2. Ideals in Polynomial Rings

2.1 Notation: In these notes, all **rings** are assumed to be **commutative** and to have an **identity**. If R is a (commutative)ring and $S \subseteq R$ is a subset, then $\langle S \rangle$ denotes the **ideal** in R **generated by** S:

$$\langle S \rangle = \Big\{ \sum_{i=1}^{l} a_i r_i \Big| a_i \in S, r_i \in R \Big\}.$$

2.2 Definition: An **integral domain** is a commutative ring with no zero divisors, which means that if $a, b \in R$ with $ab = 0$ then either $a = 0$ or $b = 0$. An ideal A in a commutative ring R is called a **principal ideal** if $A = \langle a \rangle$ for some $a \in R$. A **principal ideal domain**, or PID, is an integral domain R in which every ideal is principal. Recall that for a field $\mathbf{F}$, $\mathbf{F}[x]$ is a PID.

2.3 Note: Let $S \subseteq \mathbf{F}[x_1, \cdots, x_n]$ be any set of polynomials. Then $V(S) = V(\langle S \rangle)$.

Proof: If $x \in V(S)$ then $f(x) = 0$ for all $f \in S$ and so $\big(\sum_{i=1}^{l} f_i g_i\big)(x) = \sum_{i=1}^{l} f_i(x) g_i(x) = 0$ for all $f_i \in S$ and $g_i \in \mathbf{F}[x_1, \cdots, x_n]$. This shows that $V(S) \subseteq V(\langle S \rangle)$. On the other hand, if $x \in V(\langle S \rangle)$ then for any $f \in S$ we also have $f \in \langle S \rangle$, so $f(x) = 0$. This shows that $V(\langle S \rangle) \subseteq V(S)$.

2.4 Example: Since $\mathbf{F}[x]$ is a PID, every variety in $\mathbf{F}^1$ is of the form $V(f)$ for some $f \in \mathbf{F}[x]$, because if $X = V(S)$ and $\langle S \rangle = \langle f \rangle$ then $X = V(S) = V(\langle S \rangle) = V(\langle f \rangle) = V(f)$. Also, if $f(x) = (x - a_1)^{k_1} \cdots (x - a_l)^{k_l} g(x)$, where $g(x)$ has no roots in $\mathbf{F}$, then we have $V(f) = \{a_1, \cdots, a_l\}$.

2.5 Definition: For $E \subseteq \mathbf{F}^n$, we define the **ideal of polynomials vanishing on** E, or simply the **ideal** of E, to be the ideal

$$I(E) = \big\{ f \in \mathbf{F}[x_1, \cdots, x_n] \big| f(x) = 0 \text{ for all } x \in E \big\}.$$

A **closed ideal** in $\mathbf{F}[x_1, \cdots, x_n]$ is any ideal of the form $I(E)$ for some $E \subseteq \mathbf{F}^n$.

2.6 Theorem: *(The Correspondence Between Varieties in $\mathbf{F}^n$ and Ideals in $\mathbf{F}[x_1, \cdots, x_n]$) The maps $A \mapsto V(A)$ and $X \mapsto I(X)$ give a bijective order-reversing correspondence between the set of closed ideals A in $\mathbf{F}[x_1, \cdots, x_n]$ and the set of varieties X in $\mathbf{F}^n$. Indeed, for any sets $S, T \subseteq \mathbf{F}[x_1, \cdots, x_n]$ and $E, F \subseteq \mathbf{F}^n$ we have*

(1) If $S \subseteq T$ then $V(T) \subseteq V(S)$, and if $E \subseteq F$ then $I(F) \subseteq I(E)$.
(2) $S \subseteq I(V(S))$ and $E \subseteq V(I(E))$.
(3) $V(S) = V(I(V(S)))$ and $I(E) = I(V(I(E)))$.

Proof: Parts (1) and (2) are easy. Part (3) follows from parts (1) and (2).

