Abstract Algebra II Homework 1

Carson Connard

Section 10.1

2 Prove that $R^\times$ and M satisfy the two axioms in Section 1.7 for a *group action* of the multiplicative group $R^\times$ on the set M.

Proof. Recall that the axioms of a group action $G \times A \to A$ are (i) $g_1 \cdot (g_2 \cdot a) = (g_1 \cdot g_2) \cdot a$ for all $g_1, g_2 \in G$ and $a \in A$, and (ii) $1 \cdot a = a$ for all $a \in A$. Consider now the action $R \times M \to M$. Indeed, we know that R has identity, and therefore by the axioms of modules we have that $1 \cdot m = m$ for all $m \in M$. Also, the axioms of modules give that $(r_1 r_2)m = r_1(r_2 m)$ for all $r_1, r_2 \in R$ and $m \in M$. These properties mirror that of group actions. $\square$

3 Assume that $rm = 0$ for some $r \in R$ and some $m \in M$ with $m \neq 0$. Prove that r does not have a left inverse (i.e. there is no $s \in R$ such that $sr = 1$).

Proof. Suppose not, that is $\exists s : sr = 1$. Then $m = (sr)m = s(rm) = s \cdot 0 = 0$. $\Rightarrow\Leftarrow$ $\square$

5 For any left ideal I of R define

$$IM = \left\{ \sum_{\text{finite}} a_i m_i : a_i \in I,\ m_i \in M \right\}$$

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. We consider the 0 case separately. Indeed, $0_M \in IM$ since $0_R \in I$ and $0_M \in M$. Consider now two elements $A = \sum a_i m_i$ and $B = \sum b_i m_i$ in IM. Then for any $r \in R$, we have

$$A + rB = \sum a_i m_i + \sum r b_i m_i.$$

We must have that $A + rB \in IM$ since each sum is finite, and therefore their sum must be finite, and also $rb_i \in I$ since I is a left ideal. By the submodule criterion, we have that $IM \subset M$. $\square$

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

Proof. Let $N_i \subset M$. We aim to show that $\mathcal{N} := \bigcap_i N_i \subset M$. Certainly $\mathcal{N} \neq \emptyset$ since $0 \in N_i$ for all i, as submodules are simply subgroups with additional structure. So, take elements $n, m \in \mathcal{N}$. Since each $N_i \subset M$ and by definition of intersection, we have that $n + rm \in N_i$ for all $r \in R$ and i. Therefore $n + rm \in \mathcal{N}$ and therefore $\mathcal{N}$ satisfies the submodule criterion, giving that $\mathcal{N} \subset M$. $\square$

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

Proof. Define $\mathcal{N} := \bigcup_{i=1}^\infty N_i$. Certainly since $0 \in N_i$ for all i, we have that $0 \in \mathcal{N} \neq \emptyset$. Take elements $n, m \in \mathcal{N}$. Then there must exist some $N_i \ni n$ and $N_j \ni m$ by definition of union. Since the N_i's form an ascending chain of submodules, we have that both $n, m \in N_{\max(i,j)}$. Since this is a submodule of M, it is closed under addition and scalar multiplication, and therefore $n + rm \in N_{\max(i,j)}$ for all $r \in R$. Therefore $n + rm \in \mathcal{N} \subset M$, and by the submodule criterion, we have that $\mathcal{N} \subset M$. $\square$

9 If N is a submodule of M, the *annihilator of* N *in* R is defined to be $\text{Ann}_R(N) = \{r \in R : rn = 0 \ \forall n \in N\}$. Prove that $\text{Ann}_R(N)$ is a two-sided ideal of R.

Proof. Certainly by definition, we know that $\text{Ann}_R(N) \ni 0$ by definition. As such, $\text{Ann}_R(N) \neq \emptyset$. Now, let us take elements $a, b \in \text{Ann}_R(N)$. We see that $(a-b)n = an + (-b)n = 0 - (bn) = 0 - 0 = 0$ for any $n \in N$, which tells us that $a - b \in \text{Ann}_R(N)$ as well. By the subgroup criterion, $(\text{Ann}_R(N), +) \leq N$.

