Problem Set 1 solutions

Problem 1. Let M be an R-module and I be an ideal in R. Show that the set

$$N = \{m \in M \mid am = 0 \text{ for all } a \in I\}$$

is an R-submodule of M.

Proof. We will use the one-step test for submodules. To do that, we need to check that for any $r \in R$ and any $m, n \in N$, we have $rm + n \in N$. And indeed, if $r \in R$ and $m, n \in N$, and given any $a \in I$, we have:

- $an \in N$ by definition of N, since $n \in N$ and $a \in I$;
- $ar \in I$, since I is an ideal and $r \in R$;
- By the axioms for modules, we have $a(rm) = (ar)m$, and since $ar \in I$ and $m \in N$, we conclude that $a(rm) = (ar)m = 0$.

Finally, putting this together with the axioms for modules we get

$$a(rm + n) = a(rm) + an = 0 + 0 = 0,$$

so $rm + n \in N$. By the One-step Test for submodules, we conclude that N is a submodule of M. □

Problem 2. Show that the left R-module M is cyclic if and only if there exists a left ideal I of R such that $M \cong R/I$.

Proof. ($\Longrightarrow$) Suppose that M is a cyclic module, and let $m \in M$ be such that $M = Rm$. Consider the function

$$\begin{aligned} R &\xrightarrow{f} M \\ r &\longmapsto rm \end{aligned}$$

Note that f is surjective by our assumption that $M = Rm$. Moreover, f is a homomorphism of R-modules, since

$$\begin{aligned} f(r+s) &= (r+s)m && \text{by definition of } f \\ &= rm + sm && \text{by the module axioms} \\ &= f(r) + f(s) && \text{by definition of } f \end{aligned}$$

and

$$\begin{aligned} f(rs) &= (rs)m && \text{by definition of } f \\ &= r(sm) && \text{by the module axioms} \\ &= rf(m) && \text{by definition of } f. \end{aligned}$$

Finally, the kernel of f is a submodule of R; the submodules of R are the left ideals, so $I = \ker(f)$ is a left ideal of R. By the First Isomorphism Theorem, $M \cong R/\ker(f) = R/I$.

($\Longleftarrow$) Suppose that $M \cong R/I$, and let $f : R/I \to M$ be an isomorphism of R-modules. Let $m = f(1 + I)$. On the one hand, Rm is a submodule of. M; on the other hand, given any $n \in M$, since f is surjective there exists some $r + I \in R/I$ such that $f(r + I) = n$. Since f is a map of R-modules, we have

$$rm = rf(1 + I) = f(r(1 + I)) = f(r + I) = n.$$

Therefore, $n \in Rm$, and thus $M = Rm$. □

Problem 3. Let R be a commutative ring. Let M be an R-module, I an ideal in R, and let

$$N = \{m \in M \mid am = 0 \text{ for all } a \in I\},$$

which is an R-submodule of M by Problem 1. Show that

$$\mathrm{Hom}_R(R/I, M) \cong N.$$

Before we write a formal proof, let's understand why this is true. We saw in class that to give a homomorphism of R-modules $R \to M$ is to choose an element $m \in M$, the image of 1. To give a homomorphism of R-modules from $R/I \to M$ is the same as giving an R-module homomorphism $R \to M$ that sends I to zero, so every element in I must kill the image of 1. So giving an R-module homomorphism $R/I \to M$ is the same as choosing an element $m \in M$ that is killed by I.

Another equivalent way to say this is that once we determine the image of $1 + I$, any R-module homomorphism $f\colon R/I \to M$ is completely determined, since

$$f(r + I) = f(r(1 + I)) = rf(1 + I).$$

But for f to be well-defined, $m := f(1 + I)$ cannot be any element: since $f(0 + I) = 0$, for any $a \in I$ we must have

$$am = af(1 + I) = f(a + I) = f(0 + I) = 0,$$

so $m \in N$.

Proof 1. Consider the map

$$\begin{aligned} \mathrm{Hom}_R(R/I, M) &\xrightarrow{\Psi} N \\ f &\longmapsto f(1 + I). \end{aligned}$$

We claim that this is a well-defined isomorphism of R-modules.

- Given any $f \in \mathrm{Hom}_R(R/I, M)$, we need to check that $\Psi(f) \in N$. Consider $a \in I$ and $f \in \mathrm{Hom}_R(R/I, M)$. Then $a + I = 0 + I$, and since f is a homomorphism of R-modules, we have

  $$a\Psi(f) = af(1 + I) = f(a + I) = f(0 + I) = 0.$$

  Thus $\Psi(f) \in N$.

