FREE MODULES

Throughout, let A be a commutative ring with 1.

1. Basic Definition

Definition 1.1 (Module)**.** *An A-**module** is an abelian group M with a multiplication*

$$A \times M \longrightarrow M, \quad (a, m) \longmapsto am$$

such that for all $a, a' \in A$ and $m, m' \in M$,

$$\begin{aligned} a(m + m') &= am + am', \\ (a + a')m &= am + a'm, \\ a(a'm) &= (aa')m. \end{aligned}$$

The A-module M is **unital** *if*

$$1_A m = m \quad \text{for all } m \in M.$$

The two immediate examples are that any abelian group is a $\mathbb{Z}$-module, and any vector space over a field k is a k-module.

All modules that we encounter will be unital.

2. Mapping Property, Uniqueness

Definition 2.1 (Mapping Property of the Free Module)**.** *Let $\mathcal{S}$ be a set. The* **free A-module on $\mathcal{S}$** *is an A-module M and a map from the set to it,*

$$i : \mathcal{S} \longrightarrow M,$$

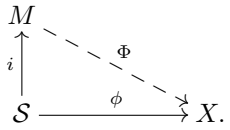
having the following property: For every map from the set to an A-module,

$$\phi : \mathcal{S} \longrightarrow X,$$

there exists a unique A-linear map from the free module to the same module,

$$\Phi : M \longrightarrow X,$$

such that $\Phi \circ i = \phi$, i.e., such that the following diagram commutes,



The definition calls for various comments.

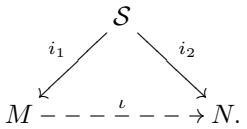
- Although i and ϕ are set maps, Φ is an A-module map. All that is required for Φ to exist as a set map is that i inject, but the issues here are matters of algebraic structure.
- Given $\mathcal{S}$ we do not yet know that the free A-module exists, or that it has any sort of uniqueness property to justify the definite article *the* in its name.
- How satisfactorily the mapping property definition explains the word *free* depends on one's experience and intuition.

The first point to settle is that any two free A-modules on a set $\mathcal{S}$ are naturally isomorphic. Thus, while we still do need to create a free A-module on $\mathcal{S}$ at some point, the specifics of how we do so are spurious.

Proposition 2.2 (Uniqueness of the Free Module)**.** *Let $\mathcal{S}$ be a set. Let M and N be free A-modules on $\mathcal{S}$,*

$$i_1 : \mathcal{S} \longrightarrow M \quad \text{and} \quad i_2 : \mathcal{S} \longrightarrow N.$$

Then there is a unique A-module isomorphism $\iota : M \longrightarrow N$ such that $\iota \circ i_1 = i_2$, i.e., such that the following diagram commutes,



Proof. Since M and N are both free A-modules on $\mathcal{S}$, there are unique A-linear maps

$$\iota : M \longrightarrow N \quad \text{such that } \iota \circ i_1 = i_2$$

and

$$\iota' : N \longrightarrow M, \quad \text{such that } \iota' \circ i_2 = i_1.$$

We want to show that ι is an isomorphism.

The composition

$$\iota' \circ \iota : M \longrightarrow M$$

is an A-linear map such that

$$(\iota' \circ \iota) \circ i_1 = \iota' \circ (\iota \circ i_1) = \iota' \circ i_2 = i_1.$$

The definition says that there is a *unique* such A-linear map, and certainly the identity map on M fits the bill. Thus $\iota' \circ \iota$ is the identity map on M, and similarly $\iota \circ \iota'$ is the identity map on N. The map ι is an isomorphism in consequence. □

3. Generators, Linear Independence

The next result explicates the sense in which the free A-module on a set $\mathcal{S}$ is free.

Proposition 3.1 (Free Module Generators, Their Independence)**.** *Let $\mathcal{S}$ be a set and let $i : \mathcal{S} \longrightarrow M$ be the free A-module on $\mathcal{S}$. Then M is generated by the set $\{i(s) : s \in \mathcal{S}\}$. Furthermore, the generators $i(s)$ are linearly independent, meaning that the only relation*

$$\sum_{s \in S} a_s i(s) = 0_M \quad \textit{each } a_s \in A, \textit{ only finitely many } a_s \textit{ nonzero}$$

is the trivial relation with all $a_s = 0$.

