1. Affine Algebraic Varieties

1.1 Notation: Throughout these notes, $\mathbf{F}$ always denotes a field and $\mathbf{F}[x_1, \cdots, x_n]$ denotes the ring of polynomials in the variables $x_1, \cdots, x_n$ over $\mathbf{F}$.

1.2 Definition: Let $S \subseteq \mathbf{F}[x_1, \cdots, x_n]$ be any set of polynomials. The **zero set** of S (or the **affine algebraic variety** cut out by S) in $\mathbf{F}^n$ is the set

$$V(S) = \left\{ x \in \mathbf{F}^n \middle| f(x) = 0 \text{ for all } f \in S \right\}.$$

If S is finite with $S = \{f_1, \cdots, f_l\}$ then we shall usually write $V(f_1, \cdots, f_l)$ instead of $V(S)$. An **affine algebraic variety** (or simply an **affine variety**) in $\mathbf{F}^n$ is a set of the form $V(S)$ for some $S \subseteq \mathbf{F}[x_1, \cdots, x_n]$.

1.3 Remark: We use the word *affine* because we are considering $\mathbf{F}^n$ as an affine space (as distinct from, say, a vector space), the word *variety* means the zero set of a collection of functions, and the word *algebraic* indicates that the functions in question are polynomials. When $\mathbf{F} = \mathbf{C}$, one can also study *analytic* varieties, which are the zero sets of collections of analytic functions.

1.4 Example: In $\mathbf{R}^1$, $V(x-1) = \{1\}$ and $V(x^2 - 3x + 2) = V\big((x-1)(x-2)\big) = \{1, 2\}$. More generally, if $f \in \mathbf{R}[x]$ then $V(f)$ is the set of roots of f in $\mathbf{R}$.

1.5 Example: In $\mathbf{R}^2$, $V(x + y - 2)$ is the line $x + y = 2$, $V(y - x^2)$ is the parabola $y = x^2$, and $V(x^2 + y^2 - 1)$ is the circle $x^2 + y^2 = 1$. If $f \in \mathbf{R}[x]$ then $V\big(y - f(x)\big)$ is the graph of $f(x)$. Also, $V(y - x^2, x + y - 2) = \{(-2, 4), (1, 1)\}$ is the set of points of intersection of the parabola $y = x^2$ with the line $x + y = 2$, while $V\big((y - x^2)(x + y - 2)\big)$ is the union of the parabola $y = x^2$ with the line $x + y = 2$. For any point $(a, b) \in \mathbf{R}^2$ we have $V(x - a, y - b) = \{(a, b)\}$. Finally, $V(y - x^3 - x^2)$ is an alpha curve and $V(y^2 - x^3)$ is a curve with a cusp at $(0, 0)$.

1.6 Example: In $\mathbf{R}^3$, $V(z - x^2 - y^2)$ is the paraboloid $z = x^2 + y^2$, $V(x^2 + y^2 + z^2 - 1)$ is the unit sphere, and $V(x^2 + y^2 - z^2)$ is a double cone. If $f \in \mathbf{R}[x, y]$ then $V(y - f(x, y))$ is the graph of $f(x, y)$. Also $V(xyz)$ is the union of the three coordinate planes, $V(xy, yz)$ is the union of the plane $y = 0$ with the x-axis, $V(y - x^2, z - x^3)$ is the twisted cubic, which is the curve given parametrically by $(x, y, z) = (t, t^2, t^3)$ and $V(x-1, y-2, z-3) = \{(1, 2, 3)\}$.

1.7 Example: In $\mathbf{R}^1$, $V(x^2 + 1) = \emptyset$, but in $\mathbf{C}^1$, $V(x^2 + 1) = \{i, -i\}$. The fundamental theorem of algebra states that if $f \in \mathbf{C}[x] \setminus \mathbf{C}$ then $V(f) \neq \emptyset$.

1.8 Example: In $\mathbf{R}^2$, we have $V(y - x^2, x - y^2) = \{(0, 0), (1, 1)\}$, which is the set of points of intersection of the two parabolas $y = x^2$ and $x = y^2$, but in $\mathbf{C}^2$, we have $V(y - x^2, x - y^2) = \big\{(0, 0), (1, 1), (\alpha, \bar{\alpha}), (\bar{\alpha}, \alpha)\big\}$, where $\alpha = e^{i\,2\pi/3}$.

1.9 Example: In $\mathbf{Q}^2$, there are infinitely many points in $V(x^2 + y^2 - 1)$ $\big($indeed, for any $(u, v) \in \mathbf{Z}^2 \setminus \{(0, 0)\}$, if we let $x = \frac{u^2 - v^2}{u^2 + v^2}$ and $y = \frac{2uv}{u^2 + v^2}$ then we will have $x^2 + y^2 = 1\big)$, but according to Fermat's Last Theorem, for $n > 2$ we have $V(x^n + y^n - 1) = \{(0, 1), (1, 0)\}$ if n is odd and $V(x^n + y^n - 1) = \{(0, 1), (0, -1), (1, 0), (-1, 0)\}$ if n is even.