Take now some arbitrary $r \in R$, and take some element $a \in \text{Ann}_R(N)$. We see that $ran = r(an) = 0$ for any $n \in N$, and therefore $ra \in \text{Ann}_R(N)$ as well. Similarly, we see $arn = a(rn) = 0$ for any $n \in N$, and therefore $ar \in \text{Ann}_R(N)$. Therefore we see that $\text{Ann}_R(N)$ is a two sided ideal of R. □

22 Suppose that A is a ring with identity 1_A that is a (unital) left R-module satisfying $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$ for all $r \in R$ and $a, b \in A$. Prove that the map $f : R \to A$ defined by $f(r) = r \cdot 1_A$ is a ring homomorphism mapping $1_R \mapsto 1_A$ and that $f(R)$ is contained in the center of A. Conclude that A is an R-algebra and that the R-module structure on A induced by its algebra structure is precisely the original R-module structure.

Proof. First note that $f(1_R) = 1_R \cdot 1_A = 1_A$. Now taking elements $r_1, r_2 \in R$, we see the following:

$$f(r_1 + r_2) = (r_1 + r_2) \cdot 1_A = r_1 \cdot 1_A + r_2 \cdot 1_A = f(r_1) + f(r_2),$$
$$f(r_1 r_2) = r_1 r_2 \cdot 1_A = r_1 \cdot (r_2 \cdot 1_A) = r_1 \cdot (r_2 \cdot 1_A 1_A) = r_2 \cdot (1_A(r_2 \cdot 1_A)) = (r_1 \cdot 1_A)(r_2 \cdot 1_A) = f(r_1)f(r_2).$$

Indeed, f is a ring homomorphism. Let us now consider the elements $r \cdot 1_A \in f(R)$ and $a \in A$. We see that

$$(r \cdot 1_A)a = r \cdot (1_A a) = r \cdot a = r \cdot (a 1_A) = a(r \cdot 1_A),$$

which gives that $f(R) \subset Z(A)$. Therefore, A is an R-algebra. Finally, the R-module structure on A induced by its algebra structure is the same as the original structure as $r \cdot a = r \cdot (a 1_A) = (r \cdot 1_A)a$. □

Section 10.2

1 Use the submodule criterion to show that kernels and images of R-module homomorphisms are submodules.

Proof. Let us take $\varphi : N \to M$ to be an R-module homomorphism. Note that by definition, $0 \in \ker \varphi$ and $0 \in \text{im}\varphi$, and so both the image and the kernel are nonempty. Now, let $n_1, n_2 \in \ker \varphi$ and $r \in R$. We see that

$$\varphi(n_1 + rn_2) = \varphi(n_1) + r\varphi(n_2) = 0 + r0 = 0.$$

So by definition, $n_1 + rn_2 \in \ker \varphi$. Therefore, $\ker \varphi$ is a submodule of N by the submodule criterion. Similarly, let us take $\varphi(n_1), \varphi(n_2) \in \text{im}\varphi$, with $r \in R$. We see that

$$\varphi(n_1) + r\varphi(n_2) = \varphi(n_1 + rn_2) \in \text{im}\varphi.$$

Therefore, we have that $\text{im}\varphi$ also is a submodule of N by the submodule criterion. □

2 Show that the relation "is R-module isomorphic to" is an equivalence relation on any set of R-modules.

Proof. Recall that an equivalence relation must be reflexive, symmetric, and transitive. We will show each property separately.
Reflexivity: Trivially any R-module M is isomorphic to itself by taking the identity map.
Symmetry: Take $\varphi : N \to M$ to be an isomorphism of R-modules. We aim to show that φ^{-1} is also an R-module isomorphism. We know that φ^{-1} is certainly a group isomorphism since φ is a group isomorphism, and so it remains to show that φ^{-1} preserves R actions. Taking $m \in M$ and $r \in R$, we have that $m = \varphi(n)$ for some $n \in N$. Moreover, since φ is an R-module isomorphism by definition, we know that $\varphi(rn) = r\varphi(n) = rm$. Therefore, we see that $\varphi^{-1}(rm) = \varphi^{-1}(\varphi(rn)) = rn = r\varphi^{-1}(m)$, and so φ^{-1} is a homomorphism of R-modules. Therefore $M \cong N$ as desired.

Transitivity: Consider the two R-module isomorphisms, $\varphi : M_1 \to M_2$ and $\psi : M_2 \to M_3$. We want to show that $\psi \circ \varphi : M_1 \to M_3$ is an R-module isomorphism. We know that $\psi \circ \varphi$ is a group isomorphism since both φ, ψ are taken to be R-module isomorphisms (and are therefore group isomorphisms). It remains to show that $\psi \circ \varphi$ preserves R actions. So, taking $r \in R$ and $m \in M_1$, we see $\psi(\varphi(rn)) = \psi(r\varphi(n)) = r\psi(\varphi(n))$ since φ, ψ are taken to be R-module isomorphisms. Therefore, we have that $M_1 \cong M_3$ as desired.
Since all three properties of an equivalence relation hold, we have that "is R-module isomorphic to" is an equivalence relation. $\square$

