linear, and then show that every polynomial acts by the displayed formula. Conclude that the two constructions undo one another.

   (c) Prove that a map $\phi : V \to W$ is $\mathbb{K}[x]$-linear as a map $V_T \to W_S$ if and only if it is $\mathbb{K}$-linear and

   $$\phi \circ T = S \circ \phi.$$

   For the reverse implication, first prove that $\phi \circ T^j = S^j \circ \phi$ by induction on j.

   (d) Prove that the $\mathbb{K}[x]$-submodules of V_T are exactly the subspaces $U \subset V$ with $T(U) \subset U$. Why does stability under T already force stability under every polynomial in T?

   (e) Show that an intertwining map carries T-invariant subspaces to S-invariant subspaces. Check directly that its kernel is T-invariant and that its image is S-invariant.

   (f) Suppose that V and W are finite dimensional. Choose bases and translate the equation $\phi \circ T = S \circ \phi$ into an equation of matrices. Deduce that $V_T \cong W_S$ exactly when the matrices of the two operators are related by an invertible change of coordinates.

For a concrete example, let $V = \mathbb{K}^2$ with basis e_1, e_2, and define a linear operator by $T(e_1) = 0$ and $T(e_2) = e_1$. The operator T is *nilpotent*, meaning that some positive power of T is zero. Here $T^2 = 0$, so a polynomial $f(x) = a_0 + a_1 x + x^2 g(x)$ acts by

$$f(T)(ue_1 + ve_2) = (a_0 u + a_1 v)e_1 + a_0 v e_2.$$

In particular, two polynomials which differ by a multiple of x^2 act in the same way. Recall the ring of dual numbers $\mathbb{K}[\varepsilon] = \mathbb{K}[x]/\langle x^2 \rangle$ from Worksheet 1.1, where $\varepsilon = x + \langle x^2 \rangle$. Every element has a unique expression $a + b\varepsilon$ with $a, b \in \mathbb{K}$, and $\varepsilon^2 = 0$. Multiplication by ε sends 1 to ε and ε to zero, just as T sends e_2 to e_1

and e_1 to zero. We use this comparison in the following exercise to identify the two modules, and then to compute their submodules and endomorphisms.

---

5. **A Nilpotent Operator and the Dual Numbers.** Throughout this exercise let V and T be as above, let $\mathbb{K}[\varepsilon] = \mathbb{K}[x]/\langle x^2\rangle$, and let $\varepsilon = x + \langle x^2\rangle$.

   (a) Use the displayed formula to compute $(2+3x+x^5)e_2$ and $x(e_1+e_2)$ in V_T. Compute these vectors when $\mathbb{K} = \mathbb{F}_2$.

   (b) Regard $\mathbb{K}[\varepsilon]$ as a $\mathbb{K}[x]$-module by $f(x)\cdot(a+b\varepsilon) \coloneqq f(\varepsilon)(a+b\varepsilon)$. Show directly that

   $$\phi : \mathbb{K}[\varepsilon] \longrightarrow V_T, \qquad a+b\varepsilon \longmapsto ae_2 + be_1$$

   is well defined, $\mathbb{K}[x]$-linear, and bijective. Explain why interchanging e_1 and e_2 in this formula would not give a module homomorphism.

   (c) Show that e_2 generates V_T as a $\mathbb{K}[x]$-module, in the sense that every vector is of the form $f(x)e_2$. Does e_2 alone span V as a $\mathbb{K}$-vector space? Explain why the two questions have different answers.

   (d) Compute $\ker(T)$ and $\operatorname{img}(T)$. Use Problem 4 to show that V_T has exactly three submodules: $\{0\}$, $\mathbb{K}e_1$, and V_T. Hint: an invariant subspace containing $ue_1 + ve_2$ with $v \neq 0$ also contains e_1.

   (e) Write an arbitrary $\mathbb{K}$-linear map $\phi : V \to V$ as a 2×2 matrix and solve the equation $\phi \circ T = T \circ \phi$. Describe every element of $\operatorname{End}_{\mathbb{K}[x]}(V_T)$, and determine which of them lie in $\operatorname{Aut}_{\mathbb{K}[x]}(V_T)$. Compare the automorphisms you find with the units of $\mathbb{K}[\varepsilon]$ from Worksheet 1.1.

