Hungerford: Algebra

IV.1. Modules

Note: $R$ is a ring.

1. If $A$ is an abelian group and $n > 0$ an integer such that $na = 0$, $\forall a \in A$, then $A$ is a unitary $\mathbb{Z}_n$-module, with the action of $\mathbb{Z}_n$ on $A$ given by $\overline{k}a = ka$, where $k \in \mathbb{Z}$ and $k \mapsto \overline{k} \in \mathbb{Z}_n$ under the canonical projection $\mathbb{Z} \mapsto \mathbb{Z}_n$.

Proof: $\forall k \in \mathbb{Z}$, let $\overline{k}$ be the non negative integer which is the remainder of $k$ when divided by $n$ (as well as the corresponding element in $\mathbb{Z}_n$). That is, for some integer $m_k$, we have $k = nm_k + \overline{k}, 0 \leq \overline{k} < n$.

Since $\forall a \in A, \; na = 0$, and so

$$ka = (nm_k + \overline{k})a = m_k(na) + \overline{k}a = 0 + \overline{k}a = \overline{k}a.$$ 

Thus it is not ambiguous to define $\overline{k}a = ka, \forall a \in A$ and $\forall \overline{k} \in \mathbb{Z}_n$.

After we have shown that $\overline{k}a = ka$ is well-defined, we shall show that this would make $A$ a unitary $\mathbb{Z}_n$-module by checking the definition. Note that $\forall \overline{k}, \overline{h} \in \mathbb{Z}_n$ and $\forall a, b \in A$, we have

(1.1) $\overline{k}(a + b) = \overline{k}(a + b) = \overline{k}a + \overline{k}b = \overline{k}a + \overline{k}b$.
(1.2) $(\overline{h} + \overline{k})a = (\overline{h} + \overline{k})a = (h + k)a = ha + ka = \overline{h}a + \overline{k}a$.
(1.3) $\overline{h}(\overline{k}a) = \overline{h}(ka) = (hk)a = \overline{h}k\overline{a}$.
(1.4) $\overline{1}a = 1a = a$.

Therefore, by the definition of modules (Definition IV-1.1), $A$ is a unitary $\mathbb{Z}_n$-module.

2. Let $f : A \mapsto B$ be an $R$-module homomorphism.

(a) $f$ is a monomorphism if and only if for every pair of $R$-module homomorphisms $g, h : D \mapsto A$ such that $fg = fh$, we have $g = h$.

(b) $f$ is an epimorphism if and only if for every pair of $R$-module homomorphisms $k, t : B \mapsto C$ such that $kf = tf$, we have $k = t$.

Proof: (a) Suppose that $f$ is a monomorphism and that a pair of $R$-module homomorphisms $g, h : D \mapsto A$ satisfying $fg = fh$. For any $d \in D$, since $fg = fh$, we have $f(g(d)) = f(h(d))$. Since $f$ is a monomorphism, we must have $g(d) = h(d)$. As $d$ is an arbitrary element in $D$, we conclude that $g = h$. 

1
Conversely, we assume that for every pair of $R$-module homomorphisms $g, h : D \to A$ such that $fg = fh$, we have $g = h$. Suppose by contradiction that $f$ is not a monomorphism. Then $\text{Ker } f \neq \{0_A\}$. Let $D = \text{Ker } f$, $g : D \to A$ be given by $g(x) = x$, $\forall x \in D$, and $h : D \to A$ be given by $h(x) = 0_A$, $\forall x \in D$. Then $\forall x \in D = \text{Ker } f$,

$$f(g(x)) = f(x) = 0_B, \text{ and } f(h(x)) = f(0_A) = 0_B,$$

and so $fg = fh$. But as $\text{Ker } f \neq \{0_A\}$, $g \neq h$, contrary to the assumption that $g$ and $h$ should have been the same. Therefore, $\text{Ker } f$ must be $\{0_A\}$ and so $f$ must be a monomorphism.

(b) Suppose that $f$ is an epimorphism and that a pair of $R$-module homomorphisms $k, t : B \to C$ satisfying $kf = tf$. For any $c \in C$, since $f$ is an epimorphism, $\exists a \in A$ such that $c = f(a)$. Since $kf = tf$, we have $k(c) = kf(a) = t(f(a)) = t(c)$, and so we conclude that $k = t$.

Conversely, for every pair of $R$-module homomorphisms $k, t : B \to C$ such that $kf = tf$, we have $k = t$. Suppose by contradiction that $f$ is not an epimorphism. Then $\text{Im } f \neq B$. Let $C = B/\text{Im } f$, $g : B \to C$ be given by $g(b) = b + \text{Im } f$ be the canonical epimorphism, $\forall b \in B$, and $h : B \to C$ be given by $h(b) = 0_B + \text{Im } f$, $\forall b \in B$. Then $\forall a \in A$,

$$k(f(a)) = f(a) + \text{Im } f = \text{Im } f, \text{ and } t(f(a)) = \text{Im } f,$$

and so $kf = tf$. But as $\text{Im } f \neq B$, $k \neq t$, contrary to the assumption that $k$ and $t$ should have been the same. Therefore, $\text{Im } f$ must be $B$ and so $f$ must be an epimorphism.

3. Let $I$ be a left ideal of a ring $R$ and $A$ an $R$-module.

(a) If $S$ is a nonempty subset of $A$, then

$$IS = \left\{ \sum_{i=1}^{n} r_i a_i : n \in \mathbb{N}^*; r_i \in I \text{ and } a_i \in S \right\}$$

is a submodule of $A$. Note that if $S = \{a\}$, then $IS = Ia = \{ra : r \in I\}$.

(b) If $I$ is a two-sided ideal, then $A/I A$ is an $R/I$-module with the action of $R/I$ given by $(r + I)(a + IA) = ra + IA$.

