Module MA3412: Integral Domains, Modules and Algebraic Integers
Section 3
Hilary Term 2014

D. R. Wilkins

Contents

3 Noetherian Rings and Modules

3.1 Modules over a Unital Commutative Ring

Definition Let R be a unital commutative ring. A set M is said to be a *module over* R (or R*-module*) if

(i) given any $x, y \in M$ and $r \in R$, there are well-defined elements $x + y$ and rx of M,

(ii) M is an Abelian group with respect to the operation $+$ of addition,

(iii) the identities

$$r(x + y) = rx + ry, \qquad (r + s)x = rx + sx,$$

$$(rs)x = r(sx), \qquad 1x = x$$

are satisfied for all $x, y \in M$ and $r, s \in R$.

Example If K is a field, then a K-module is by definition a vector space over K.

Example Let $(M, +)$ be an Abelian group, and let $x \in M$. If n is a positive integer then we define nx to be the sum $x + x + \cdots + x$ of n copies of x. If n is a negative integer then we define $nx = -(|n|x)$, and we define $0x = 0$. This enables us to regard any Abelian group as a module over the ring $\mathbb{Z}$ of integers. Conversely, any module over $\mathbb{Z}$ is also an Abelian group.

Example Any unital commutative ring can be regarded as a module over itself in the obvious fashion.

Let R be a unital commutative ring, and let M be an R-module. A subset L of M is said to be a *submodule* of M if $x + y \in L$ and $rx \in L$ for all $x, y \in L$ and $r \in R$. If M is an R-module and L is a submodule of M then the quotient group M/L can itself be regarded as an R-module, where $r(L + x) \equiv L + rx$ for all $L + x \in M/L$ and $r \in R$. The R-module M/L is referred to as the *quotient* of the module M by the submodule L.

Note that a subset I of a unital commutative ring R is a submodule of R if and only if I is an ideal of R.

Let M and N be modules over some unital commutative ring R. A function $\varphi\colon M \to N$ is said to be a *homomorphism of* R*-modules* if $\varphi(x+y) = \varphi(x)+\varphi(y)$ and $\varphi(rx) = r\varphi(x)$ for all $x, y \in M$ and $r \in R$. A homomorphism of R-modules is said to be an isomorphism if it is invertible. The kernel

$\ker\varphi$ and image $\varphi(M)$ of any homomorphism $\varphi: M \to N$ are themselves R-modules. Moreover if $\varphi: M \to N$ is a homomorphism of R-modules, and if L is a submodule of M satisfying $L \subset \ker\varphi$, then φ induces a homomorphism $\overline{\varphi}: M/L \to N$. This induced homomorphism is an isomorphism if and only if $L = \ker\varphi$ and $N = \varphi(M)$.

Definition Let $M_1, M_2, \ldots, M_k$ be modules over a unital commutative ring R. The *direct sum* $M_1 \oplus M_2 \oplus \cdots \oplus M_k$ is defined to be the set of ordered k-tuples $(x_1, x_2, \ldots, x_k)$, where $x_i \in M_i$ for $i = 1, 2, \ldots, k$. This direct sum is itself an R-module:

$$\begin{aligned}(x_1, x_2, \ldots, x_k) + (y_1, y_2, \ldots, y_k) &= (x_1 + y_1, x_2 + y_2, \ldots, x_k + y_k),\\ r(x_1, x_2, \ldots, x_k) &= (rx_1, rx_2, \ldots, rx_k)\end{aligned}$$

for all $x_i, y_i \in M_i$ and $r \in R$.

If K is any field, then K^n is the direct sum of n copies of K.

Definition Let M be a module over some unital commutative ring R. Given any subset X of M, the submodule of M generated by the set X is defined to be the intersection of all submodules of M that contain the set X. It is therefore the smallest submodule of M that contains the set X. An R-module M is said to be *finitely-generated* if it is generated by some finite subset of itself.

