BASIC MODULE ISOMORPHISMS

COLTON GRAINGER (MATH 6140 ALGEBRA 2)

Assignment due 2019-02-03

We assume R is a unital ring.

[1, No. 10.3.1]. *Given.* Let R be a unital ring. Consider sets A and B with cardinality $|A| = |B|$.

To prove. The free R-modules $F(A)$ and $F(B)$ are isomorphic in the category Rmod.

Proof. Let $f\colon A \to B$ be a bijection of sets. Now, $F(A)$ is universal in the category of modules M for which each set map $A \xrightarrow{f} M'$ into any module M' induces a short exact sequence (of R-linear maps)

$$0 \to A \to M \xrightarrow{\Phi} M' \to 0$$

such that the following diagram commutes:

$$\begin{tikzcd} A \arrow[r] \arrow[dr, "f"'] & M \arrow[d, "\Phi"] \\ & M' \end{tikzcd}$$

Likewise, $F(B)$ is universal for B. Since f^{-1} is a well defined set map, the following diagram commutes:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\iota_A"] & B \arrow[r, "f^{-1}"] \arrow[d, "\iota_B"] & A \arrow[r, "f"] \arrow[d, "\iota_A"] & B \arrow[d, "\iota_B"] \\ F(A) \arrow[r, "\exists!\Phi"] & F(B) \arrow[r, "\exists!\Psi"] & F(A) \arrow[r, "\exists!\Phi"] & F(B) \end{tikzcd}$$

Note the inclusion of A into $F(A)$ induces the identity on $F(A)$, e.g.,

$$\begin{tikzcd} A \arrow[r] \arrow[dr, "\iota_A"'] & F(A) \arrow[d, dotted, "\mathrm{id}"] \\ & F(A) \end{tikzcd}$$

Similarly, the inclusion of B into $F(B)$ induces the identity on $F(B)$. Chasing $f^{-1} \circ f = \mathrm{id}_A$ and $f \circ f^{-1} = \mathrm{id}_B$, uniqueness of the induced maps $F(A) \xrightarrow{\mathrm{id}} F(A)$ and $F(B) \xrightarrow{\mathrm{id}} F(B)$ forces

$$\Psi \circ \Phi = \mathrm{id}_{F(A)} \quad \text{and} \quad \Phi \circ \Psi = \mathrm{id}_{F(B)},$$

which demonstrates that Φ is a morphism in Rmod with a left and right inverse. We conclude that

$$\Phi\colon F(A) \to F(B)$$

is an isomorphism. □

Date: 2019-02-03.

[1, No. 10.3.3]. *Given.*

a. A linear transformation $T\colon \mathbf{R}^2 \to \mathbf{R}^2$ with associated matrix

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \qquad \text{w.r.t. the standard basis,}$$

and $V = \mathbf{R}^2$ as an $\mathbf{R}[x]$-module where x acts by the linear transformation $x.v = Av$.

b. A linear transformation $T\colon \mathbf{R}^2 \to \mathbf{R}^2$ with associated matrix

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \qquad \text{w.r.t. the standard basis,}$$

and $W = \mathbf{R}^2$ as an $\mathbf{R}[x]$-module where x acts by the linear transformation $x.w = Av$.

To prove. Both the above modules V and W are cyclic.

Proof. I claim that

$$V = \left\langle \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\rangle,$$

because $x \in \mathbf{R}[x]$ acts by $x.\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix}$ to force at least a pair of linearly independent vectors into $\left\langle \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\rangle$. Since $\mathbf{R}^2$ as a real vector space has dimension 2, scalar multiplication takes care of the rest.

Analogously, I claim

$$W = \left\langle \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\rangle$$

for $x \in \mathbf{R}[x]$ acts by $x.\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ to force two linearly independent vectors into $\left\langle \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\rangle$. $\square$

[1, No. 10.3.4]. *Given.* Let A be a finite abelian group with $|A| = m$.

To prove. A is a torsion $\mathbf{Z}$-module.

Proof. If $a \in A$, the order of the element divides the order of the group, so $ma = 0$. $\square$

To demonstrate. The infinite direct sum of cyclic groups $\bigoplus_{k=1}^{\infty} \mathbf{Z}/k\mathbf{Z}$ is a torsion $\mathbf{Z}$-module.