**Proof:** (a) We first show that $IS$ is a subgroup of $A$. Pick $x, x' \in IS$, we may assume that for positive integers $m, n$, $r_i, r'_i \in I$ and $a_i, a'_i \in A$,

$$x = \sum_{i=1}^{m} r_i a_i \text{ and } x' = \sum_{i=1}^{n} r'_i a'_i.$$

2
It follows that

\[ x - x' = \sum_{i=1}^{m+n} r_i'' a_i'' \in IS, \]

where \( r_i'' = r_i \) if \( 1 \leq i \leq n \) and \( r_i'' = -r_{i-n}' \) if \( n+1 \leq i \leq m+n \), and where \( a_i'' = a_i \) if \( 1 \leq i \leq n \) and \( a_i'' = a_{i-n} \) if \( n+1 \leq i \leq m+n \). Hence \( IS \) is a subgroup of \( A \).

To show that \( IS \) is a submodule of \( A \), we also need to show that \( \forall r \in R, \) and \( x \in IS, \) \( rx \in IS. \) Again let \( x = \sum_{i=1}^{n} r_i a_i \in IS. \) Then since \( I \) is a left ideal, \( \forall r \in R, rr_i \in I \) and so

\[ rx = r \left( \sum_{i=1}^{n} r_i a_i \right) = \sum_{i=1}^{n} r(r_i a_i) = \sum_{i=1}^{n} (rr_i a_i) \in IS. \]

(b) Since \( IA \) is a submodule of \( A, \) and since \( I \) is an ideal of \( R, \) both quotients \( A/IA \) and \( R/I \) are meaningful. Note that \( A/IA \) is a group and that \( R/I \) is a ring. It suffices to verify the definition of a module for the given action. Let \( r+I, s+I \in R/I \) and \( a+IA, b+IA \in A/IA \) be arbitrarily elements.

(3b.1) Since \( A \) is an \( R \)-module, \( r(a+b) = ra + rb. \) Thus

\[ (r+I)((a+IA) + (b + IA)) = (r+I)((a+b) + IA) = r(a+b) + IA = (ra + rb) + IA = (r+I(a + IA) + (r+I)(b + IA). \]

(3b.2) Since \( A \) is an \( R \)-module, \( (r + s)a = ra + sa. \) Thus

\[ ((r+I) + (s+I))(a + IA) = ((r + s) + I)(a + IA) = (r + s)a + IA = (ra + sa) + IA = (r + I)(a + IA) + (s + I)(a + IA). \]

(3b.3) Since \( A \) is an \( R \)-module, \( r(sa) = (rs)a. \) Thus

\[ (r+I)((s+I))(a+IA)) = (r+I)((sa) + IA) = r(sa) + IA = (rs)a + IA = (rs+I)(a+IA). \]

By the definition of modules, we conclude that \( A/IA \) is an \( R/I \)-module with the action of \( R/I \) given by \( (r+I)(a+IA) = ra + IA. \)

4. If \( R \) has an identity, then a nonzero unitary cyclic \( R \)-module \( A \) is isomorphic to an \( R \)-module of the form \( R/J, \) where \( J \) is a left ideal of \( R. \)
Proof: Let $A$ be a unitary cyclic $R$-module. Then for some element $a \in A$, $A = Ra = \{ra : r \in R\}$.

Let $J = \{x \in R : xa = 0_A\}$. We shall first show that $J$ is a left ideal of $R$. In fact, $\forall x, x' \in J$ and $\forall r \in R$, we have $xa = x'a = 0_A$ and so $(x - x')a = xa - x'a = 0_A$, and $(rx)a = r(xa)r(0_A) = 0_A$. Thus $J$ is a left ideal of $R$.

Note that $R/J$ is an additive abelian group. With the action $\forall r \in R$ and $\forall x + J \in R/J$, $r(x + J) = (rx) + J$, $R/J$ is an $R$-module.

View $R$ as an $R$-module with the ring multiplication as the action. Define a map $f : R \mapsto A$ by $f(r) = ra$, $\forall r \in R$. Then as $A = \{ra : r \in R\}$, $f$ is an onto map. Since $A$ is an $R$-module, $\forall r, s \in R$, $f(r + s) = (r + s)a = ra + sa = f(r) + f(s)$, and $f(rs) = (rs)a = r(sa) = rf(s)$. Hence $f$ is an $R$-module homomorphism. Moreover,

$$Ker f = \{r \in R : f(r) = 0_A\} = \{r \in R : ra = 0_A\} = J.$$ 

By the First Isomorphism Theorem (Theorem IV-1.7), $A \cong R/J$ is a $R$-module isomorphism.

9. If $f : A \mapsto A$ is an $R$-module homomorphism such that $ff = f$, then

$$A = Ker f \oplus Im f.$$ 

Proof: Let $a \in A$. Let $a_2 = f(a)$ and $a_1 = a - a_2$. Then $a_2 \in Im f$. Since $f$ is an $R$-module homomorphism and since $ff = f$, $f(a_1) = f(a - a_2) = f(a) - f(a_2) = f(a) - ff(a) = f(a) - f(a) = 0$, and so $a_1 \in Ker f$. It follows that any $a \in A$ can be written as $a = a_1 + a_2$ with $a_1 \in Ker f$ and $a_2 \in Im f$.

Suppose that $y \in Ker f \cap Im f$. Since $y \in Im f$, then $\exists x \in A$ such that $y = f(x)$. Since $y \in Ker f$, and since $ff = f$,

$$0 = f(y) = f(f(x)) = f(x) = y,$$

and so $Ker f \cap Im f = \{0\}$. It follows that

$$A = Ker f \oplus Im f.$$