Lecture 10-7: Modules

October 7, 2024

I will now shift gears, studying modules over rings (following Chapter 10 in the text). At first the rings will be general. Then I will spend some time on modules over commutative rings before switching back to the general case; later in the course (following Chapter 12) I will classify finitely generated modules over principal ideal domains. I will assume familiarity with the basic ring theory covered in sections 7.1 through 7.5.

Let R be a ring, not necessarily commutative (but with identity 1). A (left) R-module is essentially a vector space over R. More precisely,

Definition, p. 337

A left R-module M is an abelian group under addition such that for each $r \in R, m \in M$ there is $rm \in M$ such that

- $(r+s)m = rm + sm$ for $r, s \in R, m \in M$,
- $(rs)m = r(sm)$ for $r, s \in R, m \in M$,
- $r(m+n) = rm + rn$ for $r \in R, m, n \in M$,
- $1m = m$ for $m \in M$.

Thus a module over a field F is really the same thing as a vector space over F.

In particular any ring R (viewed as a multiplicative monoid) acts on any R-module M, in the sense of group actions; but the elements of R must act by *homomorphisms* of M as an abelian group. One defines right modules similarly, replacing the second property above by $m(rs) = (mr)s$. If R is commutative then left and right modules are the same thing, so one just speaks of R-modules.

If M is a left R-module then a submodule of R is a subgroup N of M such that $rn \in N$ for $r \in R, n \in N$ (p. 337). If N is a submodule of R then the quotient group M/N becomes an R-module by the recipe $r(m+N) = rm+N$ for $r \in R, m \in M$ (Proposition 3, p. 348). Thus in particular if I is a left ideal of R then both I and the quotient group R/I are left R-modules (and so to some extent can be treated on an equal footing). If I is a two-sided ideal of R then R/I is a module over the quotient ring R/I. More generally, if I is a two-sided ideal and M is a left R-module such that $im = 0$ for all $i \in I, m \in M$, then the recipe $(r+I)m = rm$ gives a well-defined action of R/I on M (Example 5, p. 346).

Example

There are two especially important examples, to which I will return later. First, if $R = \mathbb{Z}$, the ring of integers, then an R-module is just an abelian group A: here na is just the sum of n copies of a if n is a nonnegative integer and the negative of the sum of $-n$ copies of a if n is a nonpositive integer (Example, p. 339).

Example

The second example is more subtle. Let F be a field, V a vector space over F, and $T : V \to V$ a linear transformation. Then one can make V into a module over $F[x]$, the ring of polynomials in one variable x over F, by decreeing that any polynomial $\sum_{i=0}^{n} a_i x^i$ acts on V by the transformation $\sum_{i=0}^{n} a_i T^i$ (interpreting T^0 as the identity transformation; see the Example on p. 340). Later I will classify finitely generated modules over a principal ideal domain ($\mathbb{Z}$ and $F[x]$ are both examples of such domains) and use this to get information about both finitely generated abelian groups and transformations from a finite-dimensional vector space to itself.

Definition of module homomorphism, p. 345

If M, N are left modules over the same ring R, then a group homomorphism $\phi : M \to N$ is an *R-module homomorphism* if it commutes with the action of R, so that $\phi(rm) = r\phi(m)$ for $r \in R, m \in M$. The *kernel* and *image* of ϕ are defined as for group homomorphisms; they are submodules of M and N, respectively. One says that ϕ is an *isomorphism* (and that M and N are *isomorphic*) if the kernel of ϕ is trivial and its range is all of N. The set of all R-module homomorphisms from M to N is denoted $\hom_R(M, N)$; this is a group under addition.

If R is commutative then $\hom_R(M, N)$ is also an R-module, since the scalar multiple $r\phi$ is an R-module homomorphism from M to N if ϕ is in this case. Note that R-module homomorphisms are the module analogues of linear transformations between vector spaces over the same field.

