Algebraic Curves
Fall 2005
Professor R. Moraru

Chris Almost

Contents

1 Affine Algebraic Sets **2**
1.1 Affine Space . . . 2
1.2 Algebraic Sets . . . 2
1.3 Classification of Irreducible Algebraic Sets in $\mathbb{A}^2(\Bbbk)$ . . . 6

2 Affine Varieties **7**
2.1 Coordinate Rings . . . 7
2.2 Polynomial Maps . . . 7
2.3 Rational Functions and Local Rings . . . 9
2.4 Rational Maps . . . 11
2.5 Dimension . . . 12

3 Local Properties of Varieties **13**
3.1 Properties of the Local Ring at a Point . . . 13
3.2 Multiple Points and Tangent Lines . . . 14
3.3 Non-Singular Varieties . . . 17
3.4 Blowing-Up Singularities . . . 17

4 Projective Space **18**
4.1 Projective Varieties . . . 18
4.2 Homogeneous Ideals . . . 20
4.3 Regular and Rational Functions . . . 22
4.4 Varieties, Morphisms, and Rational Maps . . . 23

5 Projective Plane Curves **24**
5.1 Bézout's Theorem and Intersection Multiplicity . . . 24
5.2 Proof of Bézout's Theorem . . . 27
5.3 Divisors . . . 28
5.4 Elliptic Curves . . . 32

1 Affine Algebraic Sets

1.1 Affine Space

Notation. For these notes, $\Bbbk$ is a field, $\mathbb{A}^n(\Bbbk) = \mathbb{A}^n = \{(a_1,\dots,a_n) \mid a_1,\dots,a_n \in \Bbbk\}$ is affine n-space, and $\Bbbk[x_1,\dots,x_n]$ is the ring of polynomials in n variables with coefficients in $\Bbbk$.

1.1 Definition. If $f \in \Bbbk[x_1,\dots,x_n]$, a point $p = (a_1,\dots,a_n) \in \mathbb{A}^n(\Bbbk)$ such that $f(p) = f(a_1,\dots,a_n) = 0$ is a *zero* of f and

$$V(f) = \{p \in \mathbb{A}^n \mid f(p) = 0\}$$

is called the *zero set* of f. If f is non-constant, $V(f)$ is also known as the *hypersurface* defined by f.

1.2 Example.
1. In $\mathbb{R}^1$ $V(x^2+1) = \varnothing$, but in $\mathbb{C}^1$ $V(x^2+1) = \{\pm i\}$. Generally, if $n = 1$ then $V(F)$ is the set of roots of F in $\Bbbk$. If $\Bbbk$ is algebraically closed and F is non-constant then $V(F)$ is non-empty.
2. In $\mathbb{Z}_p^1$, by Fermat's Little Theorem, $V(x^p - x) = \mathbb{Z}_p^1$.
3. In $\mathbb{R}^2$ $V(x^2+y^2-1) =$ the unit circle in $\mathbb{R}^2$, and in $\mathbb{Q}^2$ it gives the rational points on the unit circle. Notice the circle admits a "rational parameterization" as follows:

$$(x,y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right), t \in \mathbb{R}$$

   When $t \in \mathbb{Z}$ then we get a point in $\mathbb{Q}^2$.
4. By Fermat's Last Theorem, if $n > 2$ then $V(x^n + y^n - 1)$ is finite in $\mathbb{Q}^2$.

Remark. A *rational curve* is a curve that admits a parameterization by rational functions. A hypersurface in $\mathbb{A}^n$ is called an *affine surface*.

1.2 Algebraic Sets

1.3 Definition. If S is any set of polynomials in $\Bbbk[x_1,\dots,x_n]$, we define

$$V(S) = \{p \in \mathbb{A}^n \mid f(p) = 0 \text{ for all } f \in S\} = \bigcap_{f \in S} V(f)$$

If $S = \{f_1,\dots,f_n\}$ then we may write $V(f_1,\dots,f_n)$ for $V(S)$. A subset $X \subseteq \mathbb{A}^n(\Bbbk)$ is an *(affine) algebraic set* if $X = V(S)$ for some $S \subseteq \Bbbk[x_1,\dots,x_n]$

Remark. A curve in $\mathbb{A}^n$ is said to be *algebraic* if it is algebraic set.

1.4 Example.
1. For any $a, b \in \Bbbk$, $\{(a,b)\}$ is an algebraic set in $\Bbbk^2$ since $\{(a,b)\} = V(x-a, y-b)$.
2. In $\mathbb{R}^2$ $V(y-x^2, x-y^2)$ is only 2 points, but in $\mathbb{C}^2$ it is 4 points. Generally, Bézout's Theorem tells us that the number of intersection points of a curve of degree n with a curve of degree m is nm in an algebraically closed field.
3. Not all curves in $\mathbb{R}^2$ are algebraic. For example, let $X = \{(x,y) \mid y - \sin x = 0\}$ and suppose that X is algebraic, so that $X = V(S)$ for some $S \subseteq \mathbb{R}[x,y]$. Then there is $F \in V(S)$ such that $F \neq 0$ and so $X = V(S) = \bigcap_{f \in S} V(f) \subseteq V(F)$. Notice that X intersected with any horizontal line $x - c = 0$ is infinite for $-1 \leq c \leq 1$. Choose c such that $F(x,c)$ is not the zero polynomial and notice that the number of solutions to $F(x,c) = 0$ is finite, so X cannot be algebraic.

4. The *twisted cubic* is the rational curve $\{(t, t^2, t^3) \mid t \in \mathbb{R}\} \subseteq \mathbb{R}^3$. It is an algebraic curve; indeed it is $V(y - x^2, z - x^3)$.

Remark. In general, suppose that C is an algebraic affine plane curve and L is a line not contained C. Then $L \cap C$ is either $\varnothing$ or a finite set of points (see Assignment 1).

1.5 Proposition. *The algebraic sets in $\mathbb{A}^1$ are $\varnothing$, finite subsets of $\mathbb{A}^1$, and $\mathbb{A}^1$ itself.*

PROOF: Clearly these sets are all algebraic. Conversely, the zero set of any non-zero polynomial is finite, so if S contains a non-zero polynomial then $V(S) \subseteq V(F)$ is finite. If $S = \varnothing$ or $S = \{0\}$ then $V(S) = \mathbb{A}^1$. □

1.6 Proposition (Properties of Algebraic Sets).

1. *If I is an ideal in the ring of polynomials generated by $S \subseteq I$ then $V(S) = V(I)$, so every algebraic set is equal to $V(I)$ for some ideal I.*
2. *If $I \subseteq J$ are ideals then $V(J) \subseteq V(I)$.*
3. *If $\{I_\alpha\}$ is a collection of ideals then $V(\bigcup_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$, so the intersection of any collection of algebraic sets is an algebraic set.*
4. *If I and J are ideals then $V(IJ) = V(I) \cup V(J)$, so the finite union of algebraic sets is an algebraic set.*
5. *$V(0) = \mathbb{A}^n$, $V(1) = \varnothing$, and $V(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\}$, so any finite set of points is algebraic.*

PROOF: Trivial. □

Remark.
1. Finiteness in property (4) is required; consider for example $\mathbb{Z}$ in $\mathbb{R}$. We have already seen how to show that this is not an algebraic set.
2. Properties (3), (4), and (5) show that the collection of algebraic sets form the closed sets of a topology on $\mathbb{A}^n$. This topology is known as the *Zariski topology*
3. The Zariski topology is strictly weaker than the metric topology (for $\Bbbk = \mathbb{Q}, \mathbb{R}, \mathbb{C}$), *i.e.* Zariski closed subsets are metically closed, but not necessarily conversely.

