Problem Set 4
Abstract Algebra II

Bennett Rennier
barennier@gmail.com

January 15, 2018

Section 10.1

Ex 1 Prove that $0m = 0$ and $(-1)m = -m$ for all $m \in M$.

Proof. We see that $0m = (0+0)m = 0m + 0m$. Cancelling a $0m$, we get that $0m = 0$. Using this, we see that $(-1)m + m = (-1)m + 1m = (-1+1)m = 0m = 0$. This proves that $(-1)m$ is the additive inverse of m, i.e. $(-1)m = -m$. $\square$

Ex 5 For any left ideal I of R define

$$IM = \{\sum_{\text{finite}} a_i m_i \mid a_i \in I, m_i \in M\}$$

to be the collection of all finite sums of elements of the form am where $a \in I$ and $m \in M$. Prove that IM is a submodule of M.

Proof. Recall that every ideal of R contains 0 and that $0 \in M$ as well. That means that $0 \cdot 0 = 0 \in IM$. Suppose that $r \in R$ and $x, y \in IM$. This means that $x = \sum_i a_i m_i$ and $y = \sum_j a_j m_j$, where $a_i, a_j \in I$ and $m_i, m_j \in M$. We see that $x + ry = \sum_i a_i m_i + r\sum_j a_j m_i = \sum_i a_i m_i + \sum_j (ra_j)m_j$. Since I is an ideal, this means that $ra_j \in I$. Thus, $x + ry$ is the finite sum of elements of the form am. This proves that $x + ry \in IM$. This proves that IM is a submodule by the submodule criterion. $\square$

Ex 6 Show that the intersection of any nonempty collection of submodules of an R-module is a submodule.

Proof. Let $\{S_i\}_{i \in I}$ be a nonempty collection of submodules. Let $S = \cap_{i \in I} S_i$. Since every submodule contains 0, this means that $0 \in S$. Let $r \in R$ and $x, y \in S$. This means that $x \in S_i$ and $y \in S_i$ for all $i \in I$. Since S_i is a R-submodule, this means that $x + ry \in S_i$ for every $i \in I$. This proves that $x + ry \in S$, which proves that S is a submodule by the submodule criterion. $\square$

Ex 7 Let $N_1 \subseteq N_2 \subseteq \ldots$ be an ascending chain of submodules of M. Prove that $\cup_{i=1}^{\infty} N_i$ is a submodule of M.

Proof. Let $N = \cup_{i=1}^{\infty} N_i$. Since $0 \in N_1$, then this means that $0 \in N$. Suppose that $r \in R$ and $x, y \in N$. This means that $x \in N_j$ and $y \in N_k$ for some $j, k \in \mathbb{N}$. Without loss of generality, assume that $j \leq k$. This means that $x \in N_j \subseteq N_k$. Since $x, y \in N_k$ and N_k is a submodule, that means that $x + ry \in N_k \subseteq N$. By the submodule criterion, this proves that N is a submodule. $\square$

Ex 9 If N is a submodule of M, the annihilator of N in R is defined to be $\{r \in R \mid rn = 0 \text{ for all } n \in N\}$. Prove that the annihilator of N in R is a 2-sided ideal of R.

Proof. Let $A_N \subseteq R$ be the annihilator of N. We see that if $x, y \in A_N$, then that means that $xn = 0$ and $yn = 0$ for all $n \in N$. This means that $(x + y)n = xn + yn = 0 + 0 = 0$, which shows that $x + y \in A_N$.

Now suppose that $x \in A_N$ and $r \in R$. Again, this means that $xn = 0$ for all $n \in N$. We see that $(xr)n = x(rn) = 0$, as $rn \in N$. We also see that $(rx)n = r(xn) = r0 = 0$ as well. This proves that $xr, rx \in A_N$, which proves that A_N is a two-sided ideal of R. $\square$

Ex 10 If I is a right ideal of R, the annihilator of I in M is defined to be $\{m \in M \mid am = 0 \text{ for all } a \in I\}$. Prove that the annihilator of I in M is a submodule of M.

Proof. Let $A_I \subseteq M$ be the annihilator of I in M. Since $0 \in M$, we see that for all $i \in I$ that $i0 = 0$. This means that $0 \in A_I$. Now suppose that $r \in R$, $x, y \in A_I$, and $i \in I$. We see that $i(x + ry) = ix + (ir)y = 0 + 0 = 0$ as $ir \in I$ since I is a right ideal. This proves that $x + ry \in A_I$, which by the submodule criterion, proves that A_I is a submodule. $\square$

Ex 11 Let M be the abelian group $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$.

a) Find the annihilator of M in $\mathbb{Z}$.

b) Let $I = 2\mathbb{Z}$. Describe the annihiltor of I in M as a direct product of cyclic groups.

