M4P63 Algebra IV

Lectured by Dr John Britnell
Typed by David Kurniadi Angdinata

Spring 2020

Syllabus

Contents

1 Modules

1.1 Modules over rings

Lecture 1 Friday 10/01/20

Let R be an **associative ring with unity**, that is an abelian group written additively with a multiplication which is associative but not necessarily commutative, with an identity 1 and distributive laws $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$. Then

$$R^* = \{r \in R \mid \exists s \in R,\ rs = 1 = sr\}$$

is the unit group of R. If $R^* = R \setminus \{0\}$ then R is a **division ring**, or a **skew field**. In the case that R is commutative, R is a **field**.

Example.

- Fields $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{F}_q$, the field with $q = p^a$ elements with p a prime and $a \geq 1$.
- Skew fields $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ where $i^2 = j^2 = k^2 = ijk = -1$.
- Other rings are polynomial rings $k[x]$ for k a field, more generally $k[x_1, \dots, x_p]$, and $\operatorname{Mat}_n k$, the $n \times n$ matrices with entries from k, a field.

Definition 1.1. Let R be a ring. A **left R-module** is an abelian group M, written additively, together with a function $* : R \times M \to M$ satisfying

$$r*(m_1 + m_2) = r*m_1 + r*m_2, \qquad (r_1 + r_2)*m = r_1*m + r_2*m, \qquad (r_1 r_2)*m = r_1*(r_2 * m), \qquad 1*m = m.$$

We write rm for $r * m$.

Example.

- R is itself a left R-module, with $*$ as ring multiplication. More generally, let I be a left ideal of R, so I is an additive subgroup, and $rI \subseteq I$ for all $r \in R$. Then I is an R-module with $*$ as ring multiplication.
- Let k be a field. Then any vector space over k is a k-module, and vice versa.
- Any abelian group is a $\mathbb{Z}$-module, with $*$ defined by $na = a + \dots + a$ for $n \in \mathbb{Z}^+$ and $a \in A$, and $(-n)a = -(na)$.
- Let k be a field. Let k^n be column vectors. Then k^n is a left $\operatorname{Mat}_n k$-module, with $*$ as the usual matrix-vector multiplication.
- Let $M \in \operatorname{Mat}_n k$. Then we can define a left $k[x]$-module structure on k^* by letting x act as M on k^*. So $\left(x^2 + 3x - 2\right) * v = M^2 v + 3Mv - 2v$.
- Let G be a group. Any representation of G over the field k is a left module for $k[G]$, the **group algebra**, a vector space over k with elements of G as a basis, with multiplication derived from that of G.

Definition 1.2. A **right R-module** is defined similarly, with the R-multiplication on the right, so M an abelian group under $+$, and a map $M \times R \to M$ satisfying

$$(m_1 + m_2)*r = m_1*r + m_2*r, \qquad m*(r_1 + r_2) = m*r_1 + m*r_2, \qquad m*(r_1 r_2) = (m * r_1)*r_2, \qquad m*1 = m.$$

Left and right modules are not quite the same. If we amend this definition by putting the ring multiplication on the left, the third axiom becomes $(r_1 r_2)m = r_2(r_1 m)$. But in a left module, we have $(r_1 r_2)m = r_1(r_2 m)$.

Definition 1.3. Let R be a ring. The **opposite ring** R^{op} is R with a redefined multiplication $r *_{R^{\mathrm{op}}} s = s *_R r$.

It is easy to see that a left R-module is the same as a right R^{op}-module and vice versa. If R is commutative then $R = R^{\mathrm{op}}$.

Exercise. Show that $\operatorname{Mat}_n k \cong \operatorname{Mat}_n k^{\mathrm{op}}$.

Except where otherwise stated, R-modules are assumed to be left R-modules.

