MA4273 Algebraic Geometry of Curves and Surfaces

Thang Pang Ern

Reference books:

(1) ???

Contents

1. Affine Algebraic Sets

1.1. *Algebraic Preliminaries*

In this course, we will take a ring R to be a commutative ring with identity. Recall from MA3201 on what ring homomorphisms are. These are maps $\varphi : R \to S$ such that $e_R \mapsto e_S$. We also recall what an integral domain (Definition 1.1) and a field (Definition 1.2) are.

Definition 1.1 (integral domain). Let D be an integral domain. Then, for all $x, y \in D$,

$$xy = 0 \quad \text{implies} \quad x = 0 \text{ or } y = 0.$$

Definition 1.2 (field). A field F is a domain such that every element has a multiplicative inverse, i.e.

$$\text{for all } x \in F \quad \text{there exists } y \in F \text{ such that } xy = e_F.$$

Definition 1.3 (field of fractions). Let D be an integral domain. Define the field of fractions K as follows:

(i) The elements of K are equivalence classes of pairs (p,q), where $p, q \in D$ and $q \neq 0$. Two pairs (p,q) and (r,s) are considered equivalent if and only if

$$p \cdot s = q \cdot r$$

(ii) The sum of two equivalence classes $[(p,q)]$ and $[(r,s)]$ is defined as

$$[(p,q)] + [(r,s)] = [(p \cdot s + q \cdot r, q \cdot s)]$$

(iii) The product of two equivalence classes $[(p,q)]$ and $[(r,s)]$ is defined as

$$[(p,q)] \cdot [(r,s)] = [(p \cdot r, q \cdot s)]$$

Proposition 1.1. Let D be an integral domain and K be its field of fractions. Then, there is the following canonical inclusion:

$$D \hookrightarrow K \quad \text{where} \quad x \mapsto (x,1) = \frac{x}{1}.$$

Definition 1.4 (polynomial ring). Let R be a ring. Define the ring of polynomials $R[x]$ as follows:

$$R[x] = \left\{ \sum_{\text{finite}} a_i x^i : a_i \in R \right\}$$

Definition 1.5 (degree). The degree of a polynomial in $R[x]$ can be defined using the following map:

$$\deg : R[x] \to \mathbb{Z}_{\geq 0} \quad \text{where} \quad \sum_{\text{finite}} a_i x^i \mapsto \max\{d : a_d \neq 0\}$$

Proposition 1.2. We have the following properties on the degree of two polynomials $f, g \in R[x]$:
(1). $\deg(fg) = \deg f + \deg g$
(2). $\deg(f+g) \leq \max\{\deg f, \deg g\}$

Naturally, we can extend Definition 1.4 to a polynomial ring of two variables.

Definition 1.6 (polynomial ring). Let R be a ring. Define the ring of polynomials in two variables x_1 and x_2, denoted by $R[x_1, x_2]$, to be as follows:

$$R[x_1, x_2] = \left\{ \sum_{i+j=k} a_{ij} x_1^i x_2^j : a_{ij} \in R \right\}$$

Recall from MA3201 on what it means for a ring R to be a unique factorisation domain (UFD).

Lemma 1.1 (Gauss' lemma). Every element factorises uniquely into prime elements up to units.

Proposition 1.3. Let R be a UFD and K be its field of fractions. Then, there exists the canonical inclusion $R \hookrightarrow K$. Also, we have the map

$$R[x] \to K[x] \quad \text{where} \quad f \mapsto f.$$

Then, f is irreducible over $R[x]$ if and only if f is irreducible over $K[x]$.

Proposition 1.4. Let R be a UFD. Then, $R[x]$ is a UFD.

Corollary 1.1. Let R be a UFD. Then, $R[x_1, \ldots, x_n]$ is a UFD.

Definition 1.7 (ideal). Let R be a commutative ring. An ideal $I \subseteq R$ is such that

$$\text{for all } a, b \in I \text{ and } r \in R \quad \text{we have} \quad a + b \in I \text{ and } ra \in I.$$

Definition 1.8 (kernel and image). Let

$$\varphi : R \to S \quad \text{be a ring homomorphism.}$$

Then,

$$\ker \varphi = \{r \in R : \varphi(r) = 0\} \quad \text{is} \quad \text{an ideal of } R$$

and

$$\operatorname{Im} \varphi = \{\varphi(r) : r \in R\}.$$

Definition 1.9. Let $I \subseteq R$ be an ideal. We say that I is generated by the set $\{x_1, \ldots, x_k\}$ and we write $I = (x_1, \ldots, x_k)$ if

$$I = \left\{ \sum r_i x_i \right\}.$$

Furthermore, I is said to be finitely-generated if there exists a finite set $G \subseteq R$ such that $I = (G)$.

Definition 1.10 (Noetherian ring). A ring R is said to be Noetherian if any ideal of R is finitely generated.

Theorem 1.1 (Hilbert basis theorem). Let R be a Noetherian ring. Then, $R[x]$ is also Noetherian.

Corollary 1.2. Let R be a Noetherian ring. Then, $R[x_1, \ldots, x_n]$ is also Noetherian.

Definition 1.11 (quotient ring). Let I be an ideal of R. Then, the quotient ring R/I contains elements of the form $a+I$. For any $\overline{a}, \overline{b} \in R/I$, we write

$$\overline{a} = a+I \text{ and } \overline{b} = b+I \quad \text{where} \quad a, b \in R.$$

As such, we have the following properties:

(i) $\overline{a+b} = (a+b)+I$

(ii) $\overline{ab} = ab+I$

Theorem 1.2. Let I be an ideal of a ring R. Then,

$$I \text{ is a prime ideal} \quad \text{if and only if} \quad R/I \text{ is an integral domain.}$$

Theorem 1.3. Let I be an ideal of a ring R. Then,

$$I \text{ is a maximal ideal} \quad \text{if and only if} \quad R/I \text{ is a field.}$$

Also, recall the definition of the characteristic of a ring.

Definition 1.12 (algebraically closed field). Let k be a field. We say that k is algebraically closed if every $f \in k[x]$ has a root in k. We write

$$\overline{k} \quad \text{to denote the algebraic closure of } k.$$

Example 1.1 (algebraic closure of $\mathbb{Q}$). Recall that $\mathbb{Q}$ denotes the field of rational numbers. The algebraic closure of $\mathbb{Q}$ is the field $\overline{\mathbb{Q}}$, which consists of all algebraic numbers, denoted by $\mathbb{A}$. Recall that an algebraic number is any complex number that is a root of some non-zero polynomial with coefficients in $\mathbb{Q}$. $\overline{\mathbb{Q}}$ is a proper subfield of $\mathbb{C}$ since there are transcendental numbers like π and e that are not contained in $\overline{\mathbb{Q}}$.

As such, $\mathbb{Q}$ is not algebraically closed.

Example 1.2 (algebraic closure of $\mathbb{C}$). The field of complex numbers $\mathbb{C}$ is algebraically closed, which is a consequence of the fundamental theorem of algebra. One recalls that this theorem states that every non-constant polynomial with complex coefficients has a root in $\mathbb{C}$. So, $\overline{C} = \mathbb{C}$.

1.2. *Affine Spaces and Algebraic Sets*

Definition 1.13 (the affine n-space). Let k be any field. By $\mathbb{A}^n(k)$, we shall mean the Cartesian product of k with itself n times. That is,

$$\mathbb{A}^n(k) = \{(a_1,\ldots,a_n) : a_i \in k \text{ for all } i = 1,\ldots,n\}.$$

We call $\mathbb{A}^n(k)$ the affine n-space over k; its elements will be called points.

In particular, for Definition 1.13,

$\mathbb{A}^1(k)$ is the affine line

$\mathbb{A}^2(k)$ is the affine plane

Definition 1.14 (zero and hypersurface). If $F \in k[X_1,\ldots,X_n]$, a point $P = (a_1,\ldots,a_n)$ in $\mathbb{A}^n(k)$ is a zero of F if

$$F(P) = F(a_1,\ldots,a_n) = 0.$$

If F is not a constant, the set of zeros of F is the hypersurface defined by F, and is denoted by $V(F)$.

Example 1.3. A hypersurface in $\mathbb{A}^2(k)$ is an affine plane curve. If F is a polynomial of degree one, $V(F)$ is a *hyperplane* in $\mathbb{A}^n(k)$; if $n = 2$, it is a line.

Example 1.4. Let $k = \mathbb{R}$. Consider $V\left(Y^2 - X\left(X^2-1\right)\right) \subseteq \mathbb{A}^2$. The graph is an example of an elliptic curve (Figure 1).

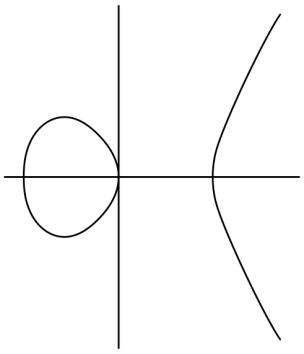


Figure 1: The equation $y^2 - x\left(x^2-1\right) = 0$

Example 1.5. Let $k = \mathbb{R}$. Consider $V\left(Y^2 - X^2(X+1)\right) \subseteq \mathbb{A}^2$. Again, the graph is an example of an elliptic curve (Figure 2).

Example 1.6. Let $k = \mathbb{R}$. Consider $V\left(Z^2 - \left(X^2+Y^2\right)\right) \subseteq \mathbb{A}^3$. The graph is an example of a cone (Figure 3).

Example 1.7. Let $k = \mathbb{R}$. Consider $V\left(Y^2 - XY - X^2Y + X^3\right) \subseteq \mathbb{A}^2$ and the corresponding graph (Figure 4).

More generally, if S is any set of polynomials in $k[X_1,\ldots,X_n]$, we let

$$V(S) = \{P \in \mathbb{A}^n : F(P) = 0 \text{ for all } F \in S\} = \bigcap_{F\in S} V(F)$$

If $S = \{F_1,\ldots,F_r\}$, we usually write

$$V(F_1,\ldots,F_r) \quad \text{instead of} \quad V(\{F_1,\ldots,F_r\}).$$

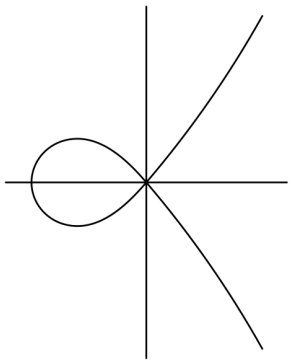


Figure 2: The equation $y^2 - x^2(x+1) = 0$

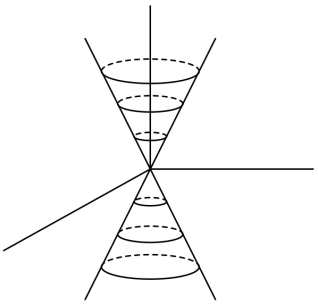


Figure 3: The equation $z^2 - \left(x^2 + y^2\right) = 0$

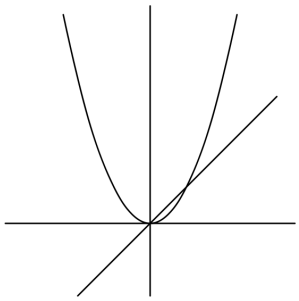


Figure 4: The equation $y^2 - xy - x^2y + x^3 = 0$

Definition 1.15 (algebraic set)**.** A subset $X \subseteq \mathbb{A}^n(k)$ is an affine algebraic set or simply an algebraic set if $X = V(S)$ for some S.