Proof. a) Claim: $A_M = (600)$. Proof: Suppose that $r \in A_M \subseteq \mathbb{Z}$. Since $(\overline{1}, \overline{1}, \overline{1}) \in M$, this means that $r(\overline{1}, \overline{1}, \overline{1}) = (\overline{r}, \overline{r}, \overline{r}) = (\overline{0}, \overline{0}, \overline{0})$. This proves that $24 \mid r$, that $15 \mid r$, and that $50 \mid r$. This means that $\operatorname{lcm}(24, 15, 50) = 600 \mid r$, proving that $r \in (600)$. For the reverse inclusion, suppose that $600n \in (600)$ where $r \in \mathbb{Z}$. Let $(\overline{m_1}, \overline{m_2}, \overline{m_3}) \in M$. We then see that $600n(\overline{m_1}, \overline{m_2}, \overline{m_3}) = (\overline{600nm_1}, \overline{600nm_2}, \overline{600nm_3}) = (\overline{25 \cdot 24nm_1}, \overline{15 \cdot 40nm_2}, \overline{50 \cdot 12nm_3}) = (\overline{0}, \overline{0}, \overline{0})$. This proves that $600n \in A_M$. Thus, $A_M = (600)$.

b) Claim: $A_I = (12)/(24) \times (15)/(15) \times (25)/(50)$. Proof: Suppose that $(\overline{j}, \overline{k}, \overline{\ell}) \in M$ annihilates (2). Then, $2(\overline{j}, \overline{k}, \overline{\ell}) = (\overline{2j}, \overline{2k}, \overline{2\ell}) = (\overline{0}, \overline{0}, \overline{0})$. This proves that $2j = 0 \pmod{24}$, $2k = 0 \pmod{15}$, and that $2\ell = 0 \pmod{50}$. This means that $j = 0 \pmod{12}$, that $k = 0 \pmod{15}$, and that $\ell = 0 \pmod{25}$. This proves that $(\overline{j}, \overline{k}, \overline{\ell} \in (12)/(24) \times (15)/(15) \times (25)/(50))$. For the reverse inclusion, suppose that $(\overline{12j}, \overline{0}, \overline{25\ell}) \in (12)/(24) \times (15)/(15) \times (25)/(50)$ and that $2n \in (2)$. We see that $2n(\overline{12j}, \overline{0}, \overline{25\ell}) = (\overline{24nj}, \overline{0}, \overline{50n\ell} = (\overline{0}, \overline{0}, \overline{0})$, which proves that $(\overline{12j}, \overline{0}, \overline{25\ell})$ annihilates (2). Thus, $A_I = (12)/(24) \times (15)/(15) \times (25)/(50) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$\square$

Ex 18 Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is rotation clockwise about the origin by $\pi/2$ radians. Show that V and 0 are the only $F[x]$-submodules for this T.

Proof. Let U be a $F[x]$-submodule of V for this T. This precisely means that U is a subspace of V and that U is T-invariant. We can clearly see that V and $\{0\}$ satisfy this. Suppose U is neither of these subspaces. Since $U \neq \{0\}$, let $(x, y) \in U$ be a nonzero element. Since U is T-invariant, then $T((x, y)) = (y, -x) \in U$. We see that $(y, -x) \neq 0$ and that (x, y) and $(y, -x)$ are linearly independent. That means that $\dim(U) \geq 2$. Since $U \subseteq V$, this proves that $U = V$. Thus, there are no other $F[x]$-submodules for this T. □

Ex 19 Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$ and let T be the linear transformation from V to V which is projection onto the y-axis. Show that V , 0, the x-axis and the y-axis are the only $F[x]$-submodules for this T.

Proof. Let U be a $F[x]$-submodule of V for this T. This precisely means that U is a subspace of V and that U is T-invariant. We can clearly see that V and $\{0\}$ satisfy this.

Let $U = \{(0, y) \mid y \in \mathbb{R}\}$ (i.e. the y-axis). Let $(0, y) \in U$ be an arbitrary element. Then $T((0, y)) = (0, y) \in U$, which proves that the y-axis is T-invariant and thus the y-axis is a $F[x]$-submodule of V for this T.

Now let $U = \{(x, 0) \mid x \in \mathbb{R}\}$ (i.e. the x-axis). Let $(x, 0) \in U$ be an arbitrary element. Then $T((x, 0)) = (0, 0) \in U$, which proves that the x-axis is T-invariant and thus the x-axis is a $F[x]$-submodule of V for this T.

