MODULES : MA 3G6 2017

DIANE MACLAGAN

1. Modules

Definition 1.1. Let R be a ring. An R-module M is an abelian group M with a multiplication map $R \times M \to M$ (written rm) satisfying:

(1) $r(m+n) = rm + rn$,
(2) $(r+r')m = rm + r'm$,
(3) $(rr')m = r(r'm)$, and
(4) $1_R m = m$ for all $r, r' \in R$, $m, n \in M$.

Example 1.2. (1) When R is a field, an R-module M is a vector space over R.
(2) For an arbitrary ring R, R is an R-module, with the map $R \times M \to R$ being multiplication.
(3) For an arbitrary ring R, and an ideal $I \subseteq R$, both I and R/I are R-modules.
(4) When $R = \mathbb{Z}$, R-modules are abelian groups. Here $ng = g + \cdots + g$ is the sum of n copies of g.

Definition 1.3. A subset $N \subseteq M$ of an R-module is a submodule if the following two conditions hold: If $m, n \in N$ then $m + n \in N$, and if $m \in N$, $r \in R$, then $rm \in N$.

Example 1.4. A submodule of the R-module R is an ideal. If R is a field, an R-submodule of M is a subspace of the vector space M.

Definition 1.5. A map $\phi\colon M \to N$ is an R-module homomorphism if it is a group homomorphism with

$$\phi(rm) = r\phi(m).$$

It is an isomorphism if it is injective and surjective.

Example 1.6. When R is a field, an R-module homomorphism is a linear map.

Definition 1.7. If $\phi\colon M \to N$ is an R-module homomorphism then

$$\ker(\phi) = \{m \in M\colon \phi(m) = 0_N\},$$

and

$$\operatorname{im}(\phi) = \{n \in N : \exists m \in M \text{ with } \phi(m) = n\}.$$

Exercise: Show that $\ker(\phi)$ is a submodule of M, and $\operatorname{im}(\phi)$ is a submodule of N.

Since a submodule N of M is a subgroup of an abelian group, we can form the quotient group M/N. This is again an R-module, with the action

$$r(m + N) = rm + N.$$

Exercise: Show that this is well-defined, so if $m + N = m' + N$, then $rm + N = rm' + N$.

Exercise: Isomorphism theorems. Show that

(1) If $\phi \colon M \to N$, then $M/\ker(\phi) \cong \operatorname{im}(\phi)$.
(2) If $L \subseteq M \subseteq N$ with L a submodule of M, and M a submodule of N, then
$$N/M \cong (N/L)/(M/L).$$
(3) If L and M are submodules of N then $(L+M)/L \cong M/(M \cap L)$, where $L + M = \{l + m : l \in L, m \in M\}$.

Hint: You already know these for abelian groups, so you just need to check the R-action obeys the axioms.

2. Free modules

Definition 2.1. Let R be a ring. The R-module R^n is

$$R = \{(r_1, \dots, r_n) : r_i \in R\},$$

where the R-action is

$$r(r_1, \dots, r_n) = (rr_1, \dots, rr_n),$$

and

$$(r_1, \dots, r_n) + (r'_1, \dots, r'_n) = (r_1 + r'_1, \dots, r_n + r'_n).$$

More generally, if A is any set, then

$$\{(r_\alpha : \alpha \in A) : r_\alpha \in R\}$$

is an R-module.

Note: In R^n, then set $\mathcal{B} = \{(1, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, \dots, 0, 1)\}$ has the property that every element of R^n can be written as an R-linear combination of elements of B. For example, when $n = 2$, we have $(r_1, r_2) = r_1(1, 0) + r_2(0, 1)$. This should remind you of a basis from linear algebra.

Definition 2.2. Let M be an R-module, and let $\mathcal{G} = \{m_\alpha : \alpha \in A\}$ be a subset of elements of M. The set $\mathcal{G}$ *generates* M *as an* R*-module* if every element $m \in M$ can be written in the form $m = \sum_{i=1}^{s} r_i m_{\alpha_i}$ for some $\alpha_1, \dots, \alpha_s \in A$, and $r_1, \dots, r_s \in R$. Here the set A may be infinite, but this is a finite sum.

