MODULES AND HOMOMORPHISMS

COLTON GRAINGER (MATH 6140 ALGEBRA 2)

Assignment due 2019-01-28

[1, No. 10.2.1]. *Given.* The definition of a submodule.

To prove. Kernels and images of R-module homomorphisms are submodules.

Proof. Let $f\colon M \to N$ be a homomorphism of modules. From our study of groups, $\ker f$ and $\operatorname{im} f$ are subgroups of M and N respectively [1, Ch. 2.2]. To argue both groups are stable under the ring action, consider $m \in M$ and $n \in N$.

inclusion	justification
$rm \in \ker f$	$f(rm) = rf(m) = r0 = 0$.
$rn \in \operatorname{im} f$	Choose $a \in f^{-1}(n)$, then $rn = rf(a) = f(ra)$. □

[1, No. 10.2.2]. *To prove.* R-module isomorphism classes partition any set of R-modules.

Proof. Let M, M', M'' be R-modules.

property	justification
Reflexivity	Because $\mathrm{id}\colon M \to M$ respects addition and intertwines the ring action, id is a module isomorphism.
Symmetry	Say $\varphi\colon M \to M'$ is a module isomorphism. By definition[1] φ^{-1} is a bijective set map. Moreover, take any elements $\varphi(m), \varphi(n) \in M'$ and $r \in R$. Additivity follows from $\varphi^{-1}(\varphi(m)) + \varphi^{-1}(\varphi(n)) = \varphi^{-1}(\varphi(m+n)) = \varphi^{-1}(\varphi(m) + \varphi(n))$. Closure under the ring action is seen by $r\varphi^{-1}(\varphi(m)) = rm = \varphi^{-1}(\varphi(rm))$.
Transitivity	Let $M \xrightarrow{f} M' \xrightarrow{g} M''$ be module isomorphisms. Then $M \xrightarrow{g\circ f} M''$ is an group isomorphism. Let $r \in R$ and $m \in M$. Consider $r(g \circ f)(m) = rg(f(m)) = g(rf(m)) = g(f(rm)) = (g \circ f)(rm)$. So $g \circ f$ is a module isomorphism. □

[1, No. 10.2.4]. *Given.* Let $A \in \mathsf{Ab}$, let $a \in A$, and say $n \in \mathbf{N}$.

To prove.

a. $\varphi_a\colon \mathbf{Z}/(n) \to A$ given by $\varphi(k + (n)) = ka$ is a well defined $\mathbf{Z}$-module homomorphism iff $na = 0$.
b. $\operatorname{Hom}_{\mathbf{Z}}(\mathbf{Z}/(n), A) \cong A_n$ where $A_n := \{a \in A : na = 0\}$.

Date: 2019-01-24.

[1]A module isomorphism is a bijective module homomorphism.

Proof.

a. The following are equivalent.

- The module homomorphism $\varphi_a \colon \mathbf{Z}/(n) \to A$ such that $\varphi(k + (n)) = ka$ is well defined.
- For each j such that $j - k \in (n)$, $ja = ka$.
- For the generators $\pm n$ of the ideal (n), $\pm na = 0$.
- For the integer n and the element $a \in A$, $na = 0$.

b. Let $\psi \colon \operatorname{Hom}_{\mathbf{Z}}(\mathbf{Z}/(n), A) \to A_n$ map $\varphi \in \operatorname{Hom}(\mathbf{Z}/(n), A)$ to a iff $\varphi(1 + (n)) = a$. From the argument above, each $\varphi \in \operatorname{Hom}(\mathbf{Z}/(n), A)$ is determined by $\varphi(1 + (n)) = 1a = a$, so ψ is well defined.

property of ψ	justification
an additive homomorphism?	For arbitrary $\varphi_1, \varphi_2 \in \operatorname{Hom}(\mathbf{Z}/(n), A)$, there's $a_1, a_2 \in A_n$ such that $\varphi_1(1 + (n)) = a_1$ and $\varphi_2(1 + (n)) = a_2$. Then $\psi \colon \varphi_1 + \varphi_2 \mapsto a_1 + a_2$.
injective?	Consider $\alpha \in \ker \psi$. Then $\alpha(1 + (n)) = 0$. So α is the zero homomorphism, i.e., $\ker \psi = 0$.
surjective?	Note that if $b \in A_n$, then $nb = 0$. Since $\lvert b \rvert$ divides n, the homomorphism $\beta(1 + (n)) = b$ is well defined. So $\operatorname{im} \psi = A_n$.

