
Lecture 4. Polynomial and power series rings; the Hilbert basis theorem

Let R be a ring. The **polynomial ring** with coefficients in R is the set

$$R[X] = \{a_0 + a_1X + \cdots + a_nX^n \mid a_i \in R, n \in \mathbb{Z}_{\geq 0}\}.$$

The addition is coefficient-wise, and the multiplication is given by the formula

$$\left(\sum_{i \geq 0} a_i X^i\right) \left(\sum_{j \geq 0} b_j X^j\right) = \sum_{i \geq 0} \left(\sum_{j+k=i, j \geq 0, k \geq 0} a_j b_k\right) X^i,$$

where all but finitely many coefficients are equal to zero. Define

$$R[X_1, \dots, X_n] = R[X_1] \cdots [X_n] = \left\{ \sum_{i_1, \dots, i_n \geq 0} a_{i_1, \dots, i_n} X_1^{i_1} \cdots X_n^{i_n} \mid a_{i_1, \dots, i_n} \in R \right\},$$

where all but finitely many coefficients are equal to zero.

< Let k be an infinite field, and $f \in k[X_1, \dots, X_n]$. Show that $f = 0$ if and only if $f(x_1, \dots, x_n) = 0$ for all $(x_1, \dots, x_n) \in k^n$. (What about if k is a finite field? Consider $X^2 - X$ in $\mathbb{F}_2[X]$.)

The **ring of formal power series** with coefficients in R is the set

$$R[[T]] = \{a_0 + a_1T + \dots \mid a_i \in R\}.$$

The addition is coefficient-wise, and the multiplication is given by the formula

$$\left(\sum_{i \geq 0} a_i T^i\right) \left(\sum_{j \geq 0} b_j T^j\right) = \sum_{i \geq 0} \left(\sum_{j+k=i, j \geq 0, k \geq 0} a_j b_k\right) T^i.$$

Define

$$R[[T_1, \dots, T_n]] = R[[T_1]] \cdots [[T_n]].$$

$k[X_1, \dots, X_n]$ is an integral domain, and a UFD. $k[X_1]$ is in fact a PID but $k[X_1, \dots, X_n]$ is not a PID for $n > 1$. For example, the ideal (X_1, X_2) is not principal.

A **monomial ideal** in $k[X, Y]$ is given by $I = (X^{i_1}Y^{j_1}, X^{i_2}Y^{j_2}, \dots, X^{i_t}Y^{j_t})$ for $i_s, j_s \in \mathbb{N}$. We can draw a picture of $k[X, Y]$ by drawing a k -basis for it, and specify a monomial ideal by drawing a staircase (in red) as follows:

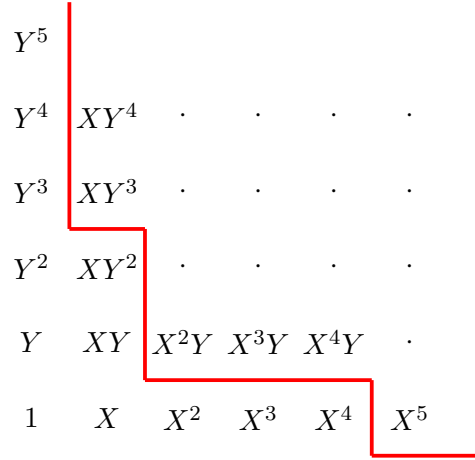


Figure 2: The monomial ideal $(XY^3, X^2Y, X^5) \subset k[X, Y]$.

A generating set of elements for a monomial ideal is given by the “corners” of the staircase.

The arithmetic cousin of $k[X, Y]$ is the ring $\mathbb{Z}[X]$.

< Let $\mathfrak{p} \subset \mathbb{Z}[X]$ be a prime ideal. Show that $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$ (use Proposition 2.5). Thus, $\mathfrak{p} \cap \mathbb{Z} = (p)$ where $p = 0$ or p is a prime number. Suppose now that $\mathfrak{p} \neq (0)$.

(i) Suppose $\mathfrak{p} \cap \mathbb{Z} = \{0\}$, then $\mathfrak{p} = (f)$ where $f \in \mathbb{Z}[X]$ is an irreducible polynomial.

(ii) Suppose $\mathfrak{p} \cap \mathbb{Z} = (p)$ with p a prime number. Then, $\mathfrak{p} = (p, f)$ where $f = 0$ or $f \in \mathbb{Z}[X]$ is a monic polynomial (leading coefficient is one) and its mod p reduction $\bar{f} \in \mathbb{F}_p[X]$ is irreducible.