The proposition tells us that the free A-module on $\mathcal{S}$, if it exists at all, must be essentially the finite formal sums $\sum_{s \in \mathcal{S}} a_s s$ with all $a_s \in A$. The problem here is that *finite formal sum* and products as of ring-elements by set-elements are not strictly legitimate within algebraic formalism. We will work around the problem soon.

Proof. Let M_o be the A-submodule of M generated by $\{i(s) : s \in \mathcal{S}\}$, let $Q = M/M_o$ be the quotient, and let $q : M \longrightarrow Q$ be the quotient map. Also, let $z : \mathcal{S} \longrightarrow Q$ and $Z : M \longrightarrow Q$ be the zero maps. Certainly

$$Z \circ i = z,$$

but also, since $i(\mathcal{S}) \subset M_o$,

$$q \circ i = z.$$

Thus the uniqueness statement in the mapping property of the free module gives $q = Z$. In other words, M_o is all of M.

As for the second statement in the proposition, suppose that

$$\sum_{s \in S} a_s i(s) = 0_M \quad \text{each } a_s \in A, \text{ only finitely many } a_s \text{ nonzero.}$$

Fix $\tilde{s} \in \mathcal{S}$ and define

$$\phi : \mathcal{S} \longrightarrow A, \quad s \longmapsto \begin{cases} 1 & \text{if } s = \tilde{s}, \\ 0 & \text{if } s \neq \tilde{s}. \end{cases}$$

Let $\Phi : M \longrightarrow A$ be the associated A-module homomorphism. Then

$$a_{\tilde{s}} = \sum_s a_s \phi(s) = \sum_s a_s (\Phi \circ i)(s) = \Phi(\sum_s a_s i(s)) = \Phi(0_M) = 0_A.$$

Since $\tilde{s}$ is arbitrary, the linear combination $\sum_s a_s i(s)$ is trivial. □

The proposition shows that in particular if the ring A is a field k then the free k-module on S is the k-vector space having basis $\{i(s) : s \in \mathcal{S}\}$. We will use this fact in the next section.

4. Invariance of Rank

Although we still don't have the free A-module on a set S, we use the characteristic mapping property to show, knowing no specifics about its construction, that its rank is well defined. The relevant underlying result is the nontrivial fact that the dimension of a vector space is well defined.

In the ring-with-unit A there exists a maximal ideal J and thus A projects to the field $k = A/J$ (if A is already a field then $J = \{0\}$). To see this, consider a chain of proper ideals,

$$J_1 \subset J_2 \subset \cdots .$$

Let $J = \bigcup_i J_i$. The fact that J is again an ideal of A is straightforward to verify. The point is that $J \subsetneq A$, and the argument is that if $1 \in J$ then $1 \in J_j$ for some j, contrary to our assumption.

Also, given an ideal J of A, not necessarily maximal, any A-module N that is annihilated by J can be viewed as an A/J-module because the action

$$(a + J)n = an$$

is well defined; and conversely any A/J-module N can be viewed as an A-module that is annihilated by J by turning the definition around,

$$an = (a + J)n.$$

We use these ideas in the next argument.

Proposition 4.1 (Invariance of Rank)**.** *Suppose that $\mathcal{S}$ is finite, and that the free A-module $i : \mathcal{S} \longrightarrow M$ also takes the form $j : \mathcal{T} \longrightarrow M$. Then $|\mathcal{S}| = |\mathcal{T}|$.*