Let $N \subset M$ be a submodule. Since N is an additive subgroup of the abelian group M, we may form the quotient group M/N, whose elements are the cosets $m+N$, with $m+N = m'+N$ if and only if $m-m' \in N$. To obtain a *quotient module*, we define a scalar multiplication by

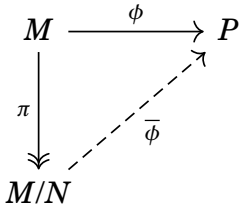
$$r(m+N) \coloneqq rm + N.$$

The fact that N is closed under the action of R guarantees that this formula does not depend on the chosen representative. Together with the addition $(m+N)+(m'+N) = (m+m')+N$, it makes M/N an R-module. The *quotient map*

$$M \xrightarrow{\ \pi\ } M/N \qquad\qquad m \longmapsto m+N$$

is a surjective module homomorphism with kernel N. Consequently, every submodule occurs as the kernel of a module homomorphism, just as every two-sided ideal occurs as the kernel of a ring homomorphism.

One way to think of M/N is as the module obtained by imposing the equations $n = 0$ for all $n \in N$. More precisely, a module homomorphism $\phi : M \to P$ which vanishes on N determines a unique module homomorphism $\overline{\phi} : M/N \to P$ such that $\overline{\phi} \circ \pi = \phi$:



This is the *universal property of quotient modules*. As with quotient rings, it describes homomorphisms out of M/N in terms of homomorphisms out of M which send N to zero. We check the construction and this property in the following exercise.

---

6. **Construction and Properties of Quotient Modules.** Throughout this exercise let $N \subset M$ be a submodule of an R-module.

   (a) Suppose $m + N = m' + N$, and prove that $rm + N = rm' + N$ for every $r \in R$, using the fact that N is closed under scalar multiplication. Write down the formulas for addition and scalar multiplication in M/N, and verify the module axioms.

   (b) Prove that $\pi : M \to M/N$, $m \mapsto m + N$, is a surjective module homomorphism with $\ker(\pi) = N$. Conclude that every submodule occurs as a kernel.

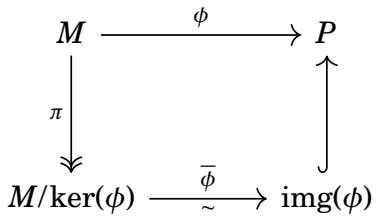
   (c) Suppose $\phi : M \to P$ is R-linear with $N \subset \ker(\phi)$. Prove that $\overline{\phi}(m + N) = \phi(m)$ is a well-defined R-linear map, and that it is the unique map $M/N \to P$ satisfying $\overline{\phi} \circ \pi = \phi$. Explain in words why a homomorphism out of M/N is the same thing as a homomorphism out of M which sends N to zero.

The construction of quotient modules also explains the relationship between the kernel and the image of a homomorphism $\phi : M \to P$. Two elements of M have the same image exactly when their difference lies in $\ker(\phi)$. Passing to $M/\ker(\phi)$ therefore identifies exactly the elements that ϕ identifies. The induced map is injective and has image $\mathrm{img}(\phi)$.

Theorem 1 (First Isomorphism Theorem for Modules)**.** *Let $\phi : M \to P$ be a homomorphism of R-modules. Then the map*

$$\overline{\phi} : M/\ker(\phi) \longrightarrow \mathrm{img}(\phi), \qquad m + \ker(\phi) \longmapsto \phi(m),$$

is an isomorphism of R-modules. In particular, there is a commutative diagram



Every module homomorphism can therefore be expressed as a quotient map followed by an isomorphism and an inclusion. If ϕ is surjective, the theorem gives $M/\ker(\phi) \cong P$. As with rings, we can recognize a quotient module by constructing a surjective homomorphism onto a module we already understand and computing its kernel. The familiar versions for abelian groups and vector spaces are special cases. We prove the theorem and apply it in the following exercise.

---

7. **The First Isomorphism Theorem and Examples.** Throughout parts (a) and (b) let $\phi : M \to P$ be a homomorphism of R-modules.