1.10 Example: In $\mathbf{Z}_p$ for p prime, Fermat's Little Theorem states that $V(x^p - x) = \mathbf{Z}_p$. More generally, if $\mathbf{F}$ is a field with p^n elements then $V\big(x^{p^n} - x\big) = \mathbf{F}$ (proof: $\mathbf{F}^*$ is a group with $p^n - 1$ elements, so for all $x \in \mathbf{F}^*$ we have $x^{p^n - 1} = 1$, and hence for all $x \in \mathbf{F}$ we have $x^{p^n} = x$).

1.11 Example: In ${\mathbf{Z}_3}^2$ we have $V(x^2+y^2-1)=\{(0,1),(0,2),(1,0),(1,2)\}$, while in ${\mathbf{Z}_7}^2$ we have $V(x^2+y^2-1)=\{(0,1),(0,6),(1,0),(2,2),(2,5),(5,2),(5,5),(6,0)\}$.

1.12 Example: (The Classification of Varieties in $\mathbf{F}^1$) Show that the affine varieties in $\mathbf{F}$ are the finite subsets of $\mathbf{F}$ (including the empty set $\emptyset$) and $\mathbf{F}$ itself.

Solution: $\emptyset$ is a variety since $V(\mathbf{F}[x])=V(1)=\emptyset$. Given any finite set $\{a_1,\cdots,a_l\}\subseteq\mathbf{F}$, let $f=(x-a_1)\cdots(x-a_l)$ and then we have $V(f)=\{a_1,\cdots,a_l\}$. Also, $\mathbf{F}$ itself is a variety since $V(\emptyset)=V(0)=\mathbf{F}$.

Conversely, let X be any variety in $\mathbf{F}$, and say $X=V(S)$. If $S=\emptyset$ or if $S=\{0\}$ then $X=V(S)=\mathbf{F}$. Otherwise, S contains a non-zero polynomial, say f. Since $f\neq 0$, f has only finitely many roots (if any), so $V(f)$ is finite (or empty), and $X=V(S)\subseteq V(f)$, so X must be finite (or empty).

1.13 Example: (Affine Spaces are Varieties) Show that every affine space in $\mathbf{F}^n$ is a variety.

Solution: Recall that an **affine space** in $\mathbf{F}^n$ is a set of the form

$$p+V=\big\{p+v\big|v\in V\big\}$$

for some $p\in\mathbf{F}^n$ and some vector space $V\subseteq\mathbf{F}^n$. Let X be an affine space in $\mathbf{F}^n$, say $X=p+V$. Let $\{u_1,\cdots,u_k\}$ be a basis for V and let A be the $n\times k$ matrix with columns $u_1,\cdots,u_k$ so that V is the column space of A. Then $x\in X$ if and only if $x=p+At$ for some $t\in\mathbf{F}^k$. Row reduce the augmented matrix $(A|x-p)$ to obtain $\begin{pmatrix} I & y \\ 0 & Bx+c\end{pmatrix}$ for some $y\in\mathbf{F}^k$, $c\in\mathbf{F}^{n-k}$ and some $(n-k)\times n$ matrix B. Then $x\in p+V$ if and only if $Bx+c=0$. The matrix equation $Bx+c=0$ is equivalent to a system of $n-k$ linear equations, and X is the variety cut out by these equations.

1.14 Definition: A **topology** on a set X is any collection $\mathcal{U}$ of subsets of X such that

1) $\emptyset\in\mathcal{U}$ and $X\in\mathcal{U}$,
2) if $U\in\mathcal{U}$ and $V\in\mathcal{U}$ then $U\cap V\in\mathcal{U}$, and
3) if $U_\alpha\in\mathcal{U}$ for each $\alpha\in A$, where A is any set, then $\bigcup_{\alpha\in A}U_\alpha\in\mathcal{U}$.

The sets in $\mathcal{U}$ are called the **open** sets of X, and the complements of the open sets are called the **closed** sets of X.

1.15 Example: $\mathbf{Q}^n$, $\mathbf{R}^n$ and $\mathbf{C}^n$ all have a standard metric topology.

1.16 Theorem: *Let X be a variety in $\mathbf{F}^n$. Then The set of all subvarieties of X is the set of closed sets in a topology on X which is called the* **Zarisky topology***. Indeed we have*

1) $V(\mathbf{F}[x_1,\cdots,x_n])=V(\{0\})=\mathbf{F}^n$ *and* $V(\emptyset)=V(\{1\})=\emptyset$,
2) $V(S)\cup V(T)=V(R)$, *where* $R=\big\{fg\big|f\in S,g\in T\big\}$, *and*
3) $\bigcap_{\alpha\in A}V(S_\alpha)=V\big(\bigcup_{\alpha\in A}S_\alpha\big)$.