6 Prove that $\hom_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n,m)\mathbb{Z}$.

Proof. Notice that §10.2 Exercise 4 tells us that $\hom_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathrm{Ann}_{\mathbb{Z}/m\mathbb{Z}}(n\mathbb{Z})$. Now $\mathrm{Ann}_{\mathbb{Z}/m\mathbb{Z}}(n\mathbb{Z})$ consists of the $x \in \mathbb{Z}/m\mathbb{Z}$ where $m|nx$. Define $d := \gcd(n,m)$. Then $\mathrm{Ann}_{\mathbb{Z}/m\mathbb{Z}}(n\mathbb{Z})$ is the cyclic module which is generated by m/d in $\mathbb{Z}/m\mathbb{Z}$. Indeed, nx is a multiple of m if and only if $(m/d)|x$. The cyclic module which is generated by m/d has d elements, and therefore is isomorphic to $\mathbb{Z}/d\mathbb{Z}$ as desired. $\square$

7 Let z be a fixed element in the center of R. Prove that the map $m \mapsto zm$ is an R-module homomorphism from M to itself. Show that for a commutative ring R, the map from $R \to \mathrm{End}_R(M)$ given by $r \mapsto rI$ is a ring homomorphism (where I is the identity endomorphism).

Proof. Notice that the map is a group homomorphism since $z(m_1+m_2) = zm_1 + zm_2$ (where $m_1, m_2 \in M$) by the axioms for modules. Now since $z \in Z(R)$, we have that $r(zm) = z(rm)$ for all $r \in R$. Therefore this map is an R-module homomorphism.

Now define φ as the map $r \mapsto rI$. We can verify the ring homomorphism conditions as follows:

$$\varphi(r_1 + r_2) = (r_1 + r_2)I = r_1 I + r_2 I = \varphi(r_1) + \varphi(r_2),$$
$$\varphi(r_1 r_2) = r_1 r_2 I = r_1 I r_2 I = \varphi(r_1)\varphi(r_2).$$

We have shown both results. $\square$

8 Let $\varphi : M \to N$ be an R-module homomorphism. Prove that $\varphi(\mathrm{Tor}(M)) \subseteq \mathrm{Tor}(N)$ (cf. §10.1 Ex. 8).

Proof. Take $t \in \mathrm{Tor}(M)$ and take some nonzero $r \in R$, such that $rm = 0$. Then $r\varphi(m) = \varphi(rm) = \varphi(0) = 0$. Therefore by definition, $\varphi(m) \in \mathrm{Tor}(N)$. $\square$

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

Proof. Let us take some element $\varphi \in \hom_R(R, M)$, and take some $r \in R$. As suggested, we want to show that $\varphi(r)$ can be expressed in terms of $\varphi(1)$. First, notice $\varphi(r) = r\varphi(1)$ since φ is an R-module homomorphism. So for notation, we can write each φ as φ_m where $\varphi_m(r) = rm$ for each $m \in M$. We shall show that $m \mapsto \varphi_m$ is an R-module homomorphism $\psi : M \to \hom_R(R, M)$.

First, we see that ψ is injective since $\varphi_{m_1} = \varphi_{m_2} \implies m_1 = 1 \cdot \varphi_{m_1} = 1 \cdot \varphi_{m_2} = m_2$. It is also surjective since each homomorphism φ_m is determined uniquely by its value on 1. We see that it is also a group homomorphism since $\varphi_{m_1+m_2}(r) = r(m_1 + m_2) = rm_1 + rm_2 = \varphi_{m_1}(r) + \varphi_{m_2}(r)$ for all $r \in R$. Finally, we have that φ preserves R actions: fixing $r_0 \in R$, we see $r_0\varphi_m(r) = r_0 rm = r(r_0 m) = \varphi_{r_0 m}(r)$ for all $r \in R$. So indeed, $m \mapsto \varphi_m$ is an R-module isomorphism. $\square$

10 Let R be a commutative ring. Prove that $\hom_R(R, R)$ and R are isomorphic as rings.

Proof. Consider the ring homomorphism (as given in problem 10.2.7) $\varphi : R \to \mathrm{End}_R(R)$ defined by $r \mapsto r \cdot \mathrm{id}_R$ with id_R the identity map on R. In particular, this is an isomorphism of the R-modules R and $\mathrm{End}_R(R)$ as shown in the previous problem. Therefore this map is bijective, and is a ring isomorphism. $\square$