1.7 Example. The Zariski topology on the affine line $\mathbb{A}^1(\Bbbk)$ is simply the finite complement topology (*i.e.* the topology generated by taking the open sets to be the sets of finite complement). Notice that this topology is not Hausdorff if $\Bbbk$ is infinite. If $\Bbbk$ is finite then this topology is equivalent to the discrete topology. In fact, if $\Bbbk$ is finite then the Zariski topology on $\mathbb{A}^n(\Bbbk)$ is equivalent to the discrete topology.

Recall that a *principal ideal domain* (PID) is an integral domain R in which every ideal is principal. In particular, $\Bbbk[x]$ is a PID. This immediately gives another proof that the algebraic sets in $\mathbb{A}^1(\Bbbk)$ are the finite sets, $\mathbb{A}^1$ and $\varnothing$. Recall as well that a ring R is *Noetherian* if every ideal of R is finitely generated.

1.8 Theorem (Hilbert Basis Theorem). *If R is Noetherian then so is $R[x]$.*

1.9 Corollary. *Every algebraic set X in $\mathbb{A}^n$ is the zero set of a finite set of polynomials.*

PROOF: Recall that $R[x][y] \cong R[x, y]$, so it follows by induction that $R[x_1, \ldots, x_n]$ is Noetherian if R is Noetherian. Fields are Noetherian, so every ideal of $\Bbbk[x_1, \ldots, x_n]$ is finitely generated. Hence if $X = V(S)$ then $X = V(\langle S \rangle) = V(S')$ where S' is finite and generates $\langle S \rangle$. □

1.10 Definition. Given any subset $X \subseteq \mathbb{A}^n(\Bbbk)$ we define $I(X)$ to be the *ideal of X*,

$$I(X) = \{f \in \Bbbk[x_1, \ldots, x_n] \mid f(p) = 0 \text{ for all } p \in X\}$$

(Note: If X is an algebraic set then $I(X)$ is sometimes known as a closed ideal, reflecting the fact that algebraic sets are closed in the Zariski topology.)

1.11 Example. The closed ideals of $\Bbbk[x]$ correspond to the algebraic sets of $\mathbb{A}^1(\Bbbk)$.

- $I(\varnothing) = \langle 1 \rangle$
- $I(\{a_1, \ldots, a_n\}) = \langle (x - a_1) \cdots (x - a_n) \rangle$
- $I(\mathbb{A}^1) = \begin{cases} 0 & \text{if } \Bbbk \text{ is infinite} \\ \langle x^{p^n} - x \rangle & \text{if } \Bbbk \text{ has } p^n \text{ elements} \end{cases}$

Notice that if $X \subseteq \mathbb{A}^1$ is infinite then $\Bbbk$ is finite and $I(X) = 0$.

1.12 Example. In $\mathbb{A}^2(\Bbbk)$, $I(\{(a,b)\}) = \langle x - a, y - b \rangle$. Clearly $\langle x - a, y - b \rangle \subseteq I(\{(a,b)\})$, so we need only prove the reverse inequality. Assume that $f \in I(\{(a,b)\})$. By the division algorithm, there is $g(x,y) \in \Bbbk[x,y]$ and $r(y) \in \Bbbk[y]$ such that $f(x,y) = (x-a)g(x,y) + r(y)$. But $0 = f(a,b) = r(b)$, so $y - b$ divides $r(y)$ and we can write $r(y) = (y-b)h(x,y)$, and hence $f = (x-a)g + (y-b)h \in \langle x - a, y - b \rangle$. Another argument to show this would be to note that $\langle x - a, y - b \rangle$ is a maximal ideal and $I(\{(a,b)\})$ is not the whole ring of polynomials.

1.13 Proposition.

1. *If $X \subseteq Y \subseteq \mathbb{A}^n(\Bbbk)$ then $I(Y) \subseteq I(X)$.*
2. *$I(\varnothing) = \Bbbk[x_1, \ldots, x_n]$*
   $I(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ for any point $(a_1, \ldots, a_n) \in \mathbb{A}^n(\Bbbk)$.
   $I(\mathbb{A}^n(\Bbbk)) = 0$ if $\Bbbk$ is infinite.
3. *$S \subseteq I(V(S))$ for any set of polynomials $S \subseteq \Bbbk[x_1, \ldots, x_n]$.*
   $X \subseteq V(I(X))$ for any set of points $X \subseteq \mathbb{A}^n(\Bbbk)$.
4. *$V(I(V(S))) = V(S)$ for any set of polynomials $S \subseteq \Bbbk[x_1, \ldots, x_n]$.*
   $I(V(I(X))) = I(X)$ for any set of points $X \subseteq \mathbb{A}^n(\Bbbk)$.

Remark. Equality does not always hold in point (3) of the last proposition.

1. Consider $I = \langle x^2 + 1 \rangle \subseteq \mathbb{R}[x]$. Then $1 \notin I$, so $I \neq \mathbb{R}[x]$. But $V(I) = \varnothing$, so $I(V(I)) = \mathbb{R}[x] \supsetneq I$.
2. Consider $X = [0,1] \subseteq \mathbb{R}$. Then $I(X) = 0$ and $V(I(X)) = \mathbb{R} \supsetneq X$.

1.14 Definition. Let $X \subseteq \mathbb{A}^n(\Bbbk)$ and $I \subseteq \Bbbk[x_1, \ldots, x_n]$ be an ideal. The *closure of X (in the Zariski topology)* is the smallest algebraic set containing X (*i.e.* the smallest closed set containing X), and is denoted $\overline{X}$. The *closure of I* is the smallest closed ideal in $\Bbbk[x_1, \ldots, x_n]$ that contains I, and is denoted $\overline{I}$.

By the last proposition, $\overline{X} = V(I(X))$ and $\overline{I} = I(V(I))$.

1.15 Example.
1. If $\Bbbk$ is infinite and $X \subseteq \mathbb{A}^1(\Bbbk)$ is any infinite set of points then $\overline{X} = \mathbb{A}^1$. In particular, the Zariski closure of any non-emtpy open set is the whole line, or every non-empty open set is Zariski dense in the affine line.
2. Let $I = \langle x^2 + y^2 - 1, x - 1 \rangle \subseteq \mathbb{R}[x,y]$. Then $\overline{I} = I(V(I)) = I(\{(1,0)\}) = \langle x - 1, y \rangle$.

