Modules over a PID

1. Show that $\mathbb{Z}/n$ (for any n) is a principal ideal ring.

2. Show that $\mathbb{Z}/n$ is a domain only if n is a prime.

3. Given an abelian group M and a ring R and a ring homomorphism $\phi : R \to \mathrm{End}(M)$.

   Given an element a in R and an element m in M, we use the notation $a \cdot m$ for the result $\phi(a)(m)$ of applying the image of a to the element m.

   (a) Use the fact that $\phi(a)$ is an endomorphism of M to show that if m' is another element of M, then $a \cdot (m + m') = a \cdot m + a \cdot m'$.

   (b) Use the fact that ϕ preserves addition and the rule of addition of endomorphisms to show that $(a + b) \cdot m = a \cdot m + b \cdot m$ when b is another element of R.

   (c) Use the rule of composition of endomorphisms and the fact that ϕ preserves multiplication to show that $a \cdot (b \cdot m) = (a \cdot b) \cdot m$.

   (d) Use the fact that ϕ preserves multiplicative identity to show that $1 \cdot m = m$.

   (e) Use the fact that ϕ preserves additive identity to show that $0 \cdot m = 0$ where the latter 0 is the additive identity in M.

4. Given an operation $a \cdot m$ of elements a of a ring R on elements m of an abelian group M satisfying the identities.

   - $a \cdot (m + m') = a \cdot m + a \cdot m'$
   - $(a + b) \cdot m = a \cdot m + b \cdot m$
   - $a \cdot (b \cdot m) = (a \cdot b) \cdot m$
   - $1 \cdot m = m$ and $0 \cdot m = 0$

   Check that $\phi(a)(m) = a \cdot m$ defines a ring homomorphism $R \to \mathrm{End}(M)$.

5. Show that $I \subset R$ is a submodule of R (as a module over R) if and only if I is an ideal of R.

6. Define an operation of a ring R on the abelian group R^n by $a \cdot (a_1, \ldots, a_n) = (a \cdot a_1, \ldots, a \cdot a_n)$. Check that this operation makes R^n into a module over R.

7. Use the natural multiplication by integers to make $\mathbb{Z}/n$ a module over $\mathbb{Z}$. Check that this is not a free module unless $n = 0$!

8. Given a ring homomorphism $f : R \to S$, this makes S a module over R by defining $a \cdot b$ as $f(a) \cdot b$ for a in R and b in S.

9. Show that the endomorphisms $\mathrm{End}(\mathbb{Q})$ of the *abelian group* of rational numbers is (as a ring) isomorphic to $\mathbb{Q}$. (Hint: Identify an endomorphism by what it does to the element 1.)

10. Show that any finitely generated subgroup of the additive group of rational numbers is of the form $\mathbb{Z} \cdot (p/q)$ (i. e. the collection of all multiples of p/q) for some rational number p/q.

11. (Five Stars!) Show that there is a proper subgroup of the rational numbers which is *not* of the form $\mathbb{Z} \cdot (p/q)$ for some rational number p/q.

12. If $f : N \to M$ is a module homomorphism, check that its image is a submodule.

13. For a module homomorphism $f : N \to M$, let $K = \{n | f(n) = 0\}$ denote the kernel in the sense of (abelian) groups. Show that it is a submodule of N.

14. If $f : N \to M$ is a homomorphism which is both 1-1 and onto then check that its inverse $g : M \to N$ is a homomorphism.

15. Check that when R is a field, then N and M are vector spaces over R and a module homomorphism $N \to M$ is the same as a linear transformation of vector spaces.

16. Given any element m in M, show that $s \mapsto s \cdot m$ defines a module homomorphism $R \to M$ where R is considered as a module over itself in a natural way.

17. Given a collection $\{m_1, \ldots, m_n\}$ of elements of M, we can define a map $R^n \to M$ by

$$(a_1, \ldots, a_n) \mapsto a_1 \cdot m_1 + \cdots + a_n \cdot m_n$$

    Check that this defines a module homomorphism.

18. Given a abelian group M and a subgroup N, we can form the abelian group M/N whose elements consist of equivalence classes under the equivalence relation $m \simeq m'$ if $m - m'$ lies in N.

    For m, m', n, n' in M, check that if $m \simeq m'$ and $n \simeq n'$, then $m + n \simeq m' + n'$.

19. Given a homomorphism $f : N \to M$, check that if $n \simeq n'$ in $N/\ker(f)$, then $f(n) = f(n')$.

20. Check that the homomorphism $f : N/\ker(f) \to M$ is one-to-one.

21. Let I be an ideal in a principal ideal domain R, then as a module over R it is free. (Hint: If $I = a \cdot R$, then show that the module homomorphism $R \to I$ given by $s \mapsto a \cdot s$ is one-to-one and onto.)