Suppose U is T-invariant but is none of these subspaces. That means that there exists an element $(x, y) \in U$, where $x \neq 0$ and $y \neq 0$. However, U is T-invariant which means that $T((x, y)) = (0, y) \in U$. These two elements are clearly not multiples of one another, so they must be linearly independent. This means that $\dim(U) \geq 2$. Since $U \subseteq V$, this means that $U = V$. This is a contradiction, proving that there are no other T-invariant subspaces, and hence no other $F[x]$-submodules. □

Section 10.2

Ex 4 Let A be any $\mathbb{Z}$-module, let a be any element of A and let n be a positive integer. Prove that the map $\varphi_a : \mathbb{Z}/n\mathbb{Z} \to A$ given by $\varphi_a(\overline{k}) = ka$ is a well-defined $\mathbb{Z}$-module homomorphism if and only if $na = 0$. Prove that $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \simeq A_n$, where $A_n = \{a \in A \mid na = 0\}$ (so A_n is the annihilator in A of the ideal (n) of $\mathbb{Z}$).

Proof. Suppose that $na = 0$ and that $\overline{x} = \overline{y} \in \mathbb{Z}/n\mathbb{Z}$. This means that $x = y + kn$ for some $k \in \mathbb{Z}$. We see that $\varphi_a(\overline{x}) = xa = xa + kna = (x + kn)a = ya = \varphi_a(\overline{y})$, as $kna = k(na) = 0$. This proves that φ is well-defined.

Now suppose that φ is well-defined. Let $x \in \mathbb{Z}$ and $y = x - n$. We see then that $\overline{x} = \overline{y}$. We also see that

$$\varphi(\overline{x}) = \varphi(\overline{y + n}) = (y + n)a = ya + na = \varphi(\overline{y}) + na$$

Since $\overline{x} = \overline{y}$, this means that $\varphi(\overline{x}) = \varphi(\overline{y})$, which proves that $na = 0$.

Let $f : A_n \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$ be defined as $f(a) = \varphi_a$. We have already proven that this map is well-defined. Suppose $a, b \in A_n$ and that $r \in \mathbb{Z}$. Then $f(a+rb)(\overline{k}) = \varphi_{a+rb}(\overline{k}) = k(a+rb) = ka + r(kb) = \varphi_a(k) + r\varphi_b(k) = f(a)(\overline{k}) + rf(b)(\overline{k}) = (f(a) + rf(b))(\overline{k})$. This proves that $f(a+rb) = f(a) + rf(b)$, which proves that f is a $\mathbb{Z}$-module homomorphism.

Now suppose that $a \in \ker f$. Then $f(a)(\overline{k}) = 0$ for all $\overline{k}$. This means that $0 = f(a)(\overline{1}) = \varphi_a(\overline{1}) = a$. This proves that $a = 0$, which means that $\ker f = \{0\}$, proving that f is injective.

Let $H \in \mathrm{Hom}_{\mathbb{A}}(\mathbb{Z}/n\mathbb{Z}, A)$. Let $a = H(\overline{1})$. We see that $na = nH(\overline{1}) = H(\overline{n}) = H(\overline{0}) = 0$, which proves that $a \in A_n$. Since H is an R-module homomorphism, this means that $H(\overline{k}) = H(k\overline{1}) = kH(\overline{1}) = ka = \varphi_a(\overline{k}) = f(a)(\overline{k})$. This proves that $H = f(a)$, which proves that f is surjective. Thus, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \simeq A_n$ as desired. □

Ex 5 Exhibit all $\mathbb{Z}$-module homomorphisms from $\mathbb{Z}/30\mathbb{Z}$ to $\mathbb{Z}/21\mathbb{Z}$.

Proof. By the previous exercise we proved that $\mathrm{Hom}(\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/21\mathbb{Z})$ is isomorphic to the annihilator of (30) in $\mathbb{Z}/21\mathbb{Z}$, call it $A \subseteq \mathbb{Z}/21\mathbb{Z}$. Claim: $A = (7)/(21)$.

Let $\overline{n} \in A$. This means that $30\overline{n} = \overline{30n} = 0 \pmod{21}$, which means that $21 \mid 30n$ or that $7 \mid 10n$. Thus, $10n = 0 \pmod 7$, which shows that $n = 0 \pmod 7$ since $\mathbb{Z}/7\mathbb{Z}$ is a field and thus has no zero divisors. This proves that $n \in (7)/(21)$.