We have seen that not every ideal is the ideal of a set of points. We would like to find a test to determine when an ideal is the ideal of a set of points. Geometrically, this occurs when the generators of the ideal are of the "smallest possible order". For example, if $I = \langle y - x^2, x - 1 \rangle$ then $V(I) = \{(1,1)\}$, but $I(\{(1,1)\}) = \langle x - 1, y - 1 \rangle$ (indeed, $y - x^2 = (y-1) - (x-1)(x+1)$), so I is not the ideal of a set of points.

Algebraically, if $I = I(X)$ for some $X \subseteq \mathbb{A}^n(\Bbbk)$ then I is radical, *i.e.*

$$I = \sqrt{I} = \{a \in R \mid a^n \in I \text{ for some } n > 0\}$$

or equivalently, $a^n \in I$ implies that $a \in I$ for all $a \in R$ and $n > 0$. To see this, let $f \in \Bbbk[x_1, \ldots, x_n]$ be such that $f^n \in I$. Then $[f(x)]^n = 0$ for every $x \in X$, so $f(x) = 0$ for every $x \in X$, and hence $f \in I(X) = I$.

1.16 Example. 1. Any prime or maximal ideal is radical.
2. $I = \langle x^2 + y^2 - 1, x - 1\rangle$ is not radical since $y^2 = (x^2 + y^2 - 1) - (x - 1)(x + 1) \in I$ but $y \notin I$.
3. $I = \langle y - x^2, y - x^3\rangle$ is not radical since if $u := x(x-1)$ then $u^2 = [(y - x^2) - (y - x^3)](x - 1) \in I$ but $u \notin I$. (Geometrically, $V(I)$ is only two distinct points, which is "too few" given the degrees of the polynomials.)
4. $I = \langle x^2 + 1\rangle \subseteq \mathbb{R}[x]$ is prime, so I is radical, but I is not the ideal of a set of points. Hence this test is not sufficient in general.

1.17 Theorem (Hilbert's Nullstellenzatz). *Let $\Bbbk$ be an algebraically closed field and $I \subseteq \Bbbk[x_1, \ldots, x_n]$ be an ideal. Then $I(V(I)) = \sqrt{I}$, so I is the ideal of a set of points if and only if $I = \sqrt{I}$.*

Consequently, if $\Bbbk$ is algebraically closed then there is a one to one correspondence between algebraic sets $X \subseteq \mathbb{A}^n(\Bbbk)$ and radical ideals $I \subseteq \Bbbk[x_1, \ldots, x_n]$. Namely, it is

$$X \mapsto I(X) \qquad \text{and} \qquad I \mapsto V(I)$$

1.18 Definition. An algebraic set $X \subseteq \mathbb{A}^n(\Bbbk)$ if *irreducible* if $X \neq \varnothing$ and X cannot be expressed at $X = X_1 \cup X_2$, where X_1 and X_2 are algebraic sets not equal to X.

1.19 Proposition. *An algebraic set $X \subseteq \mathbb{A}^n(\Bbbk)$ is irreducible if and only if $I(X)$ is prime.*

PROOF: If X is irreducible then suppose that $f, g \in \Bbbk[x_1, \ldots, x_n]$ are such that $fg \in I(X)$. Then $\langle fg\rangle \subseteq I(X)$, so $X = V(I(X)) \subseteq V(fg) = V(f) \cup V(g)$. Hence $X = (X \cap V(f)) \cup (X \cap V(g))$, so without loss of generality, $X = X \cap V(f) \subseteq V(f)$. Therefore $f \in I(X)$ and $I(X)$ is prime.

Suppose that $I(X)$ is prime but is irreducible, with $X = X_1 \cup X_2$. Then $I(X) = I(X_1) \cap I(X_2)$. If $I(X) = I(X_1)$ then $X = X_1$, which is not allowed. Hence there is $f \in I(X_1) \setminus I(X)$. But for any $g \in I(X_2)$, $fg \in I(X_1) \cap I(X_2) = I(X)$, so since $f \notin I(X)$ and $I(X)$ is prime, $g \in I(X)$. This implies that $I(X) = I(X_2)$ (and hence $X = X_2$), a contradiction. □

When $\Bbbk$ is algebraically closed, the above correspondence takes irreducible algebraic sets to prime ideals, and *visa versa*.

1.20 Proposition. *Every algebraic set $X \subseteq \mathbb{A}^n(\Bbbk)$ is a finite union of irreducible algebraic sets, and this decomposition is unique.*

PROOF: First, suppose that X is not the union of a finite number of irreducibles. Then X is reducible, so $X = X_1 \cup X_1'$, where $X_1, X_1' \subsetneq X$. Without loss of generality, X_1 is not the union of a finite number of irreducibles. Repeating this we get an infinite strictly descending chain of algebraic sets $X \supsetneq X_1 \supsetneq \cdots$. But then $I(X) \subsetneq I(X_1) \subsetneq \cdots$ is an infinite strictly ascending chain of ideals in $\Bbbk[x_1, \ldots, x_n]$, a contradiction since $\Bbbk[x_1, \ldots, x_n]$ is Noetherian.

Let $X \subseteq \mathbb{A}^n$ be an algebraic set and suppose that $X = X_1 \cup \cdots \cup X_m$, where each X_i is an irreducible algebraic set. We may assume that $X_i \not\subseteq X_j$ if $i \neq j$. Such an expression is called an *(irredundant) decomposition* of X into irreducible algebraic sets. Suppose that X also has a decompostion $Y_1 \cup \cdots \cup Y_k$. Then for any i, $X_i = X_i \cap X = \bigcup_i (X_i \cap Y_j)$. Since X_i is irreducible, $X_i = X_i \cap Y_{j_0}$ for some j_0. Similarily, $Y_{j_0} \subseteq X_{i_0}$ for some i_0, but this implies that $X_i \subseteq Y_{j_0} \subseteq X_{i_0}$, and since the decomposition is irredundant, $X_i = X_{i_0} = Y_{j_0}$. Therefore every X_i corresponds to a Y_j, and *visa versa*. □

1.21 Example. 1. Suppose that $f \in \Bbbk[x_1, \ldots, x_n]$ and $f = f_1^{r_1} \ldots f_m^{r_m}$ then $V(f) = V(f_1) \cup \cdots \cup V(f_m)$. If $\Bbbk$ is algebraically closed then this is a decomposition and $I(V(f)) = \langle f_1 \cdots f_m\rangle$.
2. Since $\Bbbk[x_1, \ldots, x_n]$ is a UFD, any ideal generated by an irreducible polynomial is prime. If $\Bbbk$ is algebraically closed then $V(p)$ is irreducible for every irreducible polynomial $p \in \Bbbk[x_1, \ldots, x_n]$ by Hilbert's Nullstellensatz. Hence when $\Bbbk$ is algebraically closed there is a one to one correspondence between irreducible polynomials in $\Bbbk[x_1, \ldots, x_n]$ and irreducible hypersurfaces in $\mathbb{A}^n(\Bbbk)$.