Lemma 3.1 *Let M be a module over some unital commutative ring R, and let $\{x_1, x_2, \ldots, x_k\}$ be a finite subset of M. Then the submodule of M generated by this set consists of all elements of M that are of the form*

$$r_1x_1 + r_2x_2 + \cdots + r_kx_k$$

for some $r_1, r_2, \ldots, r_k \in R$.

Proof The subset of M consisting of all elements of M of this form is clearly a submodule of M. Moreover it is contained in every submodule of M that contains the set $\{x_1, x_2, \ldots, x_k\}$. The result follows. ∎

3.2 Noetherian Modules

Definition Let R be a unital commutative ring. An R-module M is said to be *Noetherian* if every submodule of M is finitely-generated.

Proposition 3.2 *Let R be a unital commutative ring, and let M be a module over R. Then the following are equivalent:—*

(i) (Ascending Chain Condition) *if $L_1 \subset L_2 \subset L_3 \subset \cdots$ is an ascending chain of submodules of M then there exists an integer N such that $L_n = L_N$ for all $n \geq N$;*

(ii) (Maximal Condition) *every non-empty collection of submodules of M has a maximal element (i.e., an submodule which is not contained in any other submodule belonging to the collection);*

(iii) (Finite Basis Condition) *M is a Noetherian R-module (i.e., every submodule of M is finitely-generated).*

Proof Suppose that M satisfies the Ascending Chain Condition. Let $\mathcal{C}$ be a non-empty collection of submodules of M. Choose $L_1 \in \mathcal{C}$. If $\mathcal{C}$ were to contain no maximal element then we could choose, by induction on n, an ascending chain $L_1 \subset L_2 \subset L_3 \subset \cdots$ of submodules belonging to $\mathcal{C}$ such that $L_n \neq L_{n+1}$ for all n, which would contradict the Ascending Chain Condition. Thus M must satisfy the Maximal Condition.

Next suppose that M satisfies the Maximal Condition. Let L be an submodule of M, and let $\mathcal{C}$ be the collection of all finitely-generated submodules of M that are contained in L. Now the zero submodule $\{0\}$ belongs to $\mathcal{C}$, hence $\mathcal{C}$ contains a maximal element J, and J is generated by some finite subset $\{a_1, a_2, \ldots, a_k\}$ of M. Let $x \in L$, and let K be the submodule generated by $\{x, a_1, a_2, \ldots, a_k\}$. Then $K \in \mathcal{C}$, and $J \subset K$. It follows from the maximality of J that $J = K$, and thus $x \in J$. Therefore $J = L$, and thus L is finitely-generated. Thus M must satisfy the Finite Basis Condition.

Finally suppose that M satisfies the Finite Basis Condition. Let $L_1 \subset L_2 \subset L_3 \subset \cdots$ be an ascending chain of submodules of M, and let L be the union $\bigcup_{n=1}^{+\infty} L_n$ of the submodules L_n. Then L is itself an submodule of M. Indeed if a and b are elements of L then a and b both belong to L_n for some sufficiently large n, and hence $a + b$, $-a$ and ra belong to L_n, and thus to L, for all $r \in M$. But the submodule L is finitely-generated. Let $\{a_1, a_2, \ldots, a_k\}$ be a generating set of L. Choose N large enough to ensure that $a_i \in L_N$ for $i = 1, 2, \ldots, k$. Then $L \subset L_N$, and hence $L_N = L_n = L$ for all $n \geq N$. Thus M must satisfy the Ascending Chain Condition, as required. ∎

Proposition 3.3 *Let R be a unital commutative ring, let M be an R-module, and let L be a submodule of M. Then M is Noetherian if and only if L and M/L are Noetherian.*

Proof Suppose that the R-module M is Noetherian. Then the submodule L is also Noetherian, since any submodule of L is also a submodule of M and is therefore finitely-generated. Also any submodule K of M/L is of the form $\{L + x : x \in J\}$ for some submodule J of M satisfying $L \subset J$. But J is finitely-generated (since M is Noetherian). Let $x_1, x_2, \ldots, x_k$ be a finite generating set for J. Then

$$L + x_1, L + x_2, \ldots, L + x_k$$

is a finite generating set for K. Thus M/L is Noetherian.