Example 2.3. (1) When R is a field, an R-module M is a vector space. Then $\mathcal{G} \subseteq M$ generates M if $\mathcal{G}$ spans M.
(2) When $M = I$ is an ideal of R, then $\mathcal{G}$ generates M as an R-module if and only if $I = \langle G \rangle$ (so if and only if $\mathcal{G}$ generates I as an ideal.

Definition 2.4. A set $\mathcal{G} \subseteq M$ is a *basis* for M if $\mathcal{G}$ generates M and every element of M can be written *uniquely* as an R-linear combination of elements of $\mathcal{G}$.

Equivalently, if $\sum_{i=1}^{s} r_i m_{\alpha_i} = 0$ for $\alpha_i \in A$, then $r_1 = \cdots = r_s = 0$.

Example 2.5. (1) When R is a field, then a basis for an R-module M is a basis for M as a vector space in the sense of linear algebra.
(2) A basis for $M = R^2$ is given by $\{(1,0), (0,1)\}$.

Warning: Unlike in linear algebra, many R-modules do not have bases.

Example 2.6. Let $R = K[x,y]$, where K is a field, and let $M = \langle x, y \rangle$. Then M does not have a basis. Indeed, suppose that there was a basis $\mathcal{G}$ for M. Then we could write $x = \sum_{i=1}^{s} r_i m_i$ and $y = \sum_{j=1}^{t} r'_j m'_j$, where $m_i, m'_j \in \mathcal{G}$, and $r_i, r'_j \in R$. Then $xy = \sum_{i=1}^{s} (r_i y) m_i = \sum_{j=1}^{t} (r'_j x) m'_j$. By uniqueness, after reordering if necessary, we may assume that $s = t$, $m_i = m'_i$, and $y r_i = x r'_i$. But then x divides r_i for all i, so we can write $r_i = x \tilde{r}_i$ for $\tilde{r}_i \in R$. This means that $x = \sum_{i=1}^{s} x \tilde{r}_i m_i \in R = K[x,y]$. Since R is a domain, we then have $\sum_{i=1}^{s} \tilde{r}_i m_i = 1 \in R$. But this contradicts that $m_i \in \langle x, y \rangle$ for all i, so $\sum_{i=1}^{s} \tilde{r}_i m_i \in \langle x, y \rangle$, as $1 \notin \langle x, y \rangle$.

Definition 2.7. An R-module M is *free* if it has a basis.

Example 2.8. For any ring R, the R-module R^n is free. The $K[x,y]$-module $\langle x, y \rangle$ is not.

Exercise: Which of the following modules are free?
(1) $R = K[x,y]$, $M = \langle x^2 + y^2 \rangle$,
(2) $R = \mathbb{Z}$, $M = \mathbb{Z}^2 / \langle (1,1), (1,-1) \rangle$.
(3) $R = K[x,y]$, and $M = K[x,y]/\langle x^2 + y^2 \rangle$.

3. The Cayley-Hamilton theorem

Recall: For an $n \times n$ matrix A with entries in a field K, the characteristic polynomial is

$$p_A(x) = \det(xI - A).$$

The *Cayley-Hamilton theorem* states that $p_A(A) = 0$. Here by $p_A(A)$ we mean the following: if $p(x) = \sum a_i x^i \in K[x]$, then $p(A) = \sum a_i A^i$.
Note: Matrices still make sense over an arbitrary (commutative) ring.

An $n \times n$ matrix A with entries in R gives an R-module homomorphism $\phi\colon R^n \to R^n$ by

$$\phi(r_1, \dots, r_n) = (\sum_{j=1}^{n} a_{1j} r_j, \dots, \sum_{j=1}^{n} a_{nj} r_j).$$

This is the usual multiplication of a matrix and a vector.

Determinants of $n \times n$ matrices with entries in R also still make sense, as the definition of the determinant only involves concepts that make sense in a general ring.

