SI112: Advanced Geometry		Spring 2018
	Lecture 16-18 — May 3rd, Tuesday	
Prof. Manolis		*Scribe*: Liangzu

1 Lecture 16-18

Consistency is the last refuge of the unimaginative.

—— Oscar Wilde

1.1 Overview of This Lecture

It turns out to be a brave thoughtlessness to refer to x^α as (multi-variable) monomials, as I used to do. It is painful to type $\underline{x}$ (the underline) in LaTeX, you know, very similar to the reason why Unix pioneers use the string *cp(mv)* instead of *copy(move)* to denote the command copy(move). Brave again, the symbol x from now on will be used to denote simply a single variable.

The goal of these three lectures is to prove Hilbert Basis Theorem, as described below.

Theorem 1.1.1 (Hilbert Basis Theorem)**.** *If every ideal of a ring R is finitely generated, then so is every ideal of $R[x]$.*

Corollary 1.1.2. *If every ideal of a ring R is finitely generated, then so is every ideal of $R[x_1, x_2, \dots, x_n]$.*

1.2 Proof of Things

Definition 1.2.1 (module M over a ring R)**.** Let R be a ring. An *R-module* (or *module over R*) M consists of an abelian group $(M, +)$ and multiplication operation, denoted by juxtaposition, $R \times M \to M$ such that for all $r, s \in R$ and $u, v \in M$

- $r(u + v) = ru + rv$
- $(r + s)u = ru + su$
- $(rs)u = r(su)$
- $1u = u$

The ring R is called the *base ring* of M.

Definition 1.2.2 (submodule)**.** A *submodule* of an R-module M is a nonempty subset S of M that is an R-module in its own right, under the operations obtained by restricting the operations of M to S.

Proposition 1.2.3. *A nonempty subset S of an R-module M is a submodule if and only if it is closed under the taking of linear combinations, that is,*

$$r, s, \in R, u, v \in S \Rightarrow ru + sv \in S.$$

Proof. Left as an exercise. □

Proposition 1.2.4. *If S and T are submodules of a module M, then $S \cap T$ and $S + T$ are also submodules.*

Proof. Left as an exercise. □

Example 1.2.5. Vector space V over a field $\mathbb{F}$ is a module over $\mathbb{F}$.

Example 1.2.6. If R is a ring, then the sets $\mathbb{F}^n$, R^n are R-modules.

Example 1.2.7. The ring R is an R-module. Furthermore, every ideal of a ring R is a module, and thus a submodule of R. Finally and similarly, $R[x]$ is an R-module and every ideal of $R[x]$ is a submodule. You are invited to verify the converse: is every submodule of R or $R[x]$ an ideal?

Definition 1.2.8 (finitely generated ideal)**.** Let I be an ideal of the ring R. We said that I is *finitely generated* if there exist $\alpha_1, \alpha_2, \ldots, \alpha_n \in I$ such that for each $\alpha \in I$, there exist $r_1, r_2, \ldots, r_n \in R$ satisfying

$$\alpha = r_1\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n.$$

The set $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is called *generating set* of I. We may also write for convenience like this: $I = R\alpha_1 + R\alpha_2 + \cdots + R\alpha_n$, where the symbol Rx is defined as $Rx = \{x' : x' = rx \text{ for some } r \in R\}$.

Definition 1.2.9 (finitely generated module)**.** An R-module M is finitely generated if there exists $\alpha_1, \alpha_2, \ldots, \alpha_n \in M$ such that for each $\alpha \in M$, there exist $r_1, r_2, \ldots, r_n \in R$ satisfying

$$\alpha = r_1\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n.$$

Remark 1.2.10. Notice in Definition 1.2.8 and Definition 1.2.9 that an ideal is a subset of a ring, while the module M is over a ring.

Definition 1.2.11 (morphism of R-modules)**.** Let M and M be R-modules. Then the function $f : M \to N$ is called a *morphism* from M to N if

- $f(x + y) = f(x) + f(y)$ for all $x, y \in M$
- $f(\alpha x) = \alpha f(x)$ for all $\alpha \in R, x \in M$

In addition, we define the set

$$\mathrm{Ker}(f) = \{x \in M : f(x) = 0\}$$

as the *kernel* of f and the set

$$\mathrm{Im}(f) = \{y \in N : y = f(x) \text{ for some } x \in M\}$$

the *image* of f.

