

# MATH 7752 Homework 1

James Harbour

January 25, 2022

## Problem 1

Let  $R$  be a ring and  $M$  an  $R$ -module.

(a) Prove that for every  $m \in M$ , the map  $r \mapsto rm$  from  $R$  to  $M$  is a homomorphism of  $R$ -modules.

*Proof.* Fix  $m \in M$  and let  $\varphi$  denote the map  $r \mapsto rm$ . Fix  $x, y \in R$  and  $r \in R$ . Observe that

$$\varphi(x + y) = (x + y)m = xm + ym = \varphi(x) + \varphi(y)$$

and

$$\varphi(rx) = (rx)m = r(xm) = r\varphi(x),$$

so  $\varphi$  is an  $R$ -module homomorphism. □

(b) Assume that  $R$  is commutative and  $M$  an  $R$ -module. Prove that there is an isomorphism  $\text{Hom}_R(R, M) \simeq M$  as  $R$ -modules.

*Proof.* For  $m \in M$ , let  $\varphi_m$  denote the  $R$ -module homomorphism in part (a).

Consider the map  $\psi : M \rightarrow \text{Hom}_R(R, M)$  given by  $\psi(m) = \varphi_m$ . For  $m, n \in M$  and  $r, x \in R$ ,

$$\psi(m + n)(x) = \varphi_{m+n}(x) = x(m + n) = xm + xn = \varphi_m(x) + \varphi_n(x) = (\psi(m) + \psi(n))(x)$$

so  $\psi(m + n) = \psi(m) + \psi(n)$ , and

$$\psi(rm)(x) = \varphi_{rm}(x) = x(rm) = r(xm) = r\varphi_m(x) = (r\psi(m))(x)$$

so  $\psi(rm) = r\psi(m)$ .

Suppose  $\psi(m) = \psi(n)$ . Then  $m = \varphi_m(1) = \psi(m)(1) = \psi(n)(1) = \varphi_n(1) = n$ , so  $\psi$  is injective.

Suppose  $\varphi \in \text{Hom}_R(R, M)$ . For  $r \in R$ ,

$$\psi_{\varphi(1)}(r) = r\varphi(1) = \varphi(r),$$

so  $\psi_{\varphi(1)} = \varphi$ , i.e.  $\psi$  is surjective. □

## Problem 2

Give an explicit example of a map  $f : A \rightarrow B$  with the following properties:

- $A, B$  are  $R$ -modules.
- $f$  is a group homomorphism.
- $f$  is not an  $R$ -module homomorphism.

*Solution.* Consider  $A = B = \mathbb{C}$  viewed as  $\mathbb{C}$ -modules over themselves. Let  $f : A \rightarrow B$  be complex conjugation. For  $z, w \in A$ ,  $f(z + w) = \overline{z + w} = \bar{z} + \bar{w} = f(z) + f(w)$ , so  $f$  is a group homomorphism. However, for  $z \in A \setminus \{0\}$ ,  $f(iz) = -i\bar{z} \neq i\bar{z} = if(z)$ , so  $f$  is not an  $R$ -module homomorphism.  $\square$

## Problem 3

Let  $R$  be a ring and  $M$  an  $R$ -module.

(a) Let  $N$  be a subset of  $M$ . The *annihilator* of  $N$  is defined to be the set

$$\text{Ann}_R(N) := \{r \in R : rn = 0, \text{ for all } n \in N\}.$$

Prove that  $\text{Ann}_R(N)$  is a left ideal of  $R$ .

*Proof.* Let  $x, y \in I$  and  $r \in R$ . Fix  $n \in N$ . Noting that  $xn = 0 = yn$ , it follows that

$$(x + ry)n = xn + (ry)n = xn + r(yn) = 0.$$

Thus  $x + ry \in \text{Ann}_R(N)$ . Since all elements chosen were arbitrary,  $\text{Ann}_R(N)$  is a left ideal of  $R$ .  $\square$

(b) Show that if  $N$  is an  $R$ -submodule of  $M$ , then  $\text{Ann}_R(N)$  is an ideal of  $R$  (i.e. it is two-sided ideal).