Definition 3.1. Let M be an R-module. The set of all R-module homomorphisms $\phi\colon M \to M$ forms a (noncommutative!) ring with identity. We call this $\mathrm{End}(M)$ (here End is short for "endomorphism"). The addition on $\mathrm{End}(M)$ is given by setting $(\phi+\psi)(m) = \phi(m)+\psi(m)$, and $(\phi\psi)(m) = \phi(\psi(m))$, where $\phi, \psi \in \mathrm{End}(M)$. Thus addition is pointwise, and multiplication is composition of functions.

This is the only noncommutative ring that we will see in this module.

When $M = R^n$, the ring $\mathrm{End}(M)$ is the ring of $n \times n$ matrices with entries in R, and the multiplication is multiplication of matrices.

Definition 3.2. Given an $n \times n$ matrix A, the subring $R[A]$ of $\mathrm{End}(R^n)$ is the smallest subring of $\mathrm{End}(R^n)$ containing the identity endomorphism and A.

Exercise: Check that the "smallest subring" exists. It consists of all polynomials in A: $\sum_{i=0}^{s} a_i A^i$, where $a_i A^i$ means the scalar multiplication of the matrix A^i by the element a_i, and A^0 is the identity matrix.
Note: $R[A]$ is a commutative ring, and there is a surjective homomorphism $\psi\colon R[x] \to R[A]$ given by sending x to A.

Also, R^n is a $R[A]$-module, with the action given by

$$(\sum_{i=0}^{s} a_i A^i) v = \sum_{i=0}^{s} a_i (A^i v)$$

for $v = (r_1, \ldots, r_n) \in R^n$, where $A^i v$ is usual matrix/vector multiplication.

Theorem 3.3 (Cayley-Hamilton Theorem)**.** *Let R be a ring, and A an $n \times n$ matrix with entries in R. Write $p_A(x) = \det(xI - A)$. This is a polynomial of degree n in x with coefficients in R, and $p_A(A) = 0$.*

Example 3.4. Let $R = \mathbb{Z}/6\mathbb{Z}$, and

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

The characteristic polynomial is

$$\det \begin{pmatrix} x-1 & -2 \\ -3 & x-4 \end{pmatrix} = (x-1)(x-4) - 6 = x^2 + x + 4.$$

We have

$$A^2 = \begin{pmatrix} 1 & 4 \\ 3 & 4 \end{pmatrix},$$

so

$$A^2 + A + 4I = \begin{pmatrix} 1 & 4 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Exercise: Let $R = \mathbb{C}[x]$, and

$$A = \begin{pmatrix} x & x^2 \\ x^3 & x^4 \end{pmatrix}.$$

Compute the characteristic polynomial of A, and verify that $p_A(A) = 0$.

Proof of the Cayley-Hamilton theorem. Write $\mathbf{e}_1, \ldots, \mathbf{e}_n$ for the standard basis vectors of R^n.

We have $A\mathbf{e}_k = \sum_{j=1}^n a_{jk}\mathbf{e}_j$ for $1 \leq k \leq n$. Write δ_{jk} for the Kronecker delta: $\delta_{jk} = 1$ if $j = k$, and 0 otherwise. Then $\sum_{j=1}^n (\delta_{jk}A - a_{jk})\mathbf{e}_j = \mathbf{0} \in R^n$. Let $B = (B_{jk})$ be the $n \times n$ matrix with entries in $R[A]$ with $B_{jk} = \delta_{jk}A - a_{jk}$. Write C for the adjoint matrix of B. This is the $n \times n$ matrix with $C_{ij} = (-1)^{i+j} \det(B \backslash i\text{th column and } j\text{th row})$. This is a well-defined operation in any commutative ring, so in particular in the ring $R[A]$. As in standard linear algebra we have

$$BC = CB = \det(B)I_n.$$

Indeed,

$$\begin{aligned}(BC)_{ij} &= \sum_{k=1}^{n} B_{ik}C_{kj} \\ &= \sum_{k=1}^{n} (-1)^{k+j} B_{ik} \det(B \setminus k\text{th column, } j\text{th row}) \\ &= \det(B \text{ with } j\text{th row replaced by the } i\text{th row}) \\ &= \begin{cases} \det(B) & i = j \\ 0 & \text{otherwise.} \end{cases}\end{aligned}$$

The third equality here comes from expanding $\det(B)$ along the jth row (Check that these expansions still make sense over an arbitrary ring!).