Proof. Let J be a maximal proper ideal of A, so that A/J is a field k. Let

$$JM = \{\text{finite sums } \sum j_\alpha m_\alpha \text{ with each } j_\alpha \in J,\, m_\alpha \in M\},$$

and consider the quotient and the quotient map

$$V = M/JM, \qquad q : M \longrightarrow V.$$

The quotient has a k-vector space structure,

$$(a + J)(m + JM) = am + JM,$$

and it also can be viewed as an A-module that is annihilated by J,

$$a(m + JM) = am + JM.$$

Note that the construction of V has made no reference to either of the maps $i : \mathcal{S} \longrightarrow M$ and $j : \mathcal{T} \longrightarrow M$. We claim that

$$q \circ i : \mathcal{S} \longrightarrow V$$

is a free k-module on $\mathcal{S}$. Granting the claim, $|\mathcal{S}| = \dim_k V$ and similarly $|\mathcal{T}| = \dim_k V$, giving $|\mathcal{S}| = |\mathcal{T}|$ as desired. As mentioned already, the fact that $\dim_k V$ is well defined is itself nontrivial.

To prove the claim, consider any map

$$\phi : \mathcal{S} \longrightarrow W, \quad W \text{ a } k\text{-vector space.}$$

View W as an A-module that is annihilated by J-multiplication,

$$aw = (a + J)w, \quad a \in A,\ w \in W.$$

Then there is a unique A-linear map

$$\Psi : M \longrightarrow W, \quad \Psi \circ i = \phi.$$

Since multiplication by J annihilates W, we have for all $j \in J$ and $m \in M$,

$$\Psi(jm) = j\Psi(m) = 0_W.$$

That is, $JM \subset \ker(\Psi)$, and so there is a map

$$\Phi : V \longrightarrow W, \quad \Phi \circ q = \Psi.$$

Thus $\Phi \circ (q \circ i) = (\Phi \circ q) \circ i = \Psi \circ i = \phi$. The definition

$$\Phi(m + JM) = \Psi(m)$$

combines with the A-linearity of Ψ to show that Φ is k-linear, and the argument is complete. □

5. Additivity of Rank

Proposition 5.1 (Additivity of Rank)**.** *Let $\mathcal{S}$ and $\mathcal{T}$ be disjoint sets. Suppose that $i : \mathcal{S} \longrightarrow M$ and $j : \mathcal{T} \longrightarrow N$ are free A-modules. Let $i_M : M \longrightarrow M \oplus N$ and $j_N : N \longrightarrow M \oplus N$ be the linear maps in the characterizing mapping property of the coproduct $M \oplus N$. Define*

$$k = \left\{ \begin{matrix} i_M \circ i \text{ on } \mathcal{S} \\ j_N \circ j \text{ on } \mathcal{T} \end{matrix} \right\} : \mathcal{S} \sqcup \mathcal{T} \longrightarrow M \oplus N.$$

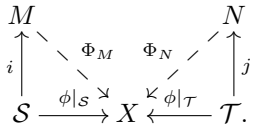
Then $k : \mathcal{S} \sqcup \mathcal{T} \longrightarrow M \oplus N$ is again a free A-module. Thus

$$\operatorname{rank}_A(M \oplus N) = \operatorname{rank}_A(M) + \operatorname{rank}_A(N).$$

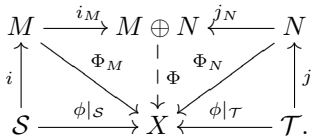
Proof. Since $\mathcal{S}$ and $\mathcal{T}$ are disjoint, any set–map from $\mathcal{S} \sqcup \mathcal{T}$ to an A-module X can be represented as follows,

$$\mathcal{S} \xrightarrow{\phi|_{\mathcal{S}}} X \xleftarrow{\phi|_{\mathcal{T}}} \mathcal{T}.$$

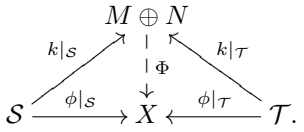
Since $i : \mathcal{S} \longrightarrow M$ and $j : \mathcal{T} \longrightarrow N$ are free, there exist unique linear maps $\Phi_M : M \longrightarrow X$ and $\Phi_N : N \longrightarrow X$ that make the following diagram commute,



The characterizing mapping property of the coproduct $M \oplus N$ is that there exist linear maps $i_M : M \longrightarrow M \oplus N$ and $j_N : N \longrightarrow M \oplus N$ such that any pair of linear maps from M and N to any X factors uniquely through $M \oplus N$. In particular, there exists a unique linear $\Phi : M \oplus N \longrightarrow X$ such that the following diagram commutes,



Consequently, so does the following subdiagram,



The diagram shows a linear $\Phi : M \oplus N \longrightarrow X$ such that $\Phi \circ k = \phi$.