Definition 1.4. Let M_1 and M_2 be R-modules. A map $f : M_1 \to M_2$ is an **R-module homomorphism** if

- f is a group homomorphism, with respect to the $+$ operation, and
- $f(rm) = rf(m)$, for $r \in R$ and $m \in M$.

If f is bijective, then it is an **R-module isomorphism**.

Definition 1.5. An additive subgroup $L \leq M$ is a **submodule** if $rL \leq L$ for $r \in R$. In this case we automatically get an R-module structure on the quotient M/L with multiplication given by $r(m+L) = rm + L$.

Theorem 1.6 (First isomorphism theorem)**.** *Let $f : M_1 \to M_2$ be an R-module homomorphism. Then* $\operatorname{Im} f \leq M_2$, $\operatorname{Ker} f \leq M_1$, *and* $\operatorname{Im} f \cong M/\operatorname{Ker} f$.

The other isomorphism theorems have R-module versions too. Lecture 2 Monday 13/01/20
Let S be a set. We have a collection of R-modules $(M_s)_S$ indexed by S.

Definition 1.7. The **direct product** is

$$\prod_{s \in S} M_s = \{(m_s)_S \mid m_s \in M_s\},$$

with coordinate-wise addition and R-multiplication, so

$$(m_s)_S + (n_s)_S = (m_s + n_s)_S, \qquad r(m_s)_S = (rm_s)_S.$$

If $M_s = M$ for all $s \in S$, then we write M^S for $\prod_{s \in S} M_s$. The **direct sum** is

$$\bigoplus_{s \in S} M_s = \{(m_s)_S \mid \text{all but finitely many coordinates } m_s \text{ are zero}\} \leq \prod_{s \in S} M_s.$$

If S is finite then the direct product and the direct sum are equal.

Example. Let $M = \mathbb{Z}_2$, as a $\mathbb{Z}$-module, and let $S = \mathbb{N}$. Then $\bigoplus_{s \in \mathbb{N}} \mathbb{Z}_2$ is a countable $\mathbb{Z}$-module but $\prod_{s \in \mathbb{N}} \mathbb{Z}_2 = \mathbb{Z}_2^{\mathbb{N}}$ is uncountable.

When $|S| = 2$, generally we write $M_1 \oplus M_2$ for the direct sum or product. There are natural injective maps

$$\begin{array}{cccc} \iota_A & : & A & \longrightarrow & A \oplus B \\ & & a & \longmapsto & (a, 0) \end{array}, \qquad \begin{array}{cccc} \iota_B & : & B & \longrightarrow & A \oplus B \\ & & b & \longmapsto & (0, b) \end{array},$$

and surjective maps

$$\begin{array}{cccc} \pi_A & : & A \oplus B & \longrightarrow & A \\ & & (a, b) & \longmapsto & a \end{array}, \qquad \begin{array}{cccc} \pi_B & : & A \oplus B & \longrightarrow & B \\ & & (a, b) & \longmapsto & b \end{array}.$$

1.2 Exact sequences

Definition 1.8. Suppose we have a sequence of R-modules

$$\dots \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} M_{n+1} \xrightarrow{f_{n+1}} \dots,$$

with maps $f_n : M_n \to M_{n+1}$. Say the sequence is **exact at** M_n if

$$\operatorname{Im} f_{n-1} = \operatorname{Ker} f_n.$$

The sequence is **exact** if it is exact everywhere. A **short exact sequence** is an exact sequence

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0.$$

Note that α is injective and β is surjective. The first isomorphism theorem implies that $B/\operatorname{Im}\alpha \cong C$, where $\operatorname{Im}\alpha \cong A$. An easy case is

$$B \cong A \oplus C,$$

with $\operatorname{Im}\alpha = A \oplus 0$ and $\operatorname{Im}\beta = C$, so $\alpha = \iota_A$ and $\beta = \pi_\beta$. We say that the short exact sequence **splits** in this case.