Now,

$$\begin{aligned}\mathbf{0} &= \sum_{k=1}^{n} (C_{kj} \sum_{i=1}^{n} (\delta_{ik}A - a_{ik})\mathbf{e}_i) \\ &= \sum_{i=1}^{n} (\sum_{k=1}^{n} C_{kj}(\delta_{ik}A - a_{ik}))\mathbf{e}_i \\ &= \sum_{i=1}^{n} \sum_{k=1}^{n} B_{ik}C_{kj}\mathbf{e}_i \\ &= \sum_{i=1}^{n} (BC)_{ij}\mathbf{e}_i \\ &= \det(B)\mathbf{e}_j.\end{aligned}$$

So $\det(B) = 0$.

Now $p_A(x) = \det(xI_n - A) \in R[x]$. The map $\phi\colon R[x] \to R[A]$ sending x to A is a homomorphism which induces a homomorphism $\psi\colon \operatorname{End}(R[x]^n) \to \operatorname{End}(R[A]^n)$ as follows. An element $f \in \operatorname{End}(R[x]^n)$ can be represented by an $n \times n$ matrix with entries in $R[x]$. The homomorphism ψ applies ϕ to each entry of this matrix. Equivalently, if $f(\mathbf{e}_i) = \sum_{j=1}^{n} h_i \mathbf{e}_j$, then $\psi(f)(\mathbf{e}_i = \sum_{j=1}^{n} \phi(h_i)\mathbf{e}_j$. The homomorphism ψ takes $xI_n - A$ to B. Thus $p_A(A) = \det(B) = 0$. $\square$

We now give a version of this theorem that applies to a more general module.

Definition 3.5. An R-module M is finitely generated if it has a finite set of generators, so there is $m_1, \dots, m_s \in M$ such that for all $m \in M$ there is $r_1, \dots, r_s$ with $m = \sum_{i=1}^{s} r_i m_i$.

For an ideal $I \subset R$, we denote by IM the submodule of M generated by $\{rm : r \in I, m \in M\}$.

Theorem 3.6. *Let M be a finitely generated R-module with n generators, let $\phi \colon M \to M$ be an R-module homomorphism, and suppose that I is an ideal of R such that $\phi(M) \subseteq IM$. Then ϕ satisfies a relation of the form*

$$\phi^n + a_1\phi^{n-1} + \cdots + a_{n-1}\phi + a_n = 0$$

where $a_i \in I^i$ for $1 \leq i \leq n$. This is a relation in the ring $\mathrm{End}(M)$.

Here I^i is the product of the ideal I with itself i times, so is the ideal generated by the products of any i elements of I. For example, if $I = \langle x, y \rangle \subseteq \mathbb{Q}[x, y]$, then $I^2 = \langle x^2, xy, y^2 \rangle$. The case that $M = R^n$ and $I = R$ is the Cayley-Hamilton theorem; in that case the relation is the characteristic polynomial. The proof of this theorem is very similar to the proof of the Cayley-Hamilton theorem.

Proof. Let $m_1, \dots, m_n$ be a generating set for M. Since $\phi(m_i) \in IM$ we can write $\phi(m_i) = \sum_{j=1}^{n} a_{ji} m_j$ with $a_{ji} \in I$. In the subring $R[\phi]$ of $\mathrm{End}(M)$ this is $\sum_{j=1}^{n} (\delta_{ji}\phi - a_{ji}) m_j = 0$. Here we regard an element $a \in R$ as the endomorphism of M given by $m \mapsto am$. Write B for the $n \times n$ matrix with entries in $R[\phi]$ with $B_{ij} = \delta_{ji}\phi - a_{ji}$, so $\sum_{j=1}^{n} B_{ij} m_j = 0$. Let C be the adjoint matrix of B. Then

$$\begin{aligned} 0 &= \sum_{i=1}^{n} C_{ki} \Big(\sum_{j=1}^{n} B_{ij} m_j\Big) \\ &= \sum_{j=1}^{n} \Big(\sum_{i=1}^{n} C_{ki} B_{ij}\Big) m_j \\ &= \sum_{j=1}^{n} (CB)_{kj} m_j \\ &= \det(B) m_k. \end{aligned}$$

