Solutions to Assignment 7

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

Solution: An ideal in $\mathbb{Z}/n$ is of the forme I/n where I is an ideal in $\mathbb{Z}$ such that $I \supset n \cdot \mathbb{Z}$. Since such an ideal is of the form $I = a \cdot \mathbb{Z}$ where a divides n. Thus I/n is generated by a.

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

Solution: If $n = a \cdot b$ where a and b are positive integers, then $a \cdot b = 0$ in $\mathbb{Z}/n$. Moreover, a and b are less than n, so we have zero-divisors in $\mathbb{Z}/n$. Conversely, if $a \cdot b = 0$ in $\mathbb{Z}/n$, then we have an expression $a \cdot b = n \cdot k$ for a multiple of n. Then n cannot be 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 $a \cdot (m + m') = a \cdot m + a \cdot m'$.

   Solution: We have

$$a \cdot (m + m') = \phi(a)(m + m') = \phi(a)(m) + \phi(a)(m') = a \cdot m + a \cdot m'$$

   (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.

   Solution: We have

$$(a + b) \cdot m = \phi(a + b)(m) = (\phi(a) + \phi(b))(m)(\phi(a)(m) + \phi(b)(m))$$

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

   Solution: We have

$$(a \cdot b) \cdot m = \phi(a \cdot b)(m) = (\phi(a) \circ \phi(b))(m)\phi(a)(\phi(b)(m)) = a \cdot (b \cdot m)$$

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

> **Solution:** We have
>
> $$1 \cdot m = (\phi(1))(m) = (1_M)(m) = m$$
>
> Where $1_M : M \to M$ denotes the identity map.

(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.

> **Solution:** We have
>
> $$0 \cdot m = (\phi(0))(m) = (0_M)(m) = 0$$
>
> Where $0_M : M \to M$ denotes the map which sends everythin to 0.

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 $R \to \mathrm{End}(M)$.

> **Solution:** The first identity shows that $\phi(a) : M \to M$ is a group homomorphism, thus we get a *map* $\phi : R \to \mathrm{End}(M)$.
>
> The second identity shows that $\phi : R \to \mathrm{End}(M)$ preserves addition. The third identity shows that $\phi : R \to \mathrm{End}(M)$ preserves multiplication. The fourth and fifth identities show that $\phi : R \to \mathrm{End}(M)$ preserves multiplicative and additive identities.

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.

> **Solution:** To be a submodule, I must be a subgroup, which means it is closed under addition. In addition, we must have $\phi(a)(I) \subset I$ which is the same as saying $a \cdot I \subset I$. Note that $(-1) \cdot b = -b$ and so the additive inverse of an element b in I automatically lies in an ideal I.

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.

Solution: We check that

$$
\begin{aligned}
a \cdot ((a_1, \ldots, a_n) + (b_1, \ldots, b_n)) = a \cdot (a_1 + b_1, \ldots, a_n + b_n) = \\
(a \cdot (a_1 + b_1), \ldots, a \cdot (a_n + b_n)) = \\
(a \cdot a_1 + a \cdot b_1, \ldots, a \cdot a_n + a \cdot b_n) = \\
(a \cdot a_1, \ldots, a \cdot a_n) + (a \cdot b_1, \ldots, a \cdot b_n) = \\
a \cdot (a_1, \ldots, a_n) + a \cdot (b_1, \ldots, b_n)
\end{aligned}
$$

Other identities above can be checked in a similar way.

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 $n = 0$!

Solution: Given any element a in $\mathbb{Z}/n$ the map $k \mapsto k \cdot a$ from $\mathbb{Z} \to \mathbb{Z}/n$ contains $n\mathbb{Z}$. So the map is not one-to-one 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.

Solution: We have already seen that $\phi : S \to \mathrm{End}(S)$ given by $\phi(s)(t) = s \cdot t$ is a ring homomorphism. Now combined with the ring homomorphism $R \to S$, this gives a ring homomorphism $R \to \mathrm{End}(S)$ as required.

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.)

Solution: Given an endomorphism $\mathbb{Q} \to \mathbb{Q}$, assume that it sends 1 to t. It is clear that it sends $2 = 1 + 1$ to $t + t = 2t$. Similarly, it sends a positive integer n to nt. Now, we can write $1 = 1/2 + 1/2$ so if $1/2$ goes to s then $t = s + s = 2s$. This means that $s = t/2$. Similarly it follows that $1/m$ goes to t/m. It then follows that n/m goes to $(n/m)t$. Thus any endomorphism is of the for $n/m \mapsto (n/m)t$ for a fixed rational number t.

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.

Solution: Since the subgroup is finitely generated, it is generated by finitely many fractions p_i/q_i. If we take q to be the product of the q_i's, it follows that this group is contained in the subgroup $(1/q) \cdot \mathbb{Z}$. Under the isomorphism $\mathbb{Z} \to (1/q) \cdot \mathbb{Z}$ (given by $n \mapsto n/q$), this corresponds to a subgroup of $\mathbb{Z}$ on the left-hand side. We have already seen that such a subgroup has the form $p \cdot \mathbb{Z}$. Hence, the given subgroup is of the form $(p/q) \cdot \mathbb{Z}$.

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.

Solution: Consider the subgroup of $\mathbb{Q}$ which consists of fractions of the form $p/2^k$ for all integers p and k. We see this is not a subgroup of the previous form and is not finitely generated.

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

Solution: Since $f(n+n') = f(n)+f(n')$ we see that the image is a subgroup. Since $f(a \cdot n) = a \cdot f(n)$ we see that the image is closed uder multiplication by elements of R.

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.

Solution: The kernel of a group homomorphism is a subgroup. We also have $f(a \cdot n) = a \cdot f(n)$. So, if $f(n) = 0$, then $f(a \cdot n) = 0$.

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.

Solution: The inverse is a group homomorphism. We only need to check that $g(a \cdot m) = a \cdot g(m)$. Now, if $n = g(m)$, then $m = f(n)$. So substituting this the identity becomes $g(a \cdot m) = a \cdot n$. Applying f to both sides we have $a \cdot m = f(a \cdot n) = a \cdot f(n)$. In that case, we see that the identity holds after applying f. Since f is one-to-one, the identity already holds before applying f!

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.

> **Solution:** The above identites for a module structure and module homomorphism are the same as those for a vector space and linear transformation.

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.

> **Solution:** We note that $(s+t) \mapsto (s+t) \cdot m = s \cdot m + t \cdot m$. This shows that this is a group homomorphism. Secondly $s \cdot (t \cdot m) = (s \cdot t) \cdot m$ so it preserves mutliplication.

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.

> **Solution:** This is just an extension of the argument given above done with n elements.

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 $m + n \simeq m' + n'$.

> **Solution:** We note that $(m+m') - (n+n') = (m-n) + (m'-n')$. Since the element $m - n$ and $m' - n'$ lie in N so does their sum.

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

> **Solution:** If $n - n'$ lies in $\ker(f)$, then $f(n - n') = 0$, so $f(n) = f(n')$.

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

Solution: This is a standard statement in the theory of group homomorphisms. It does not need any aspect of module theory for this!

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.)

Solution: Since R is a domain, the map $R \to R$ given by mutliplication by a is 1-1. Its image is precisely I, hence $R \to a \cdot R$ is an isomorphism.