Example 1.8 (Fulton p. 5 Question 11)**.** Prove that the set

$$X = \left\{\left(t, t^2, t^3\right) \in \mathbb{A}^3(k) : t \in k\right\} \quad \text{is algebraic.}$$

Solution. We have $(x,y,z) \in X$ when there exists $t \in k$ such that

$$x = t \quad y = t^2 \quad z = t^3.$$

So, the relations $y - x^2 = 0$ and $z - x^3 = 0$ must hold. That is, on the set X, the polynomials

$$f_1(x,y,z) = y - x^2 \text{ and } f_2(x,y,z) = z - x^3 \quad \text{must vanish.}$$

We claim that

$$X = V\left(y - x^2, z - x^3\right).$$

To prove the forward inclusion $\subseteq$, suppose $(x,y,z) \in X$. Then, $(x,y,z) = \left(t,t^2,t^3\right)$ for some $t \in k$. So, $y-x^2 = t^2-t^2 = 0$ and $z-x^3 = t^3-t^3 = 0$. It follows that $(x,y,z) \in V\left(y-x^2, z-x^3\right)$.

As for the reverse inclusion $\supseteq$, suppose $(x,y,z) \in V\left(y-x^2, z-x^3\right)$. Then, $y-x^2 = 0$ and $z-x^3 = 0$. As such, by parametrising using $x = t$, we have $y = t^2$ and $z = t^3$. As such, the result follows. □

Example 1.9 (Fulton p. 5 Question 11). Prove that the set

$$X = \left\{(\cos t, \sin t) \in \mathbb{A}^2(\mathbb{R}) : t \in \mathbb{R}\right\} \quad \text{is algebraic.}$$

Solution. We have $(x,y) \in X$ if there exists $t \in \mathbb{R}$ such that $x = \cos t$ and $y = \sin t$. As such, the relation $x^2 + y^2 - 1 = 0$ must hold. In other words, on the set X, the polynomial $f(x,y) = x^2+y^2-1$ must vanish. It suffices to show that

$$X = V\left(x^2+y^2-1\right).$$

For the forward inclusion, suppose $(x,y) \in X$. Then, $(x,y) = (\cos t, \sin t)$ for some $t \in \mathbb{R}$. So, $x^2+y^2-1 = 0$, and it follows that $(x,y) \in V\left(x^2+y^2-1\right)$. The proof of the reverse inclusion is similar. □

Example 1.10 (Fulton p. 5 Question 11). Prove that the set of points in $\mathbb{A}^2(\mathbb{R})$ whose polar coordinates (r,θ) satisfy the equation $r = \sin\theta$ is algebraic.

Solution. Naturally, we write x^2+y^2-y. One can show that $X = V\left(x^2+y^2-y\right)$. □

Example 1.11 (Fulton p. 5 Question 13). Prove that the set

$$X = \left\{(x,y) \in \mathbb{A}^2(\mathbb{R}) : y = \sin x\right\} \quad \text{is not algebraic.}$$

Solution. The graph of $y = \sin x$ does not satisfy any polynomial equation $p(x,y) \in \mathbb{R}[x,y]$ so it cannot be described as the zero locus of some polynomial. To be more *rigorous*, for any solution (x,y) of $P(x,y) = 0$, we note that $(x+2n\pi, y)$ for $n \in \mathbb{Z}$ is also a solution, and this occurs infinitely many times. □

Example 1.12 (Fulton p. 5 Question 13). Prove that the set

$$\left\{(\cos t, \sin t, t) \in \mathbb{A}^3(\mathbb{R}) : t \in \mathbb{R}\right\} \quad \text{is not algebraic.}$$

Solution. Same idea as Example 1.11 — consider translating by $2n\pi$ which will also yield another solution. Hence, we can obtain infinitely many solutions, which is a contradiction as there does not exist any polynomial with infinitely many roots. □

Proposition 1.5. We have the following properties:

(i) If I is the ideal in $k[X_1,\ldots,X_n]$ generated by S, then

$$V(S) = V(I) \quad \text{so} \quad \text{every algebraic set is equal to } V(I) \text{ for some } I$$

(ii) **Intersection of algebraic sets is algebraic:** if $\{I_\alpha\}$ is any collection of ideals, then

$$V\left(\bigcup_\alpha I_\alpha\right) = \bigcap_\alpha V(I_\alpha)$$

(iii) If we have ideals $I \subseteq J$, then $V(J) \subseteq V(I)$

(iv) **Finite union of algebraic sets is algebraic:** $V(FG) = V(F) \cup V(G)$ for any polynomials F and G, and

$$V(I) \cup V(J) = V(\{FG : F \in I, G \in J\})$$

(v) Finite subset of $\mathbb{A}^n(k)$ is an algebraic set: $V(0) = \mathbb{A}^n(k)$, $V(1) = \emptyset$, and

$$V(X_1 - a_1, \ldots, X_n - a_n) = \{(a_1, \ldots, a_n)\} \quad \text{for all } a_i \in K$$

Recall and **(ii)** and **(iv)** of Proposition 1.5, which respectively state that the intersection and finite union of algebraic sets are algebraic. We will see in Example 1.13 that the countable collection of algebraic sets may not be algebraic.

Example 1.13 (Fulton p. 5 Question 10)**.** Give an example of a countable collection of algebraic sets whose union is not algebraic.

Solution. Here is a classic example. For each $n \in \mathbb{Z}_{\geq 0}$, consider the algebraic set

$$X_n = \left\{(x,y) \in \mathbb{A}^2(k) : y - x^n = 0\right\} = V(y - x^n) \quad \text{which is an algebraic subset of } \mathbb{A}^2(k).$$

Define

$$X = \bigcup_{n=0}^{\infty} X_n = \bigcup_{n=0}^{\infty} \left\{(x,y) \in \mathbb{A}^2(k) : y - x^n = 0\right\}.$$

We shall prove that x is not an algebraic set. Suppose on the contrary that there exists a non-zero polynomial $f(x,y) \in k[x,y]$ such that $X = V(f)$. Then,

$$f(x,y) = 0 \quad \text{for every } (x,y) \in X.$$

Since X contains each curve $y = x^n$ for $n \in \mathbb{Z}_{\geq 0}$, then

$$f(x,x^n) = 0 \quad \text{for all } x \in k \text{ and } n \in \mathbb{Z}_{\geq 0}.$$

As this holds for infinitely many n, it forces restrictive conditions on the polynomial f. In particular, the only way

$$f(x,x^n) = 0 \quad \text{for all } x \in k \text{ and } n \in \mathbb{Z}_{\geq 0} \quad \text{is} \quad f \text{ is the zero polynomial.}$$

If f were not the zero polynomial, then for a fixed non-zero f, there is a bound on how many distinct irreducible curves of the form $y - x^n$ it could vanish on (unless it vanishes on the entire plane). However, we have infinitely many distinct curves $y = x^n$. Hence, $f = 0$ in $k[x,y]$. As $V(f) = V(0) = \mathbb{A}^2(k)$, then $X = \mathbb{A}^2(k)$. However, our union

$$X = \bigcup_{n=0}^{\infty} X_n \quad \text{is a proper subset of } \mathbb{A}^2(k),$$

which is a contradiction. □

1.3. *The Ideal of a Set of Points*

Definition 1.16 (ideal)**.** For any subset X of $\mathbb{A}^n(k)$, we consider those polynomials that vanish on X. They form an ideal in $k[X_1, \ldots, X_n]$, called the ideal of X, and we write $I(X)$. So,

$$I(X) = \{F \in k[X_1, \ldots, X_n] : F(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in X\}.$$

Proposition 1.6 gives some relations between ideals and algebraic sets.

Proposition 1.6. The following hold:

(i) If $X \subseteq Y$, then $I(Y) \subseteq I(X)$

(ii) $I(\emptyset) = k[X_1, \ldots, X_n]$

(iii) $I(\mathbb{A}^n(k)) = (0)$ if k is an infinite field

(iv) $I(\{(a_1, \ldots, a_n)\}) = (X_1 - a_1, \ldots, X_n - a_n)$ for $a_1, \ldots, a_n \in k$

(v) For any set S of polynomials and set X of points, we have

$$S \subseteq I(V(S)) \quad \text{and} \quad X \subseteq V(I(X))$$

(vi) For any set S of polynomials and set X of points, we have

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

So, if V is an algebraic set, then $V(I(V))$ and if I is the ideal of an algebraic set, then $I = I(V(I))$

Proposition 1.7. An ideal that is the ideal of an algebraic set has a property not shared by all ideals. That is,

$$I = I(X) \text{ and } F^n \in I \text{ for some } n \in \mathbb{N} \quad \text{implies} \quad F \in I.$$

Definition 1.17 (radical)**.** If I is any ideal in a ring R, the radical of I, denoted by $\mathrm{Rad}(I)$, is defined to be

$$\{a \in R : a^n \in I \text{ for some } n \in \mathbb{N}\}.$$

Proposition 1.8. $\mathrm{Rad}(I)$ is an ideal containing I.

Definition 1.18 (radical ideal)**.** An ideal I is a radical ideal if $I = \mathrm{Rad}(I)$.

Proposition 1.9. $I(X)$ is a radical ideal for any $X \subseteq \mathbb{A}^n(k)$.

1.4. *The Hilbert Basis Theorem*

Recall the Hilbert basis theorem (Theorem 1.1 and its corollary (Corollary 1.2) which as a whole, states that R is a Noetherian ring, then $R[x]$ is also Noetherian, and consequently, $R[x_1, \ldots, x_n]$ is Noetherian. We will prove this result.

Proof. Suppose $I \subseteq R[x]$ is not finitely generated. Take $f_1 \in I$ which has minimal degree in I. Subsequently, define $f_2 \in I \setminus (f_1)$ which has minimal degree in $I \setminus (f_1)$. By defining each f_i recursively, we have

$$f_n \in I \setminus (f_1, \ldots, f_{n-1}) \quad \text{of minimal degree in } I \setminus (f_1, \ldots, f_{n-1}).$$

By assumption that I is not finitely generated, we can keep picking new polynomials in this way forever, i.e. no finite subset spans I.

Let $\deg f_i = d_i$. If $d_i = 0$ for infinitely many i, then we obtain infinitely many constant elements in $I \subseteq R[x]$. However, those constants lie in R itself, giving rise to an infinite sequence in the ideal of R generated by these constants. As R is Noetherian, the ideal generated by these elements of R must be finitely generated,

contradicting our construction that each new f_i was outside the previously generated ideal.