Proof: Parts (1) and (3) are easy. To prove part (2), first suppose that $x\in V(S)\cup V(T)$, say $x\in V(S)$. Then for $f\in S$ and $g\in T$ we have $f(x)=0$ and so $(fg)(x)=0$, and hence $x\in V(R)$. Now, suppose that $x\notin V(S)\cup V(T)$. Choose $f\in S$ and $g\in T$ such that $f(x)\neq 0$ and $g(x)\neq 0$. Then $fg\in R$ but $(fg)(x)\neq 0$, so $x\notin V(R)$.

1.17 Example: As particular cases of the above parts (2) and (3), in $\mathbf{F}^n$ we have

$$V(fg) = V(f) \cup V(g) \quad \text{and} \quad V(f,g) = V(f) \cap V(g)\,.$$

1.18 Example: By part (2) of the above theorem, every finite union of varieties in $\mathbf{F}^n$ is a variety. In particular, since every one-point set is a variety, every finite set of points is a variety in $\mathbf{F}^n$. If $\mathbf{F}$ is a finite field, then every subset of $\mathbf{F}^n$ is a variety.

1.19 Example: As another particular case of part (2), in $\mathbf{F}^2$ we have

$$\begin{aligned}\big\{(a,b),(c,d)\big\} &= V(x-a,y-b)\ \cup\ V(x-c,y-d)\\ &= V\big((x-a)(x-c),(x-a)(y-d),(x-c)(y-b),(y-b)(y-d)\big)\end{aligned}$$

1.20 Example: An ordered triangle in $\mathbf{R}^2$ is an ordered triple (a_1,a_2,a_3) where the a_i are non-collinear points in $\mathbf{R}^2$. If we write $a_1=(x_1,x_2)$, $a_2=(x_3,x_4)$ and $a_3=(x_5,x_6)$, then we can consider an ordered triangle as an element of $\mathbf{R}^6$. Show that the set of ordered triangles is open (in the Zariski topology) in $\mathbf{R}^6$.

Solution: The three points a_i are collinear if and only if u and v are linearly independent, where $u=a_2-a_1=(x_3-x_1,x_4-x_2)$ and $v=a_3-a_1=(x_5-x_1,x_6-x_2)$. So if we let $f(x_1,\cdots,x_6)=(x_3-x_1)(x_6-x_2)-(x_4-x_2)(x_5-x_1)$, which is the determinant of the matrix with columns u and v, then the set of ordered triangles in $\mathbf{R}^6$ is the complement of the variety $V(f)$.

1.21 Example: An $n\times n$ matrix with entries in $\mathbf{F}$ can be considered as an element of $\mathbf{F}^{n^2}$. Show that the set $GL(n,\mathbf{F})$ of invertible $n\times n$ matrices over $\mathbf{F}$ is open in $\mathbf{F}^{n^2}$.

Solution: Let $f(x_1,\cdots,x_{n^2})$ be the determinant of the matrix with entries $x_1,\cdots,x_{n^2}$. Then f is a polynomial of degree n, and $GL(n,\mathbf{F})$ is the complement of the variety $V(f)$.

1.22 Example: More generally, show that for $0\le k\le n$, the set $M_{\le k}(n,\mathbf{F})$ of $n\times n$ matrices of rank $\le k$ is closed in $\mathbf{F}^{n^2}$, and the set $M_k(n,\mathbf{F})$ of matrices of rank k is open in $M_{\le k}(n,\mathbf{F})$.

Solution: A matrix has rank $\le k$ if and only if the determinant of every $(k{+}1)\times(k{+}1)$ sub-matrix is equal to zero, so $M_{\le k}(n,\mathbf{F})$ is the variety in $\mathbf{F}^{n^2}$ cut out by the determinants of all the $(k{+}1)\times(k{+}1)$ sub-matrices of the matrix with entries $x_1,\cdots,x_{n^2}$. Thus $M_{\le k}(n,\mathbf{F})$ is closed in $\mathbf{F}^{n^2}$. And $M_k(n,\mathbf{F})$ is the complement of $M_{\le k-1}(n,\mathbf{F})$ in $M_{\le k}(n,\mathbf{F})$.

1.23 Example: Show that if X is closed in the Zarisky topology in $\mathbf{F}^n$, where $\mathbf{F}=\mathbf{Q}$, $\mathbf{R}$ or $\mathbf{C}$, then X is also closed in the standard metric topology.

Solution: If $f\in\mathbf{F}[x_1,\cdots,x_n]$ then $f:\mathbf{F}^n\to\mathbf{F}$ is continuous in the standard metric topology (polynomials are continuous), and so $f^{-1}(C)=\{x\in\mathbf{F}^n|f(x)\in C\}$ is closed whenever C is closed, and in particular $V(f)=f^{-1}(0)$ is closed, in the standard metric topology. Now, let $X\subseteq\mathbf{F}^n$ be closed in the Zarisky topology, that is, let X be a variety. Say $X=V(S)$ where $S\subseteq\mathbf{F}[x_1,\cdots,x_n]$. Then $X=V(S)=\bigcap\limits_{f\in S}V(f)=\bigcap\limits_{f\in S}f^{-1}(0)$, which is closed in the standard metric topology, since each $f^{-1}(0)$ is closed.