Definition, p. 347

If M is a left R-module then the group $\hom_R(M, M)$ has the structure of a ring in addition to that of a group (since the composite of two homomorphisms from M to itself is another such homomorphism). This ring is called the *endomorphism ring* of M and is denoted $\mathrm{End}_R(M)$, or just $\mathrm{End}\ M$ if R is clear from context.

Let A be a subset of the left R-module M. Just as the span FS of a subset S of a vector space V over a field F is defined to be the set of all finite linear combinations $\sum f_i v_i$ with $f_i \in F$, $v_i \in S$, the span RA of A is defined to be the set of all such combinations with $f_i \in R$, $v_i \in A$; it is a submodule of M. One says that M is finitely generated if it is the span of some finite subset. By analogy with groups, one says that M is cyclic if it is generated by a single element (Definition, p. 351). More generally, given any collection $\{M_i : i \in I\}$ of submodules of M the set of all sums $\sum_{i \in I} m_i$ such that $m_i \in M_i$ and all but finitely many m_i are 0 is a submodule of M, called naturally enough the sum of the M_i and denoted $\sum M_i$ (see the definition on p. 349).

The notion of direct product of groups carries over in a natural way to modules. Given a module M with submodules M_1, M_2 suppose that $M = M_1 + M_2$ and $M_1 \cap M_2 = 0$. Then one easily checks (as for groups) that every $m \in M$ can be written *uniquely* as $m_1 + m_2$ for some $m_1 \in M_1, m_2 \in M_2$. One says that M is the (internal) direct sum of M_1 and M_2 in this situation (see Proposition 5 on p. 353). More generally, if $\{M_i; i \in I\}$ is any collection of submodules of M such that M is the sum of the M_i and the intersection of any M_i and the sum of all the others is trivial, then one says that M is the direct sum of the M_i. Note however that there is no notion of *semidirect* sum of modules (unlike the situation for groups), since the operation of addition is always commutative (so that any additive subgroup is normal).

More generally, let M_1 and M_2 be any R-modules (or even more generally, let M_i be a family of R-modules indexed by a set I). The set of ordered pairs (m_1, m_2) with $m_1 \in M_1, m_2 \in M_2$, or of tuples $(\ldots, m_i, \ldots)$ with $m_i \in M_i$ and all but finitely many m_i equal to 0) form an R-module under coordinatewise addition and scalar multiplication by R. The text denotes this module by $M_1 \times M_2$ in the first case and calls it the direct product of M_1 and M_2 (p. 353); but it is more standard to call this the direct sum of M_1 and M_2 and to denote it by $M_1 \oplus M_2$. In the more general situation M is again called the direct sum of the M_i and is denoted $\oplus_{i \in I} M_i$. This notion of direct sum coincides (up to isomorphism) with the direct sum of submodules defined on the previous slide. If I is infinite then the larger set of tuples $(\ldots, m_i, \ldots)$ with no restriction that only finitely many m_i be nonzero is also an R-module, called the direct product of the M_i and denoted $\prod_{i \in I} M_i$ (see Exercise 20, p. 357).

In the special case where each M_i is isomorphic to R itself then the direct sum $M = \oplus_{i \in I} M_i$ is called free (on I) of rank $|I|$ and denoted $R^{|I|}$, where $|I|$ is the cardinality of I (Definition, p. 354). A set $\{b_i : i \in I\}$ of elements with $b_i \in M_i$ is called (free) basis if every $m \in M$ is a unique linear combination $\sum_i r_i b_i$ with $r_i \in R$ and all but finitely many r_i equal to 0. (For example, any vector space V over a field K is a free K-module with a basis of V being a free basis). If I is infinite then the direct product $\prod_{i \in I} M_i$ of copies of R is *not* generally a free R-module (see Exercise 24, p. 358). If I is countably infinite then one sometimes distinguishes between the direct sum and product indexed by I by denoting the former by R^∞ and the latter by R^ω.