Lecture 28: Fields, Modules, and vector spaces

1. Modules

Just as groups act on sets, rings act on *abelian groups*. When a ring acts on an abelian group, that abelian group is called a *module* over that ring.

Now, when a group acts on a set, it had to act by bijections, so it had to respect the property, for instance, of the *cardinality* of the set. But for a ring to act on an abelian group, it respects a different structure—the structure of *addition* built into the abelian group. This is condition (1) in the definition below.

In this lecture, we'll set up all the definitions for the algebra of modules, just as we did for groups.

Definition 28.1. Let R be a ring, and let M be an abelian group. A *left action* of R on M is a function

$$R \times M \to M, \qquad (r,m) \mapsto rm$$

such that for all $r, s \in R$ and $m, m' \in M$, we have

(1) $r(m+m') = rm + rm'$
(2) $(r+s)m = rm + sm$.
(3) $s(rm) = (sr)m$.
(4) $1m = m$

When a left action of R on M is specified, we say that M is a *left R-module.*

Remark 28.2. Again, you should think of "multiplying by r" as scaling by some ring element. So a module is just some set with an addition, together with a notion of scaling by r.

Chit-chat 28.3. As you'll see in your homework, there's a much more succinct way to put all this. The above is the same data as a ring homomorphism $R \to \text{End}(M)$.

Chit-chat 28.4. A *right* R-module is an abelian group M together with a function $M \times R \to M$ satisfying the analogoes of (1) - (4) above.

Chit-chat 28.5. Now this might seem like a lot of data, because we have both R and M floating around. In practice, we often fix a single ring R, and just study relationships between the different M.

Exercise 28.6. Let M be a left R module. Then

$$0m = m \qquad \text{and} \qquad (-r)m = -(rm).$$

Proof. For emphasis, we will write 0_R to denote the zero element of R. Then we have By (2), we have that

$$0_R m = (0_R + 0_R)m = 0_R m + 0_R m$$

so by the cancellation law, we have that

$$0 = 0_R m$$

where on the left hand side, 0 is the additive identity of M. Similarly,

$$rm + (-r)m = (r - r)m = 0_R m = 0.$$

□

Example 28.7. (a) Let $R = \mathbb{R}$, and let $M = \mathbb{R}^n$, an n-dimensional vector space over the real numbers. Then we have a function

$$\mathbb{R} \times M \to M, \qquad (t, v) \mapsto t\vec{v}$$

i.e., we scale by t. So if $\vec{v} = (v_1, \ldots, v_n)$,

$$t\vec{v} = (tv_1, \ldots, tv_n).$$

This satisfies all the properties above.

(b) Any ring R is a left module over itself.

(c) This is an example that departs from the naivete of "scaling," and hits closer to home to the notion of "acting." Let $\mathbb{R}[t]$ be the polynomial ring over $\mathbb{R}$ with variable t. Choose an $m \times m$ matrix T, which we think of as a linear map $T : \mathbb{R}^m \to \mathbb{R}^m$. Then $\mathbb{R}^m$ is a left $\mathbb{R}[t]$-module by the action

$$(a_0 + a_1 t + \ldots + a_k t^k)v := a_0 v + a_1 T(v) + \ldots + a_k (T \circ \ldots \circ T)(v)$$

where the composition $T \circ \ldots \circ T$ happens k times.

2. $\mathbb{Z}$-modules are the same thing as abelian groups

Proposition 28.8. Every abelian group has a unique structure of a left $\mathbb{Z}$-module. In other words, a left $\mathbb{Z}$-module is the same thing as an abelian group.

Proof. Let M be a left $\mathbb{Z}$-module, and fix elements $n \in \mathbb{Z}$, $x \in M$. By property (4) and (2), we have that

$$nx = (1 + \ldots + 1)x = 1x + \ldots + 1x = x + \ldots + x.$$

On the other hand, by the exercise, we know

$$(-n)x = -(x + \ldots x).$$

So the function $\mathbb{Z} \times M \to M$ is determined completely by the abelian group structure of M. □

3. Submodules

Definition 28.9. Let R be a ring and let M be a left R-module. Then an abelian subgroup $M' \subset M$ is called a *submodule* of M if for every $r \in R$, we have

$$x \in M' \implies rx \in M'$$

Example 28.10. (a) If $R = \mathbb{R}$ and $M = \mathbb{R}^n$, a submodule is a subset closed under addition, inverses, and scaling. This is the same thing as a linear subspace of $\mathbb{R}^n$.