Example. A non-split short exact sequence of $\mathbb{Z}$-modules, or abelian groups, is

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

Proposition 1.9. *A short exact sequence*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

is split if and only if there exists an R-module homomorphism $\sigma : C \to B$ such that $\beta \circ \sigma = \mathrm{id}_C$.

Such a σ is called a **section** of β.

Proof.

$\Longrightarrow$ Suppose that the short exact sequence is split. So assume $B = A \oplus C$, with $\alpha = \iota_A$ and $\beta = \pi_C$. Now ι_C is a section for β.

$\Longleftarrow$ For the converse, suppose that σ is a section for β. We want $f : A \oplus C \xrightarrow{\sim} B$ such that $f \circ \iota_A = \alpha$ and $\beta \circ f = \pi_C$, so

$$\begin{tikzcd} & & A \oplus C \arrow[dd, "f"] \arrow[dr, "\pi_C"] & & \\ 0 \arrow[r] & A \arrow[ur, "\iota_A"] \arrow[dr, "\alpha"'] & & C \arrow[r] & 0 \\ & & B \arrow[ur, "\beta"'] & & \end{tikzcd}.$$

Define

$$\begin{array}{cccc} f & : & A \times C & \longrightarrow & B \\ & & (a, c) & \longmapsto & \alpha(a) + \sigma(c) \end{array}.$$

Need to check the following.

- f is an R-module homomorphism. [1]
- f is injective. Suppose $f(a, c) = 0$. Then $\alpha(a) + \sigma(c) = 0$. Now $\alpha(a) \in \operatorname{Im} \alpha = \operatorname{Ker} \beta$, so $\beta(\alpha(a) + \sigma(c)) = \beta(\sigma(c)) = c$. Since $\alpha(a) + \sigma(c) = 0$, we have $c = 0$. Hence $\alpha(a) = 0$, and so $a = 0$ since α is injective. We have shown that f is injective.
- f is surjective. Let $b \in B$. Let $c = \beta(b)$. We have $(\beta \circ \sigma)(c) = c = \beta(b)$, so $b - \sigma(c) \in \operatorname{Ker} \beta = \operatorname{Im} \alpha$. So there exists $a \in A$ with $\alpha(a) = b - \sigma(c)$. Then $b = \alpha(a) + \sigma(c) = f(a, c)$.
- $f \circ \iota_A = \alpha$ and $\beta \circ f = \pi_C$. Immediate from the construction of f.

□

Proposition 1.10. *The short exact sequence*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

is split if and only if there exists $\rho : B \to A$ such that $\rho \circ \alpha = \mathrm{id}_A$.

Such a ρ is a **retraction** of α.

Proof.

$\Longrightarrow$ Once again, if the short exact sequence is split then the existence of ρ is clear.

$\Longleftarrow$ Suppose that ρ is a retraction for α. We define $f : B \xrightarrow{\sim} A \oplus C$ such that $f \circ \alpha = \iota_A$ and $\pi_C \circ f = \beta$. Do this by

$$\begin{array}{cccc} g & : & B & \longrightarrow & A \oplus C \\ & & b & \longmapsto & (\rho(a), \beta(c)) \end{array}.$$

Details are omitted.

□

[1] Exercise

1.3 Projective modules

Lecture 3 Tuesday 14/01/20

Definition 1.11. An R-module M is **projective** if any surjective map $\beta : B \to M$ has a section. In other words, any short exact sequence
$$0 \to A \to B \to M \to 0$$
splits.

Example. The R-module R is projective. Let
$$0 \to A \to B \xrightarrow{\beta} R \to 0$$
be a short exact sequence. Since β is surjective, there exists $b \in B$ such that $\beta(b) = 1$. Now for all $r \in R$, $\beta(rb) = r$. Now define
$$\begin{array}{cccc} \sigma & : & R & \longrightarrow & B \\ & & r & \longmapsto & rb \end{array}.$$
Then σ is a section for β.