*Proof.* By part (a), it suffices to show that  $\text{Ann}_R(N)$  is a right ideal of  $R$ . Moreover, part (a) shows *a fortiori* that  $\text{Ann}_R(N)$  is already an abelian group, so we need only address its multiplicative structure. Let  $y \in \text{Ann}_R(N)$  and  $r \in R$ . Fix  $n \in N$ . As  $N$  is an  $R$ -submodule of  $M$ ,  $yn \in N$ , whence  $(yr)n = y(rn) = 0$  by definition. Hence  $\text{Ann}_R(N)$  is a two-sided ideal of  $R$ .  $\square$

(c) For a subset  $I$  of  $R$  the *annihilator* of  $I$  in  $M$  is defined to be the set,

$$\text{Ann}_M(I) := \{m \in M : xm = 0, \text{ for all } x \in I\}.$$

Find a natural condition on  $I$  that guarantees that  $\text{Ann}_M(I)$  is a submodule of  $M$ .

**Claim.**  $\text{Ann}_M(I)$  is an  $R$ -submodule of  $M$  if  $I$  is a right ideal of  $R$ .

*Proof.* Suppose  $I$  is a right ideal of  $R$ . As  $x \cdot 0 = 0$  for all  $x \in I$ ,  $\text{Ann}_M(I) \neq \emptyset$ . Suppose  $m, n \in \text{Ann}_M(I)$  and  $r \in R$ . Fix  $x \in I$ . By definition  $x \cdot m = 0$ . As  $I$  is a right ideal,  $xr \in I$ , so  $x \cdot (m + r \cdot n) = x \cdot m + (xr) \cdot n = 0$ . Thus  $\text{Ann}_M(I)$  is an  $R$ -submodule of  $M$ .  $\square$

(d) Let  $R$  be an integral domain. Prove that every finitely generated torsion  $R$ -module has a nonzero annihilator.

*Proof.* Let  $M$  be a finitely generated torsion  $R$ -module. Taking a generating set  $m_1, \dots, m_n \in M$  of  $M$ , for each  $k \in \{1, \dots, n\}$  there exists an  $x_k \in R^\times = R \setminus \{0\}$  such that  $x_k m_k = 0$ . As  $R^\times$  is closed under multiplication,  $r := x_1 \cdots x_n \in R^\times$  whence  $r \neq 0$ .

Now suppose that  $m \in M$ . Then there exist  $r_1, \dots, r_n \in R$  such that  $m = r_1 m_1 + \cdots + r_n m_n$ . Observe that, by the commutativity of  $R$ ,

$$rm = (x_1 \cdots x_n)(r_1 m_1 + \cdots + r_n m_n) = \sum_{k=1}^n \left( \prod_{i \neq k} x_i \right) (x_k m_k) = 0.$$

Thus  $0 \neq r \in \text{Ann}_R(M)$ , so  $M$  has nonzero annihilator. □

## Problem 4

In class we obtained a simple characterization of  $R$ -modules when  $R = \mathbb{Z}$ , and  $R = F[x]$ , with  $F$  a field. Imitate the method to find similar characterizations for  $R$ -modules in the following cases:

(a)  $R = \mathbb{Z}/n\mathbb{Z}$ , for some  $n \geq 2$ .

*Proof.* □

(b)  $R = \mathbb{Z}[x]$ .

(c)  $R = F[x, y]$ .

## Problem 5

An  $R$ -module  $M$  is called *simple* (or *irreducible*) if its only submodules are  $\{0\}$  and  $M$ . An  $R$ -module  $M$  is called *indecomposable* if  $M$  is not isomorphic to  $N \oplus Q$  for some non-zero submodules  $N, Q$ . Show that every simple  $R$ -module is indecomposable, but the converse is not true.

*Proof.* Let  $M$  be a simple  $R$ -module. Then  $M \neq 0$  as otherwise there would only be one submodule. Suppose, for the sake of contradiction, that  $M$  is not indecomposable. Then there exist some nonzero submodules  $N, Q \subseteq M$  such that  $M \cong N \oplus Q$ . By simplicity of  $M$ , it follows that  $N, Q = M$ . But then  $M \cong M \oplus M$ . Moreover,  $0 \oplus M$  is then a nonzero proper submodule of  $M \oplus M$ , whence via the isomorphism  $M \oplus M \cong M$  we obtain a nonzero proper submodule of  $M$ , contradicting the simplicity of  $M$ .