Proposition 1.2.12. *Let $f : M \to N$ be a morphism of R-modules. Then the kernel* $\mathrm{Ker}(f)$ *and image* $\mathrm{Im}(f)$ *of f are submodules of M and N, respectively.*

Proof. Let $x_1, x_2 \in \mathrm{Ker}(f), r_1, r_2 \in R$. Then

- $f(r_1x_1 + r_2x_2) = r_1f(x_1) + r_2f(x_2) = 0$, which implies $r_1x_1 + r_2x_2 \in \mathrm{Ker}\, f$.
- $f(r_1x_1) \in \mathrm{Im}(f)$.

□

Exercise 1.2.13. Let $f : M \to N$ be a morphism of R-modules. Show that $f(0) = 0$.

Proposition 1.2.14. *Let $f : M \to N$ be a morphism of R-modules. Then f is injective if and only if* $\mathrm{Ker}(f) = \{0\}$.

Proof.

- Suppose f is injective and let $x \in \mathrm{Ker}(f)$. Then $f(x) = 0 = f(0)$. This implies $x = 0$.
- Suppose $\mathrm{Ker}(f) = \{0\}$ and let $x_1, x_2 \in M$ be such that $f(x_1) = f(x_2)$. Then

$$f(x_1 - x_2) = 0 \Rightarrow x_1 - x_2 \in \mathrm{Ker}(f) \Rightarrow x_1 - x_2 = 0.$$

□

Definition 1.2.15 (exact sequence)**.** A sequence

$$M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} M_2 \xrightarrow{f_3} \cdots \xrightarrow{f_n} M_n,$$

where f_i's are morphisms and M_i are modules, is called *exact* if the image of each morphism is equal to the kernel of the next, i.e., $\mathrm{Im}(f_k) = \mathrm{Ker}(f_{k+1})$ for $k = 0, 1, \ldots, n - 1$.

Exercise 1.2.16. Let $\{0\} \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to \{0\}$ be an exact sequence. Show that f is injective and g is surjective.

Example 1.2.17. Let R be a ring and $S = \{0\} \to R \xrightarrow{f} R^n \xrightarrow{g} R^{n-1} \to \{0\}$ a sequence. Then S is exact for the function $f : \alpha \mapsto (0_1, \ldots, 0_{n-1}, \alpha)$ and the function $g : (\alpha_1, \alpha_2, \ldots, \alpha_n) \mapsto (\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$, where $a_i \in R$ for $i = 1, \ldots, n$.

You may want to review the definitions of partially ordered set and maximal element. Check lecture 1 or wikipedia.

Proposition 1.2.18 (6.1\AM)**.** *Let Σ be a partially ordered set and $\leq$ the partial order relation on Σ. The following conditions on Σ are equivalent.*

1. *Every increasing sequence $x_1 \leq x_2 \leq \cdots$ in Σ is stationary, i.e., there exists a number n such that $x_n = x_{n+1} = \ldots$.*

2. *Every nonempty subset of Σ has a maximal element.*

Proof.

1. ($1 \Rightarrow 2$) Let S is a nonempty subset of Σ. Suppose for the sake of contradiction that S has no maximal element. Then there is an element a_1 in S though a_1 is not maximal. Hence there is an element $a_2 \in S$ such that $a_1 < a_2$. But a_2 can not be a maximal element. Inductively we can construct a non-terminating strictly increasing sequence in S. This is a contradiction.

2. ($2 \Rightarrow 1$) Let $x_1 \leq x_2 \leq \cdots$ be an increasing sequence in Σ. The sequence forms a set, say S. Let x_n be a maximal element of S. Then we have $x_n = x_{n+1} = \ldots$, i.e., this sequence is stationary.