3. Consider $X = V(y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3) \subseteq \mathbb{C}^2$. Notice $y^4 - x^2 = (y^2 - x)(y^2 + x)$ and $y^4 - x^2y^2 + xy^2 - x^3 = (y^2+x)(y-x)(y+x)$, so $V(y^2+x)$ is an irreducible component of X. The other 3 points in X are $(0,0)$, $(1,1)$ and $(1,-1)$. But $(0,0) \in V(y^2+x)$, so the decomposition of X is $V(y^2+x) \cup \{(1,1)\} \cup \{(1,-1)\}$.
4. Consider $X = V(x^2 + y^2(y-1)^2) \subseteq \mathbb{R}^2$. $X = \{(0,0),(0,1)\}$, so X is reducible. But $f(x,y) = x^2 + y^2(y-1)^2$ is irreducible in $\mathbb{R}[x,y]$, indeed $f(x,y) = (x + iy(y-1))(x - iy(y-1))$ and these are irreducible factors. Since $\mathbb{R}[x,y] \subseteq \mathbb{C}[x,y]$ are UFDs, if f factors in $\mathbb{R}[x,y]$ the decompostion must agree with the decomposition we have, up to constant multiple, but this is impossible.

1.3 Classification of Irreducible Algebraic Sets in $\mathbb{A}^2(\Bbbk)$

Prime ideals may correspond to reducible algebraic sets if the field is not algebraically closed. Nonetheless, we have the following classification of irreducible algebraic sets in $\mathbb{A}^2(\Bbbk)$ when $\Bbbk$ is infinite. But first we prove the following proposition.

1.22 Proposition. *If $f, g \in \Bbbk[x,y]$ have no common factors then $V(f,g) = V(f) \cap V(g)$ is at most a finite set of points.*

PROOF: Since f and g have no common factor in $\Bbbk[x,y] = \Bbbk[x][y]$, they have no common factors in $\Bbbk(x)[y]$. Therefore $\gcd(f,g)$ exists and is 1 in $\Bbbk(x)[y]$, so there are $s,t \in \Bbbk(x)[y]$ such that $sf + tg = 1$. Hence there is $d \in \Bbbk[x]$ such that $ds = a, dt = b$, where $a,b \in \Bbbk[x][y] = \Bbbk[x,y]$. Then $af + bg = d \in \Bbbk[x]$. Now if $(x_0,y_0) \in V(f,g)$ then $d(x_0) = 0$, so there are at most finitely many possible values for x_0. Similarily, there are at most finitely many possible values for y_0, so $V(f,g)$ is finite. □

1.23 Corollary. *If $f \in \Bbbk[x,y]$ is irreducible and if $V(f)$ is infinite then $I(V(f)) = \langle f \rangle$ and $V(f)$ is irreducible.*

PROOF: We know that $\langle f \rangle \subseteq I(V(f))$. Let $g \in I(V(f))$. Then because $V(f)$ is infinite, $V(f,g) \supseteq V(f)$ is infinite, so f and g have a common factor. But f is irreducible, so $f \mid g$ and $g \in \langle f \rangle$. □

1.24 Theorem. *In $\mathbb{A}^2(\Bbbk)$, where $\Bbbk$ is infinite, the irreducible algebraic sets are*

- $\varnothing$
- $\mathbb{A}^2$
- $\{(a,b)\}$, *for $a,b \in \Bbbk$*
- $V(F)$ *where $F \in \Bbbk[x,y]$ is irreducible and $V(F)$ is an infinite set*

PROOF: Let $X \subseteq \mathbb{A}^2(\Bbbk)$ be an irreducible algebraic set. Assume that $X \neq \varnothing, \mathbb{A}^2$ or a single point. Then $I(X) \neq 0$, so there is at least on non-zero polynomial $f \in I(X)$. Moreover, any irreducible factor of f is in the prime ideal $I(X)$, since X is assumed to be irreducible. We may therefore assume that f is irreducible. We then have $I(X) = \langle f \rangle$, since clearly $\langle f \rangle \subseteq I(X)$, and suppose that there is $g \in I(X)$ such that $g \notin \langle f \rangle$. Then f and g have no common factors, so $V(f,g)$ is a finite set of points. But $X \subseteq V(f,g)$ is infinite, so $I(X) = \langle f \rangle$ and $X = V(f)$. □

Remark. If $\Bbbk$ is not algebraically closed then there are more prime ideals than irreducible algebraic sets. In general, X irreducible implies that $I(X)$ is prime, however

- distinct prime ideals may give the same algebraic set (*e.g.* $V(\langle x^2 + y^2 \rangle) = \{(0,0)\} = V(\langle x, y \rangle)$ in $\mathbb{R}^2$)
- a prime ideal may have a reducible zero set (*e.g.* $V(\langle x^2 + y^2(y-1)^2 \rangle) = \{(0,0),(0,1)\}$ in $\mathbb{R}^2$)

2 Affine Varieties

From this section $\Bbbk$ is assumed to be a fixed algebraically closed field. Affine algebraic sets will be assumed to be in $\mathbb{A}^n = \mathbb{A}^n(\Bbbk)$ for some n.

2.1 Definition. An irreducible affine algebraic set is called an *affine (algebraic) variety*, or simply a *variety* if the context is clear. Any variety X is endowed with the *induced (Zariski) topology*, whose open sets are of the form $X \cap U$ for some Zariski-open subset U of $\mathbb{A}^n$.

2.1 Coordinate Rings

2.2 Definition. Let $X \subseteq \mathbb{A}^n$ be a variety. Then $I(X)$ is prime, so $\Bbbk[x_1, \ldots, x_n]/I(X)$ is an integral domain. The quotient ring $\Gamma(X) = \Bbbk[x_1, \ldots, x_n]/I(X)$ is called the *coordinate ring* of X. (Other common notations are $\Bbbk[X]$ and $A(X)$.)

2.3 Definition. A function $F : X \to \Bbbk$ if called a *polynomial function* if there is $f \in \Bbbk[x_1, \ldots, x_n]$ such that $F(x) = f(x)$ for all $x \in X$.

Remark. Notice that two polynomials $f, g \in \Bbbk[x_1, \ldots, x_n]$ determine the same polynomial function on X if and only if $f - g \in I(X)$. Consequently, we may thing of $\Gamma(X)$ as the set of all polynomial functions on X. We will think of $\Gamma(X)$ not only as a ring but also as a $\Bbbk$-algebra, *i.e.* we will also consider the $\Bbbk$-module structure on $\Gamma(X)$.