Proposition 1.12. *An R-module M is projective if and only if whenever $\beta : B \to C$ is surjective, and $f : M \to C$, there exists $g : M \to B$ such that $f = \beta \circ g$, so*
$$\begin{tikzcd} & & & M \arrow[dl, dashed, "g"'] \arrow[d, "f"] & \\ 0 \arrow[r] & A \arrow[r] & B \arrow[r, "\beta"'] & C \arrow[r] & 0 \end{tikzcd}.$$
Such a g is called a **lift** of f.

Proof.

$\Longleftarrow$ Suppose that whenever $\beta : B \to C$ is surjective and $f : M \to C$ then there exists $g : M \to B$ with $f = \beta \circ g$. Suppose $\beta : B \to M$ is a surjective map. Define $f : M \to M$ to be id_M. Then there exists $g : M \to B$ such that $f = \beta \circ g$, so $\mathrm{id}_M = \beta \circ g$. So g is a section for β, and so M is projective.

$\Longrightarrow$ For the converse, suppose $\beta : B \to C$ is surjective, and $f : M \to C$. We construct a module X to complete a commuting square
$$\begin{tikzcd} X \arrow[r, "\epsilon"] \arrow[d, "\delta"'] & M \arrow[d, "f"] \\ B \arrow[r, "\beta"'] & C \end{tikzcd}.$$
Let X be the submodule of $B \oplus M$ defined by
$$X = \{(b, m) \mid \beta(b) = f(m)\}.$$
The maps δ and ϵ are just π_B and π_M respectively, in their restrictions to X. It is clear that $X \le B \oplus M$, and that the square above commutes. Now suppose that M is projective. Since β is surjective, we see that for all $m \in M$ there exists $b \in B$ with $\beta(b) = f(m)$. It follows that $\epsilon : X \to M$ is surjective. So ϵ has a section $\sigma : M \to X$. Define $g = \delta \circ \sigma : M \to B$, so
$$\begin{tikzcd} X \arrow[r, bend left, "\epsilon"] \arrow[d, "\delta"'] & M \arrow[l, dashed, bend left, "\sigma"] \arrow[d, "f"] \arrow[dl, dashed, "g"] \\ B \arrow[r, "\beta"'] & C \end{tikzcd}.$$
Since $\beta \circ \delta = f \circ \epsilon$, for all $m \in M$ we have
$$(\beta \circ g)(m) = (\beta \circ \delta \circ \sigma)(m) = (f \circ \epsilon \circ \sigma)(m) = (f \circ \mathrm{id}_M)(m) = f(m).$$
So $\beta \circ g = f$ as required.

$\square$

Such an X is the **pullback** of β and f, and there is a short exact sequence

$$0 \to A \to X \to M \to 0.$$

Definition 1.13. An R-module M is **free** if M is a direct sum of copies of R, so

$$M = \bigoplus_{s \in S} R.$$

A **basis** for a module M is a set T of elements such that every element $m \in M$ has a unique expression as

$$m = \sum_{i=1}^{m} r_i t_i, \qquad r_i \in R, \qquad t_i \in T.$$

If $M = \bigoplus_{s \in S} R$, then M has a basis consisting of elements with exactly one coordinate one, and the rest zero. On the other hand, if M has a basis T then it is straightforward to show that $M \cong \bigoplus_{t \in T} R$.

Proposition 1.14. *Let F be a free R-module with basis T. Let M be some R-module, and let $\psi : T \to M$ be a set map. Then ψ extends uniquely to a R-module homomorphism $\psi : F \to M$.*

Proof. Each element of F has a unique expression as $\sum_i r_i t_i$ for $r_i \in R$ and $t_i \in T$. Now define

$$\begin{array}{cccc} \psi & : & F & \longrightarrow & M \\ & & \sum_i r_i t_i & \longmapsto & \sum_i r_i \psi(t_i) \end{array}.$$

It is easy to check that this respects $+$ and R-multiplication. $\square$

Proposition 1.15. *A module M is projective if and only if there exists N such that $M \oplus N$ is free, so projective modules are direct summands of free modules.*

Proof.

