Universal Properties and Resolutions of Modules

1 Recap: Definitions

Definition 1.1. Let R be a ring. We say an abelian group $(M, +)$ is an R-module if and only if there is a map $\cdot : \mathbb{R} \times M \to M$, $(r, m) \mapsto r \cdot m$ such that for all $m, n \in M$ and $r, s \in \mathbb{R}$ we have:

1. $1 \cdot m = m$
2. $(r + s) \cdot m = r \cdot m + s \cdot m$
3. $r \cdot (m + n) = r \cdot m + r \cdot n$
4. $(rs) \cdot m = r \cdot (s \cdot m)$

Note that any ring R is an R-module over itself.

Definition 1.2. Let $\{M_i\}_{i \in \Delta}$ are R-modules, then the direct sum of these modules is defined to be

$$\bigoplus_{i \in \Delta} M_i = \{(m_i) \mid m_i \in M_i \text{ and all but finitely many } m_i = 0\}.$$

Note that if we are taking the sum of submodules M_i we say that the sum is direct if every $m \in \bigoplus_{i \in \Delta} M_i$has a unique representation as $m = \sum_{i \in \Delta} m_i$, where $m_i \in M_i$. The scalar multiplication in $\bigoplus_{i \in \Delta} M_i$ is done component wise, for example if Δ is countable we have $r \cdot (m_1, m_2, \dots) = (r \cdot m_1, r \cdot m_2, \dots)$.

Definition 1.3. Let M and N be R-modules, then a map $\varphi : M \to N$ is called a R-module homomorphisms if the following properties hold

1. $\varphi(m + n) = \varphi(m) + \varphi(n)$
2. $\varphi(r \cdot m) = r \cdot \varphi(m)$

for all $m, n \in M$ and $r \in R$. Moreover, we call φ an isomorphism if it is bijective. In this case was say that M and N are isomorphic, denoted $M \cong N$.

We will be denoting the set of all R-module homomorphisms from M to N, two R-modules by $\mathrm{Hom}_R(M, N)$. If we define addition in $\mathrm{Hom}_R(M, N)$ by $(f + g)(x) = f(x) + g(x)$ and scalar multiplication as $(r \cdot f)(x) = r \cdot f(x)$ we have that $\mathrm{Hom}_R(M, N)$ is an R-module.

Definition 1.4. Suppose that $B \subseteq M$, then we say that B is a basis if B generates M and the elements of B are linearly independent. I.e. every element $m \in M$ can be written as a linear combination of elements in B with coefficients in R and for every finite subset of $\{e_1, \dots, e_n\} \subseteq B$ the sum $\sum_{i=1}^n r_i e_i = 0$ implies $r_i = 0$ for all $1 \le i \le n$.

Definition 1.5. An R-module F is said to be a free module if $F \cong \bigoplus_{i \in \Delta} R_i$, where $R_i \cong R$. Equivalently, we can say that F is a free R-module if F has a free basis.

For an example of a free module take R a commutative ring with unity and let A be a set. Define

$$R^{\bigoplus A} = \{(r_a)_{a \in A} \mid r_a \neq 0 \text{ for finitely man indices } a \in A\}$$

with component-wise addition and the usual scalar multiplication. Note that the set $\{e_a\}$ for $a \in A$ is a basis of $R^{\bigoplus A}$, where e_a is the sequence of all zeros except for 1 in the a-th component.

Proposition 1.1 (Universal Property of Free Modules)**.** *Every R-module is the homomorphic image of a free module.*

Proof. Suppose that M is an R-module and that $f : A \to M$ is any function. Define $\iota : A \to R^{\bigoplus A}$, $\iota(a) = e_a$. Then we can define $g : R^{\bigoplus A} \to M$ by

$$g((r_a)_{a\in A}) = \sum_{a\in A} r_a f(a)$$

Note that g is indeed a module homomorphism since

$$g((r_a)_{a\in A} + (s_a)_{a\in A}) = g((r_a)_{a\in A}) + g(s_a)_{a\in A})$$

and

$$g(r(r_a)_{a\in A}) = rg((r_a)_{a\in A}).$$

Moreover, note that $f = g \circ \iota$. □

Free modules sometimes behave like vector spaces, for example Chris showed last time that.

Proposition 1.2. *Suppose that M is finitely generated free R-modules, i.e. have a finite basis, then every basis of M has the same number of elements.*

2 Tying Up Loose Ends: Exact Sequences

Let us direct our attention to exact sequences for a moment.