In other words, to give a maximal ideal of $\mathbb{Z}[X]$ we have to choose a prime number $p \in \mathbb{Z}$ and an irreducible polynomial $\bar{f} \in \mathbb{F}_p[X]$ and then consider the ideal (p, f) where $f \in \mathbb{Z}[X]$ is any lift of $\bar{f}$ to a polynomial in $\mathbb{Z}[X]$. (Check that $(p, f) = (p, g)$ if $\bar{f} = \bar{g} \in \mathbb{F}_p[X]$).

The same argument will apply to any ring of the form $A[X]$ with A a PID.

< Formulate and prove the analogous result for $k[X, Y]$.

We next give two important examples of local rings; a geometric and an arithmetic example.

The power series ring $k[[X]]$ is a local ring with the unique maximal ideal $\mathfrak{m} = (X)$. To see this, observe that the units in the power series ring are precisely the elements $f(X) = a_0 + a_1X + \dots$ with $a_0 \neq 0$.

Let $p \in \mathbb{Z}$ be a prime number, the ring $\mathbb{Z}_{(p)} := \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\} \subset \mathbb{Q}$ is a local ring with maximal ideal $\{\frac{a}{b} \in \mathbb{Z}_{(p)} : p \mid a\}$. Again, it is clear that the elements in this maximal ideal are precisely the non-units of $\mathbb{Z}_{(p)}$.

4 The ring $k[X_1, X_2, \dots, X_n]$

4.1 Hilbert basis theorem

Theorem 4.1. $k[X_1, X_2, \dots, X_n]$ is Noetherian. More generally, if R is Noetherian, then $R[X]$ is also Noetherian.

► We defined a Noetherian ring R to be a ring such that all of its ideals are finitely generated. This turns out to be equivalent to the condition that all ascending chains of ideals

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

are eventually constant, that is, there exists a sufficiently large s such that $I_s = I_{s+i}$ for all $i \geq 0$. This condition is known as **Ascending Chain Condition (ACC)**.

Indeed, let $I = \bigcup_{i=1}^{\infty} I_i$. One can check directly that I is an ideal. Now, since it is finitely generated, we can write $I = (f_1, f_2, \dots, f_m)$ for some elements $f_i \in R$. Each of the generators f_i is contained in some I_{j_i} so let s be the maximum of the j_i . Then, we have

$$I = (f_1, \dots, f_m) \subset I_s \subset I_{s+1} \subset \dots \subset I.$$

Hence the chain stabilises at I_s .

Conversely, suppose that every ascending chain stabilises and let $I \subset R$ be an ideal. Let $f_1 \in I$. If $(f_1) = I$, we are done. Otherwise, let $f_2 \in I \setminus (f_1)$. If $(f_1, f_2) = I$, we are done. Otherwise, let $f_3 \in I \setminus (f_1, f_2)$. Continuing this way, we produce an ascending chain

$$(f_1) \subset (f_1, f_2) \subset (f_1, f_2, f_3) \subset \dots$$

which must stabilise at some point hence $I = (f_1, f_2, \dots, f_m)$ for some m .

⚡ This argument is sometimes referred to as Noetherian induction. When we make infinitely many choices f_i we use the Axiom of Dependent Choice, a countable version of the Axiom of Choice. In the proof of the Hilbert basis theorem given below, we only use the first implication: if all ideals are finitely generated, then ACC holds. So, our proof does not depend on the Axiom of Choice.

Proof. (of Theorem 4.1) It suffices to prove the second statement. Indeed, a field is Noetherian, its only ideals being (0) and (1) , so the first statement follows by induction on n since $k[X_1, \dots, X_n] = k[X_1, \dots, X_{n-1}][X_n]$.

Let $I \subset R[X]$ be a nonzero ideal. We want to prove that I is finitely generated. If R were a field we could divide by leading coefficients, as in the proof that $k[X]$ is a PID. Over a general ring R we cannot, so instead we keep track of the leading coefficients themselves. For $n \geq 0$ define

$$J_n = \{a \in R : \exists f \in I \text{ of the form } f = aX^n + b_{n-1}X^{n-1} + \dots + b_1X + b_0\}.$$

Thus J_n consists of 0 (take $f = 0$) together with the leading coefficients of the elements of I of degree n . It is an ideal of R : if $a, a' \in J_n$ come from $f, f' \in I$ and $r \in R$, then $a + a'$ and ra

come from $f + f'$ and rf , which lie in I . Moreover, $J_n \subset J_{n+1}$ since if $f \in I$, then $Xf \in I$. Therefore, we have an ascending chain of ideals

$$J_0 \subset J_1 \subset \dots$$

Since R is Noetherian, this chain stabilises. So, we have $J_s = J_{s+i}$ for some s and for all $i \geq 0$.