$\Longrightarrow$ Suppose M is projective. Let F be the free module with basis $\{b_m \mid m \in M\}$. Now the map $b_m \mapsto m$ extends to an R-module homomorphism $F \to M$, which is clearly surjective. Then if $K = \operatorname{Ker} \psi$, we have a short exact sequence

$$0 \to K \to F \xrightarrow{\psi} M \to 0.$$

Since M is projective, there is a section σ for ψ, and so the short exact sequence splits, and $F \cong K \oplus M$.

Lecture 4 Friday 17/01/20

$\Longleftarrow$ Suppose that $M \oplus N = F$, a free module with basis T. Suppose $\beta : B \to C$ is surjective, and that $f : M \to C$. Note that $f \circ \pi_M : F \to C$. For each $t \in T$, let $b_t \in B$ be such that $\beta(b_t) = (f \circ \pi_M)(t)$. The set map

$$\begin{array}{ccc} T & \longrightarrow & B \\ t & \longmapsto & b_t \end{array}$$

extends to a homomorphism $\widehat{g} : F \to B$. Now define $g : M \to B$ by $g = \widehat{g} \circ \iota_M$. We need to show $f = \beta \circ g$. Take $m \in M$. Then $\iota_M(m) = (m, 0) \in F$ can be written as $\sum_i r_i t_i$, where $t_i \in T$ and $r_i \in R$. Applying π_M, $m = \sum_i r_i m_{t_i}$. Then

$$g(m) = (\widehat{g} \circ \iota_M)(m) = \widehat{g}\left(\sum_i r_i t_i\right) = \sum_i r_i b_{t_i}.$$

So

$$(\beta \circ g)(m) = \beta\left(\sum_i r_i b_{t_i}\right) = \sum_i r_i \beta(b_{t_i}) = \sum_i r_i f(m_{t_i}) = f\left(\sum_i r_i m_{t_i}\right) = f(m).$$

Hence $\beta \circ g = f$. So M is projective.

$\square$

1.4 Injective modules

Definition 1.16. Let M be an R-module. Then M is **injective** if whenever $\alpha : M \to B$ is an injective map, it has a retraction $\rho : B \to M$, so $\rho \circ \alpha = \mathrm{id}_M$. Equivalently, every short exact sequence

$$0 \to M \to B \to C \to 0$$

splits.

Example. Let k be a field. Then k-modules are vector spaces. Every k-module is injective. Suppose M and N are k-vector spaces and $\alpha : M \to N$ is a injective map. Then $\operatorname{Im} \alpha$ is a submodule, or subspace, of N. Take a basis for $\operatorname{Im} \alpha$, and extend to a basis for N. The basis vectors not in $\operatorname{Im} \alpha$ form a basis for a complementary subspace U, so $N = \operatorname{Im} \alpha \oplus U$. Now $\pi_{\operatorname{Im} \alpha}$ is surjective, and $\alpha : M \to \operatorname{Im} \alpha$ is an isomorphism. This gives a retraction $N \to M$.

If R is a general ring, the module R need not be injective.

Example. Let $R = \mathbb{Z}$. Then R-modules are abelian groups. There exists an injective $\alpha : \mathbb{Z} \to \mathbb{Q}$. But $\mathbb{Z}$ is not a quotient of $\mathbb{Q}$, [2] so no retraction exists for α.

Proposition 1.17. *An R-module M is injective if and only if whenever $\alpha : A \to B$ is injective, and $f : A \to M$, there exists $g : B \to M$ such that $f = g \circ \alpha$.*

Proof.