Definition 2.1. Suppose $\{M_n\}_{n\in\mathbb{N}}$ is a sequence of R-modules and $\varphi_n : M_n \to M_{n-1}$ are an R-module homomorphisms such that $\varphi_n\varphi_{n+1} = 0$ (equivalently $\mathrm{im}(\varphi_{n+1}) \subseteq \ker(\varphi_n)$), then the sequence

$$\dots \xrightarrow{\varphi_{n+2}} M_{n+1} \xrightarrow{\varphi_{n+1}} M_n \xrightarrow{\varphi_n} M_{n-1} \xrightarrow{\varphi_{n-2}} \dots$$

is called a complex. Moreover, if $\mathrm{im}(\varphi_{n+1}) = \ker(\varphi_n)$ we say the sequence is exact at M_n and if the sequence is exact for every $n \in \mathbb{N}$ we call the sequence an exact sequence.

Not all sequences have to have infinite length.

Definition 2.2. A short exact sequence is a sequence

$$0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$$

that is exact.

From our definition of exact sequences we have that

1. $\ker(\varphi) = 0$
2. $\mathrm{im}(\psi) = C$
3. $\ker(\psi) = \mathrm{im}(\varphi)$

so every short sequence must have these properties. For an example of an short exact sequence consider N a submodule of an R-module M then the following sequence is exact:

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\pi} C \longrightarrow 0$$

where ι maps $n \mapsto n$ and π maps $m \mapsto \overline{m}$. For another example, let $\varphi : M \to N$ be an R-module homomorphism then the sequence

$$0 \longrightarrow \ker(\varphi) \xrightarrow{\iota} M \xrightarrow{\varphi} \mathrm{im}(M) \longrightarrow 0$$

is exact, where ι maps $m \mapsto m$.

The following proposition gives a way of creating new exact sequences from exact sequences.

Proposition 2.1 (Splitting and Gluing of Exact Sequences). *1. Suppose that*

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \xrightarrow{\varphi_3} M_4$$

is an exact sequence of R-modules, then

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} N \xrightarrow{\iota} 0 \qquad \textit{and} \qquad 0 \longrightarrow N \longrightarrow M_3 \xrightarrow{\varphi_3} M_4$$

are also exact, where $N = im(\varphi_2) = \ker(\varphi_3)$ and iota is the inclusion map.

2. *Conversely, if*

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} N \xrightarrow{\iota} 0 \qquad \textit{and} \qquad 0 \longrightarrow N \longrightarrow M_3 \xrightarrow{\varphi_3} M_4$$

are exact, with N a submodule of M_3, then the sequence

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \xrightarrow{\varphi_3} M_4$$

is exact.

Note that Chris has some nice results in the notes of his talk about how sequences and Noetherian modules interact.

Lastly to finish of this section let us introduce a last definition that we will need to define projective R-modules.

Definition 2.3. A short exact sequence

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

is called a split exact sequence if the sequence is isomorphic to the sequence

$$0 \longrightarrow A \xrightarrow{\iota} A \bigoplus C \xrightarrow{\varphi} C \longrightarrow 0$$

where ι is the natural inclusion and there exists $f : B \to A \bigoplus C$ such that $f\alpha = \iota$ and $\varphi f = \beta$.

3 New Stuff: Projective Modules

Free modules are the closest we get to vector spaces however the having a basis in our module can be hard to come by as we have seen in our last presentation. Therefore, let us generalize the idea of free modules.

Definition 3.1. (Lifting Property) An R-module P is called projective if for every surjective module homomorphism $\varphi : N \to M$, two R-modules, and every module homomorphism $\psi : P \to M$ there exists a module homomorphism $\sigma : P \to N$ such that $\varphi\sigma = \psi$. As a commutative diagram we have

$$\begin{array}{ccc} & & N \\ & \overset{\sigma}{\nearrow} & \downarrow \varphi \\ P & \xrightarrow{\psi} & M \end{array}$$

Projective modules were first introduced by Cartan and Eilenberg in 1956. Here are two other equivalent definitions:

Definition 3.2. An R-module P is projective if and only if every short sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0$$

is a splitting exact sequence. In other words, there exists a R-module homomorphism $\sigma : P \to M$ such that $\varphi\sigma = id_p$ for every $\varphi : B \to P$ surjective.

Definition 3.3. An R-module P is projective if and only if there is another R-module Q such that $P \bigoplus Q$ is a free R-module.

Note that every free module is a projective module by this last definition. However, projective modules are not always free. For example in a Dedekind ring free modules are not free. Thereofore, a question of interest is when do we have the that projective modules are free modules.