If instead infinitely many f_i have positive degree, consider their leading coefficients. Denote by $\ell_i \in R$ the leading coefficient of f_i. Then $\ell_1, \ell_2, \ldots$ all lie in some ideal in R. Because R is Noetherian, the ideal in R generated by $\{\ell_1, \ell_2, \ldots\}$ must be finitely generated. Hence there exist $i_1, \ldots, i_m$ such that

$$(\ell_1, \ell_2, \ldots, \ell_n, \ldots) = (\ell_{i_1}, \ldots, \ell_{i_m}) \subseteq R.$$

By appropriate linear combinations in $R[x]$, one deduces that f_n would end up in the ideal $(f_{i_1}, \ldots, f_{i_m}) \subseteq R[x]$ for sufficiently large n, contradicting the choice of f_n. The contradiction arises from assuming that $I \subset R[x]$ was not finitely generated. Thus no such infinite construction can succeed. Therefore every ideal in $R[x]$ is finitely generated, i.e. $R[x]$ is Noetherian. The proof of the case involving n variables follows by an inductive argument. □

Corollary 1.3. Let k be a field. Then, $k[X_1, \ldots, X_n]$ is Noetherian.

1.5. *Irreducible Components of an Algebraic Set*

An algebraic set may be the union of several smaller algebraic sets.

Definition 1.19 (reducible algebraic set)**.** An algebraic set $V \subseteq \mathbb{A}^n$ is reducible if

$$V = V_1 \cup V_2 \quad \text{for some algebraic sets } V_1, V_2 \text{ in } \mathbb{A}^n \quad \text{and} \quad V_i \neq V.$$

Otherwise, V is irreducible.

Proposition 1.10. An algebraic set V is irreducible if and only if $I(V)$ is prime.

Lemma 1.2. Let $\mathcal{S}$ be any non-empty collection of ideals in a Noetherian ring R. Then,

$$\mathcal{S} \text{ has a maximal member,}$$

i.e. there is an ideal I in $\mathcal{S}$ that is not contained in any other ideal of $\mathcal{S}$.

Theorem 1.4. Let V be an algebraic set in $\mathbb{A}^n(k)$. Then, there exist unique irreducible algebraic sets $V_1, \ldots, V_m$ such that

$$V = \bigcup_{i=1}^{m} V_i \quad \text{and } V_i \subsetneq V_j \text{ for all } i \neq j.$$

The V_i are called the irreducible components of V, so

$$V = \bigcup_{i=1}^{m} V_i \quad \text{is the decomposition of } V \text{ into irreducible components.}$$

1.6. *Algebraic Subsets of the Plane*

We will take a closer look at the affine plane $\mathbb{A}^2(k)$ and find all its algebraic subsets before developing the general theory further.

Proposition 1.11. Let F and G be polynomials in $k[X,Y]$ with no common factors. Then,

$$V(F,G) = V(F) \cap V(G) \quad \text{is} \quad \text{a finite set of points.}$$

Corollary 1.4. If F is an irreducible polynomial in $k[X,Y]$ such that $V(F)$ is infinite, then

$$I(V(F)) = (F) \quad \text{and} \quad V(F) \text{ is irreducible.}$$

Corollary 1.5. Suppose k is an infinite field. Then,

$$\text{the irreducible subsets of } \mathbb{A}^2(k) \quad \text{are} \quad \mathbb{A}^2(k), \emptyset, \text{points, and irreducible plane curves } V(F),$$

where F is an irreducible polynomial and $V(F)$ is infinite.

Corollary 1.6. Assume k is an algebraically closed field and F is a non-constant polynomial in $k[X,Y]$. Let $F = F_1^{n_1} \dots F_r^{n_r}$ be the decomposition of F into irreducible factors. Then,

$$\bigcup_{i=1}^{r} V(F_i) \quad \text{is} \quad \text{the decomposition of } V(F) \text{ into irreducible components}$$

and $I(V(F)) = (F_1 \dots F_r)$.

1.7. *Hilbert's Nullstellensatz*

If we are given an algebraic set V, Proposition 1.11 gives a criterion for telling whether V is irreducible or not. What it is lacking is a way to describe V in terms of a given set of polynomials that define V. It is Hilbert's Nullstellensatz, or the *zero-locus-theorem*, which tells us the exact relationship between ideals and algebraic sets. We begin with the Weak Nullstellensatz (Lemma 1.3) before deducing the main result (Theorem 1.5).

Lemma 1.3 (Weak Nullstellensatz)**.** Let k be an algebraically closed field. If

$$I \text{ is a proper ideal in } k[X_1, \dots, X_n] \quad \text{then} \quad V(I) \neq \emptyset.$$

Theorem 1.5 (Hilbert's Nullstellensatz)**.** Let I be an ideal in $k[X_1, \dots, X_n]$, where k is an algebraically closed field. Then, $I(V(I)) = \text{Rad}(I)$.

What the main theorem (Theorem 1.5) is trying to say is as follows. First, recall that $V(I)$ is the set of points in the affine space $\mathbb{A}^n(k)$ where all polynomials in the ideal I vanish, i.e. $V(I)$ is the solution set of the polynomial equations on I. As such, $I(V(I))$ is the ideal of all polynomials that vanish on $V(I)$. If we have polynomials $F_1, \dots, F_r$ and G in $k[X_1, \dots, X_n]$ and G vanishes whenever $F_1, \dots, F_r$ vanish, then there exists an equation

$$G^N = A_1 F_1 + \dots + A_r F^r \quad \text{for some } N > 0 \text{ and } A_i \in k[X_1, \dots, X_n].$$

In short,

$$\text{a polynomial } G \text{ vanishes on } V(I) \quad \text{if and only if} \quad \text{some power of } G \text{ is contained in } I.$$

Corollary 1.7. If I is a radical ideal in $k[X_1, \dots, X_n]$, then $I(V(I)) = I$.

Corollary 1.8. If I is a prime ideal, then $V(I)$ is irreducible.

Corollary 1.9. Let F be a non-constant polynomial in $k[X_1,\ldots,X_n]$ and $F = F_1^{n_1}\ldots F_r^{n_r}$ be the decomposition of F into irreducible factors. Then,

$$V(F) = \bigcup_{i=1}^{r} V(F_i) \quad \text{is} \quad \text{the decomposition of } V(F) \text{ into irreducible components}$$

and $I(V(F)) = (F_1\ldots F_r)$.

1.8. *Modules*

Definition 1.20 (R-module). Let R be a ring. An R-module is a commutative group M, with the group law on M being $+$, the additive identity being 0_M or just 0, together with a scalar multiplication map $R\times M\to M$, such that the following properties are satisfied:

- **(i)** For all $a,b\in R$ and $m\in M$, we have $(a+b)m = am+bm$
- **(ii)** For all $a\in R$ and $m,n\in M$, we have $a(m+n) = am+an$
- **(iii)** For all $a,b\in R$ and $m\in M$, we have $(ab)m = a(bm)$
- **(iv)** For $m\in M$, we have $1_R\cdot m = m$, where 1_R is the multiplicative identity in R

Example 1.14. A $\mathbb{Z}$-module is a commutative group where

$$(\pm a)m \quad \text{is} \quad \pm(m+\ldots+m) \ a \text{ times for } a\in\mathbb{Z}_{\geq 0}.$$

Example 1.15. If R is a field, an R-module is the same thing as a vector space over R.

Example 1.16. The multiplication in R makes any ideal of R into an R-module.

Example 1.17. Let $\varphi : R\to S$ be an R-module homomorphism. Define

$$r\cdot s \text{ for } r\in R, s\in S \quad \text{by the equation} \quad r\cdot s = \varphi(r)s.$$

This makes S into an R-module. In particular, if R is a subring of a ring S, then S is an R-module.

Definition 1.21 (submodule). A subgroup N of an R-module M is a submodule if

$$\text{for all } a\in R, m\in N \quad \text{we have} \quad am\in N.$$

Definition 1.22 (finitely generated module). If S is a set of elements of an R-module M, the submodule generated by S is defined to be

$$\{r_is_i : r_i\in R, s_i\in S\}$$

and it is the smallest submodule of M that contains S. Furthermore, if $S=\{s_1,\ldots,s_n\}$ is finite, then the submodule generated by S is denoted by

$$\sum Rs_i.$$

M is said to be finitely generated if

$$M = \sum Rs_i \quad \text{for some } s_1,\ldots,s_n\in M.$$

Definition 1.23 (module finite)**.** Let R be a subset of a ring S. Then, S is module finite over R if S is finitely generated as an R-module. Furthermore, if R and S are fields and S is module finite over R, then $\dim_R S = [S : R]$.

2. Affine Varieties

2.1. *Coordinate Rings, Polynomial Maps and Coordinate Changes*

From this section onwards, we will let k denote an algebraically closed field. Recall from Definition 1.15 that $\mathbb{A}^n = \mathbb{A}^n(k)$ denotes an affine algebraic set. We also say that an irreducible affine algebraic set is an affine variety.

Definition 2.1 (coordinate ring)**.** Let $V \subseteq \mathbb{A}^n$ be a non-empty variety. Then, $I(V)$ is a prime ideal in $k[X_1,\ldots,X_n]$ so $k[X_1,\ldots,X_n]/I(V)$ is an integral domain. We call

$$\Gamma(V) = k[X_1,\ldots,X_n]/I(V) \quad \text{the coordinate ring of } V.$$

Definition 2.2. For any non-empty set V, define

$$\mathcal{F}(V,k) \quad \text{to be} \quad \text{the set of functions from } V \text{ to } k.$$

$\mathcal{F}(V,k)$ is made into a ring in the usual way as follows:

(i) For all $f,g \in \mathcal{F}(V,k)$ and $x \in V$, we have $(f+g)(x) = f(x)+g(x)$

(ii) For all $f,g \in \mathcal{F}(V,k)$, we have $(fg)(x) = f(x)g(x)$

Definition 2.3 (polynomial function)**.** If $V \subseteq \mathbb{A}^n$ is a variety, a function $f \in \mathcal{F}(V,k)$ is a polynomial function if there exists a polynomial $F \in k[X_1,\ldots,X_n]$ such that

$$f(a_1,\ldots,a_n) = F(a_1,\ldots,a_n) \quad \text{for all } (a_1,\ldots,a_n) \in V.$$

The polynomial functions form a subring of $\mathcal{F}(V,k)$ containing k.

Two polynomials functions F and G determine the same function if and only if

$$(F-G)(a_1,\ldots,a_n) = 0 \quad \text{for all } (a_1,\ldots,a_n) \in V \quad \text{or equivalently} \quad F-G \in I(V).$$

As such, we can identity $\Gamma(V)$ with the subring of $\mathcal{F}(V,k)$ consisting of all polynomial functions on V. We can view an element of $\Gamma(V)$ as a function on V or as an equivalence class of polynomials.