   (a) Use Problem 6 with $N = \ker(\phi)$ to construct $\overline{\phi} : M/\ker(\phi) \to \operatorname{img}(\phi)$. Show that the resulting map is surjective, and that if $\overline{\phi}(m + \ker(\phi)) = 0$ then $m + \ker(\phi)$ is the zero coset. Deduce that $\overline{\phi}$ is injective.

   (b) Use Problem 3 to conclude that the bijection of part (a) is an isomorphism of R-modules, which proves the theorem.

   (c) Apply the theorem to the $\mathbb{Z}$-linear map $\phi : \mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$, $a \mapsto \overline{8a}$. Compute its kernel and its image, and write the induced isomorphism down explicitly. What does it do to the class of 1?

   (d) Return to the module V_T of Problem 5. Regard T itself as a $\mathbb{K}[x]$-linear map and identify $V_T/\ker(T) \cong \operatorname{img}(T)$, describing the action of x on each side. For an invariant subspace U of an arbitrary V_T, explain why the operator induced on the quotient is $v + U \mapsto T(v) + U$.

The first isomorphism theorem also lets us compare quotients which are constructed in different ways. Let $A, B \subset M$ be submodules. Their *sum* is

$$A + B := \{a + b \mid a \in A,\ b \in B\},$$

which is the smallest submodule of M containing both A and B. Passing to $(A + B)/B$ has the effect of setting the elements of B equal to zero, so every class can be represented by an element of A alone. The part of A which becomes zero in the process is exactly $A \cap B$. The second isomorphism theorem is the precise form of this observation, and its proof is a single application of the first.

Theorem 2 (Second Isomorphism Theorem for Modules)**.** *If A and B are submodules of an R-module M, then*

$$A/(A \cap B) \xrightarrow{\sim} (A+B)/B, \qquad a+(A \cap B) \longmapsto a+B$$

is an isomorphism of R-modules.

---

8. **The Second Isomorphism Theorem.** Throughout this exercise let A and B be submodules of an R-module M.

   (a) Prove that $A+B$ and $A \cap B$ are submodules of M, and that $A+B$ is contained in every submodule of M containing both A and B.

   (b) Define $\phi : A \to (A+B)/B$ by $a \mapsto a+B$, and verify that it is a module homomorphism. Why does its image contain the class of every element $a+b$ of $A+B$?

   (c) Compute $\ker(\phi)$, and use Problem 7 to obtain the isomorphism

   $$A/(A \cap B) \cong (A+B)/B.$$

   Write down the image of a general coset, and check directly that your formula does not depend on the chosen representative.

   (d) Take $M = \mathbb{Z}$ as a $\mathbb{Z}$-module, with $A = 4\mathbb{Z}$ and $B = 6\mathbb{Z}$. Compute all four of the submodules appearing in the theorem, list the elements of both quotients, and match them under your isomorphism. Identify an element generating each quotient, and say where it goes.

Suppose $N \subset L \subset M$ are submodules. We may form M/L directly, or we may first form M/N and then take the quotient by L/N. The third isomorphism theorem says that these two constructions give isomorphic modules. The correspondence theorem describes all submodules of M/N in terms of the submodules of M which contain N.

Theorem 3 (Third Isomorphism and Correspondence Theorems)**.** *Let $N \subset M$ be a submodule and let $\pi : M \to M/N$ be the quotient map. The assignments $L \mapsto L/N = \pi(L)$ and $U \mapsto \pi^{-1}(U)$ give mutually inverse, inclusion-preserving bijections*

$$\{L \subset M \mid L \text{ a submodule containing } N\} \longleftrightarrow \{U \subset M/N \mid U \text{ a submodule}\}.$$

Moreover, for $N \subset L \subset M$ there is an isomorphism of R-modules

$$(M/N)/(L/N) \xrightarrow{\sim} M/L, \qquad (m+N)+(L/N) \longmapsto m+L.$$

Since the quotient map sends every element of N to zero, the preimage of any submodule of M/N contains N. Conversely, a submodule $L \subset M$ containing N determines the submodule $L/N \subset M/N$. The correspondence theorem says that these two constructions undo one another and preserve inclusion. We prove both statements in the following exercise.

---

9. **The Third Isomorphism and Correspondence Theorems.** Throughout this exercise let $N \subset L \subset M$ be submodules and let $\pi : M \to M/N$ be the quotient map.

