Introduction to Rings and Modules

Lecture 15, Monday June 12 2023
Ari Feiglin

Definition 15.0.1:

Let R be a ring, an R-module M is **cyclic** if it is generated by a single element. Ie. M is cyclic if and only if there exists an $m \in M$ such that

$$M = \langle m \rangle = \{rm \mid r \in R\}$$

Note that submodules of R (when viewed as a module over itself), are cyclic if and only if they are principal ideals.

Proposition 15.0.2:

Let M be an R-module, then M is cyclic if and only if there exists a left ideal $I \leq R$ such that $M \cong {}^{R}\!/_{I}$ as modules.

Note that ${}^{R}\!/_{I}$ is not necessarily a ring, but since $I \subseteq R$ is a submodule of R, ${}^{R}\!/_{I}$ is a module over R.

Proof:

If $M \cong {}^{R}\!/_{I}$ then it is sufficient to show that ${}^{R}\!/_{I}$ is cyclic. This is trivial as everything in the quotient can be generated by $1 + I$.
If M is cyclic, let us define a module homomorphism $f\colon R \longrightarrow M$ by $f(r) = rm$ where m generates M. This is a module homomorphism as $f(r_1 + r_2) = (r_1 + r_2)m = r_1m + r_2m = f(r_1) + f(r_2)$ and $f(r_1r_2) = r_1r_2m = r_1f(r_2)$ as required. This is surjective and so

$${}^{R}\!/_{\operatorname{Ker} f} \cong M$$

and $\operatorname{Ker} f$ is a submodule of R and thus a left ideal.

Suppose R is a commutative ring, what is a module over the ring $R[x]$? Let M be a module over $R[x]$, thus M is an abelian group, and it has left multiplication defined by polynomials in $R[x]$. Since constants are polynomials in $R[x]$, left multiplication on M by R is defined. So every module over $R[x]$ is a module over R (a linear space). Thus far, this is true for rings in general.
Note since if R is commutative, the mapping

$$\varphi\colon M \longrightarrow M, \quad m \mapsto xm$$

is a module homomorphism for $x \in R$, since $\varphi(m_1 + m_2) = x(m_1 + m_2) = xm_1 + xm_2 = \varphi(m_1) + \varphi(m_2)$, and $\varphi(rm) = xrm = rxm = r\varphi(m)$. Let us call this the "scalar multiplication mapping of x".
Thus if we are given a module M over $R[x]$ as a module over M and the scalar multiplication mapping of x $\varphi\colon M \longrightarrow M$, this is enough to define the operations of M over $R[x]$. In other words, a module over $R[x]$ is a module over R and the definition of $x \cdot m$ for $m \in M$.
This is because for $m \in M$ and $f = a_nx^n + \cdots + a_0 \in R[x]$ we have

$$fm = a_nx^nm + \cdots + a_0m$$

and since we have the definition of xm for every $m \in M$, we have the definition of x^nm inductively as $x^nm = x^{n-1}(xm)$. Or in other words $x^nm = \varphi^n(m)$, where φ is the scalar multiplication mapping of x.
And for the converse, if M is a module over a commutative ring R, and $\varphi\colon M \longrightarrow M$ is a module homomorphism, if we define $x \cdot m = \varphi(m)$ then this defines a module over $R[x]$:
Thus we get the following

Proposition 15.0.3:

If R is a commutative ring, then $R[x]$ modules are equivalent to R-modules with a module homomorphism over themselves.

Example 15.0.4:

Let R be a commutative ring, we will investigate the R-module

$$M = {}^{R[x]}\Big/_{((x-\lambda)^n))}$$

for $n \in \mathbb{N}$. Since this is a quotient of the ring $R[x]$, M is cyclic. By polynomial division, for any $f \in R[x]$ we have that

$$f = q \cdot (x-\lambda)^n + r$$

for $\deg r < n$. Thus as we know, ${}^{R[x]}\Big/_{((x-\lambda)^n)}$ is the set of classes whose representatives are polynomials of degree $< n$: $a_{n-1}x^{n-1} + \cdots + a_0$. Such a set induces a natural R-module, where we simply scale each polynomial (this is independent of the representative of the class, since if $f - g \in ((x-\lambda)^n$ then so is $rf - rg$).
We take the basis $B = \left\{(x-\lambda)^k + I \;\middle|\; 0 \leq k < n\right\}$ (where $I = ((x-\lambda)^n)$). This is a generating set as we can induct on the degree of $f \in I$. If f is constant, then it is a multiple of $(x-\lambda)^0$. Otherwise we can take the degree of f, m, and we have $f = q(x-\lambda)^m + r$ where $\deg r < m$ and thus induct on r (since q must be constant as otherwise the degree of $q(x-\lambda)^m$ would be more than m). This set is a linearly independent since any sum $\sum a_k(x-\lambda)^k = 0$, every $a_k = 0$ as otherwise let k be the maximum k where $a_k \neq 0$, and then the sum has a degree of k in contradiction.
And so if we let φ be the scalar multiplication mapping of x

$$\varphi((x-\lambda)^{n-1} + I) = x((x-\lambda)^{n-1} + I) = x(x-\lambda)^{n-1} + I = (x-\lambda)^n + \lambda(x-\lambda)^{n-1} + I = \lambda(x-\lambda)^{n-1} + I$$

and in general

$$\varphi((x-\lambda)^k + I) = \big((x-\lambda)^{k+1} + I\big) + \lambda\big((x-\lambda)^k + I\big)$$

So the matrix representing this homomorphism (relative to the basis B) is the Jordan block of size n (we count $(x-\lambda)^{n-1} + I$ as the first element in the basis, and go in reverse).

Example 15.0.5:

Let us now look at the cyclic module

$$M = {}^{R[x]}\Big/_{(p)}$$

for some $p \in F[x]$. We assume that p has a leading coefficient which is 1, and thus elements of M can be represented as polynomials of degree less than that of p's. We similarly denote $I = (p)$.
But now let us focus on the basis $B = (1 + I, x + I, \ldots, x^{n-1} + I)$ where $n = \deg p$. Then

$$\varphi(x^k + I) = x^{k+1} + I$$

If

$$p = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

then we have that

$$x^n + I = x^n - p + I = -a_{n-1}x^{n-1} - \cdots - a_0 + I$$

and so the matrix of φ is of the form

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ 0 & 0 & 1 & \cdots & 0 & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

This is called the **companion matrix** of p and is denote C_p.

Definition 15.0.6:

If M and N are R-modules, then we can define the R-module $M \times N$ by defining $r \cdot (m, n) = (rm, rn)$.

Theorem 15.0.7 (Classification Theorem):

Let R be a PID, and M be a finitely generated R-module. Then

(1) There exist $d_1, \ldots, d_n \in R$ which are unique up to friends where

$$M \cong {R}/{(d_1)} \times \cdots \times {R}/{(d_n)}$$

and $d_i | d_{i+1}$ for every $1 \leq i < n$. These are called **invariant elements**.

(2) There exist $p_1, \ldots, p_t$ irreducible elements, unique up to friends and $r, n_1, \ldots, n_t \geq 0$ such that

$$M \cong R^r \times {R}/{(p_1^{n_1})} \times \cdots \times {R}/{(p_t^{n_t})}$$

Note that if $R = \mathbb{Z}$, then we get the classification theorem for abelian groups.