Example 2.1. Let $V \subseteq \mathbb{A}^2$ be the variety defined by the equation

$$V = \left\{(x,y) \in \mathbb{A}^2 : y^2 = x^3 - x\right\}.$$

Recall that this is the affine curve defined by the polynomial $f(x,y) = y^2 - x^3 + x$ in the polynomial ring $k[x,y]$ for some algebraically closed field k. The ideal $I(V) \subseteq k[x,y]$ is generated by the polynomial $f(x,y) = y^2 - x^3 + x$, so $I(V) = \left(y^2 - x^3 + x\right)$. Hence, the coordinate ring of V is

$$\Gamma(V) = k[x,y]/\left(y^2 - x^3 + x\right).$$

This ring, or integral domain to be more specific, consists of all polynomials in x and y, modulo the equivalence relation defined by $y^2 = x^3 - x$. For example, we can write y^3 in $\Gamma(V)$ can be simplified as

$$y^3 = y \cdot y^2 = y\left(x^3 - x\right) = x^3 y - xy.$$

Definition 2.4 (polynomial map). Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be varieties. A mapping

$$\varphi : V \to W \quad \text{is a polynomial map}$$

if there exist $T_1, \ldots, T_m \in k[X_1, \ldots, X_n]$ such that

$$\varphi(a_1, \ldots, a_n) = (T_1(a_1, \ldots, a_n), \ldots, T_m(a_1, \ldots, a_n)) \quad \text{for all } (a_1, \ldots, a_n) \in V.$$

Any mapping $\varphi : V \to W$ induces a homomorphism $\widetilde{\varphi} : \mathcal{F}(W,k) \to \mathcal{F}(V,k)$ by setting $\overline{\varphi}(f) = f \circ \varphi$. If φ is a polynomial map, then $\widetilde{\varphi}(\Gamma(W)) \subseteq \Gamma(V)$ so $\widetilde{\varphi}$ restricts to a homomorphism from $\Gamma(W)$ to $\Gamma(V)$. If $f \in \Gamma(W)$ is the $I(W)$-residue of a polynomial F, then $\widetilde{\varphi}(f) = f \circ \varphi$ is the $I(V)$-residue of the polynomial $F(T_1, \ldots, T_m)$. Also, we often write $T = (T_1, \ldots, T_m)$.

Proposition 2.1. Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^n$ be affine varieties. Then, there exists a natural one-to-one correspondence between

$$\text{the polynomial maps } \varphi : V \to W \quad \text{and} \quad \text{the homomorphism } \widetilde{\varphi} : \Gamma(W) \to \Gamma(V).$$

Any such φ is the restriction of a polynomial map from $\mathbb{A}^n$ to $\mathbb{A}^m$. So,

$$V \text{ and } W \text{ are isomorphic} \quad \text{if and only if} \quad \text{their coordinate rings are isomorphic.}$$

If $T = (T_1, \ldots, T_m)$ is a polynomial map from $\mathbb{A}^n$ to $\mathbb{A}^m$ and F is a polynomial in $k[X_1, \ldots, X_m]$, let $F^T = \widetilde{T}(F) = F(T_1, \ldots, T_m)$. For ideals I and algebraic sets V in $\mathbb{A}^m$, we let I^T denote the ideal in $k[X_1, \ldots, X_n]$ generated by $\{F^T : F \in I\}$ and V^T be the algebraic set $T^{-1}(V) = V(I^T)$, where $I = I(V)$. If V is the hypersurface of F, then V^T is the hypersurface of F^T.

Definition 2.5 (affine coordinate change). An affine change of coordinates on $\mathbb{A}^n$ is a polynomial map

$$T : \mathbb{A}^n \to \mathbb{A}^n \quad \text{such that} \quad \deg(T_i) = 1 \text{ and } T \text{ is bijective.}$$

If

$$T_i = \sum a_{ij} X_j + a_{i0} \quad \text{then} \quad T = T'' \circ T' \text{ for some linear map } T' \text{ and translation } T_i'' = X_i + a_{i0}.$$

Example 2.2 (affine coordinate change on $\mathbb{A}^2$). Let $T : \mathbb{A}^2 \to \mathbb{A}^2$ be defined by

$$T(X,Y) = (2X + 3Y + 1, -X + 4Y + 5).$$

One checks that the degree of each term in T_1 and T_2 is 1, so $\deg(T_1) = \deg(T_2) = 1$. The transformation matrix associated with the linear part of T is

$$\mathbf{A} = \begin{bmatrix} 2 & 3 \\ -1 & 4 \end{bmatrix} \quad \text{which is invertible.}$$

As such, T is bijective. The linear map and translation map are given by

$$T'(X,Y) = (2X + 3Y, -X + 4Y) \text{ and } T''(X,Y) = (X + 1, Y + 5) \quad \text{respectively.}$$

One checks that $T = T'' \circ T'$.

Proposition 2.2. The following properties hold:

(i) T is invertible if and only if T' is invertible

(ii) If T and U are affine change of coordinates on $\mathbb{A}^n$, then so are $T \circ U$ and T^{-1}; T is an isomorphism of the variety with itself

2.2. *Rational Functions and Local Rings*

Definition 2.6 (rational function). Let $V \subseteq \mathbb{A}^n$ be a non-empty variety and $\Gamma(V)$ be its coordinate ring. Since $\Gamma(V)$ is an integral domain, we can form its quotient field, known as the field of rational functions on V. It is denoted by $k(V)$. An element of $k(V)$ is a rational function on V.

If f is a rational function on V and $P \in V$, then f is defined at P if

$$\text{there exist } a, b \in \Gamma(V) \quad \text{such that} \quad f = \frac{a}{b} \text{ and } b(P) \neq 0.$$

Note that there may be many different ways to write f as the ratio of polynomial functions; f is defined at P if it s possible to find a denominator for f that does not vanish at P.

Example 2.3. Consider the variety

$$V = V(XW - YZ) \subseteq \mathbb{A}^4.$$

So, V consists of all points $(x, y, z, w) \in k^4$ such that the equation $xw - yz = 0$ holds. The coordinate ring of V is $\Gamma(V) = k[X, Y, Z, W] / (XW - YZ)$, which consists of equivalence classes of polynomials in $k[X, Y, Z, W]$ where two polynomials are considered equivalent if their different is a multiple of $XW - YZ$.

Consider the fractions X/Y and Z/W, which are viewed as rational functions in the field of fractions $k(V)$. Since $XW = YZ$, observe that

$$\frac{X}{Y} = \frac{Z}{W} \quad \text{since} \quad XW = YZ \text{ implies } XW/(YW) = YZ/(YW).$$

Of course, this is provided that $Y \neq 0$ and $W \neq 0$.

Definition 2.7 (local ring and pole set). Let $P \in V$. Define $\mathcal{O}_P(V)$ to be the set of rational functions f on V that are defined at P. This is called the local ring of V at P. The set of points $P \in V$ where f is not defined is called the poly set of f.

One checks that $\mathcal{O}_P(V)$ forms a subring of $k(V)$ containing $\Gamma(V)$ and that

$$k \subseteq \Gamma(V) \subseteq \mathcal{O}_P(V) \subseteq k(V).$$

Proposition 2.3. The following properties hold:

(i) The pole set of a rational function is an algebraic subset of V

(ii) $\Gamma(V) = \bigcap_{p \in V} \mathcal{O}_P(V)$

2.3. *Discrete Valuation Rings*

Definition 2.8 (discrete valuation ring)**.** Let R be an integral domain that is not a field. Then, any ring R satisfying either of the following conditions is said to be a discrete valuation ring (DVR):

(i) R is Noetherian and local, and the maximal ideal is principal

(ii) There is an irreducible element $t \in R$ such that every non-zero $z \in R$ may be written uniquely as

$$z = ut^n \quad \text{for some unit } u \in R \text{ and } n \in \mathbb{Z}_{\geq 0}.$$

We say that t is a uniformising parameter for R and any other uniformising parameter is of the form ut for some unit u in R.

Example 2.4. A classic example of a DVR is as follows:

$$R = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : p \text{ does not divide } b \right\} \quad \text{where} \quad p \text{ is prime.}$$

Here, $\mathbb{Z}_{(p)}$ is the localization of $\mathbb{Z}$ at the prime ideal (p). Note that R is Noetherian and local with the unique maximal ideal

$$\mathfrak{m} = \left\{ \frac{a}{b} \in \mathbb{Z}_{(p)} : p \mid a \right\}.$$

This maximal ideal is principal, so R is indeed a DVR by **(i)** of Definition 2.8. We can also view this example from **(ii)** of Definition 2.8. Note that the prime p is an irreducible element of $\mathbb{Z}_{(p)}$. Every non-zero $z \in \mathbb{Z}_{(p)}$ can be uniquely written as

$$z = up^n \quad \text{for some unit in } \mathbb{Z}_{(p)} \text{ and } n \in \mathbb{Z}_{\geq 0}.$$

Definition 2.9. Let K be the quotient field of a DVR R. Then, any non-zero element $z \in K$ has a unique expression $z = ut^n$, where u is a unit in R and $n \in \mathbb{Z}$. We say that n is the order of z and it can be written as $n = \operatorname{ord}(z)$; we define $\operatorname{ord}(0) = \infty$.

2.4. *Forms*

Definition 2.10. We define a form to be a homogeneous polynomial where all terms have the same total degree.

Example 2.5. For example, for the polynomial

$$F(X,Y,Z) = 3X^2Y + 5Y^2Z + 7XZ^2,$$

the total degree of each term is 3. Since all terms have the same degree, then F is a form of degree 3.

Let R be an integral domain. Now, we wish to connect a general polynomial in $R[X_1,\ldots,X_n]$ to a form in $R[X_1,\ldots,X_n,X_{n+1}]$. Suppose F is a form of degree d in $R[X_1,\ldots,X_n,X_{n+1}]$. By definition, all terms of F have total degree d. The map $F \mapsto F_*$ removes X_{n+1} by setting $X_{n+1} = 1$. FOrmally,

$$F_* = F(X_1,\ldots,X_n,1).$$

F_* is now a polynomial in $R[X_1,\ldots,X_n]$ which is no longer homogeneous as substituting $X_{n+1} = 1$ mixes terms of different degrees. For example, if $F = X_1^2X_{n+1} + X_2X_{n+1}^2$ which is a form of degree 3 in $R[X_1,X_2,X_{n+1}]$, then

$$F_* = X_1^2 \cdot 1 + X_2 \cdot 1^2 = X_1^2 + X_2.$$

This process is known as dehomogenization.

Conversely, we can consider the map f^* (known as homogenization) which transforms a general polynomial into a form. Say f is a polynomial in $R[X_1,\ldots,X_n]$ with terms of varying degrees. Write f as $f = f_0 + f_1 + \ldots + f_d$, where f_i is the homogeneous part of degree i. The map $f \mapsto f^*$ lifts f to a homogeneous polynomial in $R[X_1,\ldots,X_n,X_{n+1}]$ by introducing a new variable X_{n+1}, so

$$f^* = X_{n+1}^d f_0 + X_{n+1}^{d-1} f_1 + \ldots + f_d \quad \text{which ensures } f^* \text{ is homogeneous of degree } d.$$

Alternatively, f^* can be written compactly as

$$f^* = X_{n+1}^d f\left(\frac{X_1}{X_{n+1}},\ldots,\frac{X_n}{X_{n+1}}\right).$$

Here, the substitution $X_i \to X_i/X_{n+1}$ homogenizes f, and multiplying by X_{n+1}^d ensures that all terms have degree d. For example, if $f = X_1^2 + X_2$, then

$$f^* = X_{n+1}^2 \cdot X_1^2 + X_{n+1}^1 \cdot X_2 = X_1^2 X_{n+1} + X_2 X_{n+1}^2.$$

Example 2.6 (Fulton p. 24 Question 33). Factor $Y^3 - 2XY^2 + 2X^2Y + X^3$ into linear factors in $\mathbb{C}[X,Y]$.