   (a) Show that $L/N = \{\ell + N \mid \ell \in L\}$ is a submodule of M/N, and that $\phi : M/N \to M/L$, $m + N \mapsto m + L$, is well defined and R-linear. Where do you use the inclusion $N \subset L$?

   (b) Show that ϕ is surjective with $\ker(\phi) = L/N$. Deduce the third isomorphism theorem, and write its formula on a coset of a coset.

   (c) If U is a submodule of M/N, prove that $\pi^{-1}(U)$ is a submodule of M containing N.

   (d) Prove the two identities
   $$\pi^{-1}(L/N) = L, \qquad \pi\big(\pi^{-1}(U)\big) = U,$$
   and conclude that $L \mapsto L/N$ and $U \mapsto \pi^{-1}(U)$ are inverse bijections. This is the correspondence theorem.

   (e) Check that both assignments preserve inclusion. What is $\pi^{-1}(0)$, and what is $\pi^{-1}(M/N)$? Explain why the submodules of M which do not contain N are excluded.

   (f) Take $M = \mathbb{Z}$ and $N = 12\mathbb{Z}$. List every submodule of $\mathbb{Z}$ containing $12\mathbb{Z}$, together with its corresponding submodule of $\mathbb{Z}/12\mathbb{Z}$. Then take $L = 4\mathbb{Z}$ and write out the third isomorphism theorem for these particular modules.

Let M and P be R-modules. The set $\mathrm{Hom}_R(M,P)$ is itself an abelian group under pointwise addition:

$$(f+g)(m) = f(m) + g(m), \qquad (-f)(m) = -f(m),$$

with the zero homomorphism as its identity element. Thus the collection of homomorphisms between two modules is again an algebraic object of the same general kind. Over a commutative ring, pointwise scalar multiplication also makes $\mathrm{Hom}_R(M,P)$ an R-module. Since our rings need not be commutative, we use only its abelian group structure here.

Maps out of cyclic modules give the first computations of this kind. Such a map is determined by the image of a generator, but that image is not arbitrary: it must satisfy whatever relations the generator satisfies. For a positive integer m, a homomorphism from $\mathbb{Z}/m\mathbb{Z}$ to an abelian group P is therefore the same thing

as an element $y \in P$ with $my = 0$. When $P = \mathbb{Z}/n\mathbb{Z}$ this description leads to

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/\gcd(m,n)\mathbb{Z}.$$

In the following exercise we construct this isomorphism by finding the possible images of $\overline{1}$, and then use the same description to compute kernels and images in some examples.

---

10. **Homomorphisms between Cyclic Abelian Groups.** Throughout parts (b) through (g) let $m, n \geq 1$ be integers and put $d := \gcd(m,n)$.

    (a) Let M and P be R-modules. Check that pointwise addition and negation preserve R-linearity. Identify the zero map, and verify that $\mathrm{Hom}_R(M,P)$ is an abelian group.

    (b) Show that a homomorphism $\phi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is determined by $y = \phi(\overline{1})$, and prove that $my = 0$ is necessary. Conversely, if $my = 0$, show that $\phi(\overline{a}) = ay$ is well defined and a homomorphism.

    (c) Write $m = dm'$ and $n = dn'$ with $\gcd(m', n') = 1$. Show that $my = 0$ in $\mathbb{Z}/n\mathbb{Z}$ exactly when y is represented by a multiple of n'. Hint: use Bézout's identity to justify the divisibility step.

    (d) Show that the assignment

    $$\mathbb{Z}/d\mathbb{Z} \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}), \qquad \overline{t} \longmapsto \left(\overline{a} \longmapsto \overline{a(n/d)t}\right)$$

    is a well-defined isomorphism of abelian groups. In particular, exactly how many such homomorphisms are there?

    (e) List every map $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$ by its value on $\overline{1}$, and compute the kernel and the image of each. Check Problem 7 against these examples, both numerically and by writing down the induced isomorphism.

    (f) Consider $\phi : \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/18\mathbb{Z}$ with $\phi(\overline{1}) = \overline{6}$. Verify that it exists, and compute its kernel, its image, and the induced isomorphism on the quotient. Does a map with $\phi(\overline{1}) = \overline{1}$ exist? Explain using the relation satisfied by $\overline{1}$ in the domain.

