COMMUTATIVE ALGEBRA NOTES - LECTURE 9

ENNES MEHMEDBASIC

In this lecture we look at some useful facts about when a ring or module is Noetherian, finishing with a proof of the Hilbert basis theorem, which states that if R is a Noetherian ring, then so is $R[x]$.

Reminder. A ring R is Noetherian if its ideals satisfy the ascending chain condition. A module M is Noetherian if its submodules satisfy the ascending chain condition.

1. Facts About Noetherian Rings/Modules

Proposition 1.1. *Let R be a ring, and let*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

be a short exact sequence of R-modules. Then M is Noetherian if and only if M' and M'' are both Noetherian.

Proof. First we assume that M is Noetherian. Let $M'_1 \subset M'_2 \subset \cdots$ be an ascending chain of submodules of M'. Then $f(M'_1) \subset f(M'_2) \subset \cdots$ is an ascending chain of submodules of M, since f is an R-module map. Since M is Noetherian, there exists some $n \in \mathbb{N}$ such that $f(M'_n) = f(M'_k)$ for all $k \geq n$. And because f is injective, it follows that $M'_n = M'_k$ for all $k \geq n$, so M' satisfies the ascending chain condition. Hence M' is a Noetherian R-module.
Now let $M''_1 \subset M''_2 \subset \cdots$ be an ascending chain of submodules of M''. Then $g^{-1}(M''_1) \subset g^{-1}(M''_2) \subset \cdots$ is an ascending chain of submodules of M, since g is an R-module map. So there exists $m \in \mathbb{N}$ such that $g^{-1}(M''_m) = g^{-1}(M''_k)$ for all $k \geq m$. It follows by the surjectivity of g that $M''_m = g(g^{-1}(M''_m)) = g(g^{-1}(M''_k)) = M''_k$ for all $k \geq m$, and so M'' satisfies the ascending chain condition. Hence M'' is also a Noetherian R-module.
Conversely, suppose that M' and M'' are both Noetherian. We show that then M is also a Noetherian R-module.
Let $M_1 \subset M_2 \subset \cdots$ be a chain of submodules in M. Then $f^{-1}(M_1) \subset f^{-1}(M_2) \subset \cdots$ and $g(M_1) \subset g(M_2) \subset \cdots$ are chains of submodules in M' and M'' respectively. Then there exists $n \in \mathbb{N}$ such that $f^{-1}(M_n) = f^{-1}(M_k)$ and $g(M_n) = g(M_k)$ for all $k \geq n$. We show that $\{M_k\}_{k\in\mathbb{N}}$ stabilises at n.
Let $x \in M_{n+j}$ where $j \geq 1$. Then $g(x) \in g(M_{n+j}) = g(M_n)$, and so there exists $p \in M_n$ such that $g(x) = g(p)$. This implies that $x - p \in \ker(g) = \mathrm{im}(f)$. Now p is also in M_{n+j}, so $f^{-1}(x-p) \subset f^{-1}(M_{n+j}) = f^{-1}(M_n)$, from which it follows by the

injectivity of f that there is a unique element $q \in f^{-1}(M_n)$ such that $f(q) = x - p$. Therefore $x - p \in M_n$, and so $x = (x - p) + p \in M_n$. Hence $M_n = M_{n+j}$ for all $j \geq 1$, and so M is a Noetherian R-module (since the chain $\{M_k\}_{k\in\mathbb{N}}$ was arbitrary). □

We next derive some corollaries from this proposition.

Corollary 1.2. *Let R be a ring, $M_1, \ldots, M_n$ R-modules. Then $M_1, \ldots, M_n$ are Noetherian R-modules if and only if $M_1 \oplus \cdots \oplus M_n$ is a Noetherian R-module.*

Proof. Suppose $M_1, \ldots, M_n$ are Noetherian R-modules. Then there is a (split) short exact sequence $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$, and it follows from Proposition 1.1 that $M_1 \oplus M_2$ is a Noetherian R-module. Using this process inductively, and the fact that $M_1 \oplus \cdots \oplus M_k = (M_1 \oplus \cdots \oplus M_{k-1}) \oplus M_k$, we get that $M_1 \oplus \cdots \oplus M_n$ is a Noetherian R-module.
Conversely, suppose $M_1 \oplus \cdots \oplus M_n$ is a Noetherian R-module. Then for each $j \in \{1, \ldots, n\}$ there is a short exact sequence

$$0 \to \bigoplus_{k\neq j} M_k \to M_1 \oplus \cdots \oplus M_n \to M_j \to 0.$$

