M3P8 LECTURE NOTES 7: R-MODULES

1. Definitions

Definition 1.1. An *R-module* M is an abelian group (with operation denotes $+_M$ or simply $+$) together with an multiplication law: $R \times M \to M$ such that:

(1) $r(m_1 + m_2) = rm_1 + rm_2$ for all $r \in R$, $m_1, m_2 \in M$,
(2) $(r + s)m = rm + sm$ for all $r, s \in R$, $m \in M$,
(3) $(rs)m = r(sm)$ for all $r, s \in R$, $m \in M$, and
(4) $1_R m = m$ for all $m \in M$.

Example 1.2. The multiplication and addition on R naturally makes R into an R-module. More generally, any ideal of R is an R-module.

Example 1.3. If $f : R \to S$, then f makes S into an R-module, where the addition is addition in S, and the multiplication law is defined by $r \cdot s = f(r)s$. In particular any quotient R/I is an R-module.

Example 1.4. Let $R = \mathbb{Z}$, and let M be an abelian group. The M has the unique structure of a $\mathbb{Z}$-module, as follows: property (2) from the module axioms shows that for any n in $\mathbb{Z}_{\geq 0}$ and $m \in M$, $nm = m+m+\ldots m$, where there are n summands on the right. Similarly $(-n)m = -(m + m + \ldots m)$. Thus the multiplication law $\mathbb{Z} \times M \to M$ is forced on us, and one checks that it does satisfy properties (1) - (4) above. Informally, we say that abelian groups "are" $\mathbb{Z}$-modules.

Example 1.5. If R is a field, then R-modules are just R-vector spaces.

Example 1.6. Let S be a set, and let M be the set of R-valued functions $f : S \to R$. We add and multiply pointwise: $f + f'$ is the function that takes $s \in S$ to $f(s) + f'(s)$, and rf is the function that takes s to $rf(s)$. This is clearly an R-module. Also of interest is the submodule F_S of M that consists of functions $f : S \to R$ such that $f(s) = 0_R$ for all but finitely many s. The module F_S is called the *free R-module on the set S* and will be very important for us.

2. Submodules, Quotients, and Direct Sums

Let M be an R-module. A subset N of M is an *R-submodule* of M if N is an additive subgroup of M, and for all $n \in N$, $r \in R$, we have $rN \in N$. If S is any subset of N, we define the R-submodule of M generated by S to be the set of all elements of M of the form $r_1 s_1 + r_2 s_2 + \cdots + r_n s_n$, where the r_i are elements of R and the s_i are elements of S. It is the smallest R-submodule of M containing S.

Definition 2.1. An R-module M is *finitely generated* if there is a finite subset S of M such that the R-submodule of M generated by S is all of M.

Let M be a module and N an R-submodule of M. Then we say two elements m, m' of M are *congruent modulo* N if their different $m - m'$ lies in N. This is easily seen to be an equivalence relation, and the equivalence classes are the cosets $m + N$, for $m \in M$.

The set of equivalence classes is denoted M/N; it has the natural structure of an R-module, where $(m+N)+(m'+N) = (m+m')+N$ and $r(m+N) = rm + N$. This module is called the *quotient of M by N*.

Given two modules M and N, the direct sum $M \oplus N$ is the set of ordered pairs (m, n) with $(m, n)+(m', n') = (m+m', n+n')$ and $r(m, n) = (rm, rn)$ for $m, m' \in M$, $n, n' \in N$ and $r \in R$.

Example 2.2. Let M be an R-module and I an ideal of R. Then we can form the submodule IM of M consisting of all elements of M of the form $i_1m_1 + i_2m_2 + \cdots + i_rm_r$ where the i_r are in I and the m_r are in M. This is a submodule of M, so we can form the quotient M/IM. Then M/IM is certainly an R-module, but it is also an R/I-module: one can define a multiplication $R/I \times M/IM \to M/IM$ by $(r+I)(m+IM) = (rm+IM)$. As always one has to check that this is well-defined, but this is straightforward: we need that if $r - r'$ lies in I, and $m - m'$ lies in IM, then $rm - r'm'$ lies in IM. But $rm - r'm' = (r - r')m + r'(m - m')$ which is clearly in IM.

3. Module homomorphisms, Kernels, and Images

Definition 3.1. A map $f : M \to N$ of R-modules is called a *homomorphism of R-modules* if f is a homomorphism of the underlying abelian groups and $f(rm) = rf(m)$ for all $r \in R$ and $m \in M$. The *kernel* of f is the set $\{m \in M : f(m) = 0\}$, and the image of f is the set $\{n \in N : \exists m \in M : f(m) = n\}$.

It is easy to see that the kernel and image of a homomorphism of R-modules $f : M \to N$ are submodules of M and N, respectively.

Note that in particular there is a natural homomorphism from M to M/N, taking m to $m + N$. This homomorphism has the following 'universal property', exactly analogous to the universal property of the quotient construction for rings:

Proposition 3.2. *Let N be a submodule of M, and let $f : M \to M'$ be an R-module homomorphism whose kernel contains N. Then there is a unique homomorphism $\overline{f} : M/N \to M'$ such that $\overline{f}(m+N) = f(m)$ for all $m \in M$. In particular the kernel of $\overline{f}$ is the image of* $\ker f$ *in M/N.*

Proof. The proof is identical to that for quotient rings, and will be omitted. □

4. Free Modules

Definition 4.1. Let M be an R-module. A subset S of M is a *basis* for M if the following two conditions hold:

- S *spans* M; that is, the R-submodule of M generated by S is all of M, and
- S is *linearly independent*; that is, for any collection $s_1, \dots, s_n$ of *distinct* elements of S, and any $r_1, \dots r_n \in R$, $r_1 s_1 + \cdots + r_n s_n$ is nonzero in M unless all r_i are zero.