    (g) Use the possible orders of $\phi(\overline{1})$ to show that an injection $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ exists exactly when $m \mid n$, while a surjection exists exactly when $n \mid m$. Write down explicit maps in both cases.

We finish by describing module structures in terms of ring homomorphisms. Recall from Worksheet 1.1 that for an abelian group M, the endomorphism ring $\mathrm{End}_{\mathbb{Z}}(M) = \mathrm{Hom}_{\mathbb{Z}}(M,M)$ has pointwise addition and multiplication given by composition, with $fg = f \circ g$. Its multiplicative identity is Id_M.

If M is an R-module, then multiplication by a scalar r is an additive map $\rho(r) : M \to M$, where $\rho(r)(m) = rm$. The module axioms say exactly that the resulting function

$$\rho : R \longrightarrow \mathrm{End}_{\mathbb{Z}}(M)$$

is a ring homomorphism. For instance, the associativity axiom $(rs)m = r(sm)$ becomes the identity $\rho(rs) = \rho(r) \circ \rho(s)$, and the identity axiom $1_R m = m$ becomes $\rho(1_R) = \mathrm{Id}_M$, which is condition (iii) in the definition of a ring homomorphism. Conversely, any such ring homomorphism defines an R-module structure on the abelian group M. Thus giving an R-module structure on M is the same thing as giving a ring homomorphism $R \to \mathrm{End}_{\mathbb{Z}}(M)$.

Once an R-action has been fixed we may form the ring $\mathrm{End}_R(M)$ of those endomorphisms which respect it. This is a subring of $\mathrm{End}_{\mathbb{Z}}(M)$, with the same addition, composition, and identity element, and it acts on M by *evaluation*, $f \cdot m = f(m)$. The condition $f(rm) = rf(m)$ says precisely that this action commutes with the original one. Note that over a noncommutative ring the scalar operators $\rho(r)$ need not themselves be R-linear, which is why the target of ρ is $\mathrm{End}_{\mathbb{Z}}(M)$ and not $\mathrm{End}_R(M)$. The column module over $\mathrm{Mat}_2(\mathbb{K})$ makes this distinction concrete, as we see in the following exercise.

---

11. **Module Structures and Endomorphism Rings.** Throughout this exercise let M be an R-module.

    (a) Check the ring axioms for $\mathrm{End}_{\mathbb{Z}}(M)$. For one of the two distributive laws you will need that the operators are additive; identify which one, and explain why the other is formal. Show that $\mathrm{End}_R(M)$ is a subring containing the same identity element.

    (b) Starting from the module structure, define

    $$\rho : R \to \mathrm{End}_{\mathbb{Z}}(M), \qquad \rho(r)(m) = rm.$$

    Show that each $\rho(r)$ is additive and that ρ is a ring homomorphism, and identify which module axiom gives each property.

    (c) Conversely, given a ring homomorphism $\rho : R \to \mathrm{End}_{\mathbb{Z}}(M)$, set $rm := \rho(r)(m)$ and verify the module axioms. Show that this construction inverts the one in part (b). Describe $\rho(x)$ for a $\mathbb{K}[x]$-module V_T.

    (d) Prove that M is a left $\mathrm{End}_R(M)$-module by evaluation, $f \cdot m = f(m)$, using the convention $fg = f \circ g$. Show also that the condition $f(rm) = rf(m)$ says that these operators commute with the original scalar operators.

    (e) For the column module $M = \mathbb{K}^2$ over $R = \mathrm{Mat}_2(\mathbb{K})$, show that ρ is injective. Show also that $\rho(A)$ need not be R-linear, by taking $A = E_{12}$ and $B = E_{21}$ and comparing $A(Be_1)$ with $B(Ae_1)$; here E_{ij} denotes the matrix units of Worksheet 1.1.

    (f) Determine $\mathrm{End}_{\mathrm{Mat}_2(\mathbb{K})}(\mathbb{K}^2)$. First use the scalar matrices to show that every module endomorphism is $\mathbb{K}$-linear, and then require its matrix to commute with E_{11}, E_{12}, and E_{21}. Compare the answer with the endomorphism ring you computed in Problem 5, and say what each computation tells you about the module.
