1. Some affine geometry

Apollonius was perhaps the greatest of the Greek geometers. He lived around 200 BC. One of his most famous results is:

The locus of points, whose distances from two fixed points are in a constant ratio, is a circle.

This is one of the harder results one can prove using only classical geometry. However using just a little algebra makes the result almost completely trivial.

Change coordinates so that the first point A is at the origin and the second point B lies on the x-axis,

$$A = (0, 0) \qquad\qquad B = (a, 0).$$

Let $P = (x, y)$ be a general point of the locus described above. Let m be the fixed ratio. By assumption

$$|PA| = m|PB|.$$

So we have

$$|PA|^2 = x^2 + y^2 \qquad\qquad |PB|^2 = (x - a)^2 + y^2.$$

Thus

$$x^2 + y^2 = m^2(x - a)^2 + m^2y^2.$$

After a little manipulation we get

$$(x - \alpha)^2 + y^2 = \alpha^2 - \beta$$

for appropriate α and β, that is, we get a circle.

There are two general principles to be gleaned from this example:

- To solve problems in analytic geometry, a little bit of algebra goes a long way.
- Since we introduce coordinates to solve this problem, we get to choose where to put the origin.

Definition 1.1. *Let K be a field.* ***Affine n-space over K****, is a copy of a K-vector space V of dimension n. An* ***affine linear subspace*** *Λ is is the translate of a linear subspace of V.*

$\mathbb{A}^n_K$ is the copy of affine space associated to the standard vector space $V = K^n$ of dimension n.

In other words, affine space is nothing more than a vector space without a preferred point and a line in the affine plane is what a calculus student would call a line but not an undergraduate math major. We will invariably drop the word affine.

Definition 1.2. *Let K be an algebraically closed field.*

*An **affine subvariety** V of $\mathbb{A}^n_K$ is any subset of $\mathbb{A}^n_K$ defined by the zeroes of a collection of polynomials.*

Example 1.3. *Any linear space is an affine variety; any conic is an affine variety (a parabola, circle, ellipse, hyperbola, etc).*

$$C = \{\, (x, y) \in \mathbb{A}^2_K \,|\, y^2 = x^2 + x^3 \,\}$$

*is an affine variety called a **nodal cubic**; it is the zero set of $y^2-x^2-x^3$. Similarly*

$$C = \{\, (x, y) \in \mathbb{A}^2_K \,|\, y^2 = x^3 \,\}$$

*is an affine variety called a **cuspidal cubic**; it is the zero set of y^2-x^3.*

If S is a set of polynomials in the polynomial ring $K[x_1, x_2, \dots, x_n]$ it is convenient to let $V(S)$ be the common zero set.

Definition-Lemma 1.4. *The **Zariski topology** on $\mathbb{A}^n_K$ is the topology whose closed subsets are the affine subvarieties.*

Proof. The empty set is defined by the polynomial 1 and $\mathbb{A}^n_K$ is defined by the polynomial 0.

If V_α are closed subsets then we may find subsets $S_\alpha \subset K[x_1, x_2, \dots, x_n]$ such that $V_\alpha = V(S_\alpha)$. If

$$S = \bigcup_\alpha S_\alpha \qquad \text{then} \qquad V = \bigcap_\alpha V(S),$$

so that the intersection of closed sets is closed.

If V_1 and V_2 are two closed sets defined by polynomial subsets S_1 and S_2 so that $V_i = V(S_i)$ then

$$V = V_1 \cup V_2 = V(S),$$

where $S = S_1 S_2$ is the set of all products. Thus the union of two closed subsets is closed and we have a topology. □

Example 1.5. *Note that any finite subset of $\mathbb{A}^n_K$ is a Zariski closed subset.*

Example 1.6. *Consider closed subsets of $\mathbb{A}^1_K$. If $f(x) \in K[x]$ is a polynomial in one variable then $f(x)$ factors,*

$$f(x) = \lambda(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Thus either $f(x)$ is identically zero, or constant but never zero, or $f(x)$ vanishes at only finitely many points $\alpha_1, \alpha_2, \dots, \alpha_n$. In particular the only proper closed subsets of $\mathbb{A}^1_K$ are finite subsets. Thus the Zariski topology is not Hausdorff.

Given an affine subvariety V it is natural to wonder about the degrees of polynomials definining V. Let f be a polynomial with no constant term. Note that f and x_1f, x_2f, $\dots$, x_nf have the same zero set, so clearly we should focus on minimising the degrees of a defining set S.

If V consists of d points in $\mathbb{A}^n_K$ then it is not hard to see that V is defined by polynomials of degree d. Moreover, in general, we cannot do better than this. If $n = 1$ then the smallest degree of a polynomial vanishing at d points is d; more generally if we take d points on a line then and if $f(x_1, x_2, \dots, x_n)$ is a polynomial vanishing on those points but not on the line then f has degree at least d.