Solution. One checks that $F(X,Y)$ is a form of degree 3. Assume that $F(X,Y) = 0$. Suppose there exist $a,b,c \in \mathbb{C}$ such that

$$X^3 + 2X^2Y - 2XY^2 + Y^3 = (X - aY)(X - bY)(X - cY).$$

Upon expanding the RHS and comparing the coefficients, we have

$$a + b + c = 2 \quad ab + ac + bc = -2 \quad abc = -1.$$

By Vieta's formula, these are the roots of the polynomial $x^3 - 2x^2 + 2x - 1 = 0$. As such, we have the desired factorisation into linear factors. □

Proposition 2.4. The following properties hold:

(i) $(FG)_* = F_* G_*$ and $(fg)^* = f^* g^*$

(ii) If $F \neq 0$ and r is the highest power of X_{n+1} that divides f, then

$$X_{n+1}^r (F_*)^* = F \quad \text{and} \quad (f^*)_* = f$$

(iii) Let $r = \deg g$, $s = \deg f$, and $t = r + s - \deg(f+g)$. Then,

$$(F+G)_* = F_* + G_* \quad \text{and} \quad X_{n+1}^t (f+g)^* = X_{n+1}^r f^* + X_{n+1}^s g^*$$

3. Local Properties of Plane Curves

3.1. *Multiple Points and Tangent Lines*

Recall that affine plane curves correspond to non-constant polynomials $F \in k[X,Y]$ without multiple factors, where F is determined up to multiplication by a non-zero constant. There are times it is useful to allow F to have multiple factors, so we modify our definition slightly.

Definition 3.1 (equivalent polynomials). Two polynomials $F, G \in k[X,Y]$ are equivalent if

$$\text{there exists a non-zero } \lambda \in k \quad \text{such that} \quad F = \lambda G.$$

We define an affine plane curve to be an equivalence class of non-constant polynomials under this equivalence relation.

Definition 3.2. The degree of a curve is the degree of a defining polynomial for the curve.

Example 3.1. A curve of degree one is a line, so we speak of the line $aX + bY + c = 0$ or the line given by the equation $aX + bY + c = 0$.

Definition 3.3. If

$$F = \prod F_i^{e_i} \quad \text{where} \quad \text{the } F_i \text{ are the irreducible factors of } F,$$

we say that the F_i's are the components of F and the e_i's are the multiplicity of the component F_i. F_i is a simple component if $e_i = 1$, and multiple otherwise.

Definition 3.4. Let F be a curve and $P = (a,b) \in F$. The point P is a simple point of F if either derivative $F_X(P) \neq 0$ or $F_Y(P) \neq 0$. In this case, the line

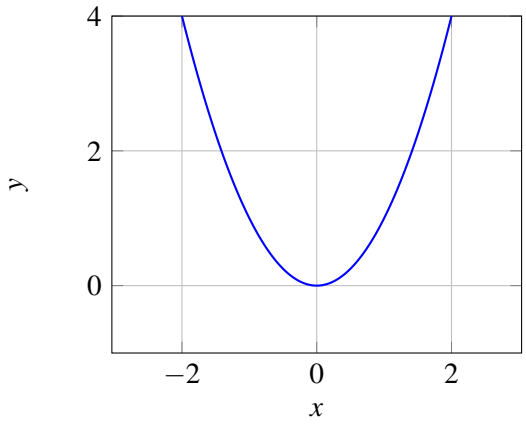
$$F_X(P)(X-a) + F_Y(P)(Y-b) = 0 \quad \text{is the tangent line to } F \text{ at } P.$$

A point that is not simple is said to be multiple. A curve with only simple points is a non-singular curve.

Example 3.2. Consider the following graph. It is given by the expression $Y - X^2$. Note that $F_X(X,Y) = -2X$ and $F_Y(X,Y) = 1$. Since F_Y never vanishes, the curve $F(X,Y)$ does not have any multiple points. Equivalently, all points are simple. As such, the line

$$-2a(X-a) + (Y-b) = 0 \quad \text{is the tangent line to } F \text{ at } P = (a,b).$$

We can rewrite this as $Y = 2aX - a^2$. Moreover, the curve is non-singular.



Example 3.3.

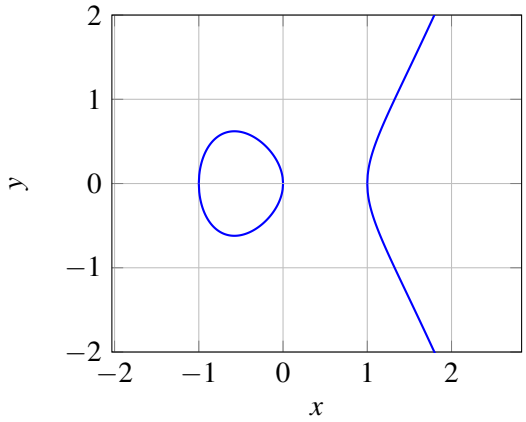
Example 3.4. Consider the following graph which is an example of an elliptic curve. It is given by the expression $Y^2 - X^3 + X$. We have

$$F_X(X,Y) = -3X^2 + 1 \quad \text{and} \quad F_Y(X,Y) = 2Y.$$

Suppose $F_X = 0$. Then, $X = \pm 1/\sqrt{3}$. Note that $X = 1/\sqrt{3}$ lies outside the domain, so we consider $X = -1/\sqrt{3}$. However, $\left(-1/\sqrt{3}, 0\right)$ does not lie on the elliptic curve. It follows that the curve is non-singular.

Also, the equation of the tangent line is

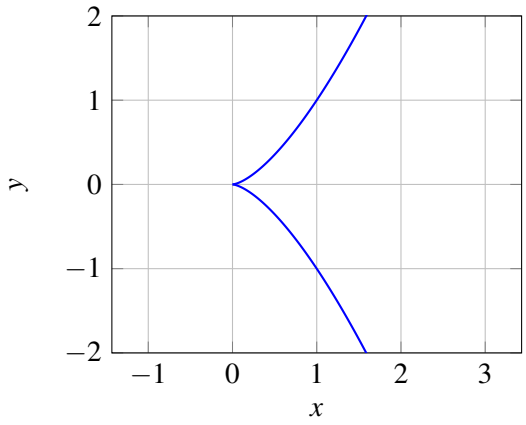
$$\left(-3a^2 + 1\right)(X - a) + 2b(Y - b) = 0 \quad \text{or equivalently} \quad Y = \frac{\left(3a^2 - 1\right)(X - a)}{2b} + b.$$



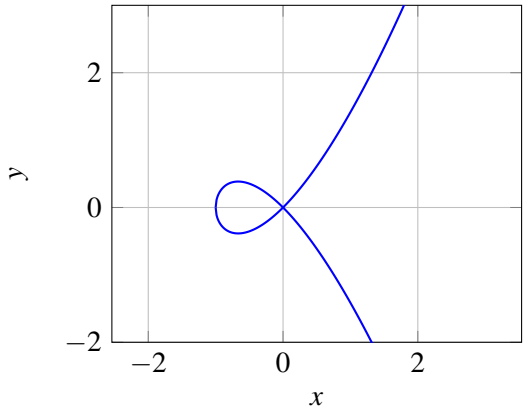
Example 3.5. Consider the following graph. It is given by the expression $Y^2 - X^3$. One checks that

$$F_X(X,Y) = -3X^2 \quad \text{and} \quad F_Y(X,Y) = 2Y.$$

Clearly, $P = (0,0)$ is the only multiple point on this curve.



Example 3.6. Consider the graph of the following curve (not an elliptic curve since the X^2 term is present). It is given by the expression $Y^2 - X^3 - X^2$. Again, one checks that $P = (0,0)$ is the only multiple point on the curve as $F_X(X,Y) = -3X^2 - 2X$ and $F_Y(X,Y) = 2Y$.



Consider the following graph known as a rose with three petals. It is given by the expression

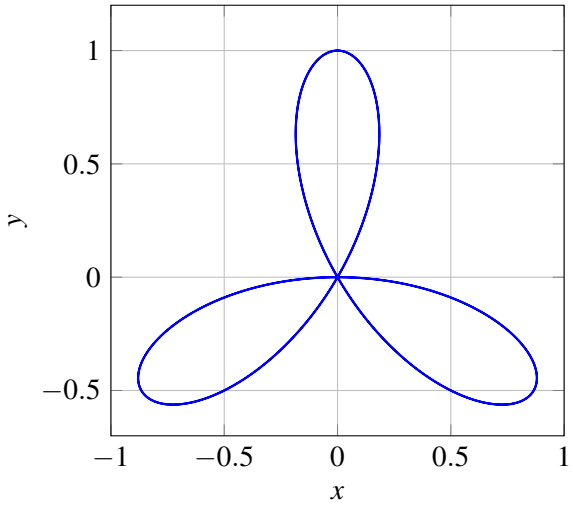
$$\left(X^2+Y^2\right)^2 + 3X^2Y - Y^3.$$

We see that $P = (0,0)$ is the only multiple point on the curve. To see why, we have

$$\begin{aligned} F_X(X,Y) &= 8X\left(X^2+Y^2\right) + 6XY \\ F_Y(X,Y) &= 8Y\left(X^2+Y^2\right) + 3\left(X^2-Y^2\right) \end{aligned}$$

At $P = (0,0)$, one checks that $F_X(0,0) = F_Y(0,0)$ so $(0,0)$ is a multiple point. Note that for any other point $P = (X,Y)$, the partial derivatives cannot vanish simultaneously, i.e. no other point on the curve satisfies both

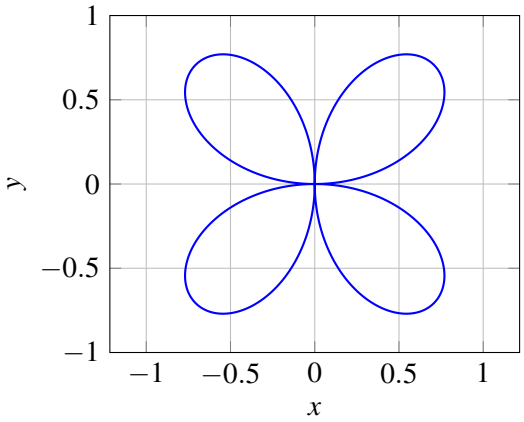
$F_X(X,Y) = 0$ and $F_Y(X,Y) = 0$.



Example 3.7. Lastly, consider the graph of the following rose with four loops given by the expression

$$F(X,Y) = \left(X^2+Y^2\right)^3 - 4X^2Y^2.$$

By considering F_X and F_Y, one can deduce that $P = (0,0)$ is the only multiple point on the curve.



Definition 3.5 (multiplicity). Let F be any curve and $P = (0,0)$. Write

$$F = F_m + F_{m+1} + \ldots + F_n \quad \text{where } F_i \text{ is a form in } k[X,Y] \text{ of degree } i \text{ and } F_m \neq 0.$$

Define m to be the multiplicity of F at $P = (0,0)$, and write $m = m_P(F)$.

Note that $m_P(F) > 0$. Using the rules for derivatives, one can check that

$$P \text{ is a simple point on } F \quad \text{if and only if} \quad m_P(F) = 1.$$

In this case, F_1 is the tangent line to F at P. If $m = 2$, P is a double point; if $m = 3$, P is a triple point and so on.