So $\det(B) \in R[\phi]$ satisfies $\det(B)m_k = 0$ for all k, and $\det(B)m = 0$ for all $m \in M$. Thus $\det(B) = 0$ in $\mathrm{End}(M)$. Expanding the determinant gives a polynomial in ϕ of the desired form. $\square$

4. Nakayama's lemmas

We finish this topic with several important corollaries of the Cayley-Hamilton theorem and its generalization, each of which is called Nakayama's lemma by some authors.

Corollary 4.1. *If M is a finitely generated R-module and I is an ideal of R with $IM = M$, then there exists $r \in R$ such that $r - 1 \in I$, and $rM = 0$.*

Proof. Applying Theorem 3.6 in the case that ϕ is the identity homomorphism we get

$$\mathrm{id} + \sum_{i=1}^{n-1} a_i \,\mathrm{id} + a_n = 0,$$

with $a_i \in I^i$, so $(1 + \sum_{i=1}^n a_i)\,\mathrm{id} = 0$. Set $r = 1 + \sum_{i=1}^n a_i$. Then $r - 1 \in I$, and $rm = 0$ for all $m \in M$. $\square$

Corollary 4.2. *Let R be a local ring with maximal ideal $\mathfrak{m}$, and M a finitely generated R-module. If $M = \mathfrak{m}M$, then $M = 0$.*

Proof. By Corollary 4.1 there is $r \in R$ with $r - 1 \in \mathfrak{m}$ and $rm = 0$ for all $m \in M$. But then $r \notin \mathfrak{m}$ (as otherwise $1 \in \mathfrak{m}$), so r is a unit, and thus $m = r^{-1}rm = r^{-1}0 = 0$ for all $m \in M$. $\square$

The last version is the one most commonly called Nakayama's lemma.

Corollary 4.3. *Let R be a local ring with maximal ideal $\mathfrak{m}$. If M is a finitely generated R-module and $m_1, \dots, m_s \in M$ are elements whose images span the $k = R/\mathfrak{m}$-vector space $\overline{M} = M/\mathfrak{m}M$, then $m_1, \dots, m_s$ generate M.*

Proof. Let N be the submodule of M generated by $m_1, \dots, m_s$. Since the $m_i + \mathfrak{m}M$ span $M/\mathfrak{m}M$, each element of M can be written as $m = \sum_{i=1}^s r_i m_i + m'$ where $r_i \in R$ and $m' \in \mathfrak{m}M$. Thus $m = n + m'$ for $n \in N$. Thus $m + N = m' + N$, so $M/N = \mathfrak{m}M/N$. By Corollary 4.2 this implies that $M/N = 0$. So $N = M$, and $m_1, \dots, m_s$ generates M. $\square$

Warning: These corollaries all need M to be finitely generated.

Example 4.4. Let $R = \mathbb{Z}_{\langle 2 \rangle} = \{a/b \in \mathbb{Q} : 2 \not| b\}$, and $M = \mathbb{Q}$. Then M is an R-module. Note that $2\mathbb{Q} = \mathbb{Q}$, as $a/b = 2(a/2b)$, but $\mathbb{Q} \neq 0$. This does not contradict Corollary 4.2, as M is not a finitely generated R-module. (Why not?)

The last two also need R to be local.

Example 4.5. $\mathbb{Z}$ is a $\mathbb{Z}$-module, $\langle 2\rangle$ is a maximal ideal of $\mathbb{Z}$, 5 generates $\mathbb{Z}/2\mathbb{Z}$, but not $\mathbb{Z}$. This does not contradict Corollary 4.3 because $\mathbb{Z}$ is not a local ring.