2.4 Example.
1. If $X = \mathbb{A}^n$ then $I(X) = 0$, so $\Gamma(X) = \Bbbk[x_1, \ldots, x_n]$.
2. If X is a single point then $\Gamma(X) = \Bbbk$ since defining a function on a point is the same as fixing a value for that point.
3. If $X = V(y - x^2) \subseteq \mathbb{A}^2$ then $\Gamma(X) = \Bbbk[x, y]/\langle y - x^2 \rangle \cong \Bbbk[\overline{x}]$, where $\overline{x}$ is the residue class of x in $\Gamma(X)$.

Looking at $\Bbbk[x_1, \ldots, x_n]/I(X)$ gives a test for irreducibility since $\Bbbk[x_1, \ldots, x_n]/I(X)$ is a domain if and only if $I(X)$ is prime, which happens if and only if X is irreducible.

2.2 Polynomial Maps

2.5 Definition. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be two varieties. A function $\varphi : X \to Y$ is called a *polynomial map* if there are polynomials $f_1, \ldots, f_m \in \Bbbk[x_1, \ldots, x_n]$ such that $\varphi(x) = (f_1(x), \ldots, f_m(x))$ for every $x \in X$.

2.6 Example.
1. Polynomial functions $F : X \to \Bbbk \cong \mathbb{A}^1$ are polynomial maps.
2. Any linear map $\mathbb{A}^n \to \mathbb{A}^m$ is a polynomial map.
3. Affine maps $\mathbb{A}^n \to \mathbb{A}^m : x \mapsto Ax + b$ are polynomial maps.
4. Projections and inclusions are polynomial maps.

2.7 Definition. Two varieties X and Y are *isomorphic* if there is an invertible polynomial map $\varphi : X \to Y$ such that φ^{-1} is also a polynomial map. We say φ is an *isomorphism* and we write $X \cong Y$.

2.8 Example.

1. $\varphi : V(y - x^2) \to \mathbb{A}^1 : (x, x^2) \mapsto x$ has a polynomial inverse $\varphi^{-1}(t) = (t, t^2)$, so $V(y - x^2) \cong \mathbb{A}^1$.

2. $\varphi : \mathbb{A}^1 \to X = V(y^2 - x^3) : t \mapsto (t^2, t^3)$ is a bijective polynomial map. Indeed, in the metric topology over $\mathbb{C}$, φ is a homeomorphism. However, φ does not have a polynomial inverse. Suppose that $\varphi^{-1} : X \to \mathbb{A}^1$ is polynomial. Then φ^{-1} is a polynomial function on X, so it is an element of $\Gamma(X)$. Moreover, $\Gamma(X) = \Bbbk[x,y]/\langle y^2 - x^3\rangle$. Since $\overline{y}^2 = \overline{x}^3$ in $\Gamma(X)$, any polynomial $f(x,y)$ can be written as $p(\overline{x}) + \overline{y}q(\overline{x})$ in $\Gamma(X)$. Therefore $\varphi^{-1}(x,y) = p(x) + yq(x)$ for some $p, q \in \Bbbk[x]$, and the composition $t \mapsto (t^2, t^3) \mapsto p(t^2) + t^3 q(t^2)$, as expression of degree at least 2 in t. In particular, $\varphi^{-1}(t^2, t^3) \neq t$, so φ does not have a polynomial inverse.

2.9 Example. Any two varieties which are isomorphic via an affine coordinate change are said to be *affinely equivalent*. For example, any conic (a curve given by a polynomial of degree 2) is affinely equivalent to a parabola, a hyperbola, an ellipse, the union of two lines, or a double line.

2.10 Proposition. *Suppose that $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ are varieties and $\varphi : X \to Y$ is a polynomial map.*

1. *$\varphi^{-1}(Z) \subseteq X$ is an algebraic set, for every algebraic set $Z \subseteq Y$.*
2. *If $\varphi : X \to Y$ is onto then Z is irreducible if $\varphi^{-1}(Z) \subseteq X$ is irreducible, for any algebraic set $Z \subseteq Y$.*

PROOF: 1. This is simply that statement that φ is continuous in the Zariski topology. Indeed, if $Z = V(g_1, \ldots, g_r)$ then $\varphi^{-1}(Z) = V(g_1 \circ \varphi, \ldots, g_r \circ \varphi)$.

2. If $Z = Z_1 \cup Z_2$ then $\varphi^{-1}(Z) = \varphi^{-1}(Z_1) \cup \varphi^{-1}(Z_2)$. If $\varphi^{-1}(Z)$ is irreducible, without loss of generality suppose $\varphi^{-1}(Z) = \varphi^{-1}(Z_1)$. Then since φ is onto, $Z = Z_1$. □

So far we have three ways to test whether an algebraic set $X \subseteq \mathbb{A}^n$ is irreducible.

1. Is $I(X)$ is prime?
2. Is $\Gamma(X)$ is an integral domain?
3. Can we express X as the preimage of a variety in a polynomial map?

2.11 Example. Consider $X = V(y - x^2, z - x^3) \subseteq \mathbb{A}^3$, the twisted cubic. Note that $I(X) = \langle y - x^2, z - x^3\rangle$. One inclusion is obvious, and for any $f \in I(X)$, by applying the division algorithm twice (once with respect to y and once with respect to z), we can write $f(x,y,z) = (y - x^2)g(x,y,z) + (z - x^3)h(x,z) + r(x)$. For all $x \in \Bbbk$, $(x, x^2, x^3) \in X$, so $r(x) = 0$ for all $x \in \Bbbk$, hence $r = 0$ and $f \in \langle y - x^2, z - x^3\rangle$. In the quotient ring $y = x^2$ and $z = x^3$, so $\Bbbk[x,y,z]/I(X)$ is isomorphic to $\Bbbk[x]$, an integral domain. Therefore X is irreducible.

On the other hand, define $\varphi : \mathbb{A}^1 \to X : t \mapsto (t, t^2, t^3)$. φ is a surjective polynomial map. Therefore $\mathbb{A}^1 = \varphi^{-1}(X)$ is irreducible (if $\Bbbk$ is infinite), so X is irreducible.

We would like to know how polynomial maps act on the coordinate rings. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be varieties and $\varphi : X \to Y$ be a polynomial map. If $g \in \Gamma(Y)$ then $g \circ \varphi \in \Gamma(X)$, so

$$\varphi^* : \Gamma(Y) \to \Gamma(X) : g \mapsto g \circ \varphi$$

is a well-defined map, called the *pullback* of φ.

2.12 Proposition (Functoriality).

1. *If $\varphi = id_X$ then $\varphi^* = id_{\Gamma(X)}$.*
2. *If $\varphi : X \to Y$ and $\psi : Y \to Z$ then $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.*
3. *$\varphi^* : \Gamma(Y) \to \Gamma(X)$ is a $\Bbbk$-algebra homomorphism.*

PROOF: Exercise. □

2.13 Theorem. *Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be varieties. Then $X \cong Y$ if and only if $\Gamma(X) \cong \Gamma(Y)$.*

PROOF: If $X \cong Y$ then let $\varphi : X \to Y$ be an invertible polynomial map (with polynomial inverse). In particular, φ^* and $(\varphi^{-1})^*$ are both $\Bbbk$-algebra homomorphisms, and $(\varphi^*)^{-1} = (\varphi^{-1})^*$. Hence $\Gamma(X) \cong \Gamma(Y)$.