As for uniqueness, any linear map Φ as in the previous diagram gives rise to the linear maps $\Phi \circ i_M : M \longrightarrow X$ and $\Phi \circ j_N : N \longrightarrow X$ such that $\Phi \circ i_M \circ i = \phi|_{\mathcal{S}}$ and $\Phi \circ j_N \circ j = \phi|_{\mathcal{T}}$. Thus $\Phi \circ i_M$ and $\Phi \circ j_N$ are unique since M and N are free, and then Φ is unique by the mapping property of the coproduct.

This proof assumes some construction of the coproduct $M \oplus N$. The usual construction with ordered pairs will do. □

6. Existence

Finally we construct the free A-module on $\mathcal{S}$. The gadget is a small formalism to encode the intuitive idea of finite formal A-linear combinations of $\mathcal{S}$.

Proposition 6.1 (Existence of the Free Module)**.** *Let $\mathcal{S}$ be a set. Then a free A-module on $\mathcal{S}$ exists.*

Proof. Let M be the set of functions

$$f : \mathcal{S} \longrightarrow A, \quad f(s) = 0 \text{ for all but finitely many } s.$$

The addition and scalar-multiplication of such functions is what it must be,

$$\begin{aligned} (f+g)(s) &= f(s) + g(s) \quad \text{for all } s, \\ (af)(s) &= a(f(s)) \qquad\quad \text{for all } s. \end{aligned}$$

In particular, for each $\tilde{s} \in S$, define

$$f_{\tilde{s}} : \mathcal{S} \longrightarrow A, \quad s \longmapsto \begin{cases} 1 & \text{if } s = \tilde{s}, \\ 0 & \text{if } s \neq \tilde{s}. \end{cases}$$

This $f_{\tilde{s}}$ is the stand-in for $\tilde{s}$ itself in the algebraic structure M, of course. Thus, define

$$i : \mathcal{S} \longrightarrow M, \quad i(s) = f_s.$$

To show that this is a free module on $\mathcal{S}$, we must verify the desired mapping property. Thus, consider any map from $\mathcal{S}$ to an A-module,

$$\phi : \mathcal{S} \longrightarrow X.$$

Define, correspondingly,

$$\Phi : M \longrightarrow X, \quad \Phi(f) = \sum_{s \in \mathcal{S}} \phi(s) f(s).$$

The linearity of Φ is straightforward to verify. For example,

$$\begin{aligned} \Phi(f+g) &= \sum_{s \in \mathcal{S}} \phi(s)(f+g)(s) = \sum_{s \in \mathcal{S}} \phi(s)(f(s) + g(s)) \\ &= \sum_{s \in \mathcal{S}} (\phi(s) f(s) + \phi(s) g(s)) = \sum_{s \in \mathcal{S}} \phi(s) f(s) + \sum_{s \in \mathcal{S}} \phi(s) g(s) \\ &= \Phi(f) + \Phi(g). \end{aligned}$$

And similarly $\Phi(af) = a\Phi(f)$. Especially, for any $\tilde{s} \in \mathcal{S}$,

$$\Phi(i(\tilde{s})) = \Phi(f_{\tilde{s}}) = \sum_{s \in \mathcal{S}} \phi(s) f_{\tilde{s}}(s) = \phi(\tilde{s}).$$

And clearly Φ is only possible linear map from M to X such that $\Phi(f_s) = \phi(s)$ for all s. □

To repeat, the argument has shown that the intuitive notion of *finite formal A-linear combinations* has a precise construction as an A-module with no reference to undefined terms.