2.7 Definition: For $E \subseteq \mathbf{F}^n$, we define the **closure** of E, denoted by $\overline{E}$, to be the smallest variety in $\mathbf{F}^n$ which contains E, and for $S \subseteq \mathbf{F}[x_1, \cdots, x_n]$, we define the **closure** of S, denoted by $\overline{S}$, to be the smallest closed ideal containing S. The above theorem implies that

$$\overline{E} = V(I(E)) \quad \text{and} \quad \overline{S} = I(V(S)).$$

and also that E is a variety $\iff E = \overline{E}$ and that S is a closed ideal $\iff S = \overline{S}$.

2.8 Example: Describe all the closed ideals in $\mathbf{F}[x]$.

Solution: The closed ideals are of the form $I(X)$ where X is a variety in $\mathbf{F}$, and we have already described all the varieties in $\mathbf{F}$. We have

$$I(\emptyset) = \big\{ f \in \mathbf{F}[x] \big| f(x) = 0 \text{ for all } x \in \emptyset \big\} = \langle 1 \rangle = \mathbf{F}[x]$$

$$I(\{a_1, \cdots, a_l\}) = \big\{ f \in \mathbf{F}[x] \big| f(a_i) = 0 \text{ for all } i \big\} = \Big\langle \prod_{i=1}^{l} (x - a_i) \Big\rangle ,$$

$$I(\mathbf{F}) = \big\{ f \in \mathbf{F}[x] \big| f(x) = 0 \text{ for all } x \in \mathbf{F} \big\} = \begin{cases} \langle 0 \rangle = \{0\} & \text{if } \mathbf{F} \text{ is infinite} \\ \big\langle x^{p^n} - x \big\rangle & \text{if } \mathbf{F} \text{ has } p^n \text{ elements.} \end{cases}$$

2.9 Example: Let $\mathbf{F}$ be an infinite field, let $f \in \mathbf{F}[x]$ and let $X = V(y - f(x)) \subseteq \mathbf{F}^2$. Show that $I(X) = \langle y - f(x) \rangle$.

Solution: We have $\langle y - f(x) \rangle \in I(V(\langle y - f(x) \rangle)) = I(X)$, so we only need to show that $I(X) \subseteq \langle y - f(x) \rangle$. Let $g \in I(X)$. Since $y - f(x)$ is monic and of degree 1 in y, we can use the division algorithm to write $g(x, y) = (y - f(x))q(x, y) + r(x)$ for some $q \in \mathbf{F}[x, y]$ and $r \in \mathbf{F}[x]$. Since $g \in I(X)$, $g(x, y) = 0$ for all $(x, y) \in X$, that is for all (x, y) with $y = f(x)$, so we have $g(x, f(x)) = 0$ for all $x \in \mathbf{F}$. Notice that $g(x, f(x)) = r(x)$, so we have $r(x) = 0$ for all $x \in \mathbf{F}$. Since $\mathbf{F}$ is infinite, this implies that $r = 0 \in \mathbf{F}[x]$, and so $g(x, y) = (y - f(x))q(x, y) \in \langle y - f(x) \rangle$ as required.

2.10 Definition: An ideal A in a ring R is said to be **finitely generated** if it is of the form $A = \langle a_1, \cdots, a_\ell \rangle$ for some $a_i \in R$. A ring R is called **Noetherian** when every ascending chain of ideals $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$ eventually becomes constant, that is there exists an index ℓ such that $A_k = A_\ell$ for all $k \geq \ell$.

2.11 Theorem: *Let R be a (commutative) ring. Then R is Noetherian if and only if every ideal in R is finitely generated.*

Proof: Suppose that R is Noetherian. Let $A \subseteq R$ be any ideal. If $A = \{0\}$ then of course A is finitely generated, so suppose that $A \neq \{0\}$. Let $0 \neq a_1 \in A$, and set $A_1 = \langle a_1 \rangle$. Now, for each $k = 2, 3, 4, \cdots$, as long as $A_k \neq A$, we choose $a_{k+1} \in A \setminus A_k$ and set $A_{k+1} = A + \langle a_{k+1} \rangle = \langle a_1, \cdots, a_{k+1} \rangle$. Then the chain of ideals $A_1 \subsetneqq A_2 \subsetneqq A_3 \subsetneqq \cdots$ must eventually stabilize, so we obtain $A = A_\ell = \langle a_1, \cdots, a_\ell \rangle$ for some index ℓ. Thus A is finitely generated.

