CONTENTS

1 MODULES

1.1 MODULES AND ALGEBRAS

Modules are a generalization of vector spaces, replacing the field of scalars with a unital ring of scalars.

Definition 1. Let R be a unital ring. A **(left)** R**-module** is an additive abelian group M with a left action $R \times M \to M$ satisfying

1. $\lambda(x+y) = \lambda x + \lambda y$;
2. $(\lambda + \mu)x = \lambda x + \mu x$;
3. $\lambda(\mu x) = (\lambda\mu)x$; and
4. $1_R x = x$.

Right R**-modules** are defined similarly.

Note that if R is commutative, then a left R-module is the same thing as a right R-module. If F is a field, then an F-module is the same thing as an F-vector space.

Proposition 1. Basic properties of modules:

1. $\lambda 0_M = 0_M$;
2. $0_R x = 0_M$;
3. $\lambda(-x) = -(\lambda x) = (-\lambda)x$.

If R is a division ring, then we also have

4. $\lambda x = 0_M \implies \lambda = 0_R$ or $x = 0_M$.

The definition of modules gives us addition and scalar multiplication, but we still don't have a way of multiplying module elements together. Providing this is exactly the role of an algebra, which adds a ring structure to a module. **It seems like there isn't much of a difference between a ring a an algebra, so you should ask someone about this...**

Definition 2. Let R be a commutative unital ring. An R-**algebra** is an R-module M along with a "multiplication" map

$$\begin{aligned} M \times M &\to M \\ (x, y) &\mapsto xy. \end{aligned}$$

This map distributes over addition and satisfies

$$\lambda(xy) = (\lambda x)y = x(\lambda y).$$

Why is R commutative? We can form more specific types of algebras by putting restrictions on the multiplication map. **Associative and commutative algebras** have associative and commutative multiplication maps, respectively. A **unital** algebra has a multiplicative identity. A **division algebra** is a unital associative algebra in which every nonzero element has a multiplicative inverse.

1.2 SUBMODULES

A module is just an abelian group with a left action, so we can define a submodule to be just a subgroup that respects this action.

Definition 3. A **submodule** of an R-module M is a subgroup of M that is closed under the left action of R on M.

A module N is a submodule of M if and only if N is closed under subtraction and scalar multiplication (the subtraction emcompasses both addition and additive inverses). From this we infer the following simple characterization of a submodule.

Proposition 2. N is an submodule of M if and only if

$$\lambda x + \mu y \in N$$

for all $x, y \in N$ and $\lambda, \mu \in R$.

Thus given any set $S \subseteq M$, we can form a submodule of M by adding in all linear combinations of the elements of S. This could be a good enough definition of $\langle S \rangle$, but we have to make sure that we aren't adding in any unnecessary terms. The following definition ensures this is the case, the next proposition shows that the definition makes sense, and the following theorem shows that our definition is equivalent to the linear combination approach.

Definition 4. Given a set $S \subseteq M$, let $\langle S \rangle$ denote the intersection of all submodules of M containing S.

Proposition 3. If $\{M_\alpha\}_\alpha$ is a family of submodules of M, then $\bigcap_\alpha M_\alpha$ is also a submodule of M.

Theorem 1. Let $S \subseteq M$, and let $LC(S)$ denote the set of all linear combinations of S. Then

$$\langle S \rangle = \begin{cases} \{0\} & \text{if } S = \varnothing, \\ LC(S) & \text{otherwise.} \end{cases}$$

Proof. The case $S = \varnothing$ is clear since all subgroups must contain 0, so assume S is nonempty. It's clear that $LC(S)$ is a submodule of M. Since $S \subseteq LC(S)$, this means $LC(S)$ is a submodule of M containing S, i.e. $\langle S \rangle \subseteq LC(S)$. But every linear combination of S must be in any submodule containing S, so $LC(S) \subseteq \langle S \rangle$ too. Thus $\langle S \rangle = LC(S)$. □