To see that the converse does not hold, consider  $R = \mathbb{Z}$  and  $M = \mathbb{Z}$  considered as a  $\mathbb{Z}$ -module over itself. Note that  $2\mathbb{Z} \subseteq \mathbb{Z}$  is a nonzero proper submodule of  $\mathbb{Z}$ , so  $M$  is not simple. To see that  $M$  is indecomposable, note that all nonzero submodules of  $M$  are of the form  $a\mathbb{Z}$  for some  $a \in \mathbb{Z} \setminus \{0\}$ , and for any  $a, b \in \mathbb{Z} \setminus \{0\}$ ,  $ab \in a\mathbb{Z} \cap b\mathbb{Z}$ . Hence, no sum of the required form would be direct. □

## Problem 6

Let  $R$  be a ring. An  $R$ -module  $M$  is called *cyclic* if it is generated as an  $R$ -module by a single element.

(a) Prove that every cyclic  $R$ -module is of the form  $R/I$  for some left ideal  $I$  of  $R$ .

*Proof.* Let  $M$  be a cyclic  $R$ -module. Then there exists an  $m \in M$  such that  $M = Rm$ . Consider the map  $\varphi : R \rightarrow M$  given by  $\varphi(r) = rm$  for  $r \in R$ . By problem 1 part (a),  $\varphi$  is an  $R$ -module homomorphism; moreover,  $\varphi$  is surjective since  $m$  generates  $M$ . Let  $I = \ker(\varphi)$ , a left ideal of  $R$  (actually two-sided, but we are identifying  $R$  with its left regular module over itself so a priori  $I$  is just a left  $R$ -submodule). Then, by the first isomorphism theorem,  $M = \varphi(R) \cong R/\ker(\varphi) = R/I$ .  $\square$

(b) Show that the simple  $R$ -modules are precisely the ones which are isomorphic to  $R/\mathfrak{m}$  for some maximal left ideal  $\mathfrak{m}$ .

*Proof.* On one hand,  $\mathfrak{m}$  be a maximal left ideal of  $R$ . By the correspondence theorem applied to the natural projection, the only  $R$ -submodules of  $R/\mathfrak{m}$  are  $\{0\}$  and  $R/\mathfrak{m}$ , so  $R/\mathfrak{m}$  is simple (and so is every  $R$ -module isomorphic to it).

On the other hand, suppose  $M$  is a nonzero simple  $R$ -module. Take  $m \in M \setminus \{0\}$ . Then by the simplicity of  $M$ ,  $Rm = M$  i.e.  $M$  is a cyclic module generated by  $m$ . Part (a) implies that there is some left ideal  $\mathfrak{m}$  of  $R$  such that  $M \cong R/\mathfrak{m}$ . Suppose that  $I$  is a proper left ideal of  $R$  such that  $\mathfrak{m} \subseteq I \subsetneq R$ . Applying the natural projection, we see that  $0 \subseteq I/\mathfrak{m} \subsetneq R/\mathfrak{m}$ , whence simplicity of  $R/\mathfrak{m}$  implies that  $I/\mathfrak{m}$  is trivial i.e.  $I = \mathfrak{m}$ . Thus by definition  $\mathfrak{m}$  is a maximal left ideal.  $\square$

(c) Show that any non-zero homomorphism of simple  $R$ -modules is an isomorphism. Deduce that if  $M$  is simple, its endomorphism ring  $\text{End}_R(M) := \text{Hom}_R(M, M)$  is a division ring. This result is known as *Schur's Lemma*.

*Proof.* Suppose that  $M, N$  are simple  $R$ -modules and let  $f : M \rightarrow N$  be a nonzero  $R$ -module homomorphism. As  $f(M) \neq 0$  is a submodule of  $N$ , by simplicity  $f(M) = N$  i.e.  $f$  is surjective. As  $f$  is nonzero,  $\ker(f)$  is a nonzero submodule of  $M$  whence  $\ker(f) = 0$  i.e.  $f$  is injective. Hence  $f$  is an isomorphism.