Now suppose that every ideal in R is finitely generated. Let $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$ be an ascending chain of ideals in R. Let $A = \bigcup_{i=1}^{\infty} A_i$. Then A is an ideal in R, so A is finitely generated, say $A = \langle a_1, \cdots, a_k \rangle$. Then every a_i is contained in some A_{k_i}. Hence if we let ℓ be the maximum of the k_i, then every $a_i \in A_\ell$ and we have $A = \langle a_1, \cdots, a_k \rangle \subseteq A_\ell \subseteq A$. So in fact $A = A_\ell$ and the chain of ideals stabilizes.

2.12 Theorem: *(Hilbert's Basis Theorem) If R is Noetherian then so is $R[x]$.*

Proof: Suppose that R is Noetherian. Let A be any ideal in $R[x]$. For $k = 0, 1, 2, \cdots$ let A_k be the set of all $r \in R$ such that $r = 0$ or r is the leading coefficient of some polynomial $f \in A$ of degree k. Then the sets A_k are ideals in R and $A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots$. Since R is Noetherian, this chain must end, so we can choose m so that $A_k = A_m$ for all $k \geq m$. Also, every A_k is finitely generated, say $A_k = \langle a_{k1}, a_{k2}, \cdots, a_{k\,l_k} \rangle$. For each a_{ki} choose a polynomial $f_{ki} \in A$ of degree k with leading coefficient a_{ki}. Let $B = \langle f_{ki} \big| k \leq m, i \leq l_k \rangle \subseteq A$. We claim that in fact $A = B$, which is finitely generated, and hence $R[x]$ is Noetherian.

We now prove the claim. If $f \in A$ is a polynomial of degree 0 then f is actually equal to its leading coefficient, so $f \in \langle f_{01}, \cdots, f_{0\,l_0} \rangle \subseteq B$. Suppose, inductively, that every polynomial g in A of degree less than k is in B, and let f be any polynomial in A of degree k. We consider two cases. Case 1: suppose that $k \leq m$. The leading coefficient of f is in $A_k = \langle a_{k1}, \cdots, a_{k\,l_j} \rangle$, say the leading coefficient is $a = \sum c_i a_{ki}$. Notice that the polynomial $h = \sum c_i f_{ki}$ is in B and has the same degree and the same leading coefficient as f, so the polynomial $g = f - h$ has degree less than k and is in A. By the induction hypothesis, $g \in B$, and so we have $f = g + h \in B$. Case 2: suppose that $k > m$. The leading coefficient of f is in $A_k = A_m = \langle a_{m1}, \cdots, a_{m\,l_m} \rangle$, say the leading coefficient is $a = \sum c_i a_{mi}$. Then the polynomial $h = x^{k-m} \sum c_i f_{mi}$ is in B and has the same degree and the same leading coefficient as f, so the polynomial $g = f - h$ has degree less than k and lies in A. By the induction hypothesis, $g \in B$ and so again $f = g + h \in B$. By induction, we see that $A \subseteq B$, and so $A = B$ as required.

2.13 Corollary: $\mathbf{F}[x_1, \cdots, x_n]$ *is Noetherian.*

Proof: Since $\mathbf{F}[x_1]$ is a PID, it is Noetherian. Suppose, inductively, that $\mathbf{F}[x_1, \cdots, x_k]$ is Noetherian. Then by the Hilbert basis theorem $\mathbf{F}[x_1, \cdots, x_{k+1}] = \mathbf{F}[x_1, \cdots, x_k][x_{k+1}]$ is also Noetherian.

2.14 Corollary: *Every variety in* $\mathbf{F}^n$ *is the zero set of a finite set of polynomials.*

Proof: Let X be a variety in $\mathbf{F}^n$. Say $X = V(S)$ where $S \subseteq \mathbf{F}[x_1, \cdots, x_n]$, and say $\langle S \rangle = \langle f_1, \cdots, f_l \rangle$. Then $X = V(S) = V(\langle S \rangle) = V(\langle f_1, \cdots, f_l \rangle) = V(f_1, \cdots, f_l)$.