If $\{M_\alpha\}_\alpha$ is a family of submodules of M, then $\bigcup_\alpha M_\alpha$ won't be a submodule in general (unlike $\bigcap_\alpha M_\alpha$), but it can certainly generate one. $\langle \cup_\alpha M_\alpha \rangle$ can be interpreted as the smallest submodule of M containing each of the M_α, and we can construct it by once again filling in all the missing linear combinations. (**recall that all linear combinations must be finite by defn**)

Proposition 4. Let $\mathcal{A}$ be some index set, and let $\mathbb{P}^\star(\mathcal{A})$ denote the set of all nonempty finite subsets of $\mathcal{A}$. Then $\langle \bigcup_\alpha M_\alpha \rangle$ is all finite sums of the form

$$\sum_{\beta \in \mathcal{B}} m_\beta,$$

where $\mathcal{B} \in \mathbb{P}^\star(\mathcal{A})$ and $m_\beta \in M_\beta$.

Proof. All linear combinations of the elements of $\bigcup_\alpha M_\alpha$ is this form, and $LC = \langle \bigcup_\alpha M_\alpha \rangle$ by Theorem 1 since $\bigcup_\alpha M_\alpha$ is nonempty (it must contain 0). □

This motivates the notation

$$\sum_\alpha M_\alpha \doteq \langle \bigcup_\alpha M_\alpha \rangle$$

and the terminology "sum of the family $\{M_\alpha\}_\alpha$."

Theorem 2 (Modular Law)**.** Let M be an R-module, and let A, B, C be submodules of M with $C \subseteq A$. Then

$$A \cup (B + C) = (A \cup B) + C.$$

I have no idea why the book introduced this now.

1.3 MORPHISMS

As usual, an R-morphism respects the structure of R-modules.

Definition 5. An R-**morphism** is a map $f : M \to N$ between R-modules satisfying

1. $f(x + y) = f(x) + f(y)$;
2. $f(\lambda x) = \lambda f(x)$.

Note that if R is a field, then an R-morphism is just a linear map.

Proposition 5. Basic properties an R-morphism $f : M \to N$.

1. $f(0_M) = 0_N$.
2. $f(-x) = -f(x)$.

Because we like to be fancy, we'll use categorical language to describe specific variants of R-morphisms:

$$\begin{aligned} R\text{-monomorphism} : &\qquad M \rightarrowtail N, \\ R\text{-epimorphism} : &\qquad M \twoheadrightarrow N. \end{aligned}$$

It's straightforward to show that the inverse of a bijective R-morphism is also an R-morphism, i.e. an R-isomorphism is just a bijective R-morphism. The usual properties of composed morphisms of course hold too:

- The composition of morphisms/monos/epis is a morphism/mono/epi.
- If $g \circ f$ is mono, then so is f.
- If $g \circ f$ is epi, then so if g.

As you might expect, a map between modules induces maps between their submodules.

Proposition 6. Suppose we have an R-morphism $f : M \to N$. Then for any submodule X of M, the image $f(X)$ is a submodule of N. Additionally, for any submodule Y of N, the preimage $f^{-1}(Y)$ is a submodule of M.

These maps induce maps between the entire submodule lattices $L(M)$ and $L(N)$:

$$\begin{tikzcd} L(M) \arrow[r, bend left, "f^{\rightarrow}"] & L(N) \arrow[l, bend left, "f^{\leftarrow}"] \end{tikzcd} \qquad \begin{aligned} f^{\rightarrow} &: X \mapsto f(X) \\ f^{\leftarrow} &: Y \mapsto f^{-1}(Y) \end{aligned}$$

Note that $f^{\rightarrow}$ and $f^{\leftarrow}$ are inclusion-preserving. We can also show how they interact with each other.