Hence, by Proposition 1.1, M_j is a Noetherian R-module for all $j \in \{1, \ldots, n\}$. □

Corollary 1.3. *Let R be a Noetherian ring. Then M is a Noetherian R-module if and only if M is finitely generated as an R-module.*

Proof. Suppose M is not finitely generated as an R-module. Take $m_1 \in M$ such that $m_1 \neq 0$. Then $R \cdot m_1 \subsetneq M$. Define the sequence inductively by choosing $m_{n+1} \in M \setminus (R \cdot m_1 + \cdots + R \cdot m_n)$. Therefore the chain of submodules $R \cdot m_1 \subset R \cdot m_1 + R \cdot m_2 \subset \cdots$ does not stabilise, and so M is not a Noetherian ring. Hence if M is Noetherian, it is finitely generated as an R-module.
Conversely, suppose that M is finitely generated as an R-module, so $M = R \cdot m_1 + \cdots + R \cdot m_r$. Hence we have a surjective map

$$f : R^r \to M$$
$$(x_1, \ldots, x_r) \mapsto x_1 \cdot m_1 + \cdots + x_r \cdot m_r$$

from which we can construct the short exact sequence

$$0 \to \ker(f) \to R^r \to M \to 0.$$

R can be considered as an R-module, and in this case, the submodules are precisely the same subsets as the ideals of R, so R is a Noetherian R-module. From Corollary 1.2 it follows that R^r is a Noetherian R-module. Hence, by Proposition 1.1, M is a Noetherian R-module. □

Corollary 1.4. *Let R be a Noetherian ring, and $\varphi : R \to S$ a ring homomorphism such that S is finitely generated as an R-module (where $r \cdot s = \varphi(r)s$ for $r \in R$ and $s \in S$). Then S is a Noetherian ring.*

Proof. As S is finitely generated as an R-module, we have that S is a Noetherian R-module from Corollary 1.3. Now let $I < S$ be an ideal. Then $st \in I$ for all $s \in S$ and $t \in I$. In particular, $\varphi(r)t \in I$ for all $r \in R$ and $t \in I$. Hence the ideals of the ring S are all submodules of the R-module S. Therefore the ideals of S satisfy the ascending chain condition, and so S is a Noetherian ring. □

Remark. Note also that if M is a Noetherian R-module, then all submodules of M are Noetherian. This is because if N is a submodule of M, then submodules of N are also submodules of M. The same however is not true for subrings of Noetherian rings. Consider the ring of algebraic integers $\mathbf{A}$ (defined to be the set of roots in $\mathbb{C}$ of monic polynomials in $\mathbb{Z}[x]$) as a subring of the complex numbers $\mathbb{C}$. Then $\mathbb{C}$ is clearly Noetherian, as it only contains two ideals. On the other hand $(2) \subset (2^{\frac{1}{2}}) \subset \cdots \subset (2^{\frac{1}{2^n}}) \subset \cdots$ is an ascending chain of ideals in $\mathbf{A}$ which never stabilises, and so $\mathbf{A}$ is not a Noetherian ring.

2. The Hilbert Basis Theorem

History. Let Γ be a finite group acting on an arbitrary ring R (for example, the symmetric group on n symbols acting on the ring $\mathbb{Z}[x_1, \ldots, x_n]$ by permuting the variables). It was a general question around the time of Hilbert's proof of this theorem whether or not $R^\Gamma := \{f \in R | \gamma \cdot f = f \ \forall \gamma \in \Gamma\}$ was finitely generated. Hilbert used this theorem to acquire a general result (which will be constructed in a future lecture).