Suppose  $M$  is simple and  $f \in \text{End}_R(M) \setminus \{0\}$ . Then  $f$  is an isomorphism, so the set-theoretic inverse  $f^{-1}$  is in fact an  $R$ -module isomorphism and  $f^{-1} \in \text{End}_R(M)$ . Hence  $\text{End}_R(M)$  is a division ring.  $\square$

## Problem 7

Show that  $\mathbb{Q}$  is not a free  $\mathbb{Z}$ -module, that is  $\mathbb{Q}$  is not isomorphic to a direct sum of the form  $\bigoplus_I \mathbb{Z}$ , for any index set  $I$ . More generally, let  $R$  be a PID which is not a field and  $K = \text{frac}(R)$  be its fraction field. Show that  $K$  is not a free  $R$ -module.

*Proof.*  $\square$

## Problem 8

Let  $R$  be a commutative ring. Recall that an ideal  $I$  of  $R$  is called *nilpotent* if there exists some  $n \in \mathbb{N}$  such that  $I^n = 0$ .

(a) Let  $i \in I$ . Show that the element  $r = 1 - i$  is invertible in  $R$ .

*Proof.* As  $I$  is a nilpotent ideal, there exists an  $n \in \mathbb{N}$  such that  $I^n = 0$ . Then  $i^n = 0$ , so

$$1 = 1 - i^n = (1 - i)(1 + i + \cdots + i^{n-1}),$$

whence  $1 - i \in R^\times$ .  $\square$

**(b)** Let  $M, N$  be  $R$ -modules and let  $\varphi : M \rightarrow N$  be an  $R$ -module homomorphism. Show that  $\varphi$  induces an  $R$ -module homomorphism,  $\bar{\varphi} : M/IM \rightarrow N/IN$ .

*Proof.* Let  $\pi_M : M \rightarrow M/IM$  and  $\pi_N : N \rightarrow N/IN$  be the natural projections. Define a map  $\bar{\varphi} : M/IM \rightarrow N/IN$  by  $\bar{\varphi}(m + IM) := \varphi(m) + IN = (\pi_N \circ \varphi)(m)$ . To see that this map is well defined, suppose that  $m + IM = m' + IM$ . Then there exist  $i_1, \dots, i_s \in I$  and  $m_1, \dots, m_s \in M$  such that  $m - m' = i_1 m_1 + \dots + i_s m_s$ . So

$$\varphi(m - m') = \varphi(i_1 m_1 + \dots + i_s m_s) = i_1 \varphi(m_1) + \dots + i_s \varphi(m_s) \in IN,$$

whence  $\pi_N(\varphi(m)) - \pi_N(\varphi(m')) = \pi_N(\varphi(m - m')) = 0$ , so  $\pi_N(\varphi(m)) = \pi_N(\varphi(m'))$ . □

**(c)** Prove that if  $\bar{\varphi}$  is surjective, then  $\varphi$  is itself surjective.

*Proof.* Suppose that  $\bar{\varphi}$  is surjective. Then  $N/IN = \bar{\varphi}(M/IM) = (\bar{\varphi} \circ \pi_M)(M) = (\pi_N \circ \varphi)(M) = \varphi(M)/IN$ . Take  $n \in N$ . Then there exists an  $m \in M$  such that  $n + IN = \bar{\varphi}(m + IM) = \varphi(m) + IN$ , whence  $n - \varphi(m) \in IN$ . It follows that  $n = \varphi(m) + (n - \varphi(m)) \in \varphi(M) + IN$ , whence  $N = \varphi(M) + IN$ . As  $I$  is a nilpotent ideal, there exists a  $k \in \mathbb{N}$  such that  $I^k = 0$ . Observe that

$$N = \varphi(M) + IN = \varphi(M) + I(\varphi(M) + IN) = \varphi(M) + I^2 N = \dots = \varphi(M) + I^k N = \varphi(M),$$

so  $\varphi$  is surjective. □

## Problem 9

Let  $G$  be a finite group and  $k$  a field. Consider the group ring  $k[G]$ .

**(a)** Let  $M$  be a  $k$ -vector space with a  $G$ -action. Show that  $M$  becomes a  $k[G]$ -module. Conversely, if  $M$  is a  $k[G]$ -module, show that  $M$  is a  $G$ -set.

**(b)** Let  $M, N$  be two  $k[G]$ -modules. Show that  $\text{Hom}_k(M, N)$  becomes a  $k[G]$ -module with the following  $G$ -action: For  $g \in G$  and  $\varphi : M \rightarrow N$  a  $k[G]$ -homomorphism define

$$(g \cdot \varphi)(m) := g\varphi(g^{-1}m), \text{ for } m \in M.$$