Proposition 7. Let f be an R-morphism $M \to N$. If $A \in L(M)$ and $B \in L(N)$, then

1. $f^{\to}(A \cap f^{\leftarrow}(B)) = f^{\to}(A) \cap B$;
2. $f^{\leftarrow}(B + f^{\to}(A)) = f^{\leftarrow}(B) + A$.

Prove this.

Corollary 1. If $A \in L(M)$ and $B \in L(N)$, then

1. $f^{\to}(f^{\leftarrow}(B)) = B \cap \operatorname{Im} f$;
2. $f^{\leftarrow}(f^{\to}(A)) = A + \operatorname{Ker} f$.

Is there a way to generalize this to something other than modules? If we have a morphism $f : X \to Y$, will $f(x)$ and $f^{-1}(y)$ have that proerty if x and y have the property, respectively?

Is the defn of R-morphism really just saying that it preserves module-ness by respecting linear combs?

f inj: There is a map $g : B \to A$ such that $g \circ f = 1_A$.
f surj: There is a map $g : B \to A$ such that $f \circ g = 1_B$.

1.3.1 LIFTS AND EXTENSIONS OF R-MORPHISMS

It's common to want to extend or lift an R-morphism. The following propositions give criteria for when this is possible.

Proposition 8. Suppose A, B, C are nonempty.

$$\begin{tikzcd}
& B \arrow[d, "f"] \\
C \arrow[ur, dashed, "\exists!\, h"] \arrow[r, "g"] & A
\end{tikzcd}$$

Suppose f is monic. Then there is a unique R-morphism h lifting g if and only if $\operatorname{Im} g \subseteq \operatorname{Im} f$. In this case, h is epic if and only if $\operatorname{Im} g = \operatorname{Im} f$.

Proof. The forward direction of the first statement is clear. To go backwards, note that any c, there is a b such that $g(c) = f(b)$ since $\operatorname{Im} g \subseteq \operatorname{Im} f$. Define h by $c \mapsto b$, then $f(h(c)) = f(b) = g(c)$, so h lifts g. This map is well-defined and unique since f is monic. To show it's an R-morphism, use the morphism properties of f and g to show $f(h(\lambda c)) = f(\lambda h(c))$ and $f(h(c_1 + c_2)) = f(h(c_1) + h(c_2))$, then use the fact that f is monic.

If h is epic, it's straightforward to show that $\operatorname{Im} f \subseteq \operatorname{Im} g$, which proves their equality. Conversely, fix b and suppose $\operatorname{Im} f = \operatorname{Im} g$. Then $f(b) = g(c) = f(h(c))$ for some c, which implies $b = h(c)$ since f is monic. □

Lemma 1. Suppose f and g are R-morphisms. If $\operatorname{Ker} f \subseteq \operatorname{Ker} g$, then

$$f(x) = f(y) \implies g(x) = g(y).$$

Proof. If $f(x) = f(y)$, then $f(x-y) = 0$, so $x - y \in \operatorname{Ker} f \subseteq \operatorname{Ker} g$. Thus $g(x-y) = 0$, so $g(x) = g(y)$. □

Proposition 9. Suppose A, B, C are nonempty.

$$\begin{tikzcd} & B \arrow[d, dashed, "\exists!\ h"] \\ A \arrow[ru, "f"] \arrow[r, "g"] & C \end{tikzcd}$$

Suppose f is epic. Then there is a unique R-morphism h extending g if and only if $\operatorname{Ker} f \subseteq \operatorname{Ker} g$. In this case, h is monic if and only if $\operatorname{Ker} f = \operatorname{Ker} g$.

Proof. The forward direction of the first statement is clear. To go backwards, since f is epic, any b can be written $b = f(a)$ for some a. Then define $h : b \mapsto g(a)$. This clearly lifts g, and it is well-defined and unique by the preceding lemma. Showing it's an R-morphism is a standard check by writing $b = f(a)$ and using the morphism properties of f and g.