□

Remark 1.2.19. If Σ is the set of submodules of a module M, ordered by set inclusion $\subset$, then the condition (1) is called *ascending chain condition* (a.c.c or ACC for short). A module M satisfying either of these equivalent conditions is said to be *Noetherian* (after Emmy Noether).

Definition 1.2.20 (Noetherian)**.** Let M be an R-module. R is *Noetherian* if it satisfies the ACC on the set of its submodules.

Exercise 1.2.21. Prove that if a module is Noetherian, then all of its submodules are Noetherian.

Proposition 1.2.22 (6.2\AM)**.** *M is Noetherian R-module if and only if every submodule of M is finitely generated.*

Proof.

- Suppose that M is a Neotherian R-module. Let N be a submodule of M. We need to prove that N is finitely generated. Let Σ be the set of all finitely generated submodules of N. Then we know that Σ is not empty ($\{0\} \in \Sigma$) and there therefore exists some maximal element N_0 of Σ (why?). If $N = N_0$ we are done. Otherwise let $y \in N \backslash N_0$, then $N_0 + Ry$ properly contains N_0. But the set $N_0 + Ry$ properly containing N_0 is finitely generated, implying $N_0 + Ry \in \Sigma$, which contradicts the maximality of N_0.

- Suppose that every submodule of M is finitely generated. Let $M_1 \subset M_2 \subset \cdots$ be an ascending chain of submodules of M. Then $N = \cup_{i=1}^{\infty} M_i$ is a submodule of M (why?). Hence N is finitely generated, i.e., there exist some $x_1, x_2, \ldots, x_n \in N$ such that $N = Rx_1 + Rx_2 + \cdots Rx_n$. Now suppose $x_i \in M_{k_i}$ for $i = 1, \ldots, n$ and let $k = \max_{i=1,\ldots,n}\{k_i\}$. Then $x_1, x_2, \ldots, x_n \in M_k$. Then we have

  $$N = Rx_1 + Rx_2 + \cdots + Rx_n \subset M_k \subset N,$$

  which means $M_k = N$. Hence $N = M_k = M_{k+1} = \ldots$, that is, the ascending chain

  $$M_1 \subset M_2 \subset \cdots$$

  is stable.

□

Hilbert Basis Theorem (Theorem 1.1.1) then can be equivalently stated as follows.

Theorem 1.2.23. *If R is a Noetherian ring, then $R[x]$ is a Noetherian ring.*

Corollary 1.2.24. *If R is a Noetherian ring, then $R[x_1, x_2, \ldots, x_n]$ is a Noetherian ring.*

Exercise 1.2.25 (p)**.** Let $f : M' \to M$ be a morphism of R-modules and S', S submodules of M', M respectively. Prove that $f(S'), f^{-1}(S)$ are submodules of M, M' respectively.

Lemma 1.2.26 (p)**.** *Let $f : M' \to M$ be an injective function and let S_1, S_2 be subset of M such that $f^{-1}(S_1) = f^{-1}(S_2)$. Then $S_1 \cap \mathrm{Im}(f) = S_2 \cap \mathrm{Im}(f)$.*

Proof. It is enough to show $S_1 \cap \mathrm{Im}(f) \subset S_2 \cap \mathrm{Im}(f)$. Another direction can be proved directly by symmetry. Let $y \in S_1 \cap \mathrm{Im}(f)$. Specifically $y \in \mathrm{Im}(f)$. Hence there exists a unique $x \in M'$ such that $x = f^{-1}(y) \iff f(x) = y$. This implies

$$x \in f^{-1}(S_1) = f^{-1}(S_2) \Rightarrow y = f(x) \in S_2.$$

□

Remark 1.2.27. Lemma 1.2.26 can be proved pictorially.

Remark 1.2.28. After Exercise1.2.25 and Lemma 1.2.26, we are able to prove the following proposition. Note that I pointed to a wrong way in piazza for this proposition. The mistake I made is that I manipulated submodules as pure sets. As a remainder, when we say that a module is Neotherian, we are saying that it is the set of its submodules that satisfy ascending chain condition.

Proposition 1.2.29 (6.3\AM)**.** *Let $\{0\} \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to \{0\}$ be an exact sequence. Then M is Neotherian if and only if M' and M'' are Neotherian.*

Proof.