Since F_m is a form in two variables, we can write

$$F_m = \prod L_i^{r_i} \quad \text{where} \quad \text{the } L_i\text{'s are distinct lines.}$$

Definition 3.6 (tangents and ordinary points)**.** The L_i's are called the tangent lines to F at $P=(0,0)$ and r_i is the multiplicity of the tangent. The line L_i is a simple tangent if $r_i=1$. A double tangent is defined similarly.

If F has m distinct tangents at P, we say that P is an ordinary multiple point of F. An ordinary double point is called a node. We call a line through P a tangent of multiplicity zero if it is not tangent to F at P.

Let

$$F=\prod F_i^{e_i} \quad \text{be} \quad \text{the factorisation of } F \text{ into irreducible components.}$$

Then,

$$m_p(F)=\sum e_i m_P(F_i).$$

Also, if L is a tangent line to F_i with multiplicty r_i, then

$$L \text{ is tangent to } F \quad \text{with} \quad \text{multiplicity } \sum e_i r_i.$$

In particular, a point P is a simple point of F if and only if P belongs to just one component F_i of F, F_i is a simple component of F, and P is a simple point of F_i.

Example 3.8 (simple point)**.** Consider the curve $F(X,Y)=Y-X$, which is a straight line passing through the origin $P=(0,0)$. Note that the degree of F is 1, so $F_1=Y-X$ and $m_P(F)=1$. Since $m_P(F)=1$, the origin is a simple point, and the tangent to F at P is the line $L: Y-X=0$, which coincides with the curve itself.

Example 3.9 (ordinary double point)**.** Consider the curve $F(X,Y)=Y^2-X^2$, which represents two intersecting lines. We write F as

$$F(X,Y)=(Y-X)(X+Y),$$

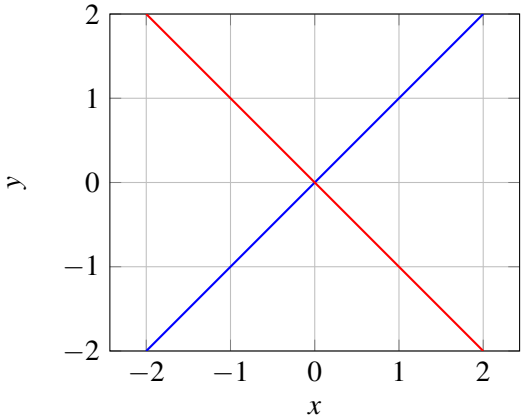
for which the lowest degree term is $F_2=(Y-X)(Y+X)$, so $m_P(F)=2$. At $P=(0,0)$, the tangents are

$$L_1: Y-X=0 \quad \text{and} \quad L_2: Y+X=0.$$

These are simple tangent as $r_1=r_2=1$. Since there are two distinct tangents at P, we say that P is an ordinary double point, also known as a node.

Example 3.10 (cusp)**.** Consider the curve $F(X,Y)=Y^2-X^3$, which describes a cusp. The term of lowest degree is $F_2=Y^2$, so $m_P(F)=2$. The tangents at $P=(0,0)$ are determined by $F_2=Y^2$, which is $L_1: Y=0$ with multiplicity $r_1=2$. There is only one tangent, which is a double tangent as $r_1=2$. To conclude, P is not an ordinary multiple point. Instead, it is a cusp.

Example 3.11 (tacnode)**.** Consider the curve $F(X,Y)=Y^4-X^4$, which describes a *tacnode*. Consider the following graph:



We can write F as

$$F(X,Y) = (Y-X)^2 (Y+X)^2.$$

The lowest-degree term is $F_4 = (Y-X)^2 (Y+X)^2$, so $m_P(F) = 4$. The tangents at $P = (0,0)$ are

$$L_1 : Y - X = 0 \quad \text{and} \quad L_2 : Y + X = 0$$

with multiplicities $r_1 = 2$ and $r_2 = 2$ respectively. Since each tangent has a multiplicity greater than 1, then P is not an ordinary multiple point. Instead, in Algebraic Geometry, we call it a *tacnode*.

In fact, we can extend the aforementioned definitions to an arbitrary point $P = (a,b) \neq (0,0)$. Define T to be the translation that takes $(0,0)$ to P. So, $T(x,y) = (x+a, y+b)$. Then, $F^T = F(X+a, Y+b)$. Define $m_P(F)$ to be $m_{(0,0)}\left(F^T\right)$, i.e. write $F^T = G_m + G_{m+1} + \ldots + G_i$, where $G_m \neq 0$, and let $m = m_p(F)$. If

$$G_m = \prod L_i^{r_i} \quad \text{with} \quad L_i = \alpha_i X + \beta_i Y,$$

the lines $\alpha_i (X-a) + \beta_i (Y-b)$ are defined to be the tangent lines to F at P, and r_i is the multiplicity of the tangent. Note that T takes the points of F^T to F, and the tangents to F^T at $(0,0)$ to the tangents to F at P. Since $F_X(P) = F_X^T(0,0)$ and $F_Y(P) = F_Y^T(0,0)$, we say that P is a simple point on F if and only if $m_P(F) = 1$.

3.2. *Multiplicites and Local Rings*

Let F be an irreducible plane curve and $P \in F$. Recall that this means that the set of all (x,y) such that $f(x,y) = 0$ cannot be expressed as the union of two proper subvarieties. Now, we will find the multiplicity of P on F in terms of the local ring $\mathcal{O}_P(F)$.

Definition 3.7. For any polynomial $G \in k[X,Y]$,

$$\text{denote its image in } \Gamma(F) = k[X,Y]/(F) \quad \text{by} \quad g.$$

Theorem 3.1. *P is a simple point of F if and only if $\mathcal{O}_P(F)$ is a DRV. In this case, if $L = aX + bY = c$ is any line through P that is not tangent to F at P, then the image l of L in $\mathcal{O}_P(F)$ is a uniformizing parameter for $\mathcal{O}_P(F)$.*

Example 3.12. Let $\mathbb{C}$ be our base field and consider the irreducible plane curve $f(X,Y) = Y^2 - X^3 - X^2$. Let $P = (0,0)$, which lies on F. Clearly, P is a simple point by computing the partial derivatives F_X and F_Y (or by Example 3.6).

The local ring $\mathcal{O}_P(F)$ consists of functions defined on F near P, modulo the ideal generated by f. Explicitly, we have

$$\mathcal{O}_P(F) = \mathbb{C}[X,Y]/\left(Y^2 - X^3 - X^2\right).$$

This is a DVR. Consider the line L through $P = (0,0)$ given by $L : Y - X = 0$. Substituting $Y = X$ into $f(X,Y)$, we obtain $f(X,X) = X^2(X-1) = 0$. Thus, L intersects F at P and another point $(1,1)$. Since L is not tangent to F at P, the image of L, denoted by l, is a uniformizing parameter in $\mathcal{O}_P(F)$.

Suppose P is a simple point on an irreducible curve F. Let

$$\text{ord}_P^F \quad \text{be} \quad \text{the order function on } k(F) \text{ defined by the DVR } \mathcal{O}_P(F).$$

When F is fixed, we may simply write ord_P. Also, if $G \in k[X,Y]$ and g is the image of G in $\Gamma(F)$, we write $\text{ord}_P^F(G)$ instead of $\text{ord}_P^F(g)$.

Next, again suppose P is a simple point on F and L is a line through P. Then,

$$\operatorname{ord}_P^F(L)\begin{cases}=1 & \text{if } L \text{ is not tangent to } F \text{ at } P;\\ >1 & \text{if } L \text{ is tangent to } F \text{ at } P.\end{cases}$$

Theorem 3.2. Let P be a point on an irreducible curve F. Then, for sufficiently large n, we have

$$m_P(F)=\dim_k\left(\mathfrak{m}_P(F)^n/\mathfrak{m}_P(F)^{n+1}\right).$$

In particular, the multiplicity of F at P depends only on the local ring $\mathcal{O}_P(F)$.

3.3. *Intersection Numbers*

Let F and G be plane curves and $P\in\mathbb{A}^2$. We now wish to define the intersection number of F and G at P for which it will be denoted by $I(P,F\cap G)$.

Definition 3.8 (proper intersection)**.** For plane curves F and G and $P\in\mathbb{A}^2$, we say that F and G intersect properly at P if F and G have no common component that passes through P.

(1) For any F, G and P such that F and G intersect properly at P, we have $I(P,F\cap G)\in\mathbb{Z}_{\geq 0}$. Also, $I(P,F\cap G)=\infty$ if F and G do not intersect properly at P.

(2) $I(P,F\cap G)=0$ if and only if $P\notin F\cap G$. $I(P,F\cap G)$ depends only on the components of F and G that pass through P. Also, if F or G is a non-zero constant, then $I(P,F\cap G)=0$.

(3) If T is affine change of coordinates on $\mathbb{A}^2$ and $T(Q)=P$, then

$$I(P,F\cap G)=I\left(Q,F^T\cap G^T\right).$$

(4) $I(P,F\cap G)=I(P,G\cap F)$

We say that two curves F and G intersect transversally at P if P is a simple point both on F and G, and if the tangent line to F at P is different from the tangent line to G at P. We need the intersection number to be one when F and G meet transversally at P. More generally, we require the following:

(5) $I(P,F\cap G)\geq m_P(F)\,m_P(G)$, with equality occurring if and only if F and G have no tangent lines in common at P.

(6) The intersection numbers should add when we take unions of curves. That is, if

$$F=\prod F_i^{r_i} \text{ and } G=\prod G_j^{s_j} \quad \text{then} \quad I(P,F\cap G)=\sum_{i,j} r_i s_j I(P,F_i\cap G_j).$$

(7) If F is irreducible, then

$$\text{for any } A\in k[X,Y] \quad \text{we have} \quad I(P,F\cap G)=I(P,F\cap(G+AF)).$$

We have two more useful properties.