Definition 1.7. *The **span of a subset** $V \subset \mathbb{A}^n_K$ is the smallest linear space containing V.*

*We say that the points of V are in **linear general position** if any subset of $k \leq n$ points spans a linear space of dimension $k - 1$.*

Remark 1.8. *If V has at least $n+1$ points then V is in linear general position if and only if any subset of cardinality $n + 1$ spans the whole of $\mathbb{A}^n_K$.*

Note that a linear space is the same as a Zariski closed subset defined by linear polynomials. A **hyperplane** is a linear space defined by a single equation.

Theorem 1.9. *If $V \subset \mathbb{A}^n_K$ is any set of $d \leq 2n$ points in linear general position then V is defined by quadratic polynomials.*

Proof. We do the case $d = 2n$; the general case follows in a similar fashion.

We have

$$V = \{\, p_1, p_2, \dots, p_{2n} \,\}.$$

Let q be a point which belongs to the zero set of every quadratic polynomial which vanishes on the whole of V. We have to show that $q \in V$.

Suppose that we decompose V into two subsets of cardinality n, $V = V_1 \cup V_2$. Both subsets V_1 and V_2 define hyperplanes H_1 and H_2, both of which are defined by linear polynomials. The union $H_1 \cup H_2$ is defined by the product, a quadratic polynomial. By what we just said, $q \in H_1 \cup H_2$, so that q must belong to either H_1 or H_2.

Let $k \leq n$ be the smallest integer such that q belongs to the span of k points of $p_1, p_2, \dots, p_{2n}$. Renumbering we may assume that q belongs to the span of $p_1, p_2, \dots, p_k$. Pick a subset Σ of cardinality $n - k + 1$ of $V - \{\, p_1, p_2, \dots, p_k \,\}$. Let Λ be the hyperplane spanned by p_2, p_3, $\dots$, p_k and Γ. Note that q does not belong Λ, since p_1 belongs to the span of p_2, p_3, $\dots$, p_k and q and Λ doesn't contain p_1.

Thus q belongs to the hyperplane spanned by the other n points of V. Varying Γ, q must belong to the intersection of these hyperplanes, which is just p_1. Thus $q = p_1$. $\square$

Definition-Lemma 1.10. *Let $V \subset \mathbb{A}^n_K$ be any subset.*

*The **ideal** $I = I(V)$ of V is the set of all polynomials vanishing on V,*

$$I = \{ f \in K[x_1, x_2, \dots, x_n] \,|\, f(v) = 0, v \in V \} \trianglelefteq K[x_1, x_2, \dots, x_n].$$

Proof. We check I is an ideal. $0 \in I$ and so I is non-empty. If f and $g \in I$ then and p and $q \in K[x_1, x_2, \dots, x_n]$ then

$$(pf + qg)(v) = p(v)f(v) + q(v)g(v) = 0 \qquad \text{for all} \qquad v \in V,$$

so that $pf + qg \in I$ and I is an ideal. $\square$

Lemma 1.11.

(1) If $S_1 \subset S_2 \subset K[x_1, x_2, \dots, x_n]$ then $V(S_2) \subset V(S_1)$.
(2) If $V_1 \subset V_2 \subset \mathbb{A}^n_K$ then $I(V_2) \subset I(V_1)$.
(3) If V_1 and V_2 are two subsets of $\mathbb{A}^n_K$ and $I_i = I(V_i)$ then

$$I(V_1 \cup V_2) = I(V_1) \cap I(V_2).$$

(4) $V \subset \mathbb{A}^n_K$ is any subset then $V(I(V)$ is the Zariski closure of V.

Proof. Straightforward. $\square$

If $S \subset K[x_1, x_2, \dots, x_n]$ is a collection of polynomials it is natural to consider the ideal of all polynomials vanishing on the zero set of S, that is, to consider $I(V(S))$. The first guess is that this is simply the ideal generated by S.

Example 1.12. *Let $I = \langle x^2 \rangle \subset K[x]$. The zero set is the origin in $\mathbb{A}^1_K$ and the ideal of the zero set is $\langle x \rangle$.*

All rings R are commutative with an identity.

