Problem Set 2 solutions

Problem 1. Given a homomorphism of R-modules $f\colon M \to N$, show that $\ker(f)$ is an R-submodule of M.

Solution. It is sufficient to show that the One-Step Test for submodules applies. Given $r \in R$ and $a, b \in \ker(f)$, we need to show that $ra + b \in \ker(f)$. Since $a, b \in \ker(f)$, we have $f(a) = f(b) = 0$. Moreover, since f is a homomorphism of R-modules, we have

$$f(ra + b) = rf(a) + b = r0 + 0 = 0.$$

Therefore, $ra + b \in \ker(f)$, and we conclude that $\ker(f)$ is a submodule of M.

Problem 2. Show that there is a $\mathbb{Z}$-module isomorphism $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}/m) \cong \mathbb{Z}/\gcd(m, n)$.

Solution. Using Problem 3 from Problem Set 1, $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}/n)$ is isomorphic to the submodule of $\mathbb{Z}/n$ given by

$$T_m(\mathbb{Z}/n) = \{[x]_n \in \mathbb{Z}/(n) \mid m[x]_n = [0]_n\}.$$

Since subgroups of cyclic groups are cyclic, $T_m(\mathbb{Z}/n)$ is cyclic, and so we only need to show its order is $\gcd(m, n)$ in order to know that $T_m(\mathbb{Z}/n) \cong \mathbb{Z}/\gcd(m, n)$, since any two cyclic groups of the same order are isomorphic.

We have the following equivalences:

$$m[x]_n = [0]_n \iff mx \equiv 0 \pmod{n} \iff n \mid mx \iff \frac{n}{\gcd(m,n)} \mid \frac{m}{\gcd(m,n)} x.$$

Since the integers $\frac{n}{\gcd(m,n)}$ and $\frac{m}{\gcd(m,n)}$ are coprime, the last statement is equivalent to $\frac{n}{\gcd(m,n)} \mid x$, or $x \in \left(\left[\frac{n}{\gcd(m,n)}\right]_n\right)$. Recall a fact from Math 817: If G is cyclic of order n, generated by y, then y^j has order $n/\gcd(n, j)$. Applying this to $y = [1]_n$ and $j = \left[\frac{n}{\gcd(m,n)}\right]$, it follows that

$$\left|\left(\left[\frac{n}{\gcd(m,n)}\right]_n\right)\right| = \frac{n}{\gcd\left(n, \frac{n}{\gcd(m,n)}\right)} = \frac{n}{\frac{n}{\gcd(m,n)}} = \gcd(m, n).$$

Problem 3. Let R be a commutative ring. Given an R-module M, its **annihilator** is the ideal

$$\operatorname{ann}(M) := \{a \in R \mid am = 0 \text{ for all } m \in M\}.$$

Show that if there is an isomorphism of R-modules $M \cong N$, then $\operatorname{ann}(M) = \operatorname{ann}(N)$.

Solution. Let $f\colon M \to N$ be an isomorphism of R-modules. Given $r \in \operatorname{ann}(M)$ and $n \in n$, since f is surjective we can find $m \in M$ such that $n = f(m)$, and since f is a homomorphism of R-modules we have

$$rn = rf(m) = f(rm).$$

But $r \in \operatorname{ann}(M)$ by assumption, and thus $rm = 0$. Finally, f is a homomorphism, so

$$rn = f(rm) = f(0) = 0.$$

We conclude that $r \in \operatorname{ann}(N)$. This shows that $\operatorname{ann}(M) \subseteq \operatorname{ann}(N)$. On the other hand, there also exists an isomorphism $g\colon N \to M$ (the inverse of f), and thus we conclude that $\operatorname{ann}(N) \subseteq \operatorname{ann}(M)$. Therefore $\operatorname{ann}(M) = \operatorname{ann}(N)$.

Problem 4. Let R be a commutative ring with $1 \neq 0$. An R-module M is **simple** if it has no nontrivial submodules. Show that M is a simple if and only if there exists a maximal ideal $\mathfrak{m}$ of R such that $M \cong R/\mathfrak{m}$.
Note: recall that a proper ideal $\mathfrak{m}$ is **maximal** if it is maximal with respect to inclusion, meaning that for any ideal I, $\mathfrak{m} \subseteq I$ implies $\mathfrak{m} = I$ or $\mathfrak{m} = R$.

Solution. ($\Rightarrow$) Assume M is simple and pick any element $m \in M$ with $m \neq 0_M$. Consider the submodule Rm of M generated by m. Since $m \neq 0$, then $Rm \neq 0$. Since M is simple, we conclude that $M = Rm$. By Problem Set 1, Problem 2, every cyclic module is isomorphic to R/I for some ideal I. Therefore, $M \cong R/I$ for some ideal I.

By the lattice isomorphism theorem for modules, submodules of R/I are in bijective correspondence with submodules of R that contain I. A submodule of R is the same thing as an ideal, and since R/I is irreducible, we must have that there are no proper ideals of R that properly contain I — that is, I must be maximal. So $M \cong R/\mathfrak{m}$ for a maximal ideal $\mathfrak{m} = I$.

($\Leftarrow$) Assume $M \cong R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ of R. By the Lattice Isomorphism Theorem, the submodules of $R/\mathfrak{m}$ correspond to submodules I of R containing $\mathfrak{m}$. But a submodule of R is the same as an ideal, and since $\mathfrak{m}$ is maximal the only ideals $I \supseteq \mathfrak{m}$ are $\mathfrak{m}$ and R. Therefore, the only submodules of $R/\mathfrak{m}$ are $R/\mathfrak{m}$ and $\mathfrak{m}/\mathfrak{m} = 0$, and thus $R/\mathfrak{m}$ is simple. We conclude that M is simple.

Problem 5. Let R be a ring with $0 \neq 1$. Prove that if M is an R-module and N is a submodule of M such that N and M/N are finitely generated, then M is finitely generated.

Proof. Suppose that $\{n_1, \ldots, n_l\} \subseteq N$ generates N and $\{m_1 + N, \ldots, m_k + N\} \subseteq M/N$ generates M/N. We will show that the finite set $\{n_1, \ldots, n_l, m_1, \ldots, m_k\}$ generates M.

Pick $x \in M$. Then

$$x + N = \sum_{i=1}^{l} r_i(m_i + N) = \left(\sum_i r_i m_i\right) + N$$

for some $r_i \in R$, since $\{m_1 + N, \ldots, m_k + N\} \subseteq M/N$ generates M/N. Thus $x - \sum_{i=1}^{l} r_i m_i \in N$. Since $\{n_1, \ldots, n_l\} \subseteq N$ generates N, we can now find some $s_j \in R$ such that

$$x - \sum_{i=1}^{l} r_i m_i = \sum_{j=1}^{k} s_j n_j.$$

Thus

$$x = \sum_{i=1}^{l} r_i m_i + \sum_{j=1}^{k} s_j n_j.$$

Since x was an arbitrary element of M, this proves that the set $\{n_1, \ldots, n_l, m_1, \ldots, m_k\}$ generates M. $\square$