Theorem 3.1 (Quillen-Suslin, 1976)**.** *Every finitely generated projective module over a polynomial ring is free.*

More generally, we have the following theorem.

Theorem 3.2. *Every projective module is a free module in a principle ideal domain.*

4 Setup for Dylan: Local Rings

One of the topics of interest for future talks in local rings so let us define them here.

Definition 4.1. A ring is called local if it has a unique maximal ideal. We usually denote a local ring as an ordered pair $(R, \mathfrak{m})$, where $\mathfrak{m}$ is the unique maximal idea.

Theorem 4.1. *A ring is local if and only if the set of non-units is an idea of R.*

Proof. ($\Longrightarrow$) Suppose that $(R, \mathfrak{m})$ is a local ring and let $I = R \setminus U(R)$. Let $a, b \in I$, then $\langle a \rangle$ and $\langle b \rangle$ are proper ideals of R since $1 \notin \langle a \rangle$ and $1 \notin \langle b \rangle$. Since $\mathfrak{m}$ is maximal we have that $\langle a \rangle, \langle b \rangle \subseteq \mathfrak{m}$. Thus $a, b \in \mathfrak{m}$. Moreover, $a - b \in \mathfrak{m}$ and hence $a - b \notin U(R)$ since if it was $\mathfrak{m} = R$ which is a contradiction. Thus, $a - b \in I$.

Now let $r \in \mathbb{R}$. Note since $a \in \mathfrak{m}$ we have that $ra \in \mathfrak{m}$. With similar reasoning to above we have that $ra \in I$.

($\Longleftarrow$) Note that $1 \notin I$ so I is a proper ideal of R. Let M be an arbitrary maximal ideal then we have that $M \subseteq I$. Since M is maximal $M = I$. □

Theorem 4.2. *Suppose R is a ring with a maximal ideal $\mathfrak{m}$. If every element of $1 + \mathfrak{m}$ is a unit of R then R is a local ring.*

Proof. Let $a \in R \setminus \mathfrak{m}$ then $\mathfrak{m} \subset \langle a \rangle + \mathfrak{m}$. By maximality of $\mathfrak{m}$ we have $\langle a \rangle + \mathfrak{m} = R$. Since $\langle a \rangle + \mathfrak{m} = R$ we have that $1 \in \langle a \rangle + \mathfrak{m}$ so there exists $r \in R$ and $m \in \mathfrak{m}$ such that $ra + m = 1$ thus $ra = 1 - m$. This gives us that $ra \in 1 + \mathfrak{m}$ so ra is a unit making a a unit. Therefore $\mathfrak{m} = R \setminus U(R)$ and by the previous theorem R is a local ring. □

As for some examples of local rings we have

1. Note that every field is a local ring since the only idea of a field is 0.
2. The ring $\mathbb{Z}/p^n\mathbb{Z}$ has a maximal ideal of $\langle p \rangle$.
3. $R[[x]]$ the formal power series of over a local ring is local. The maximal idea is the non-units, i.e. the elements with a constant term.

The following result is the connection will connect local rings with projective modules.

Theorem 4.3 (Kaplansky's Theorem on Projective Modules,)**.** *A projective module over a local ring is free.*

Note that the proof of this statement using the Rank-Nullity Theorem and Nakayama's Lemma and shoes that P is a finitely generated projective module over $(R, \mathfrak{m})$.

Theorem 4.4 (Characterization of Local Rings)**.** *Let R be a ring. Then the following are equivalent.*

1. *R is a local ring.*
2. *Every projective module over R is free and has an indecomposable decomposition $M = \bigoplus_{i \in I} M_i$ such that for each maximal direct summand L of M, there is a decomposition $M = (\bigoplus_{j \in J} M_j) \bigoplus L$ for some subset $J \subseteq I$.*

5 We Got Here: Projective Resolutions

Definition 5.1. Given an R-module M, we say the infinite sequence of modules P_i

$$\cdots \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

is a projective resolution if the sequence is exact and P_i is projective for all i.

The usual example of a projective resolution is the Koszul complex of a regular sequence, which is a free resoltion of the idea genereated by the sequence.

Note that this sequence usually gets abbreviated to $P. \to M \to 0$. Moreover, we say that this infinite sequence is finite if there is a $P_n \neq 0$ such that for all $P_m = 0$ for all $m \geq n$. In this case the exact sequence has the following form:

$$\cdots \longrightarrow 0 \longrightarrow \cdots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow P_2 \longrightarrow P_1 \longrightarrow 0$$

Definition 5.2. The length of a finite projective resolution the n described above.