Now suppose that $7\overline{n} \in (7)/(21)$ and that $30k \in (30)$. We see that $30k \cdot 7\overline{n} = \overline{21 \cdot 10kn} = \overline{0}$. This proves that $7\overline{n}$ is an annihilator of (30). Thus, $A = (7)/(21) \simeq \mathbb{Z}/3\mathbb{Z}$.

This proves that there are exactly three module homomorphisms from $\mathbb{Z}/30\mathbb{Z}$ to $\mathbb{Z}/21\mathbb{Z}$. If we just look at them as group homomorphisms, then we see that they are uniquely determined by the image of $\overline{1}$. This means that the three $\mathbb{Z}$-module homomorphisms are the ones specified by $\overline{1} \mapsto \overline{0}$, $\overline{1} \mapsto \overline{7}$, and $\overline{1} \mapsto \overline{14}$. □

Ex 9 Let R be a commutative ring. Prove that $\mathrm{Hom}_R(R, M)$ and M are isomorphic as left R-modules. [Show that each element of $\mathrm{Hom}_R(R, M)$ is determined by its value on the identity of R.]

Proof. Let $\varphi : \mathrm{Hom}_R(R, R) \to R$ be the evaluation map at 1. That is if $f \in \mathrm{Hom}_R(R, R)$, then $\varphi(f) = f(1)$. We see that $\varphi(f+g) = (f+g)(1) = f(1) + g(1) = \varphi(f) + \varphi(g)$ and that $\varphi(cf) = (cf)(1) = cf(1) = c\varphi(f)$, which means that φ is an R-module homomorphism.

Suppose $\varphi(g) = \varphi(f)$. Then $g(1) = f(1)$. Since these are R-module homomorphisms, this means that $g(r) = rg(1) = rf(1) = f(r)$ for all $r \in R$. This proves that $f = g$, and thus that φ is injective. Now suppose $x \in R$. We see that left multiplication is clearly an R-module homomorphism. This means that $f(r) = rx$ is in $\mathrm{Hom}_R(R, R)$. We then see that $\varphi(f) = f(1) = x$, which proves that φ is surjective. Thus, $\mathrm{Hom}_R(R, R) \simeq R$ as R-modules. □

Ex 10 Let R be a commutative ring. Prove that $\mathrm{Hom}_R(R, R)$ and R are isomorphic as rings.

Proof. We saw in the last exercise that $\varphi(f) = f(1)$ was a bijection. We have already proven that the evaluation map is a ring homomorphism. Thus, φ is a ring isomorphism between $\mathrm{Hom}_R(R, R)$ and R. □

Ex 11 Let $A_1, A_2, \dots, A_n$ be R-modules and let B_i be a submodule of A_i for each $i = 1, 2, \dots, n$. Prove that

$$(A_1 \times \cdots \times A_n)/(B_1 \times \cdots \times B_n) \simeq (A_1/B_1) \times \cdots \times (A_n/B_n).$$

Proof. Let $\varphi : \prod_i A_i \to \prod_i (A_i/B_i)$ where $\varphi(a_1, \dots, a_n) = (a_1 + B_1, \dots, a_n + B_n)$. Let $r \in R$ and let $(x_1, \dots, x_n), (y_1, \dots, y_n) \in \prod_i A_i$. We see that

$$\begin{aligned}
&\varphi((x_1, \dots, x_n) + r(y_1, \dots, y_n)) = \varphi(x_1 + ry_1, \dots, x_n + ry_n) \\
&= (x_1 + ry_1 + B_1, \dots, x_n + ry_n + B_n) = (x_1 + B_1, \dots, x_n + B_n) + r(y_1 + B_1, \dots, y_n + B_n) \\
&\qquad = \varphi(x_1, \dots, x_n) + r\varphi(y_1, \dots, y_n)
\end{aligned}$$

which proves that φ is a R-module homomorphism. Let $(x_1 + B_1, \dots, x_n + B_n) \in \prod_i (A_i/B_i)$ be an arbitrary element. Then $\varphi(x_1, \dots, x_n) = (x_1 + B_1, \dots, x_n B_n)$. This proves that φ is surjective. Finally, we see that if $\varphi(x_1, \dots, x_n) = (x_1 + B_1, \dots, x_n + B_n) = (B_1, \dots, B_n)$, then this means that $x_i + B_i = B_i$, which is equivalent to $x_i \in B_i$. Thus, $(x_1, \dots, x_n) is \prod_i B_i$. This argument is reversible, proving that $\ker \varphi = \prod_i B_i$. By the First Isomorphism Theorem, this proves that

$$\prod_i A_i / \prod_i B_i = \prod_i (A_i/B_i)$$

□