Definition-Lemma 1.13. *Let $I \trianglelefteq R$ be an ideal in a ring R. The **radical of** I, denoted $\sqrt{I}$, is the ideal of all elements of r such that $r^m \in I$ for some natural number m.*

*We say that I is a **radical ideal** if it is equal to its radical.*

Proof. $0 \in \sqrt{I}$ so that the radical is non-empty. If i and $j \in \sqrt{I}$ then we may find m and n such that $i^m, j^n \in I$. Let r and $s \in R$.

$$(ri + sj)^{m+n} = \sum_l \binom{n+m}{l} r^l i^l s^{n+m-l} j^{n+m-l} \in I,$$

so that $ri + sj \in \sqrt{I}$ and $\sqrt{I}$ is an ideal. $\square$

Theorem 1.14 (Hilbert's Nullstellensatz)**.** *Let K be an algebraically closed field.*

If $I \subset K[x_1, x_2, \dots, x_n]$ then

$$I(V(I)) = \sqrt{I}.$$

Corollary 1.15. *There is an inclusion reversing correspondence between Zariski closed subsets of $\mathbb{A}^n_K$ and radical ideals of $K[x_1, x_2, \dots, x_n]$.*

Definition 1.16. *Let X be a topological space. We say that X is* ***irreducible*** *if for every pair of closed subsets X_1 and X_2, such that $X_1 \cup X_2 = X$, we have either $X = X_1$ or $X = X_2$.*

Compare this definition with the definition of connected. Clearly the definition of irreducible is stronger than connected; in practice most connected topological spaces are rarely irreducible. For example if X is irreducible (and has at least two points) then it is not Hausdorff.

Lemma 1.17. *Let X be an irreducible topological space.*

Then every non-empty open subset is dense.

Proof. Let U be a non-empty open subset. If U is not dense then there is another non-empty open subset U such that $U \cap V$ is empty. Let F and G be their complements. Then F and G are two proper closed subsets, whose union is X, a contradiction. □

Lemma 1.18. *A Zariski closed subset $X \subset \mathbb{A}^n_K$ is irreducible if and only if $I(X)$ is a prime ideal.*

Proof. Suppose that X is irreducible. Let f_1 and f_2 be two elements of $K[x_1, x_2, \dots, x_n]$ such that $f_1 f_2 \in I$. Let $X_i = V(f_i)$. Then X_i are closed subsets of X and $X = X_1 \cup X_2$ since $f_1 f_2$ vanishes on X. As X is irreducible $X = X_i$ some i and so $f_i \in I$. But then I is prime.

Now suppose that I is prime. Let $X = X_1 \cup X_2$ and let $I_i = I(X_i)$. Then

$$I = I(X) = I(X_1 \cup X_2) = I_1 \cap I_2.$$

As I is prime, $I = I_i$ some i and $X = X_i$. □

Example 1.19. *A finite set is irreducible if and only if its cardinality is less than two.*

The nodal and cuspidal cubics are irreducible.

Definition 1.20. *Let X be a topological space. We say that X is* ***Noetherian*** *if the set of closed subsets satisfies DCC (the descending chain condition). That is, any sequence of descending closed subsets*

$$\dots \subset X_n \subset X_{n-1} \subset \dots \subset X_1 \subset X_0.$$

eventually stablises, so that we may find n_0 such that $X_n = X_{n+1}$ for all $n \geq n_0$.

Theorem 1.21. *Any affine variety is Noetherian.*

Proof. Let $X \subset \mathbb{A}^n$ be a closed subset. We may as well suppose that $X = \mathbb{A}^n$. By (1.11) it suffices to check that the set of radical ideals satisfies the ACC. But Hilbert's basis theorem says that the set of all ideals satisfies the ACC. □

Principle 1.22 (Noetherian Induction)**.** *Let P be a property of topological spaces, satisfying the following inductive hypothesis: if X is a topological space and every proper closed subset $Y \subset X$ satisfies property P, then X satisfies property P.*

Then every Noetherian topological space satisfies property P.

Proof. Suppose not. Let X be a Noetherian topological space, minimal with the property that it does not satisfy property P.

Let $Y \subset X$ be a proper closed subset. By minimality of X, Y satisfies property P. By the inductive hypothesis, X then satisfies property P, a contradiction. □

Lemma 1.23. *Let X be a Noetherian topological space.*

Then X has a decomposition into closed irreducible factors

$$X = X_1 \cup X_2 \cup \cdots \cup X_n,$$

where X_i is not contained in X_j, unique up to re-ordering of the factors.

Proof. If X is irreducible there is nothing to prove. Otherwise we may assume that $X = A \cup B$, where A and B are proper closed subsets. By the principle of Noetherian Induction, we may assume that A and B are the finite union of closed irreducible factors. Taking the union, and discarding any redundant factors (that is, any subset contained in another subset), we get the existence of such a decomposition.

Now suppose that

$$X_1 \cup X_2 \cup \cdots \cup X_m = Y_1 \cup Y_2 \cup \cdots \cup Y_n.$$

Consider

$$X_m = (X_m \cap Y_1) \cup (X_m \cap Y_2) \cup (X_m \cap Y_3) \cup \cdots \cup (X_m \cap Y_n).$$

By irreducibility of X_m, there is an index j such that $X_m \subset Y_j$. Thus $m \leq n$ and for every i there is a j such that $X_i \subset Y_j$. By symmetry, for every j there is a k such that $Y_j \subset X_k$. In this case $X_i \subset X_k$ and so $i = k$, by assumption. Thus $X_i = Y_j$. □