We conclude $\psi \colon \operatorname{Hom}(\mathbf{Z}/(n), A) \xrightarrow{\sim} A_n$. □

[1, No. 10.2.5]. *To exhibit.* All $\mathbf{Z}$-module homomorphisms from $\mathbf{Z}/30\mathbf{Z}$ to $\mathbf{Z}/12\mathbf{Z}$.

Exhibition. Take $1 + (30)$ as a generator of $\mathbf{Z}/(30)$. All the unique homomorphisms from $\mathbf{Z}/(30)$ to $\mathbf{Z}/(12)$ are determined by the image of $1 + (30)$ in $\mathbf{Z}/(12)$, whose order must divide 30. In particular, there are 6 possible images.

element	order	determines $\mathbf{Z}/(30) \to \mathbf{Z}(12)$?
$0 + (12)$	1	yes
$1 + (12)$	12	
$2 + (12)$	6	yes
$3 + (12)$	4	
$4 + (12)$	3	yes
$5 + (12)$	12	
$6 + (12)$	2	yes
$7 + (12)$	12	
$8 + (12)$	3	yes
$9 + (12)$	4	
$10 + (12)$	6	yes
$11 + (12)$	12	

So Hom has cardinality 6. Moreover, Hom is isomorphic to a quotient of $\mathbf{Z}/(12)$. (Verify.) Thence we conclude $\operatorname{Hom}_{\mathbf{Z}}(\mathbf{Z}/(30), \mathbf{Z}/(12)) \cong \mathbf{Z}/(6)$. □

[1, No. 10.2.6]. *To prove.* $\operatorname{Hom}_{\mathbf{Z}}(\mathbf{Z}/(n), \mathbf{Z}/(m)) \cong \mathbf{Z}/(n, m)\mathbf{Z}$.

Proof. Fix the base ring $\mathbf{Z}$. By [1, p. 10.2.4], the module $\operatorname{Hom}_{\mathbf{Z}}(\mathbf{Z}/(n), \mathbf{Z}/(m))$ is isomorphic to $\{a + (m) : n(a + (m)) = na + (m) = 0 + (m)\}$ by the 1-1 correspondence $a + (m) \leftrightarrow \varphi$ if and only if $\varphi(1 + (m)) = a + (m)$.

We'll establish a set bijection between Hom and $\{0, \dots, d - 1\}$ where $d = \gcd(m, n)$. Knowing the cardinality of Hom, and that Hom is isomorphic to a quotient of $\mathbf{Z}/(m)$, we will argue that $\operatorname{Hom} \cong \mathbf{Z}/(m, n)$.

So let $\varphi \in \text{Hom}$ such that $\varphi(1+(m)) = a+(m)$. Then $na+(m) = 0+(m)$. So[2] $na = km$. Let $d = \gcd(m,n)$. Factorize n and m so that $n = \nu d$ and $m = \mu d$. Now the condition on a is $\nu da = k\mu d$. Thence $a = \frac{k\mu}{\nu}$, which we assume is an integer in $\{0,\ldots,m-1\}$. Since μ and ν are coprime, k must be $\{0,\nu,\ldots,d(\nu-1)\}$, which establishes the set bijections:

$$\begin{aligned}\{0,\ldots,d(\nu-1)\} &\leftrightarrow \{a+(m) : n(a+(m)) = 0+(m)\}\\ &\leftrightarrow \text{Hom}_{\mathbf{Z}}(\mathbf{Z}/(n), \mathbf{Z}/(m)).\end{aligned}$$

Because Hom is isomorphic to a quotient of the cyclic group $\mathbf{Z}/(m)$, and because $|\text{Hom}| = d = \gcd(m,n)$, we conclude that $\text{Hom} \cong \mathbf{Z}/(m,n)$. $\square$

[1, No. 10.2.7]. *Given.* Let z be a fixed element in the center of R.

To prove.

a. The map $\varphi\colon m \mapsto zm$ is an R-module endomorphism of M.
b. For a commutative ring R the map from R to $\text{End}_R(M)$ given by $\psi\colon r \mapsto rI$ is a ring homomorphism (where I is the identity endomorphism.)

Proof.

a. Let $m,n \in M$, and $r \in R$. For additivity, observe $\varphi(m+n) = z(m+n) = zm+zn = \varphi(m)+\varphi(n)$. For closure under the ring action, consider $r\varphi(m) = rzm = zrm = \varphi(rm)$.

b. Let $r,s \in R$. Consider $\psi(r+s) = (r+s)I = rI+sI = \psi(r)+\psi(s)$, with also $\psi(rs) = (rs)I = r(sI) = rI(sI) = \psi(r)\psi(s)$. $\square$

[1, No. 10.2.9]. *Given.* Let R be a commutative ring.