Conversely, suppose that L and M/L are Noetherian. We must show that M is Noetherian. Let J be any submodule of M, and let $\nu(J)$ be the image of J under the quotient homomorphism $\nu\colon M \to M/L$, where $\nu(x) = L + x$ for all $x \in M$. Then $\nu(J)$ is a submodule of the Noetherian module M/L and is therefore finitely-generated. It follows that there exist elements $x_1, x_2, \ldots, x_k$ of J such that $\nu(J)$ is generated by

$$L + x_1, L + x_2, \ldots, L + x_k.$$

Also $J \cap L$ is a submodule of the Noetherian module L, and therefore there exists a finite generating set $y_1, y_2, \ldots, y_m$ for $J \cap L$. We claim that

$$\{x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_m\}$$

is a generating set for J.

Let $z \in J$. Then there exist $r_1, r_2, \ldots, r_k \in R$ such that

$$\nu(z) = r_1(L+x_1)+r_2(L+x_2)+\cdots+r_k(L+x_k) = L+r_1x_1+r_2x_2+\cdots+r_kx_k.$$

But then $z-(r_1x_1+r_2x_2+\cdots+r_kx_k) \in J\cap L$ (since $L = \ker\nu$), and therefore there exist $s_1, s_2, \ldots, s_m$ such that

$$z - (r_1x_1 + r_2x_2 + \cdots + r_kx_k) = s_1y_1 + s_2y_2 + \cdots + s_my_m,$$

and thus

$$z = \sum_{i=1}^{k} r_ix_i + \sum_{j=1}^{m} s_iy_i.$$

This shows that the submodule J of M is finitely-generated. We deduce that M is Noetherian, as required. ∎

Corollary 3.4 *The direct sum $M_1 \oplus M_2 \oplus \cdots \oplus M_k$ of Noetherian modules $M_1, M_2, \ldots M_k$ over some unital commutative ring R is itself a Noetherian module over R.*

Proof The result follows easily by induction on k once it has been proved in the case $k = 2$.

Let M_1 and M_2 be Noetherian R-modules. Then $M_1 \oplus \{0\}$ is a Noetherian submodule of $M_1 \oplus M_2$ isomorphic to M_1, and the quotient of $M_1 \oplus M_2$ by this submodule is a Noetherian R-module isomorphic to M_2. It follows from Proposition 3.3 that $M_1 \oplus M_2$ is Noetherian, as required. ∎

One can define also the concept of a module over a non-commutative ring. Let R be a unital ring (not necessarily commutative), and let M be an Abelian group. We say that M is a *left R-module* if each $r \in R$ and $m \in M$ determine an element rm of M, and the identities

$$r(x + y) = rx + ry, \qquad (r + s)x = rx + sx, \qquad (rs)x = r(sx), \qquad 1x = x$$

are satisfied for all $x, y \in M$ and $r, s \in R$. Similarly we say that M is a *right R-module* if each $r \in R$ and $m \in M$ determine an element mr of M, and the identities

$$(x + y)r = xr + yr, \qquad x(r + s) = xr + xs, \qquad x(rs) = (xr)s, \qquad x1 = x$$

are satisfied for all $x, y \in M$ and $r, s \in R$. (If R is commutative then the distinction between left R-modules and right R-modules is simply a question of notation; this is not the case if R is non-commutative.)

3.3 Noetherian Rings and Hilbert's Basis Theorem

Let R be a unital commutative ring. We can regard the ring R as an R-module, where the ring R acts on itself by left multiplication (so that $r \,.\, r'$ is the product rr' of r and r' for all elements r and r' of R). We then find that a subset of R is an ideal of R if and only if it is a submodule of R. The following result therefore follows directly from Proposition 3.2.