(8) If P is a simple point on F, then $I(P,F\cap G)=\operatorname{ord}_P^F(G)$

(9) If F and G have no common components, then

$$\sum_P I(P,F\cap G)=\dim_k\left(k[X,Y]/(F,G)\right).$$

Theorem 3.3. There is a unique intersection number $I(P, F \cap G)$ defined for all plane curves F and G and all points $P \in \mathbb{A}^2$ satisfying the properties in Definition 3.8. It is given by the formula

$$I(P, F \cap G) = \dim_k \left(\mathcal{O}_P \left(\mathbb{A}^2 \right) / (F, G) \right).$$

Example 3.13. We attempt to calculate $I(P, E \cap F)$, where

$$E = \left(X^2 + Y^2\right)^2 + 3X^2Y - Y^3 \quad \text{is the rose with three loops} \quad \text{and}$$
$$F = \left(X^2 + Y^2\right)^3 - 4X^2Y^2 \quad \text{is the rose with four loops.}$$

Let $P = (0,0)$. We replace F with $F - \left(X^2 + Y^2\right) E$ to simplify the computation. The idea is to eliminate higher-order terms of F that are divisible by E as they do not affect the intersection number at P. After substitution, we have

$$F - \left(X^2 + Y^2\right) E = Y \left(\left(X^2 + Y^2\right) \left(Y^2 - 3X^2\right) - 4X^2Y \right) = YG.$$

Here,

$$G = \left(X^2 + Y^2\right) \left(Y^2 - 3X^2\right) - 4X^2Y.$$

Now, the intersection number $I(P, E \cap F)$ reduces to $I(P, E \cap (YG))$. Since G is still complicated and involves X^2 terms, we apply a substitution $G \to G + 3E$, which simplifies G. After substituting, we obtain

$$G + 3E = Y \left(5X^2 - 3Y^2 + 4Y^3 + 4X^2Y\right) = YH \quad \text{where} \quad H = 5X^2 - 3Y^2 + 4Y^3 + 4X^2Y.$$

We note that

$$I(P, E \cap (YG)) = I(P, E \cap Y) + I(P, E \cap G)$$

and

$$I(P, E \cap F) = I(P, E \cap Y) + I(P, E \cap G).$$

One sees by directly substituting $Y = 0$ into E that $I(P, E \cap Y) = I\left(P, X^4 \cap Y\right) = 4$. Geometrically, what this means is the line $Y = 0$ meets the local branch of E with multiplicity 4 at the origin. Hence,

$$I(P, E \cap F) = 4 + I(P, E \cap G).$$

Recall that $G + 3E = YH$. Hence,

$$I(P, E \cap G) = I(P, E \cap (YH)) = I(P, E \cap Y) + I(P, E \cap H).$$

Since $I(P, E \cap Y) = 4$, then

$$I(P, E \cap G) = 4 + I(P, E \cap H).$$

Hence,

$$I(P, E \cap F) = 8 + I(P, E \cap H).$$

Recall **(5)** of Definition 3.8 which states that

$$I(P, F \cap G) \geq m_P(F)\, m_P(G)$$

and equality holds if and only if F and G have no tangent line in common at P. Note that at $(0,0)$, the curves $E=0$ and $H=0$ do not share a tagnent line so equality holds. That is to say,

$$I(P,E\cap H)=m_P(E)\,m_P(H).$$

At this juncture, recall that the multiplicity $m_P(F)$ of a curve F at a point $P=(0,0)$ is the smallest degree of the non-zero homogeneous terms in the polynomial $H(X,Y)$. By expanding E and H into their homogeneous parts, we have

$$E(X,Y)=X^4+2X^2Y^2+Y^4+3X^2Y-Y^3 \quad \text{and} \quad F=5X^2-3Y^2+4Y^3+4X^2Y,$$

for which we infer that $m_P(E)=3$ and $m_P(H)=2$, so $I(P,E\cap H)=3\cdot 2=6$. We conclude that $I(P,E\cap F)=14$.

4. Projective Varieties

4.1. *Projective Space*

Suppose we wish to study all the points of intersection of two curves, say for instance $Y^2 = X^2 + 1$ and the line $Y = \alpha X$, where $\alpha \in k$. If $\alpha \neq \pm 1$, they intersect at two points. If $\alpha = \pm 1$, they do not intersect, but the curve is asymptotic to the line. We wish to enlarge the plane in such a way that two such curves intersect at infinity.

One common way to achieve this is as follows: for each point $(x,y) \in \mathbb{A}^2$, identify it with the point $(x,y,1) \in \mathbb{A}^3$. Every point $(x,y,1)$ determines a line in $\mathbb{A}^3$ that passes through $(0,0,0)$ and $(x,y,1)$. Also, every line through $(0,0,0)$ except those lying in the plane $z = 0$ corresponds to exactly one such point. The lines through $(0,0,0)$ in the plane $z = 0$ can be thought of as corresponding to the *points at infinity*. As such, we have the following definition of the projective n-space (Definition 4.1).

The big picture here is that Projective Geometry extends the usual affine geometry by adding *points at infinity* or *lines at infinity* to make parallel lines meet.

Definition 4.1 (projective space). Let k be an arbitrary field. The projective n-space over k, denoted by $\mathbb{P}^n(k)$ or just $\mathbb{P}^n$, is defined to be

$$\text{the set of all lines through } (0,\ldots,0) \text{ in } \mathbb{A}^{n+1}(k).$$

Any point $(x) = (x_1,\ldots,x_{n+1}) \neq (0,\ldots,0)$ determines a unique such line, which is $\{(\lambda x_1,\ldots,\lambda x_{n+1}) : \lambda \in k\}$. Two such points (x) and (y) determine the same line if and only if there exists a non-zero $\lambda \in k$ such that $y_i = \lambda x_i$ for all $1 \leq i \leq n+1$. In this case, (x) and (y) are equivalent — $\mathbb{P}^n$ may be identified with the set of equivalence class of points in $\mathbb{A}^{n+1} \setminus \{(0,\ldots,0)\}$.

The elements of $\mathbb{P}^n$ will be called points. If a point $P \in \mathbb{P}^n$ is determined as above by some $(x_1,\ldots,x_{n+1}) \in \mathbb{A}^{n+1}$, we say that $(x_1,\ldots,x_{n+1})$ are homogeneous coordinates for P. We often write $[x_1 : \ldots : x_{n+1}]$ to indicate that $(x_1,\ldots,x_{n+1})$ are homogeneous coordinates for P.

Let

$$U_i = \{[x_1 : \ldots x_{n+1}] \in \mathbb{P}^n : x_i \neq 0\}.$$

Then, each $P \in U_i$ can be written uniquely in the form

$$P = [x_1 : \ldots x_{i-1} : 1 : x_{i+1} : \ldots : x_{n+1}].$$

The coordinates $(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_{n+1})$ are the non-homogeneous coordinates for P with respect to U_i. If we define

$$\varphi_i : \mathbb{A}^n \to U_i \quad \text{via} \quad \varphi_i(a_1,\ldots,a_n) = [a_1 : \ldots : a_{n-1} : 1 : a_i : \ldots : a_n],$$

then there is a bijective correspondence between the points of $\mathbb{A}^n$ and the points of U_i. Note that

$$\mathbb{P}^n = \bigcup_{i=1}^{n+1} U_i \quad \text{so} \quad \mathbb{P}^n \text{ is covered by } n+1 \text{ sets, each of which looks just like the affine } n\text{-space.}$$

We will usually concentrate on U_{n+1}.

Definition 4.2 (hyperplane at infinity). Define the hyperplane at infinity, H_∞, as follows:

$$H_\infty = \mathbb{P}^n \setminus U_{n+1} = \{[x_1 : \ldots : x_{n+1}] : x_{n+1} = 0\}$$

So, H_∞ may be identified with $\mathbb{P}^{n-1}$. As such, we infer that

$$\mathbb{P}^n = U_{n+1} \cup H_\infty$$

is the union of an affine n-space and a set that gives all directions in an affine n-space.

Example 4.1. $\mathbb{P}^0(k)$ is obviously a point.

Example 4.2. We define

$$\mathbb{P}^1(k) = \{[x:1] : x \in k\} \cup \{[1:0]\} \quad \text{or} \quad \text{the projective line over } k$$

to be the affine line plus one point at infinity

Example 4.3. We define

$$\mathbb{P}^2(k) = \left\{[x:y:1] : (x,y) \in \mathbb{A}^2\right\} \cup \left\{[x:y:0] : [x:y] \in \mathbb{P}^1\right\}$$

to be the projective plane over k. It is the usual affine plane $\mathbb{A}^2(k)$ extended by adding a line at infinity, for which the line is denoted by H_∞. By adding a single *point at infinity* for each direction in the plane, this makes lines in Projective Geometry extend indefinitely and intersect at infinity.

Example 4.4. Consider a line $Y = mX + b$ in $\mathbb{A}^2$. A line in the affine plane can be written in projective coordinates as $[x:y:z]$, where $y = mx + bz$ and $z \neq 0$. In Projective Geometry, we make equations *homogeneous* so they are invariant under equivalence classes. The affine line $Y = mX + b$ becomes the projective set

$$\left\{[x:y:z] \in \mathbb{P}^2 : y = mx + bz\right\}.$$

When $z = 0$, the equation reduces to a single point $[1:m:0]$. All lines with the same slope m intersect the same point on the line at infinity.

Example 4.5. Consider the curve $Y^2 = X^2 + 1$ in $\mathbb{A}^2$. In Projective Geometry, the equation becomes $Y^2 = X^2 + Z^2$, which describes a curve in the projective plane $\mathbb{P}^2(k)$. The affine part of the curve is $[x:y:z] \in \mathbb{P}^2$, where $z \neq 0$.

At the line at infinity, we have $z = 0$, so the equation reduces to $Y^2 = X^2$. This yields two points

$$[1:1:0] \text{ and } [1:-1:0] \quad \text{which are the points where the curve intersects } H_\infty.$$

In $\mathbb{A}^2$, these points correspond to where the lines $Y = X$ and $Y = -X$ intersect the curve.

4.2. *Projective Algebraic Sets*

In this section, we develop the idea of algebraic sets in Projective Geometry, i.e. $\mathbb{P}^n = \mathbb{P}^n(k)$. The concepts are entirely similar to those for affine algebraic sets. To start off, a point $P \in \mathbb{P}^n$ is a zero of a polynomial $F \in k[X_1, \ldots, X_{n+1}]$ if

$$F(x_1, \ldots, x_{n+1}) = 0$$

for every choice of homogeneous coordinates $(x_1, \ldots, x_{n+1})$ for P. We then write $F(P) = 0$. If F is a form and F vanishes at one representative of P, then it vanishes at every representative.

Definition 4.3 (projective algebraic set). For any set S of polynomials in $k[X_1,\ldots,X_{n+1}]$, let

$$V(S) = \{P \in \mathbb{P}^n : P \text{ is a zero of each } F \in S\}.$$

Such a set is an algebraic set in $\mathbb{P}^n$.

For any set $X \subseteq \mathbb{P}^n$, let

$$I(X) = \{F \in k[X_1,\ldots,X_{n+1}] : \text{every } P \in x \text{ is a zero of } F\}$$

denote the ideal of X. An ideal $I \subseteq k[X_1,\ldots,X_{n+1}]$ is said to be homogeneous if for every

$$F = \sum_{i=0}^{m} F_i \in I \quad \text{where} \quad F_i \text{ is a form of degree } i \quad \text{we also have } F_i \in I.$$

Proposition 4.1. An ideal $I \subseteq k[X_1,\ldots,X_{n+1}]$ is homogeneous if and only if it is generated by a finite set of forms.

Definition 4.4 (projective variety). An algebraic set $V \subseteq \mathbb{P}^n$ is irreducible if it cannot be written as the union of two smaller algebraic sets. If this is satisfied, we say that V is a projective variety.

At this juncture, to avoid confusion, we will write V_p and I_p for the projective operations and V_a and I_a for the affine ones. If V is an algebraic set in $\mathbb{P}^n$, we define

$$C(V) = \left\{(x_1,\ldots,x_{n+1}) \in \mathbb{A}^{n+1} : [x_1 : \ldots : x_{n+1}] \in V \quad \text{or} \quad (x_1,\ldots,x_{n+1}) = (0,\ldots,0)\right\}$$

to be the cone over V. If $V \neq \emptyset$, then $I_a(C(V)) = I_p(V)$. Also, if I is a homogeneous ideal in $k[X_1,\ldots,X_{n+1}]$ such that $V_p(I) \neq \emptyset$, then $C(V_p(I)) = V_a(I)$. This reduces many questions about $\mathbb{P}^n$ to questions about $\mathbb{A}^{n+1}$.