- $\Rightarrow$) Suppose M is Neotherian. We need to prove M' (resp. M'') is Neotherian. Let $N_1 \subset N_2 \subset \cdots$ be an ascending chain of the submodules of M' (resp. M''). Then by Exercise 1.2.25,

  $$f(N_1) \subset f(N_2) \subset \cdots \text{ (resp. } g^{-1}(N_1) \subset g^{-1}(N_2) \subset \cdots)$$

  is an ascending chain of the submodules of M. This implies that there is some $n \in \mathbb{N}^+$ such that

  $$f(N_n) = f(N_{n+i}) \text{ (resp. } g^{-1}(N_n) = g^{-1}(N_{n+i}))$$

  for $i \in \mathbb{N}$ and thus $N_n = N_{n+i}$ for $i \in \mathbb{N}$ (by injectivity of f or surjectivity of g). Hence M' (resp. M'') is Neotherian.

- $\Leftarrow$) Suppose M' and M'' are Neotherian. We need to prove M are Neotherian. Let $S_1 \subset S_2 \subset \cdots$ be an ascending chain of the submodules of M. Then by Exercise 1.2.25,

  $$f^{-1}(S_1) \subset f^{-1}(S_2) \subset \cdots \text{ and } g(S_1) \subset g(S_2) \subset \cdots$$

  are ascending chains of the submodules of M' and M'' respectively, which implies that there are some n' and n'' such that

  $$f^{-1}(S_{n'}) = f^{-1}(S_{n'+i}) \text{ and } g(S_{n''}) = g(S_{n''+j})$$

  for $i, j \in \mathbb{N}$. Let $n = \max\{n', n''\}$. It is enough to show that $S_n = S_{n+k}$ for $k \in \mathbb{N}$. But $S_n \subset S_{n+k}$, it suffices to show that for each $a_{n+k} \in S_{n+k}$, we have $a_{n+k} \in S_k$.

  Let $a_{n+k} \in S_{n+k}$. That $g(S_{n+k}) = g(S_n)$ implies that there exists some $b_n \in S_n \subset S_{n+k}$ such that

  $$g(a_{n+k}) = g(b_n) \Rightarrow g(a_{n+k} - b_n) = 0 \Rightarrow a_{n+k} - b_n \in \text{Ker}(g) = \text{Im}(f).$$

But $a_{n+k} - b_n \in S_{n+k}$, hence by Lemma 1.2.26,

$$a_{n+k} - b_n \in S_{n+k} \cap \mathrm{Im}(f) = S_n \cap \mathrm{Im}(f) \Rightarrow a_{n+k} - b_n \in S_n.$$

Now we can conclude $a_{n+k} \in S_n$ since $b_n \in S_n$.

□

Lemma 1.2.30. *Let R be a Neotherian ring. Then R^n is Neotherian for each $n \in \mathbb{N}^+$.*

proof skeleton. Recall Example 1.2.17, Proposition 1.2.29 and use induction on n. □

Proposition 1.2.31 (6.5\AM)**.** *Let R be a Neotherian ring and M finitely generated R-module. Then M is Neotherian.*

proof skeleton. There exist some $x_1, x_2, \ldots, x_n \in M$ such that $M = Rx_1 + Rx_2 + \cdots + Rx_n$. By Lemma 1.2.30 and Proposition 1.2.29, it is enough to find a morphism $f : R^n \to M$ with f surjective. □

Now we are ready to prove the theorem.

Theorem 1.2.32 (7.5\AM, Hilbert Basis Theorem)**.** *If R is a Noetherian ring, then $R[x]$ is a Noetherian ring.*

Proof. It is enough to prove that every ideal $\overline{I}$ of $R[x]$ is finitely generated. Let

$$I = \{a \in R : \ a \text{ is the leading coefficient of } f \text{ for some } f \in \overline{I}\}.$$

Then I is an ideal since

- $0 \in I$,
- If $\alpha \in I$ and $r \in R$, then $r\alpha \in I$, and
- If $\alpha_1, \alpha_2 \in I$, then $\alpha_1 + \alpha_2 \in I$ (If $\alpha_1, \alpha_2 \in I$ then there exist $f_1, f_2 \in \overline{I}$ such that $f_1 = \alpha_1 x^{m_1} + \cdots$ and $f_2 = \alpha_2 x^{m_2} + \cdots$. Suppose without loss of generality that $m_1 \geq m_2$ and consider $f_1 + x^{m_1 - m_2} f_2$).

