
Lecture 5. Affine varieties; monomial orderings

4.2 Affine varieties

Let $S \subset k[X_1, \dots, X_n]$. We let the **affine variety** defined by S to be

$$\mathcal{V}(S) = \{(x_1, \dots, x_n) \in k^n : f(x_1, \dots, x_n) = 0 \text{ for all } f \in S\}$$

Note that if we set $I = (S)$ the ideal generated by S and apply the Hilbert basis theorem to write $I = (f_1, \dots, f_h)$ for some finite number of polynomials, then

$$\mathcal{V}(S) = \mathcal{V}(I) = \mathcal{V}(\{f_1, \dots, f_h\})$$

hence every affine variety is defined as the vanishing locus of a finite set of polynomials.

Given a subset $U \subset k^n$, we define an ideal

$$\mathcal{I}(U) = \{f \in k[X_1, \dots, X_n] : f(x_1, x_2, \dots, x_n) = 0 \text{ for all } (x_1, x_2, \dots, x_n) \in U\}$$

Thus, we have maps between subsets of k^n and subsets of $k[X_1, \dots, X_n]$.

$$\{S \subset k[X_1, \dots, X_n]\} \begin{matrix} \mathcal{V} \\ \mathcal{I} \end{matrix} \{U \subset k^n\}$$

◁ Show that $S_1 \subset S_2$ implies $\mathcal{V}(S_2) \subset \mathcal{V}(S_1)$, and $U_1 \subset U_2$ implies $\mathcal{I}(U_2) \subset \mathcal{I}(U_1)$. Use the set $U = \{(0, i) : i \in \mathbb{Z}\} \subset \mathbb{C}^2$ to show that it can happen that $U_1 \subsetneq U_2$ but $\mathcal{I}(U_1) = \mathcal{I}(U_2)$.

◁ Note that $U \subset \mathcal{V}(\mathcal{I}(U))$ for any subset $U \subset k^n$. Prove that if U is an affine variety, then $U = \mathcal{V}(\mathcal{I}(U))$.

In general, for a set $U \subset k^n$, $\mathcal{V}(\mathcal{I}(U))$ is the smallest affine variety containing U , and is called the **Zariski closure** of U and denoted by $\overline{U}$.

► $\mathcal{I}$ forgets multiplicities: in $k[X]$ we have $\mathcal{V}(X^2) = \{0\}$ and $\mathcal{I}(\{0\}) = (X)$, so $\mathcal{I}(\mathcal{V}(I)) \neq I$ in general. In fact $\mathcal{I}(U)$ is always a radical ideal, since if f^m vanishes on U then so does f .

► $\mathcal{V}(I + J) = \mathcal{V}(I) \cap \mathcal{V}(J)$.

► $\mathcal{V}(IJ) = \mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$.

► Hilbert's Nullstellensatz which we will see later in the course implies that if k is algebraically closed, $\mathcal{V}(I : J^\infty) = \overline{\mathcal{V}(I)} \setminus \mathcal{V}(J)$.

Basic questions:

- Let $f_1, f_2, \dots, f_s \in k[X_1, \dots, X_n]$ and $I = (f_1, f_2, \dots, f_s)$. Given $f \in k[X_1, \dots, X_n]$, how can we decide if $f \in I$? Does f vanish on the affine variety $U = \mathcal{V}(I)$ defined by I ?
- Given $S \subset k[X_1, \dots, X_n]$, is it true that $\mathcal{V}(S) \neq \emptyset$?
- Suppose $U = \mathcal{V}(S) \subset k^n$ is non-empty, what is the dimension of U ?

We will answer all these questions in the next few sections but first we have to develop some tools.

4.3 Gröbner bases

We work in the ring $k[X_1, \dots, X_n]$. Let us introduce some notation.

$\mathbb{N}^n = \{\alpha = (\alpha_1, \dots, \alpha_n) : \alpha_i \in \mathbb{N}\}$.

$X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \dots X_n^{\alpha_n}$. We write $|\alpha| = \alpha_1 + \alpha_2 + \dots + \alpha_n$ for the total degree of X^α .

We write an element $f \in k[X_1, \dots, X_n]$ as $f = \sum_{\alpha} a_{\alpha} X^{\alpha}$ with $a_{\alpha} \in k$ such that $\{\alpha : a_{\alpha} \neq 0\}$ is a finite set.

Unlike the case of $k[X]$, when $n > 1$ it is unclear which monomial has the highest degree. For example, what is the highest degree monomial in $f(X, Y) = X^2 Y + 42 X Y^2$?

To address this we introduce the following notion.

Definition 4.3. Let $\leq$ be a total ordering on $\mathbb{N}^n$. We say that $\leq$ is a **monomial ordering** if

- $0 = (0, \dots, 0) \leq \alpha$ for all $\alpha \in \mathbb{N}^n$.
- If $\alpha \leq \beta$, then $\alpha + \gamma \leq \beta + \gamma$ for all $\gamma \in \mathbb{N}^n$.

Since $\alpha \mapsto X^\alpha$ identifies $\mathbb{N}^n$ with the set of monomials, a monomial ordering is the same thing as an ordering of the monomials of $k[X_1, \dots, X_n]$. Being a total ordering means that any two monomials are comparable, so every non-zero polynomial has a well-defined largest term.

$\triangleleft$ Show that $X^\alpha | X^\beta$ implies that $\alpha \leq \beta$ for any monomial ordering $\leq$.