Demo. Let (a_k) be an element of the direct sum $\bigoplus_{k=1}^{\infty} \mathbf{Z}/k\mathbf{Z}$. Now, all but finitely many coordinates of (a_k) are zero. So the annihilating integer

$$m = \operatorname{lcm}\{k \colon a_k = 0 \text{ in } (a_k)\}$$

is well defined. In each coordinate, the order of the element divides the order of the group, whence

$$m(a_k) = (ma_k) = 0.$$

We've shown $\bigoplus_{k=1}^{\infty} \mathbf{Z}/k\mathbf{Z}$ is an infinite abelian torsion module. $\square$

[1, No. 10.3.5]. *Given.* Let R be an entire ring. Say M is a finitely generated torsion R-module. Let G be a finite generating set for M.

To prove. There's an $r \in R$ such that for all $m \in M$, $rm = 0$.

Proof. We construct such an annihilating element r. Note first G is a finite subset of an R-torsion module. So there's a finite collection of nonzero ring elements

$$\{r_g \in R \setminus \{0\} : r_g g = 0, g \in G\}.$$

Now form the (nonzero, as R is entire) product

$$r = \prod_{g \in G} r_g \in R,$$

which I claim will kill each $m \in M$.

So say $m \in M$. Because G generates M, there's a surjection

$$\bigoplus_{g \in G} R \to M \quad \text{such that} \quad s_g \mapsto s_g g.$$

Thence $m = \sum_{k \in G} s_g g$; this with commutativity sets up the right action by r:

$$rm = r\left(\sum_g s_g g\right) = \sum_g s_g r g = \sum_g s_g(0) = 0.$$

We conclude there's a nonzero element r in the entire ring R that kills every element of the finitely generated module M. $\square$

[1, No. 10.3.6]. *Given.* Let M be a finitely generated R-module, with finite generating set G. Say $\varphi\colon M \to N$ is an epimorphism.

To prove. Quotients of M may be finitely generated by a set with $|G|$ (or fewer) elements.

Proof. Because there's a bijective correspondence between quotients of M and isomorphism classes of R-linear images of M, it suffices to argue that $N \cong M/\ker\varphi$ is generated finitely generated by $\varphi(G)$.

By assumption φ is surjective. If $n \in N$, there's $m \in M$ such that $\varphi(m) = n$. Moreover, because G is a generating set for M, there's *another* surjection

$$\bigoplus_{g \in G} R \to M, \quad \text{defined by} \quad r_g \mapsto r_g g.$$

We may choose an R-linear combination $\sum_{g \in G} r_g g$ that's equal to m, then map it through φ to find

$$n = \sum_{g \in G} r_g \varphi(g).$$

We have demonstrated that $\varphi(G)$ is a generating set for N. Because φ is a well defined function, $|\varphi(G)| \leq |G|$. We conclude that N may be finitely generated by $|G|$ elements or less. $\square$

[1, No. 10.3.7]. *Given.* Let M and N be R-modules, with M/N and N finitely generated. Say G and H are finite subsets of M for which

$$N = R\{G\} \quad \text{and} \quad M/N = R\{h + N : h \in H\}.$$

To prove. M is finitely generated.

Proof. I claim $M = R\{G \cup H\}$. We proceed to express an arbitrary $m \in M$ as an R-linear combinations of $G \cup H$. It's convenient to work with the natural projection $\pi\colon M \to M/N$. By hypothesis,

$$\pi(m) = \sum_{h \in H} r_h(h + N).$$

Then, in the fiber, we find

$$\begin{aligned} m &= \sum_{h \in H}\left(h + \sum_{g \in G} r_g g\right) \\ &= \sum_h r_h h + \sum_h \sum_g r_h r_g g. \end{aligned}$$

We conclude $m \in R\{G \cup H\}$. $\square$

[1, No. 10.3.8]. *Given.* The direct sum of countably many copies of the integers, $\bigoplus_1^\infty \mathbf{Z}$.

To prove. $\bigoplus_1^\infty \mathbf{Z}$ is *not* a finitely generated $\mathbf{Z}$-module.