Since R is Neotherian and I is a submodule of R, by Proposition 1.2.22, I is finitely generated, i.e.,

$$I = R\alpha_1 + R\alpha_2 + \cdots R\alpha_n$$

for some $\alpha_1, \alpha_2, \ldots, \alpha_n \in I$. Then there exist $f_1, f_2, \ldots, f_n \in \overline{I}$ such that

$$f_i = \alpha_i x^{m_i} + \cdots \text{ for } i = 1, 2, \ldots, n.$$

Let $d_{\max} = \max\{m_1, m_2, \ldots, m_n\}$ and Let $\overline{\overline{I}}$ be the ideal generated by $f_1, f_2, \ldots, f_n$. Then $\overline{\overline{I}} \subset \overline{I}$. Let $f = \alpha x^m + \cdots \in \overline{I}$. Then $\alpha \in I$ and thus there exist $r_1, r_2, \ldots, r_n \in R$ such that

$$\alpha = r_1\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n = \Sigma_{i=1}^n r_i\alpha_i.$$

Noticing that $\Sigma_{i=1}^n r_i f_i x^{m-m_i} \in \overline{\overline{I}} \subset \overline{I}$, the polynomial $f - \Sigma_{i=1}^n r_i f_i x^{m-m_i}$ is in $\overline{I}$ and its degree is less than m. Proceeding in this way, we can go on subtracting elements of $\overline{\overline{I}}$ from f until we obtain a polynomial $g \in \overline{I}$ of degree less than $d_{\max}$ (can we obtain a polynomial of degree less than $d_{\min} = \min\{m_1, m_2, \ldots, m_n\}$?). That is, $f = h + g$, where $h \in \overline{\overline{I}}$ and $g \in \overline{I}$ is a polynomial of degree less than $d_{\max}$.

Let M be the R-module (finitely) generated by $1, x, x^2, \cdots, x^{d_{\max}}$. Then $g \in M \cap \overline{I}$ and

$$\overline{I} = \overline{\overline{I}} + M \cap \overline{I}.$$

We know from Proposition 1.2.31 that M is Neotherian. Hence $M \cap \overline{I}$ as a submodule of M (by Proposition 1.2.4) is finitely generated by Proposition 1.2.22. Let $M \cap \overline{I}$ be (finitely) generated by $g_1, g_2, \ldots, g_k$, then $\overline{I}$ is (finitely) generated by $f_1, f_2, \ldots, f_n$ and $g_1, g_2, \ldots, g_k$. □

Corollary 1.2.33. *If every ideal of a ring R is finitely generated, then so is every ideal of $R[x_1, x_2, \ldots, x_n]$.*

Proof. It holds for the case $n = 1$ because of Theorem 1.2.32. Suppose inductively that it holds for the case $n-1$, i.e., $R[x_1, x_2, \ldots, x_{n-1}]$ is Neotherian. Then (you may want to review the multiplication of two ideals)

$$R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}]R[x_n]$$

is a polynomial ring $R[x_n]$ over the Neotherian ring $R[x_1, x_2, \ldots, x_{n-1}]$. Again by Theorem 1.2.32, $R[x_1, x_2, \ldots, x_n]$ is Neotherian. That is, the case n holds. □

Corollary 1.2.34. *$\mathbb{F}[x]$ is Neotherian for any field $\mathbb{F}$.*

The topics for the next lecture are *quotient spaces* and *localization*.

1.3 Further Reading

- AM: `http://www.saheleriyaziyat.net/images/k1zut2e5peefixbx6kty.pdf`.
- Chapter 2 of this book: Ideals, Varieties, and Algorithms.