If h is monic, then for $a \in \operatorname{Ker} g$, we have $h(f(a)) = g(a) = 0$. But since f is monic, this implies $f(a) = 0$, so $a \in \operatorname{Ker} f$. Thus $\operatorname{Ker} g \subseteq \operatorname{Ker} f$, and we already know the opposite inclusion. Conversely, using the $b = f(a)$ fact, $h(b_1) = b(b_2) \implies g(a_1) = g(a_2)$, so $a_1 - a_2 \in \operatorname{Ker} g = \operatorname{Ker} f$, so $b_1 = f(a_1) = f(a_2) = b_2$. □

1.3.2 EXACT SEQUENCES

We'll start out by noting some obvious characterizations of morphisms in terms of exact sequences. Quick reminder if if a sequence is exact, the composition of any two subsequent morphisms is 0.

Proposition 10. Monos, epis, and isos in terms of exact sequences:

1. f is monic $\iff 0 \to M \xrightarrow{f} N$ is exact.
2. f is epic $\iff M \xrightarrow{f} N \to 0$ is exact.
3. f is iso $\iff 0 \to M \xrightarrow{f} N \to 0$ is exact.

Now to prove that a bunch of diagrams commute. I don't include any diagram chases, but luckily only the Four Lemma needs one.

Proposition 11. The diagram commutes if the row is exact and $\theta g = 0$.

$$\begin{tikzcd}
& & A \arrow[dl, dashed, "\exists!\, h"'] \arrow[d, "g"] & \\
0 \arrow[r] & X \arrow[r, "f"] & Y \arrow[r, "\theta"] & Z
\end{tikzcd}$$

Proof. Our assumptions say that f is monic and $\operatorname{Im} g \subseteq \operatorname{Ker} \theta = \operatorname{Im} f$, so h exists and is unique by Proposition 8. □

Corollary 2. The diagram commutes if $fg = 0$.

$$\begin{tikzcd}
& P \arrow[dl, dashed, "\exists!\, h"'] \arrow[d, "g"] & \\
\operatorname{Ker} f \arrow[r, hook] & M \arrow[r, "f"] & N
\end{tikzcd}$$

Proof. Note that the bottom row is exact. Then we can invoke the previous proposition. □

Theorem 3 (Four Lemma)**.** Suppose the following diagram of R-modules and R-morphisms commutes and has exact rows.

$$\begin{tikzcd}
A \arrow[r] \arrow[d, "\alpha"] & B \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & D \arrow[d, "\delta"] \\
A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & D'
\end{tikzcd}$$

Then the following hold:

1. If α, γ are epic and δ is monic, then β is epic.
2. If α is epic and β, γ are monic, then γ is monic.

Theorem 4 (Five Lemma)**.** Suppose the following diagram of R-modules and R-morphisms commutes and has exact rows.

$$\begin{tikzcd}
A \arrow[r] \arrow[d, "\alpha_1"] & B \arrow[r] \arrow[d, "\alpha_2"] & C \arrow[r] \arrow[d, "\alpha_3"] & D \arrow[r] \arrow[d, "\alpha_4"] & E \arrow[d, "\alpha_5"] \\
A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & D' \arrow[r] & E'
\end{tikzcd}$$

If $\alpha_1, \alpha_2, \alpha_4, \alpha_5$ are iso, then so is α_3.

Proof. Apply the Four Lemma to the first three squares to show that α_3 is monic, and to the last three squares to show that α_3 is epic. Since it's an R-morphism, this is enough to show it's iso. □

Corollary 3. Suppose the following diagram of R-modules and R-morphisms commutes and has exact rows.

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "\alpha"] & B \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

If α, γ are iso, then so is β.

Check D&F about the case ”any two are iso”.

This last corollarly is just a special case of the Five Lemma when our two rows are short exact sequences. **If the D&F case applies here, that would be very useful for determining when a map of SESs is iso.**