► **Lexicographic Order $\leq_{lex}$:** Let $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \dots, \beta_n)$. Define $\alpha <_{lex} \beta$ if the first non-zero entry of $\beta - \alpha \in \mathbb{Z}^n$ is positive, and $\alpha \leq_{lex} \beta$ if $\alpha <_{lex} \beta$ or $\alpha = \beta$. Thus $\alpha <_{lex} \beta$ means that $\alpha_i < \beta_i$ for the first index i with $\alpha_i \neq \beta_i$.

► By contrast, the ordering of $\mathbb{N}^n$ in which $\alpha \leq \beta$ if $\alpha_i \leq \beta_i$ for all i , that is, $X^\alpha | X^\beta$, satisfies both conditions of Definition 4.3 but is not total when $n > 1$: for example, $(1, 0)$ and $(0, 1)$ are not comparable. The lexicographic order is a total ordering refining it.

► **Graded Lexicographic Order $\leq_{glex}$:** Define $\alpha \leq_{glex} \beta$ if either $|\alpha| < |\beta|$ or if $|\alpha| = |\beta|$ and $\alpha \leq_{lex} \beta$.

$\triangleleft$ Order the terms of the polynomial $f(X, Y, Z) = XY^2Z + Z^2 + X^3 + X^2Z^2$ with respect to $\leq_{lex}$ and $\leq_{glex}$.

► Let $A \in GL(n, \mathbb{R})$ be a matrix such that the first non-zero entry of each column is positive. Define $\alpha <_A \beta$ if the first non-zero entry of $A(\beta - \alpha) \in \mathbb{R}^n$ is positive. Each row of A is a weight vector: monomials are compared by their first weight, ties are broken by the second weight, and so on. Since A is invertible, any two distinct α, β are comparable, and the condition on the columns Ae_j says exactly that $0 <_A e_j$ for all j . For example, the matrices

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 0 & 0 & \cdots & 0 & -1 \\ 0 & 0 & \cdots & -1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & -1 & \cdots & 0 & 0 \end{pmatrix}$$

define $\leq_{lex}$, $\leq_{grlex}$ and the **graded reverse lexicographic order** $\leq_{grevlex}$, respectively. In the last one, monomials of the same total degree are compared by their exponent of X_n , the smaller exponent being the larger monomial, with ties broken by the exponent of X_{n-1} , and so on. Note that this matrix has negative entries, but the first non-zero entry of each column is still positive. In fact, any monomial ordering on $\mathbb{N}^n$ arises this way for some matrix A .⁵

◁ Show that $\leq_A$ is a monomial ordering.

■ In what follows, we fix a monomial ordering $\leq$.

■ For $\alpha, \beta \in \mathbb{N}^n$, we often write $X^\alpha \leq X^\beta$ to mean that $\alpha \leq \beta$.

Given a non-zero polynomial

$$f = a_{\alpha^{(1)}} X^{\alpha^{(1)}} + a_{\alpha^{(2)}} X^{\alpha^{(2)}} + \dots + a_{\alpha^{(s)}} X^{\alpha^{(s)}}$$

where $\alpha^{(i)} \in \mathbb{N}^n$ with $\alpha^{(1)} > \alpha^{(2)} > \dots > \alpha^{(s)}$ and all the coefficients $a_{\alpha^{(i)}}$ are non-zero, we define

$$\begin{aligned} LT(f) &:= a_{\alpha^{(1)}} X^{\alpha^{(1)}} && \text{leading term} \\ LM(f) &:= X^{\alpha^{(1)}} && \text{leading monomial} \\ LC(f) &:= a_{\alpha^{(1)}} && \text{leading coefficient} \end{aligned}$$

The ideal membership problem is easy to solve for monomial ideals.

Lemma 4.4. *Let $I \subset k[X_1, \dots, X_n]$ be a **monomial ideal**, that is, an ideal generated by a (possibly infinite) set G of monomials, and let $f \in k[X_1, \dots, X_n]$. Then $f \in I$ if and only if every term of f is divisible by a monomial in G .*

Proof. Suppose $f \in I$, then $f = \sum_{i=1}^s h_i g_i$ for some polynomials $h_i \in k[X_1, \dots, X_n]$ and monomials $g_i \in G$. Write $h_i = \sum a_{i,\alpha} X^\alpha$, then $f = \sum_{i,\alpha} a_{i,\alpha} X^\alpha g_i$. Hence, all the terms of f are divisible by monomials in G . The other direction is clear. $\square$

Lemma 4.5. *Let $(g_i)_{i \geq 1}$ be a sequence of monomials such that $g_1 \geq g_2 \geq g_3 \geq \dots$. Then, there exists $r \geq 1$ such that $g_r = g_{r+1} = g_{r+2} = \dots$.*

Proof. Let $I = (g_i : i \geq 1)$. By the Hilbert basis theorem (Theorem 4.1), the ascending chain of ideals $(g_1) \subset (g_1, g_2) \subset \dots$ stabilises, so there exists r such that $I = (g_1, \dots, g_r)$. Now, for $i > r$, we have $g_i \leq g_r$. On the other hand, since $g_i \in I$, by the previous lemma, there exists $j \in \{1, \dots, r\}$ such that $g_j | g_i$, and so $g_j \leq g_i$. Since $j \leq r$, we get $g_r \leq g_j \leq g_i$, hence $g_i = g_r$. $\square$

⁵L Robbiano - Term orderings on the polynomial ring.