Now, since R is Noetherian, for each $m \leq s$, we have that J_m is finitely generated. Thus, we can write $J_m = (a_{m,1}, a_{m,2}, \dots, a_{m,r_m})$. By definition of J_m for each $a_{m,j}$ with $1 \leq j \leq r_m$, there is a polynomial $f_{m,j} \in I$ of degree m with leading coefficient $a_{m,j}$.

Finally, we claim that the finitely many polynomials $f_{m,j}$ ($0 \leq m \leq s$, $1 \leq j \leq r_m$) generate I . Let $I' \subset I$ be the ideal they generate. We show by induction on the degree of f that every $f \in I$ lies in I' . This is clear for $f = 0$. Let $f \in I$ have degree m and leading coefficient a , so that $a \in J_m$. If $m \leq s$, write $a = \sum_i b_i a_{m,i}$ with $b_i \in R$ and put $g = \sum_i b_i f_{m,i}$. If $m > s$, then $a \in J_m = J_s$, so write $a = \sum_i b_i a_{s,i}$ with $b_i \in R$ and put $g = \sum_i b_i X^{m-s} f_{s,i}$. In both cases $g \in I'$ and $g = aX^m + (\text{terms of degree } < m)$, so $f - g \in I$ has degree less than m . By induction $f - g \in I'$, hence $f \in I'$. $\square$

► Let us run the proof on the monomial ideal $I = (XY^3, X^2Y, X^5)$ of Figure 2, regarded as an ideal of $R[X]$ with $R = k[Y]$. Since I is spanned by the monomials $X^i Y^j$ lying above the staircase, J_n is spanned by the Y^j with $X^n Y^j \in I$. In other words, J_n is generated by Y^h where h is the height of the staircase above the column of X^n :

$$J_0 = 0, \quad J_1 = (Y^3), \quad J_2 = J_3 = J_4 = (Y), \quad J_n = R \text{ for } n \geq 5.$$

So $s = 5$, and the proof produces the generators $XY^3, X^2Y, X^3Y, X^4Y, X^5$ of I . These include the corners of the staircase, but the generating set produced by the proof is not minimal: X^3Y and X^4Y are multiples of X^2Y .

< Run the proof on the same ideal I , but regarded as an ideal of $R[Y]$ with $R = k[X]$. Which generators does it produce? Note that this time the chain J_n stabilises at a proper ideal of R .

► Here is an arithmetic cousin of the previous example: $I = (4, 2X, X^2) \subset \mathbb{Z}[X]$. Here $J_0 = (4)$, $J_1 = (2)$ and $J_n = \mathbb{Z}$ for $n \geq 2$, so the chain of ideals J_n grows for a while before it stabilises, and the proof returns the generators $4, 2X, X^2$. Note that the generators coming from the lower J_m cannot be dropped: every element of $(4, X^2)$ has X -coefficient divisible by 4, so $2X \notin (4, X^2)$.

► The finiteness of the number of variables is essential. The polynomial ring $k[X_1, X_2, X_3, \dots]$ in infinitely many variables is not Noetherian, since the chain

$$(X_1) \subset (X_1, X_2) \subset (X_1, X_2, X_3) \subset \dots$$

never stabilises. In the proof above, finiteness enters through the induction on n .

► Not every subring of a Noetherian ring is Noetherian.

◁ Show that

$$R = \{f(X, Y) = \sum a_{ij} X^i Y^j \mid i, j \geq 0, \text{ and } i > 0 \text{ if } j \neq 0\}$$

is a subring of the Noetherian ring $k[X, Y]$ but R is not Noetherian.

◁ Prove that if R is Noetherian, $R[[T]]$ is also Noetherian.

Corollary 4.2. *Any finitely generated algebra over $\mathbb{Z}$ or over a field k is Noetherian.*

Proof. The assumption is that the ring is $R[X_1, \dots, X_n]/I$ for some n and $R = \mathbb{Z}$ or $R = k$. We know that the ideals of $R[X_1, \dots, X_n]/I$ are images of the ideals of $R[X_1, \dots, X_n]$ that contain I . The latter are finitely generated since $R[X_1, \dots, X_n]$ is Noetherian by Theorem 4.1 (note that $\mathbb{Z}$ is Noetherian, being a PID). $\square$