Theorem 4.1 (Projective Nullstellensatz). Let I be a homogeneous ideal in $k[X_1,\ldots,X_{n+1}]$. Then, the following hold:

(i) $V_p(I) = \emptyset$ if and only if there exists $N \in \mathbb{Z}$ such that I contains all forms of degree $\geq N$

(ii) If $V_p(I) \neq \emptyset$, then $I_p(V_p(I)) = \mathrm{Rad}(I)$

Proposition 4.2. Every element $f \in \Gamma$ may be written uniquely as

$$f = f_0 + \ldots + f_m \quad \text{where} \quad f_i \text{ is a form of degree } i.$$

Let $k_h(V)$ be the quotient field of $\Gamma_h(V)$. We call this the homogeneous function field of V. In contrast with the case of affine varieties, no elements of $\Gamma_h(V)$, except the constants, determine functions on V. Likewise, most elements of $k_h(V)$ cannot be regarded as functions. However, if f and g are both forms in $\Gamma_h(V)$ of the same degree d and g is non-zero, then f/g does define a function. In fact,

$$\frac{f(\lambda x)}{g(\lambda x)} = \frac{\lambda^d f(x)}{\lambda^d g(X)} = \frac{f(x)}{g(x)},$$

so the value of f/g is independent of the choice of homogeneous coordinates.

The function field of V, denoted by $k(V)$, is deifned to be

$$\{z \in k_h(V) : z = f/g \text{ for some forms } f,g \in \Gamma_h(V) \text{ of the same degree}\}.$$

One can check that $k(V)$ is indeed a subfield of $k_h(V)$. Also, $k \subseteq k(V) \subseteq k_h(V)$. Elements of $k(V)$ are called rational functions on V.

We then consider $\mathbb{A}^n \subseteq \mathbb{P}^n$ by means of the map $\varphi_{n+1} : \mathbb{A}^n \to U_{n+1} \subseteq \mathbb{P}^n$. Here, we study the relations between the algebraic sets in $\mathbb{A}^n$ and those in $\mathbb{P}^n$. Let V be an algebraic set in $\mathbb{A}^n$ and $I = I(V) \subseteq k[X_1, \ldots, X_n]$ be an ideal. Let I^* be the ideal in $k[X_1, \ldots, X_{n+1}]$ generated by $\{F^* : F \in I\}$. This I^* is a homogeneous ideal; we define V^* to be $V(I^*) \subseteq \mathbb{P}^n$. Conversely, let V be an algebraic set in $\mathbb{P}^n$, and $I = I(V) \subseteq k[X_1, \ldots, X_n]$. Let I_n be the ideal in $k[X_1, \ldots, X_n]$ generated by $\{F_* : F \in I\}$. Define V_* to be $V(I_*) \subseteq \mathbb{A}^n$.

4.3. *Multiprojective Space*

We wish to make the Cartesian products of two varieties into a variety. Since $\mathbb{A}^n \times \mathbb{A}^m$ may be identified with $\mathbb{A}^{n+m}$, this is not difficult for affine varieties. However, the product $\mathbb{P}^n \times \mathbb{P}^m$ requires some discussion.

Write $k[X,Y]$ for $k[X_1, \ldots, X_{n+1}, Y_1, \ldots, Y_{m+1}]$. A polynomial $F \in k[X,Y]$ is called a biform of bidegree (p,q) if F is a form of degree p when considered as a polynomial in $X_1, \ldots, X_{n+1}$ (make a similar claim for the Y_j's) with coefficients in $k[Y_1, \ldots, Y_{m+1}]$. Every $F \in k[X,Y]$ may be uniquely written as

$$F = \sum_{p,q} F_{p,q} \quad \text{where } F_{p,q} \text{ is a biform of degree } (p,q).$$

If S is any set of biforms in $k[X_1, \ldots, X_{n+1}, Y_1, \ldots, Y_{m+1}]$, let

$$V(S) = \{(x,y) \in \mathbb{P}^n \times \mathbb{P}^m : F(x,y) = 0 \text{ for all } F \in S\}.$$

A subset $V \subseteq \mathbb{P}^n \times \mathbb{P}^m$ will be called algebraic if $V = V(S)$ for some S. For any $V \subseteq \mathbb{P}^n \times \mathbb{P}^m$, define

$$I(V) = \{F \in k[X,Y] : F(x,y) = 0 \text{ for all } (x,y) \in V\}.$$

5. Projective Plane Curves

5.1. *Linear Systems of Curves*

A projective plane curve is a hypersurface in $\mathbb{P}^2$ except that as with affine curves, we want to allow multiple components. We say that two non-constant forms $F, G \in k[X,Y,Z]$ are equivalent if there exists a non-zero $\lambda \in k$ such that $G = \lambda F$. A projective plane curve is an equivalence class of forms. The degree of a curve is the degree of a defining form. Curves of degree 1, 2, 3 and 4 are called lines, conics, cubics, and quartics respectively. The notations and conventions regarding affine curves carry over to projective curves, thus we speak of simple and multiple components and we write $\mathcal{O}_P(F)$ instead of $\mathcal{O}_P(V(F))$ for an irreducible F.

Note that when $P = [x : y : 1]$, then $\mathcal{O}_P(F)$ is canonically isomorphic to $\mathcal{O}_{(x,y)}(F_*)$, where $F_* = F(X,Y,1)$ is the corresponding affine curve. This makes computations more manageable by reducing to affine tools.

If P is a simple point on F, i.e. $m_p(F) = 1$, and F is irreducible, then $\mathcal{O}_P(F)$ is a discrete valuation ring. Let ord_P^F denote the corresponding order function on $k(F)$. If G is a form on $k[X,Y,Z]$ and $G_* \in \mathcal{O}_P(\mathbb{P}^2)$ is determined as the old $G_* = G(X,Y,1)$, and $\overline{G}_*$ is the residue of G_* in $\mathcal{O}_P(F)$, we define $\mathrm{ord}_P^F(G)$ to be $\mathrm{ord}_P^F(\overline{G}_*)$. Equivalently, $\mathrm{ord}_P^F(G)$ is the order at P of G/H, where H is any form of the same degree as G with $H(P) \neq 0$.

Definition 5.1 (intersection number and tangency)**.** Let F and G be projective plane curves and $P \in \mathbb{P}^2$. Define the intersection number $I(P, F \cap G)$ to be $\dim_k(\mathcal{O}_P(\mathbb{P}^2)/(F_*, G_*))$, which is independent of the way F_* and G_* are formed.

We define a line L to be tangent to a curve F at P if $I(P, F \cap L) > m_P(F)$. A point P in F is an ordinary multiple point of F if F has $m_P(F)$ distinct tangents at P.

Example 5.1. Note that

$$I(P, F \cap G) = \dim_k \left(\mathcal{O}_P(\mathbb{P}^2)/(F_*, G_*)\right)$$

where F_*, G_* are the affine parts of the homogeneous forms F, G, and $P = [x : y : 1] \in \mathbb{P}^2$. Take for example a line and a conic intersecting transversely. Let

$$F(X,Y,Z) = X^2 + Y^2 - Z^2 \quad \text{and} \quad G(X,Y,Z) = Y.$$

So, F denotes the unit circle and G denotes the line $Y = 0$. The point $P = [1 : 0 : 1]$ corresponds to $(1,0) \in \mathbb{A}^2$. The respective affine forms are $F_*(x,y) = x^2 + y^2 - 1$ and $G_*(x,y) = y$. At $(1,0)$, we compute the intersection number, which is

$$I(P, F \cap G) = \dim_k(\mathcal{O}_{(1,0)}/(x^2 - 1, y)).$$

Here, the ideal is simplified using the relation $y = 0$ so the generator $x^2 + y^2 - 1$ simplifies to $x^2 - 1$. We then change coordinates via $u = x - 1$ so that $(1,0) \mapsto (0,0)$. In this local ring, the ideal becomes $(u^2 + 2u, y)$ so the quotient is generated by $1, u$. Hence, $I(P, F \cap G) = 2$. Next, since the multiplicity $m_P(F) = 1$ and $I > m_P(F)$, the line $Y = 0$ is tangent to the circle at $(1,0)$.

Example 5.2. Recall that a line L is tangent to a curve F at P if $I(P, F \cap L) > m_P(F)$. We consider the interaction between a parabola and a tangent line. Let

$$F(X,Y,Z) = YZ - X^2 \quad \text{and} \quad L(X,Y,Z) = Y - 2XZ.$$

Let $p = [0 : 0 : 1]$ which corresponds to $(0,0) \in \mathbb{A}^2$. The affine forms are $F_*(x,y) = y - x^2$ and $G_*(x,y) = y - 2x$. We compute

$$I(P, F \cap L) = \dim_k \left(\mathcal{O}_{(0,0)}/(y - x^2, y - 2x)\right).$$

Replacing both y's with 0 yields

$$\mathcal{O}_{(0,0)}/(x^2-2x) = \mathcal{O}_{(0,0)}/(x(x-2)).$$

In the local ring at $(0,0)$, $x(x-2)$ has multiplicity 2, so $I(P,F\cap L)=2$. Now, $m_P(F)=2$ since $y-x^2$ vanishes to order 2 at $x=0$), and $I(P,F\cap L)=m_P(F)$, so this is not a tangent line.

We often wish to study all curves of a given degree $d\geq 1$. Let $M_1,\ldots,M_N$ be a fixed ordering of the set of monomials in X,Y,Z of degree d, where $N=\frac{(d+1)(d+2)}{2}$. Giving a curve F of degree d is the same thing as choosing $a_1,\ldots,a_N\in k$, not all zero, and letting $F=\sum a_iM_i$, except that $(a_1,\ldots,a_N)$ and $(\lambda a_1,\ldots,\lambda a_N)$ determine the same curve. In other words, each curve F of degree d corresponds to a unique point in $\mathbb{P}^{N-1}=\mathbb{P}^{d(d+3)/2}$ and each point of $\mathbb{P}^{d(d+3)/2}$ represents a unique curve. We often identify F with its corresponding point in $\mathbb{P}^{d(d+3)/2}$ and say the curves of degree d form a projective space of dimension $\frac{d(d+3)}{2}$.

Example 5.3. If $d=1$, then each line $aX+bY+cZ$ corresponds to the point $[a:b:c]\in\mathbb{P}^2$, so the lines in $\mathbb{P}^2$ form a $\mathbb{P}^2$.

Example 5.4. If $d=2$, then the conic $aX^2+bXY+cXZ+eYZ+fZ^2$ corresponds to the point $[a:b:c:d:e:f]\in\mathbb{P}^5$, so the conics form a $\mathbb{P}^5$.

One can continue the above and deduce that the cubics form a $\mathbb{P}^9$ and the quartics form a $\mathbb{P}^{14}$ and so on. If we put conditions on the set of all curves of degree d, the curves that satisfy the conditions form a subset of $\mathbb{P}^{d(d+3)/2}$. If this subset is a linear subvariety, then it is called a linear system of plane curves.