Proof by contradiction. Suppose G is a finite generating set such that

$$\mathbf{Z}\{G\} = \bigoplus_1^\infty \mathbf{Z}.$$

Find the (well-defined) maximum, taken over finite G and finite nonzero coordinates of each element of G,

$$k := \max\{i \colon g_i \neq 0, (g_i) \in G\}.$$

Now consider $(h_i) \in \bigoplus_1^\infty \mathbf{Z}$ where $h_k = 1$ and $h_i = 0$ for all other indices $i \neq k$. It is visible that $(h_i) \notin \mathbf{Z}\{G\}$, which is absurd. Our supposition that $\bigoplus_1^\infty \mathbf{Z}$ could be finitely generated must have been false. □

[1, No. 10.3.9]. *Given.* An R-module M and the definition of *irreducibility* in the category Rmod.

To prove. M is irreducible if and only if $M \neq 0$ and M is a cyclic module with any nonzero element as a generator.

Proof. ($\Rightarrow$) Let M be irreducible. Then $M \neq 0$. If m is a nonzero element of M, then the nontrivial submodule $R\{m\}$ must be M.

($\Leftarrow$) Let $M \neq 0$ and say any nonzero $m \in M$ does generate M. Let $N \subset M$ be a submodule. Either N is trivial or not. If not, then the nonzero element $n \in N$ generates M. In particular, $M = R\{n\} \subset N \subset M$. Because a nontrivial submodule N of M must be M itself, we conclude M is irreducible. □

To exhibit. We exhaustively list all irreducible $\mathbf{Z}$-modules.

Exhibition.

kind of $\mathbf{Z}$-module	isomorphism class rep	parameter
cyclic	$\mathbf{Z}/(k)$	$k \in \mathbf{Z}_{\geq 0}$
nontrivial cyclic	$\mathbf{Z}/(n)$	$n \in \mathbf{Z}_{\geq 0} \setminus \{1\}$
irreducible	$\mathbf{Z}/(p)$	p is a prime integer

[1, No. 10.3.10]. *Given.* Let R be a commutative unital ring. Let M be an R-module.

To prove. M is irreducible if and only if $M \cong R/\mathfrak{m}$ where $\mathfrak{m}$ is a maximal ideal of R.

Proof. ($\Rightarrow$) Let M be irreducible. By [1, No. 10.3.9], there's a unique surjective R-linear map

$$\varphi \colon R \to M$$

such that $\varphi(r) = rm$, where m is any nonzero element. (If m is zero, then $\varphi \colon R \to 0$ is trivial.) In particular $R/\ker\varphi \cong M$. By the lattice isomorphism theorem for modules, $R/\ker\varphi$ has no nontrivial proper submodules.

Motivated by the fact that R is an object in both Rmod and CRing, we set out the following thesaurus.

description	in CRing	in Rmod
"normal" subobjects	ideals	submodules
"simple" objects	fields	irreducible modules

Because $R/\ker\varphi$ has no nontrivial proper submodules, it is a field. Thence $\ker\varphi$ is a maximal ideal.

($\Leftarrow$) Say that $\varphi \colon R \to M$ and $\ker\varphi$ is a maximal ideal of R. Then $R/\ker\varphi$ is a field. In particular, $R/\ker\varphi$ is nonempty and has no nontrivial proper submodules. So $M \cong R/\ker\varphi$ is irreducible. □

[1, No. 10.3.10]. *Given.* Let M and N be irreducible R-modules.

To prove. Any nontrivial R-linear map from $M \to N$ is an isomorphism of R-modules.

Proof. Say $\varphi\colon M \to N$ is a nontrivial R-linear map. Then $\ker\varphi \neq M$. Since M is irreducible, the submodule $\ker\varphi = 0$. So

$$0 \to M \xrightarrow{\varphi} N \quad \text{is exact.}$$

Now nontrivial M embeds as $\varphi(M) \subset N$. Because N is irreducible, $\varphi(M) = N$. So

$$0 \to M \xrightarrow{\varphi} N \to 0 \quad \text{is exact.}$$

Given. Say M is irreducible.

To prove. (*Shur's Lemma*) $\mathrm{End}_R(M)$ is a division ring.

Proof by contrapositive. We take the ring structure on $\mathrm{End}_R(M)$ for granted. Here we'll focus on (the lack of) zero divisors. So suppose α and β are nontrivial R-endomorphisms of M. The composition $\beta \circ \alpha$ is a nontrivial endomorphism. Because M is irreducible $\beta \circ \alpha$ is an isomorphism. Because $M \neq 0$, $\beta \circ \alpha$ is not the zero homomorphism. So $\mathrm{End}_R(M)$ has no zero divisors, and thence is a division ring. ☐

References

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