$\Longleftarrow$ Suppose that whenever $\alpha : A \to B$ is injective, and $f : A \to M$, there exists $g : B \to M$ such that $f = g \circ \alpha$. Suppose that $\alpha : M \to B$ is injective. We have a map $M \to M$, namely id_M. There exists $g : B \to M$ such that $\mathrm{id}_M = g \circ \alpha$. So g is a retraction for α, and so M is injective.

$\Longrightarrow$ For the converse, suppose $\alpha : A \to B$ is injective, and M is an injective module, with $f : A \to M$. We define a module Y completing a square

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "f"'] & B \arrow[d, "\delta"] \\ M \arrow[r, "\epsilon"'] & Y \end{tikzcd},$$

with $\epsilon \circ f = \delta \circ \alpha$. Let Y be a quotient of $B \oplus M$, by the kernel

$$K = \{(\alpha(a), -f(a)) \mid a \in A\}.$$

Let $\gamma : B \oplus M \to (B \oplus M)/K$ be the canonical quotient map. Then we define $\delta = \gamma \circ \iota_B$ and $\epsilon = \gamma \circ \iota_M$. By construction, we have

$$\begin{aligned} (\epsilon \circ f)(a) &= (\gamma \circ \iota_M \circ f)(a) = \gamma(0, f(a)) = (0, f(a)) + K \\ &= (\alpha(a), 0) + K = \gamma(\alpha(a), 0) = (\gamma \circ \iota_B \circ \alpha)(a) = (\delta \circ \alpha)(a). \end{aligned}$$

Hence $\epsilon \circ f = \delta \circ \alpha$. Claim that ϵ is injective. Suppose $\epsilon(m) = 0$. Then $\iota_M(m) \in K$, so $(0, m) = (\alpha(a), -f(a))$ for some $a \in A$. But $\alpha(a) = 0$ implies that $a = 0$, and so $m = -f(0) = 0$. Since M is injective, ϵ has a retraction $\rho : Y \to M$. Define $g : B \to M$ by $g = \rho \circ \delta$, so

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "f"'] & B \arrow[d, "\delta"] \arrow[dl, dashed, "g"'] \\ M \arrow[r, bend right, "\epsilon"'] & Y \arrow[l, dashed, bend right, "\rho"'] \end{tikzcd},$$

We know that $(\epsilon \circ f)(a) = (\delta \circ \alpha)(a)$ for all $a \in A$. So

$$f(a) = (\mathrm{id}_M \circ f)(a) = (\rho \circ \epsilon \circ f)(a) = (\rho \circ \delta \circ \alpha)(a) = (g \circ \alpha)(a),$$

so $f = g \circ \alpha$ as required.

□

[2] Exercise

We know that projectives are direct summands of free modules. We might hope for a dual version of this for injective modules. But there is no straightforward way of doing this. Lecture 5 Monday 20/01/20

Proposition 1.18 (Baer's criterion for injectivity)**.** *Let M be an R-module. Then M is injective if and only if every R-module map $f : I \to M$, where I is a left ideal of R, has the form $f(x) = xm$ for some $m \in M$. Equivalently, every map $I \to M$ extends to a map $R \to M$.*

Why are these two conditions equivalent? If $f(x) = xm$ for $x \in I$, then we can extend f to R by $f(r) = rm$. Conversely, suppose that $f : I \to M$ extends to $f^+ : R \to M$. Let $m = f^+(1)$. Then for all $r \in R$, $f^+(r) = rm$, and so $f(x) = xm$ for $x \in I$.

Proof. The proof requires Zorn's lemma. Let X be a non-empty set, partially ordered by $\leq$. If every chain, or totally ordered subset, in X has an upper bound in X, then X has a maximal element.