Theorem 2.1 (Hilbert Basis Theorem)**.** *Let R be a Noetherian ring. Then $R[x]$ is also a Noetherian ring.*

Proof. Let $I < R[x]$ be an ideal. We show that I is finitely generated.
Define $J_n := \{r \in R | \exists f \in I \text{ where } f(x) = rx^n + \cdots\}$, so J_n is the set of all leading coefficients of polynomials of degree n in I (we define the leading coefficient of f to be zero if $\deg(f) < n$). Denote the leading coefficient of a polynomial f by $\mathrm{LC}(f)$.
J_n is an ideal, since if $r \in R$ and $s \in J_n$, then there exists some $f \in I$ such that $\mathrm{LC}(f) = s$, and hence $\mathrm{LC}(rf) = rs$, so that $rs \in J_n$. Clearly J_n is closed under addition and subtraction.
Note also that $J_n \subset J_{n+1}$ for all $n \in \mathbb{N}$. This is because if $r \in J_n$, then there is a polynomial $f \in R[x]$ such that $\deg(f) = n$ and $LC(f) = r$. Then $xf(x)$ is a polynomial of degree $n+1$ with leading coefficient r.
Therefore $\{J_n\}_{n \in \mathbb{N}}$ is an ascending chain of ideals in R, which stabilises because R is Noetherian. So there is $n \in \mathbb{N}$ such that $J_n = J_k$ for all $k \geq n$.
Let $m \leq n$. Then since J_m is finitely generated, we can write $J_m = (r_{m,1}, \ldots, r_{m,i_m})$. And so for each m, j where $0 \leq m \leq n$ and $1 \leq j \leq i_m$, there exists a polynomial $f_{m,j} \in I$ such that $\mathrm{LC}(f_{m,j}) = r_{m,j}$ and $\deg(f_{m,j}) = m$. Consider the finite set $S = \{f_{m,j} | 0 \leq m \leq n, 1 \leq j \leq i_m\}$. We show that S generates the ideal I, using induction on the degree of f.

Let $f \in I$. If $\deg(f) = 0$ or $f = 0$, then $f \in J_0$ if we identify constant polynomials with the value of the constant, so $f \in (f_{0,j} | j = 1, \ldots, i_0)$.
Now suppose that $f \in (S)$ for all f with degree less than m. We show that if $\deg(f) = m$, then $f \in (S)$ by splitting this into two cases.
(Case 1) If $m \geq n$, then $r = \mathrm{LC}(f) \in J_m = J_n$, therefore $r = \sum_{j=1}^{i_n} b_j r_{n,j}$ for some $b_j \in R$. Then the polynomial

$$f - \sum_{j=1}^{i_n} b_j x^{m-n} f_{n,j}$$

has degree less than m since the leading term of the sum is equal to the leading term of f, so we can apply the induction hypothesis to get that

$$f - \sum_{j=1}^{i_n} b_j x^{m-n} f_{n,j} = \sum_{k=1}^{l} c_k g_k \Rightarrow f = \sum_{j=1}^{i_n} b_j x^{m-n} f_{n,j} + \sum_{k=1}^{l} c_k g_k$$

for some $c_k \in R[x]$ and some $g_k \in S$. Therefore $f \in (S)$.
(Case 2) If $m < n$, then $r = \mathrm{LC}(f) \in J_m$, therefore $r = \sum_{j=1}^{i_m} b_j r_{m,j}$ for some $b_j \in R$. Then the polynomial

$$f - \sum_{j=1}^{i_m} b_j f_{m,j}$$

has degree less than m, for the same reason as in Case 1. Hence we can apply the induction hypothesis to get that

$$f - \sum_{j=1}^{i_m} b_j f_{m,j} = \sum_{k=1}^{l} c_k g_k \Rightarrow f = \sum_{j=1}^{i_m} b_j f_{m,j} + \sum_{k=1}^{l} c_k g_k$$

where again $c_k \in R[x]$ and $g_k \in S$. Therefore $f \in (S)$.
So we have shown that $I \subset (S)$, but then $S \subset I$ implies that $I = (S)$. As I was an arbitrary ideal in $R[x]$, it follows that all ideals of $R[x]$ are finitely generated, and hence $R[x]$ is a Noetherian ring. □

Corollary 2.2. *If R is a Noetherian ring, then so is $R[x_1, \ldots, x_n]$ for all $n \geq 1$.*

Proof. By the Hilbert basis theorem, if $R[x_1, \ldots, x_k]$ is Noetherian, then so is $R[x_1, \ldots, x_{k+1}]$. Since R is Noetherian, it follows directly from the Hilbert basis theorem that $R[x]$ is Noetherian, and so using these two facts, we have that $R[x_1, \ldots, x_n]$ is Noetherian for all $n \geq 1$. □