Conversely, suppose that $\Gamma(X) \cong \Gamma(Y)$. Then there is a $\Bbbk$-algebra isomorphism $\Phi : \Gamma(Y) \to \Gamma(X)$. We need to show that there is an isomorphism $\varphi : X \to Y$ such that $\Phi = \varphi^*$. Suppose that the coordinates in $\mathbb{A}^m$ are $t_1, \ldots, t_m$. Then $\overline{t}_i \in \Gamma(Y)$, for all i, so $\Phi(t_i) \in \Gamma(X)$. Set $\varphi_i = \Phi(t_i)$ for all i. Then $\varphi : X \to \mathbb{A}^m : x \mapsto (\varphi_1(x), \ldots, \varphi_m(x))$ is a well-defined polynomial map. We need to show that $\varphi(X) \subseteq Y$; it is enough to show that for every $g \in I(Y)$, $g(\varphi(x)) = 0$ for all $x \in X$. Note that if $g \in I(Y)$ then $\Phi(g) = 0$ in $\Gamma(X)$. Moreover, since Φ is a $\Bbbk$-algebra homomorphism,

$$\Phi(g(t_1, \ldots, t_m)) = g(\Phi(t_1), \ldots, \Phi(t_m))$$

Hence for all $x \in X$, $0 = \Phi(g)(x) = g(f_1(x), \ldots, f_n(x)) = g(\varphi(x))$. Therefore $\varphi : X \to Y$ and $\Phi = \varphi^*$. □

In the terminology of Category Theory, the contravariant functor Γ is an equivalence of categories between the category of affine varieties with polynomial maps as morphisms, and the category of finitely generated $\Bbbk$-algebras that are integral domains with algebra homomorphisms as morphisms.

2.14 Example.
1. Is $X = V(yx - 1) \subseteq \mathbb{A}^2$ isomorphic to $\mathbb{A}^1$? No, since $\Gamma(\mathbb{A}^1) = \Bbbk[t]$ while $\Gamma(X)$ is the ring of Laurent series, $\Bbbk[x, x^{-1}]$.
2. We have seen that $\varphi : \mathbb{A}^1 \to X = V(y^2 - x^3) \subseteq \mathbb{A}^2 : t \mapsto (t^2, t^3)$ is a bijection but not an isomorphism. Indeed, $\varphi^* : \Gamma(X) \to \Gamma(\mathbb{A}^1) = \Bbbk[t] : \overline{x} \mapsto t^2 : \overline{y} \mapsto t^3$ is not an isomorphism since t is not in the image.

What conditions can one impose on $\varphi : X \to Y$ to ensure that the pullback is injective? For $g \in \Gamma(Y)$, $\varphi^*(g) = 0$ if and only if $g \circ \varphi(x) = 0$ for all $x \in X$, which is to say that $g \in I(\varphi(X))$. Now φ^* is injective if and only if $\varphi^*(g) = 0$ implies that g is zero on Y. Hence φ^* is injective if and only if $I(\varphi(X)) = I(Y)$, or

$$Y = \overline{Y} = V(I(Y)) = V(I(\varphi(X)) = \overline{\varphi(X)}$$

To restate, φ^* is injective if and only if $\varphi(X)$ is dense in Y.

2.15 Definition. A polynomial map $\varphi : X \subseteq \mathbb{A}^n \to Y \subseteq \mathbb{A}^m$ between two affine varieties is called *dominant* if $\varphi(X)$ is dense in Y.

2.16 Theorem. *Let $\varphi : X \subseteq \mathbb{A}^n \to Y \subseteq \mathbb{A}^m$ be a polynomial map between affine varieties X and Y. Then*

1. *φ^* is injective if and only if φ is dominant.*
2. *φ^* is surjective if and only if φ has a polynomial left inverse.*

PROOF: Exercise. □

2.3 Rational Functions and Local Rings

2.17 Definition. Let $X \subseteq \mathbb{A}^n$ be a variety and $\Gamma(X)$ its coordinate ring. Since $\Gamma(X)$ is a domain, we may consider its field of fractions, which we will denote $\Bbbk(X)$. In this context, $\Bbbk(X)$ is called the *field of rational functions* on X, or the *function field* of X. Its elements are rational functions.

2.18 Definition. In contrast to polynomial functions, rational functions are not necessarily defined at every point in X. A rational function F is said to be *regular* (or *defined*) at $p \in X$ if F can be written as $\frac{a}{b}$ for some $a, b \in \Gamma(X)$ such that $b(p) \neq 0$. The *value* of F at p is defined to by $F(p) = \frac{a(p)}{b(p)}$. A point where F is not defined is called a *pole* and the set of all such points is called the *pole set* of F.

2.19 Example. If $\mathrm{ch}(\Bbbk) \neq 2$ then $f = \frac{1-\overline{y}}{\overline{x}}$ is a rational function on $X = V(x^2+y^2-1)$ with pole set $\{(0,-1)\}$. Indeed, there are two points on X with x-coordinate equal to 0, but at $(0,1)$ we have

$$f = \frac{(1-\overline{y})(1+\overline{y})}{\overline{x}(1+\overline{y})} = \frac{\overline{x}^2}{\overline{x}(1+\overline{y})} = \frac{\overline{x}}{1+\overline{y}}$$

so $(0,1)$ is not a pole of f. If $(0,-1)$ were not a pole then there would be $a, b \in \Gamma(X)$ such that $\frac{1-\overline{y}}{\overline{x}} = \frac{a}{b}$ with $b(0,-1) \neq 0$. Hence $(1-\overline{y})b = a\overline{x}$, so lifting to $\Bbbk[x,y]$ we get $(1-y)\tilde{b} = \tilde{a}x$, where $\tilde{b}(0,-1) \neq 0$. But then at $(0,-1)$ we have $2\tilde{b}(0,-1) = \tilde{a}(0,-1) = 0$, a contradiction since $\mathrm{ch}(\Bbbk) \neq 2$. (Note: if $\mathrm{ch}(\Bbbk) = 2$ then $x^2+y^2-1 = (x+y-1)(x+y+1)$, so X is not a variety.)

2.20 Definition. For $p \in X$, $\mathcal{O}_p(X)$ is the *local ring at* p, the set of all rational functions on X that are defined at p. The ideal $M_p(X) = \{f \in \mathcal{O}_p(X) \mid f(p) = 0\}$ of $\mathcal{O}_p(X)$ is the *maximal ideal* at p.