Proposition 3.5 *Let R be a unital commutative ring. Then the following are equivalent:—*

(i) (Ascending Chain Condition) *if $I_1 \subset I_2 \subset I_3 \subset \cdots$ is an ascending chain of ideals of R then there exists an integer N such that $I_n = I_N$ for all $n \geq N$;*

(ii) (Maximal Condition) *every non-empty collection of ideals of R has a maximal element (i.e., an ideal which is not contained in any other ideal belonging to the collection);*

(iii) (Finite Basis Condition) *every ideal of R is finitely-generated.*

Definition A unital commutative ring is said to be a *Noetherian ring* if every ideal of the ring is finitely-generated. A *Noetherian domain* is a Noetherian ring that is also an integral domain.

Note that a unital commutative ring R is Noetherian if it satisfies any one of the conditions of Proposition 3.5.

Corollary 3.6 *Let M be a finitely-generated module over a Noetherian ring R. Then M is a Noetherian R-module.*

Proof Let $\{x_1, x_2, \ldots, x_k\}$ be a finite generating set for M. Let R^k be the direct sum of k copies of R, and let $\varphi\colon R^k \to M$ be the homomorphism of R-modules sending $(r_1, r_2, \ldots, r_k) \in R^k$ to

$$r_1 x_1 + r_2 x_2 + \cdots + r_k x_k.$$

It follows from Corollary 3.4 that R^k is a Noetherian R-module (since the Noetherian ring R is itself a Noetherian R-module). Moreover M is isomorphic to $R^k / \ker \varphi$, since $\varphi\colon R^k \to M$ is surjective. It follows from Proposition 3.3 that M is Noetherian, as required. ∎

If I is a proper ideal of a Noetherian ring R then the collection of all proper ideals of R that contain the ideal I is clearly non-empty (since I itself belongs to the collection). It follows immediately from the Maximal Condition that I is contained in some maximal ideal of R.

Lemma 3.7 *Let R be a Noetherian ring, and let I be an ideal of R. Then the quotient ring R/I is Noetherian.*

Proof Let L be an ideal of R/I, and let $J = \{x \in R : I + x \in L\}$. Then J is an ideal of R, and therefore there exists a finite subset $\{a_1, a_2, \ldots, a_k\}$ of J which generates J. But then L is generated by $I + a_i$ for $i = 1, 2, \ldots, k$. Indeed every element of L is of the form $I + x$ for some $x \in J$, and if

$$x = r_1 a_1 + r_2 a_2 + \cdots + r_k a_k$$

, where $r_1, r_2, \ldots, r_k \in R$, then

$$I + x = r_1(I + a_1) + r_2(I + a_2) + \cdots + r_k(I + a_k),$$

as required. ∎

Hilbert showed that if R is a field or is the ring $\mathbb{Z}$ of integers, then every ideal of $R[x_1, x_2, \ldots, x_n]$ is finitely-generated. The method that Hilbert used to prove this result can be generalized to yield the following theorem.

Theorem 3.8 (Hilbert's Basis Theorem) *If R is a Noetherian ring, then so is the polynomial ring $R[x]$.*

Proof Let I be an ideal of $R[x]$, and, for each non-negative integer n, let I_n denote the subset of R consisting of those elements of R that occur as leading coefficients of polynomials of degree n belonging to I, together with the zero element of R. Then I_n is an ideal of R. Moreover $I_n \subset I_{n+1}$, for if $p(x)$ is a polynomial of degree n belonging to I then $xp(x)$ is a polynomial of degree $n+1$ belonging to I which has the same leading coefficient. Thus $I_0 \subset I_1 \subset I_2 \subset \cdots$ is an ascending chain of ideals of R. But the Noetherian ring R satisfies the Ascending Chain Condition (see Proposition 3.5). Therefore there exists some natural number m such that $I_n = I_m$ for all $n \geq m$.