$\Longleftarrow$ Suppose $\alpha : A \to B$, where α is injective. Suppose $f : A \to M$. We want to show there exists $g : B \to M$ such that $f = g \circ \alpha$. We have $\operatorname{Im}\alpha \leq B$. Define

$$X = \{(L, h) \mid \operatorname{Im}\alpha \leq L \leq B,\ h : L \to M,\ f = h \circ \alpha\}.$$

Note that $X \neq \emptyset$ since $\left(\operatorname{Im}\alpha, f \circ \alpha^{-1}\right)$ is in it. Define $\leq$ on X by $(L_1, h_1) \leq (L_2, h_2)$ if $L_1 \leq L_2$ and h_2 extends h_1, so $h_2|_{L_1} = h_1$. Suppose $\{(L_s, h_s) \mid s \in S\}$ is a chain in X. Set $L = \bigcup_{s \in S} L_s$. Then $\operatorname{Im}\alpha \leq L \leq B$. Define

$$\begin{array}{cccc} h & : & L & \longrightarrow & M \\ & & l & \longmapsto & h_s(l) \end{array}, \qquad l \in L_s.$$

This does not depend on the choice of s. Then (L, h) is an upper bound for the chain $\{(L_s, h_s) \mid s \in S\}$. Hence X has a maximal element, (L_0, h_0). We want to show that $L_0 = B$. Then we may set $g = h_0$. Suppose that $L_0 \neq B$. Let $b \in B \setminus L_0$. Note that $Rb \leq B$. Consider

$$L_0 + Rb = \{l + rb \mid l \in L_0,\ r \in R\} \leq B.$$

We would like to extend h_0 to h_0^+ by specifying an image for $h_0^+(b)$. The problem is that $Rb \cap L_0$ may not be $\{0\}$, and if $rb \in L_0$ then we require $rh_0^+(b) = h_0(rb)$, otherwise h_0^+ will not be well-defined. Note that

$$I = \{r \in R \mid rb \in L_0\}$$

is a left ideal for R. Suppose that M has the condition from Baer's criterion, so every map $I \to M$ has the form $x \mapsto xm$ for some $m \in M$. Note that $\{xb \mid x \in I\}$ is a submodule of L_0. Define a map

$$\begin{array}{ccccc} \delta & : & I & \longrightarrow & M \\ & & x & \longmapsto & h_0(xb) \end{array}.$$

This is an R-module homomorphism. So $\delta(x) = xm$ for some $m \in M$. Hence $h_0(xb) = xm$ for all $x \in I$. So we can safely define $h_0^+(b) = m$. Now $\left(L_0 + Rb, h_0^+\right) \in X$, and $(L_0, h_0) < \left(L_0 + Rb, h_0^+\right)$, which contradicts the maximality of (L_0, h_0). Hence $L_0 = B$, and we are done.

$\Longrightarrow$ The converse is left as an exercise. [3]

$\square$

Example 1.19.

- Suppose R is a field. Then the only ideals of R are zero and R. Any map $0 \to M$, for M an R-module, can be extended to the zero map $R \to M$. Hence any R-module is injective.
- Let $\mathbb{Z}$ be a module for itself. The ideals of $\mathbb{Z}$ are $k\mathbb{Z}$ for $k \in \mathbb{Z}$. Define

$$\begin{array}{ccccc} f & : & k\mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & & km & \longmapsto & m \end{array}.$$

If $k \neq 0, \pm 1$, then $f(k) = 1$, and so $f(x) \neq xm$ for $m \in \mathbb{Z}$, since one is not divisible by k in $\mathbb{Z}$. So Baer's criterion fails, and $\mathbb{Z}$ is not injective. We already knew that $\mathbb{Z} \to \mathbb{Q}$ has no retraction.

[3] Exercise

- $\mathbb{Q}$ is injective as a $\mathbb{Z}$-module. Suppose we have a map $f : k\mathbb{Z} \to \mathbb{Q}$. Let $q = f(k)$. Then $f(kt) = qt = (q/k)\, kt$. So $f(x) = x\,(q/k)$ for all x, so $\mathbb{Q}$ satisfies Baer's criterion.