$\mathcal{O}_p(X)$ is a subring of the function field that contains the coordinate ring, *i.e.* $\Gamma(X) \subseteq \mathcal{O}_p(X) \subseteq \Bbbk(X)$. Consider the evaluation homomorphism $\mathcal{O}_p(X) \to \Bbbk$. It is surjective with kernel equal to $M_p(X)$. This shows that $\mathcal{O}_p(X)/M_p(X) \cong \Bbbk$, so $M_p(X)$ is indeed a maximal ideal. Moreover, an element $f \in \mathcal{O}_p(X)$ is a unit if and only if $f(p) \neq 0$, so that $M_p(X) = \{\text{non-units}\}$ and it is the unique maximal ideal.

Remark. The local ring captures all of the local properties of the variety, *i.e.* properties that only depend on neighbourhoods of points.

2.21 Definition. $\mathcal{O}(X)$ is the *ring of regular functions*, the set of rational functions that are defined for all $p \in X$, *i.e.* $\mathcal{O}(X) = \bigcap_{p \in X} \mathcal{O}_p(X)$. The elements of $\mathcal{O}(X)$ are called *regular* functions.

Clearly $\Gamma(X) \subseteq \mathcal{O}(X)$. In fact, we have that $\Gamma(X) = \mathcal{O}(X)$ when $\Bbbk$ is algebraically closed, but not in general.

2.22 Theorem.

1. *The pole set of a rational function on X is an algebraic subset of X.*
2. $\mathcal{O}(X) = \Gamma(X)$.

PROOF: Let $X \subseteq \mathbb{A}^n(\Bbbk)$ be a variety and $f \in \Bbbk(X)$. For any $g \in \Bbbk[x_1,\ldots,x_n]$, $\overline{g}$ is the residue of g in $\Gamma(X)$. Let $J_f = \{g \in \Bbbk[x_1,\ldots,x_n] \mid \overline{g}f \in \Gamma(X)\}$, an ideal of $\Bbbk[x_1,\ldots,x_n]$ that contains $I(X)$. Moreover, $V(J_f)$ is the set of points where f is not defined; the pole set of f.

We need only show that $\mathcal{O}(X) \subseteq \Gamma(X)$. If $f \in \mathcal{O}(X)$ then the pole set V_f of f is empty. Therefore $\Bbbk[x_1,\ldots,x_n] = I(V_f) = I(V(J_f)) = \sqrt{J_f}$ since $\Bbbk$ is algebraically closed. But then $1 \in \sqrt{J_f}$, so $1 \in J_f$, which implies that $f \in \Gamma(X)$. □

Remark. The set of all points where some rational function is defined is an open subset of X since the pole set is algebraic. This open subset is called the *domain* of the function. f is completely determined by its restriction to its domain.

1. If a rational function is defined on a closed (non-empty) subset of X then it is defined on all of X since the domain is both open and closed and X is irreducible.
2. If a rational function f is zero on an open subset U of X then f is zero everywhere. Indeed, if $U \subsetneq X$ and $f \neq 0$ then $X_1 = X \setminus U$ is a closed proper subset of X. Write $f = \frac{a}{b}$ where a is not zero. Let $X_2 = V(a)$, another closed proper subset of X. Then $X = X_1 \cup X_2$, contradicting that X is irreducible.

Rational functions can be defined as equivalence classes of pairs (f,U) where f is a regular function on an open subset U of X, where the equivalence is defined by $(f,U) \sim (g,V)$ if $U \cap V \neq \varnothing$ and $f|_{U\cap V} = g|_{U\cap V}$.

2.4 Rational Maps

2.23 Definition. If $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ are varieties, a *rational map* $\varphi : X \to Y$ is a map of the form $(\varphi_1(x), \ldots, \varphi_m(x))$ for some $\varphi_i \in \Bbbk(X)$. We say that φ is *regular* at $x \in X$ if every φ_i is regular at x. At regular points, $\varphi(x)$ is the *image* of x.

Note that φ may not be defined at every $x \in X$, but the domain of φ is an open subset of X — it is the intersection of the domains of the maps φ_i.

2.24 Definition. A rational map $\varphi : X \to Y$ is called *dominant* if $\overline{\varphi(X)} = Y$.

2.25 Example (Stereographic projection). Let $\varphi : X = V(x^2 + y^2 - 1) \to \mathbb{A}^1 : (x, y) \mapsto \frac{x}{1-y}$. Then the only pole of φ is $(0, 1)$ and $\varphi(X) = \mathbb{A}^1$. Stereographic projection is dominant.

Given two rational maps $\varphi : X \to Y$ and $\psi : Y \to Z$, the composition of ψ and φ is not defined if $\varphi(X) \cap (\text{domain } \psi)$ is empty. By requiring that φ be dominant we can bypass this problem.

2.26 Definition. A dominant rational map $\varphi : X \to Y$ is *birational* or a *birational equivalence* if φ has an inverse rational map that is also dominant. In this case, X and Y are said to be *birational* or *birationally equivalent*, denoted $X \sim Y$.

2.27 Example.
1. $\varphi : X = V(xy - 1) \to \mathbb{A}^1 : (x, y) \mapsto x$ is a polynomial map that is not surjective. But it is a dominant rational map, and $\varphi^{-1} : x \mapsto (x, \frac{1}{x})$ is another dominant rational map. Therefore $V(xy-1) \sim \mathbb{A}^1$, but not isomorphic. Indeed, $\Gamma(X) = \Bbbk[x, x^{-1}] \ncong \Gamma(\mathbb{A}^1)$, but $\Bbbk(X) \cong \Bbbk(t) = \Bbbk(\mathbb{A}^1)$.
2. $\varphi : \mathbb{A}^1 \to X = V(y^2 - x^3) : t \mapsto (t^2, t^3)$ is a bijection but not an isomorphism. But $\varphi^{-1} : (x, y) \mapsto \frac{y}{x}$ is a rational inverse, so φ is a birational map and $V(y^2 - x^3) \sim \mathbb{A}^1$. Also, $\Bbbk(\mathbb{A}^1) = \Bbbk(t) \cong \Bbbk(X)$ via $f(t) \mapsto f(\frac{x}{y})$.

2.28 Definition. A variety $X \subseteq \mathbb{A}^n$ that is birationally equivalent to $\mathbb{A}^m$, for some m, is said to be *rational*.

The above two examples are rational, and any conic is rational. There are curves that are not rational, *e.g.* elliptic curves are not rational.

Let $\varphi : X \to Y$ be a rational map. We would like to define the *pullback* of φ as $\varphi^* : \Bbbk(Y) \to \Bbbk(X) : f \mapsto f \circ \varphi$. For this to be a well-definition, φ must be dominant (to ensure the composition) and φ^* must be a field homomorphism (and therefore injective). Clearly $\varphi^* : \Gamma(Y) \to \Bbbk(X) : f \mapsto f \circ \varphi$ is a ring homomorphism. Moreover, it is injective since if $0 = \varphi^*(g) = g \circ \varphi$ then g is zero on $\varphi(X)$, but φ is dominant so $\varphi(X)$ is dense in Y. Thus $g = 0$. Thus φ^* extends to an injective $\Bbbk$ algebra homomorphism $\Bbbk(Y) \to \Bbbk(X)$.