(b) Let R be a commutative ring. Then $I \subset R$ is an ideal if and only if it is a submodule of R.

(c) Let $M = \mathbb{R}^m$ be a module over $\mathbb{R}[t]$ given by a linear transformation $T : \mathbb{R}^k \to \mathbb{R}^k$. Then a submodule is a linear subspace V such that $T(V) \subset V$. In other words, it is a *T-invariant subspace* of V.

4. Module homomorphisms

Definition 28.11. Let M and N be left R-modules. Then an R-module homomorphism, or a *map of R-modules*, or a *module homomorphism*, is a function

$$f : M \to N$$

such that f is a group homomorphism, and

$$f(rx) = rf(x)$$

for all $r \in R, x \in M$.

An R-module *isomorphism* is a homomorphism which is a bijection.

Definition 28.12. The *kernel* and *image* of an R-module homomorphism $f : M \to N$ is the kernel and image of f as a group homomorphism.

Chit-chat 28.13. This means $\ker(f) = \{x \text{ such that } f(x) = 0\}$ and $\operatorname{im}(f) = \{y \in N \text{ such that } y = f(x) \text{ for some } x \in M\}$.

Example 28.14. (a) Let $M \cong \mathbb{R}^n$ and $N \cong \mathbb{R}^m$ with the scaling module structure over $\mathbb{R}$. Then a linear map $M \to N$ is a homomorphism of $\mathbb{R}$-modules.

(b) (No obvious example following example (b) from before.)

(c) Let $M = \mathbb{R}^m$ be a left module over $R = \mathbb{R}[t]$, given by a linear transformation T. Let $N = \mathbb{R}^n$ be a left module over $\mathbb{R}[t]$ given by a linear transformation $S : \mathbb{R}^n \to \mathbb{R}^n$. Then an R-module homomorphism is a linear map

$$f : \mathbb{R}^m \to \mathbb{R}^n$$

with the property that

$$f(T(v)) = S(f(v)).$$

Definition 28.15. Let M and N be left R-modules. Then the set of all R-module homomorphisms is denoted

$$\hom_R(M, N).$$

Proposition 28.16. $\hom_R(M, N)$ is a left R-module.

PROOF. This will be in your homework next week, too. □

5. Direct sums and free modules

Last week we defined a left R-module to be an abelian group M together with a scaling map $R \times M \to M$.

Definition 28.17. Let M and N be left R-modules. Then we define the *direct sum*

$$M \oplus N$$

to be equal to $M \times N$ as a group, and to have the R-module structure

$$r(m, n) := (rm, rn).$$

PROOF THAT $M \oplus N$ IS AN R-MODULE. We know it's an abelian group. On the other hand

$$1(m, n) := (1m, 1n) = (m, n)$$

since M and N are modules. And we have

$$\begin{aligned} r((m,n)+(m',n')) &= r(m+m',n+n') \\ &= (r(m+m'),r(n+n')) \\ &= (rm+rm',rn+rn') \qquad (3) \\ &= (rm,rn)+(rm',rn') \\ &= r(m,n)+r(m',n'). \end{aligned}$$

Note (3) is where we used that M and N are left R-modules. I'll leave the verification of other properties to you. □

Example 28.18. If $R=\mathbb{R}$, and M and N are also $\mathbb{R}$ considered as a module over itself, then

$$\mathbb{R}\oplus\mathbb{R}\cong\mathbb{R}\times\mathbb{R}\cong\mathbb{R}^2$$

as a group, and we have the usual scaling actions

$$r(x_1,x_2)=(rx_1,rx_2).$$

Remark 28.19. We have an obvious isomorphism

$$(M\oplus N)\oplus O\cong M\oplus(N\oplus O), \qquad (m,n,o)\mapsto(m,n,o).$$

Definition 28.20. Let R be a ring. Then the direct sum module

$$R^n := R\oplus\ldots\oplus R$$

is called the *free R-module of rank n.*