A module M that has a basis is called a *free* R-module. The cardinality of the basis is called the *rank* of M over R.

Remark 4.2. If R is a field, then the notion of a basis for an R-module coincides with the usual notion for vector spaces. In this case (at least if one assumes the Axiom of Choice) every R-module has a basis. When R is not a field only very special modules have bases; for instance any quotient R/I of R, for I a nonzero ideal, has no basis.

Example 4.3. The ring R is a free module of rank one over R, with basis $\{1_R\}$. More generally any unit $u \in R^\times$ gives a basis of R as an R-module.

Recall that the free module F_S on a set S was defined to be the set of functions $f : S \to R$ such that $f(s) = 0$ for all but finitely many $s \in S$. For each $s \in S$, we have an element e_s of F_S defined by $e_s(t) = 0$ for all $t \in S$ with $t \neq s$, $e_s(s) = 1$. Then the e_s form a basis for F_S. In particular, given $f \in M$, let $s_1, \dots, s_n$ be the set of elements in S on which f is nonzero. Then f can be written as $f(s_1)e_{s_1} + f(s_2)e_{s_2} + \cdots + f(s_n)e_{s_n}$, so the e_s span F_S. On the other hand, for all $s_1, \dots, s_n \in S$ distinct, $\sum r_i e_{s_i}$ takes the value r_i at s_i for all i, and thus is only the zero function when all r_i are zero. Thus F_S is free, justifying its name.

Proposition 4.4. *Let M and N be free modules. Then $M \oplus N$ is free. Moreover, if M and N are free of ranks r and s respectively, then $M \oplus N$ is free of rank $r + s$.*

Proof. If S is a basis for M and T is a basis for N, one easily checks that the set of elements of $M \oplus N$ of the form $(s, 0)$ for $s \in S$ or $(0, t)$ for $t \in T$ is a basis for $M \oplus N$, which immediately proves the claim. □

Free modules have the following universal property:

Proposition 4.5. *Let F_S be the free R-module on a set S. Then for any R-module N, and any map* of sets *$g : S \to N$, there is a unique homomorphism of R-modules $\phi_g : F_S \to N$ such that $\phi_g(e_s) = g(s)$ for all $s \in S$.*

Proof. Define ϕ_g by $\phi_g(f) = \sum_{s \in S} f(s)g(s)$; note that this is a finite sum since all but finitely many s have $f(s) = 0$. Then it is clear that this is an R-module homomorphism. On the other hand suppose ψ is any other map $F_S \to N$ with $\psi(e_s) = g(s)$ for all s. Then we can write $f = \sum f(s)e_s$ (again a finite sum), so $\psi(f) = \sum f(s)g(s) = \phi_g(s)$, so uniqueness is clear. □

The image of ϕ_g is the submodule of N generated by the elements $g(s)$, for $s \in S$.

Corollary 4.6. *Any two free modules of the same rank are isomorphic.*

Proof. Let M be a free module and S a basis for M. Let T be any set of the same cardinality as S, and let $g : T \to S$ be any bijection. Then there is a map $\phi_g : F_T \to M$ such that $\phi_g(e_t) = g(t)$. Since elements of S are linearly independent, this map is injective; since elements of S span M, this map is surjective. Thus M is isomorphic to F_T. Since M was arbitrary, any module of rank equal to the cardinality of T is isomorphic to F_T and the result follows. □

5. Generators and Relations

Now let M be any R-module, and let S a subset of M generating M. Then we have a natural map $F_S \to S$ taking e_s to s for all $s \in S$, and this map is surjective. Let K be the kernel of this map. Elements of K are called *relations* among S. Explicitly, an element of K is a map $f : S \to R$ such that $f(s) = 0$ for all but finitely many s, and $\sum f(s)s = 0$. In other words, each element of K encodes a linear relation among the elements of S; it is a measure of how far the elements of S are from being linearly independent.

Let T be a subset of K that generates K. Then in the same was as above, we get a surjection: $F_T \to K$ taking e_t to t. Composing with the inclusion of K in F_S gives us a map $\phi : F_T \to F_S$ whose image is K.

The map $F_S \to M$ identifies M with the quotient F_S/K, and hence with $F_S/\phi(F_T)$. A description of a module as a quotient of a free module by the image of a map of free modules is called a *presentation* of M; if both modules have finite rank the presentation is called *finite*. A module that has a finite presentation is called *finitely presented*.

Put another way, a presentation is a description of a module M in terms of:

- a generating set S for M, and
- a generating set T for the linear relations satisfied by S.

When S and T are finite we can encode a presentation in a matrix, called the *presentation matrix*. Write $S = \{s_1, \dots, s_n\}$ and $T = \{t_1, \dots t_m\}$. Then for each i we can write $\phi(t_i)$ as a sum $\sum r_{ij} e_{s_j}$, and let A be the m by n matrix whose i, j entry is r_{ij}. Then A gives a map from $R^m \to R^n$, and the quotient of R^n by the submodule AR^m of R^n is isomorphic to M.