To prove. $\text{Hom}_R(R,M)$ and M are isomorphic as left R-modules.

Proof. Let $\varphi \in \text{Hom}$ be mapped by $\psi\colon \varphi \mapsto \varphi(1)$ into M.

property of ψ	justification
an R-module homomorphism?	Say $\alpha,\beta \in \text{Hom}$ and $r \in R$. Then $\psi(\alpha+\beta) = (\alpha+\beta)(1) = \alpha(1)+\beta(1) = \psi(\alpha)+\psi(\beta)$.
injective?	Suppose $\alpha \in \ker\psi$. Then α is mapped to $0 \in M$. So $\alpha(1) = 0$ which implies that for each $r \in R$, $\alpha(r) = \alpha(r1) = r\alpha(1) = r0 = 0$. So α is the zero homomorphism.
surjective?	Pick an arbitrary $m \in M$. Is there $\beta \in \text{Hom}$ such that $\beta(1) = m$? Yes. R-linearly extending the provisional definition $\beta(1) = m$, we'd have $\beta(r) = rm$, which does define a module homomorphism β. $\square$

[1, No. 10.2.10]. *Given.* Let R be a commutative unital ring.

To prove. $\text{Hom}_R(R,R) =: \text{End}_R(R)$ and R are isomorphic as rings.

Proof. Consider the map $\psi\colon R \to \text{End}(R)$ such that $r \mapsto rI$.

property of ψ	justification
a ring homomorphism?	Special case of [1, No. 10.2.7] when considering R as a module over itself.

[2]My choice of notation due to `https://math.stackexchange.com/questions/381891`.

property of ψ	justification
injective?	Consider $\ker \psi$. Say $r \in R$ and for each $\varphi \in \operatorname{End}(R)$, $rI\varphi = r\varphi = 0$. Then for each $s \in R$, $0 = r\varphi(s) = \varphi(rs)$. In particular for $\varphi = \mathrm{id} \in \operatorname{End}(R)$ and $s = 1 \in R$, we have $0 = \mathrm{id}(r)$. So $r = 0$.
surjective?	Say $\varphi \in \operatorname{End}(R)$. There's some $r \in R$ such that $\varphi(1) = r$. By [1, p. 10.2.9], that $\varphi(1) = r$ determines φ by extending R-linearly. (E.g., for $s \in R$, $\varphi(s) = s\varphi(1) = sr$.) $\square$

[1, No. 10.2.11]. *Given.* Let $A_1, A_2, \ldots, A_n$ be R-modules and let the B_j be submodules of the A_j, resp.

To prove. $(A_1 \times \cdots \times A_n)/(B_1 \times \cdots \times B_n) \cong (A_1/B_1) \times \cdots \times (A_n/B_n)$.

Proof by universal property. Suppose that a passerby R-module C has homomorphisms φ_j into the A_j/B_j.

$$\begin{tikzcd}
C \arrow[drr, bend left, "\varphi_2"] \arrow[ddr, bend right, "\varphi_1"'] & & \\
& \prod A_j / \prod B_j \arrow[ul, dotted, "\psi"'] \arrow[r, "\pi_2"'] \arrow[d, "\pi_1"] & A_2/B_2 \\
& A_1/B_1 &
\end{tikzcd}$$

Define

$$\pi_i \colon \left(\prod_j A_j\right) / \left(\prod_j B_j\right) \to A_i/B_i$$
$$(a_1, \ldots, a_n) + \prod_j B_j \mapsto a_i + B_i.$$

Observe that the π_i are well defined and surjective as $a_i \notin B_j$ for $i \neq j$. To see that $\left(\prod_j A_j\right) / \left(\prod_j B_j\right)$ is the product of the quotients A_j/B_j, suppose now that $C = \prod_1^n (A_j/B_j)$ *is the product indeed* (explaining the otherwise ridiculous reversed arrow for ψ) with homomorphisms φ_j as the standard coordinate projections. By the universal property of products, there's a unique homomorphism $\psi\colon \prod A/\prod B \to C$ such that $\varphi_j \circ \psi = \pi_j$ for all j. Factorization through the φ_j forces $\ker \psi = \cap_j \ker \pi_j = (0_{A_1}, \ldots, 0_{A_n}) + \prod_j B_j$, which is trivial. So $\psi\colon \prod A/\prod B \xrightarrow{\sim} C$. $\square$

References

[1] D. Dummit and R. Foote, *Abstract algebra.* Prentice Hall, 2004.