- We claim that Ψ is an R-module homomorphism. Given $f, g \in \mathrm{Hom}_R(R/I, M)$, we have

  $$\begin{aligned} \Psi(f + g) &= (f + g)(1 + I) \\ &= f(1 + I) + g(1 + I) \quad \text{by definition of } f + g \\ &= \Psi(f) + \Psi(g). \end{aligned}$$

  Moreover, for any $r \in R$ we have

  $$\begin{aligned} \Psi(rf) &= (rf)(1 + I) \\ &= f(r(1 + I)) && \text{by definition of } rf \\ &= rf(1 + I) && \text{since } f \text{ is a homomorphism of } R\text{-modules} \\ &= r\Psi(f). \end{aligned}$$

- We claim that Ψ is injective. Indeed, given $f, g \in \operatorname{Hom}_R(R/I, M)$,

  $$\Psi(f) = \Psi(g) \implies f(1+I) = g(1+I),$$

  but the image of $1+I$ completely determines the homomorphism, so this implies that $f = g$.

- We claim that Ψ is surjective. Given $n \in N$, consider the function

  $$\begin{aligned} R/I &\xrightarrow{f} M \\ r &\longmapsto rn. \end{aligned}$$

  Given any $r + I = s + I$ in R/I, we have $r - s \in I$. Since $n \in N$, we conclude that

  $$(r-s)n = 0 \implies rn = sn.$$

  Thus $f(r+I) = f(s+I)$, and f is a well-defined function. Moreover, for any $r+I, s+I \in R/I$ and any $t \in R$, we have

  $$f((r+I)+(s+I)) = f((r+s)+I) = (r+s)n = rn + sn = f(r+I) + f(s+I),$$

  and

  $$f(t(r+I)) = f(tr+I) = (tr)n = t(rn) = tf(n).$$

  Therefore, f is a homomorphism of R-modules. By construction, we see that

  $$\Psi(f) = f(1+I) = 1n = n.$$

  We conclude that Ψ is indeed surjective

We have shown that Ψ is an isomorphism of R-modules. □

Proof 2. Consider the map

$$\begin{aligned} N &\xrightarrow{\Psi} \operatorname{Hom}_R(R/I, M) \\ n &\longmapsto (r + I \mapsto rn). \end{aligned}$$

We claim that this is a well-defined isomorphism of R-modules.

- For any $n \in N$, we claim that the function $f_n : R/I \to N$ given by $f_n(r+I) = rn$ is a well-defined function. Given $r, s \in R$ such that $r + I = s + I$, we have $r - s \in I$, so by definition of N we know that $(r-s)n = 0$. Thus $rn = sn$, and therefore $f_n(r+I) = f_n(s+I)$.

- For any $n \in N$, we claim that the function $f_n : R/I \to N$ given by $f_n(r+I) = rn$ is a homomorphism of R-modules. Indeed: for any $r, s \in R$, we have

  $$f_n((r+I)+(s+I)) = f_n((r+s)+I) = (r+s)n = rn + sn = f_n(r+I) + f_n(s+I)$$

  and

  $$f_n(r(s+I)) = f_n(rs+I) = (rs)n = r(sn) = rf_n(r+I).$$

The two points above together say that Ψ is a well-defined function.

- Ψ is a homomorphism of abelian groups, since for any $a, b \in N$ and any $r \in R$, we have

  $$\Psi(a+b)(r+I) = f_{a+b}(r+I) = r(a+b) = ra+rb = f_a(r+I)+f_b(r+I) = \Psi(a)(r+I)+\Psi(b)(r+I).$$

  Therefore, $\Psi(a+b) = \Psi(a) + \Psi(b)$.

- Ψ is an R-linear map, since for all $r, s \in R$ and $a \in N$, we have

  $$\begin{aligned} \Psi(ra)(s+I) &= f_{ra}(s+I) && \text{by definition} \\ &= s(ra) && \text{by definition} \\ &= (sr)a && \text{since } N \text{ is an } R\text{-module} \\ &= (rs)a && \text{since } R \text{ is commutative} \\ &= f_a(rs+I) && \text{by definition} \\ &= rf_a(s+I) && \text{since } f_a \text{ is an } R\text{-module homomorphism} \\ &= r\Psi(a)(s+I) && \text{by definition.} \end{aligned}$$

- Ψ is surjective: given $f \in \mathrm{Hom}_R(R/I, M)$ and any $a \in I$ we have

  $$\begin{aligned} af(1+I) &= f(a(1+I)) && \text{since } f \text{ is an } R\text{-module map} \\ &= f(a+I) \\ &= f(0+I) && \text{since } a \in I \\ &= 0_M && \text{since } f \text{ is in particular a homomorphism of abelian groups.} \end{aligned}$$

  Thus $n := f(1+I) \in N$. Since f is R-linear, we have

  $$f(r+I) = rf(1+I) = rn = f_n(r) = \Phi(n)(r) \implies f = \Psi(n).$$

- Ψ is injective: given $a, b \in N$, if $\Psi(a) = \Psi(b)$ then in particular

  $$a = f_a(1+I) = \Psi(a)(1+I) = \Psi(b)(1+I) = f_b(1+I) = b.$$

$\square$