Now each ideal I_n is finitely-generated, hence, for each $n \leq m$, we can choose a finite set $\{a_{n,1}, a_{n,2}, \ldots, a_{n,k_n}\}$ which generates I_n. Moreover each generator $a_{n,i}$ is the leading coefficient of some polynomial $q_{n,i}$ of degree n belonging to I. Let J be the ideal of $R[x]$ generated by the polynomials $q_{n,i}$ for all $0 \leq n \leq m$ and $1 \leq i \leq k_n$. Then J is finitely-generated. We shall show by induction on $\deg p$ that every polynomial p belonging to I must belong to J, and thus $I = J$. Now if $p \in I$ and $\deg p = 0$ then p is a constant polynomial whose value belongs to I_0 (by definition of I_0), and thus p is a linear combination of the constant polynomials $q_{0,i}$ (since the values $a_{0,i}$ of the constant polynomials $q_{0,i}$ generate I_0), showing that $p \in J$. Thus the result holds for all $p \in I$ of degree 0.

Now suppose that $p \in I$ is a polynomial of degree n and that the result is true for all polynomials p in I of degree less than n. Consider first the case when $n \leq m$. Let b be the leading coefficient of p. Then there exist $c_1, c_2, \ldots, c_{k_n} \in R$ such that

$$b = c_1 a_{n,1} + c_2 a_{n,2} + \cdots + c_{k_n} a_{n,k_n},$$

since $a_{n,1}, a_{n,2}, \ldots, a_{n,k_n}$ generate the ideal I_n of R. Then

$$p(x) = c_1 q_{n,1}(x) + c_2 q_{n,2}(x) + \cdots + c_k q_{n,k}(x) + r(x),$$

where $r \in I$ and $\deg r < \deg p$. It follows from the induction hypothesis that $r \in J$. But then $p \in J$. This proves the result for all polynomials p in I satisfying $\deg p \leq m$.

Finally suppose that $p \in I$ is a polynomial of degree n where $n > m$, and that the result has been verified for all polynomials of degree less than n.

Then the leading coefficient b of p belongs to I_n. But $I_n = I_m$, since $n \geq m$. As before, we see that there exist $c_1, c_2, \ldots, c_{k_m} \in R$ such that

$$b = c_1 a_{m,1} + c_2 a_{m,2} + \cdots + c_{k_n} a_{m,k_m},$$

since $a_{m,1}, a_{m,2}, \ldots, a_{m,k_m}$ generate the ideal I_n of R. Then

$$p(x) = c_1 x^{n-m} q_{m,1}(x) + c_2 x^{n-m} q_{m,2}(x) + \cdots + c_k x^{n-m} q_{m,k}(x) + r(x),$$

where $r \in I$ and $\deg r < \deg p$. It follows from the induction hypothesis that $r \in J$. But then $p \in J$. This proves the result for all polynomials p in I satisfying $\deg p > m$. Therefore $I = J$, and thus I is finitely-generated, as required. ∎

Theorem 3.9 *Let R be a Noetherian ring. Then the ring $R[x_1, x_2, \ldots, x_n]$ of polynomials in the indeterminates $x_1, x_2, \ldots, x_n$ with coefficients in R is a Noetherian ring.*

Proof It is easy to see that $R[x_1, x_2, \ldots, x_n]$ is naturally isomorphic to $R[x_1, x_2, \ldots, x_{n-1}][x_n]$ when $n > 1$. (Any polynomial in the indeterminates $x_1, x_2, \ldots, x_n$ with coefficients in the ring R may be viewed as a polynomial in the indeterminate x_n whose coefficients are in the polynomial ring $R[x_1, x_2, \ldots, x_{n-1}]$.) The required results therefore follows from Hilbert's Basis Theorem (Theorem 3.8) by induction on n. ∎

Corollary 3.10 *Let K be a field. Then every ideal of the polynomial ring $K[x_1, x_2, \ldots, x_n]$ is finitely-generated.*