2.29 Proposition (Functoriality).

1. $id_X^* = id_{\Bbbk(X)}$
2. *If $\varphi : X \to Y$ and $\psi : Y \to Z$ are both dominant rational maps then $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.*
3. *φ^* is an injective $\Bbbk$-algebra homomorphism.*

PROOF: Exercise. □

2.30 Theorem. *Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be varieties. Then $X \sim Y$ if and only if $\Bbbk(X) \cong \Bbbk(Y)$.*

PROOF: If $X \sim Y$ then there are dominant rational maps $\varphi : X \to Y$ and $\psi : Y \to X$ such that $\varphi \circ \psi = \psi \circ \varphi = id$. Then their pullbacks are also inverses, so $\varphi^* : \Bbbk(Y) \to \Bbbk(X)$ is an isomorphism.

Given a $\Bbbk$-algebra homomorphism $\Psi : \Bbbk(Y) \to \Bbbk(X)$, it suffices to find a dominant rational map $\varphi : X \to Y$ such that $\Psi = \varphi^*$. If $t_1, \ldots, t_m$ are the coordinate functions on $\mathbb{A}^m$ then set $\varphi_i = \psi(t_i)$ for $i = 1, \ldots, m$. This gives

a rational map $\varphi : X \to \mathbb{A}^n : x \mapsto (\varphi_1(x), \ldots, \varphi_m(x))$. Note that $\varphi(X) \subseteq Y$ by the same proof as in the coordinate ring case. The only thing left to prove is that $\overline{\varphi(X)} = Y$. Since Y is closed, $\overline{\varphi(X)} \subseteq Y$. Let $g \in I(\varphi(X))$. Then for all $x \in X$, $\Psi(g)(x) = \varphi(g(x)) = 0$. Therefore $\Psi(g) = 0$, so $g = 0$ since Ψ is injective. In particular, $g(Y) = 0$, so $Y \subseteq V(I(\varphi(X)) = \overline{\varphi(X)}$. □

This one to one correspondence is an equivalence between the category of varieties with dominant rational maps as morphisms and the category of finitely generated field extensions of $\Bbbk$. The contravariant functor is $X \mapsto \Bbbk(X)$.

2.31 Corollary. *For any two affine varieties X and Y, the following conditions are equivalent.*

1. $X \sim Y$
2. $\Bbbk(X) \cong \Bbbk(Y)$
3. *There are open sets $U \subseteq X$ and $V \subseteq Y$ such that $U \cong V$.*

2.5 Dimension

2.32 Definition. The *dimension* of a variety X is the transcendence degree of the function field $\Bbbk(X)$; it is denoted $\dim X$. If $Y \subseteq X$ is a subvariety of X then $\dim X - \dim Y$ is called the *codimension* of Y in X; it is written $\operatorname{codim} Y$ or $\operatorname{codim}_X Y$. Varieties of dimension 1 are *curves*, varieties of dimension 2 are *surfaces*, varieties of dimension n are called *n-folds*.

Dimension is invariant under birational equivalence.

1. $\mathbb{A}^n$ has dimension n since in $\Bbbk(x_1, \ldots, x_n) \cong \Bbbk(\mathbb{A}^n)$ the coordinate functions $x_1, \ldots, x_n$ are algebraically independent. It follows that $\mathbb{A}^n$ and $\mathbb{A}^m$ cannot be birational if $m \neq n$.
2. If $X = \{pt\}$ then $\Bbbk(X) = \Bbbk$, so $\dim X = 0$.
3. Irreducible plane curves have dimension 1. Suppose $X = V(f)$ for some irreducible polynomial $f \in \Bbbk[x, y]$. Note that x and y are algebraically independent in $\Bbbk[x, y]$, and they cannot both be factors of f since f is irreducible. Suppose that $x \nmid f$. Then $\overline{x} \neq 0$ in $\Gamma(X)$ and $f(\overline{x}, \overline{y}) = 0$ implies that $\overline{x}$ and $\overline{y}$ are algebraically dependent in $\Gamma(X)$. Therefore the transcendence degree of $\Bbbk(X)$ must be 1.

2.33 Theorem. *If Y is a proper subvariety of $X \subseteq \mathbb{A}^m$ then* $\dim Y < \dim X$.

PROOF: Suppose that $\dim X = n$. Then any $n+1$ of the coordinate functions $x_1, \ldots, x_m$ are algebraically dependent as elements of $\Bbbk(X)$, and also as elements of $\Bbbk(Y)$. Therefore $\dim Y \leq \dim X$. Suppose that $\dim Y = \dim X$. We will show that $Y = X$ by showing that $I(Y) \subseteq I(X)$, a contradiction. Since $\dim Y = n$ there are coordinate functions $x_{i_1}, \ldots, x_{i_n}$ whose images are algebraically independent in $\Bbbk(Y)$. Then $x_{i_1}, \ldots, x_{i_n}$ must be algebraically independent in $\Bbbk(X)$. Let $u \in \Gamma(X)$ with $u \neq 0$. Then u depends algebraically on $x_{i_1}, \ldots, x_{i_n}$, *i.e.* there is a polynomial $a \in \Bbbk[t_1, \ldots, t_{n+1}]$ such that

$$a(u, x_{i_1}, \ldots, x_{i_n}) = a_k(x_{i_1}, \ldots, x_{i_n})u^k + \cdots + a_0(x_{i_1}, \ldots, x_{i_n})$$

is zero on X. Since $\Gamma(X)$ is a domain we may assume a is irreducible and $a_0(x_{i_1}, \ldots, x_{i_n})$ is non-zero on X. Note that $a(u, x_{i_1}, \ldots, x_{i_n})$ is also non-zero on Y. Suppose that $u = 0$ on Y. But then $a_0(x_{i_1}, \ldots, x_{i_n}) = 0$ on Y, a contradiction since $x_{i_1}, \ldots, x_{i_n}$ are algebraically independent in Y. Since $u \neq 0$ on X implies $u \neq 0$ on Y we have that $I(Y) \subseteq I(X)$. □

It follows that if $\dim X = 0$ then X is a point.

2.34 Theorem. *Every irreducible hypersurface in $\mathbb{A}^n$ has codimension 1.*

PROOF: Let $X = V(f)$, where $f \in \Bbbk[x_1, \ldots, x_n]$ is irreducible and non-constant. Suppose that x_n appears in the expression of f. Then $x_1, \ldots, x_{n-1}$ are algebraically independent in X, since if not there is a polynomial g that involves only the variables $x_1, \ldots, x_{n-1}$ that is zero on X. This implies that $g \in I(X) = \langle f \rangle$, so $f \mid g$ and x_n appears in the expression for g, leading to a contradiction. Therefore $\dim X \geq n-1$. The last theorem implies that $\dim X = n-1$, so $\operatorname{codim} X = 1$. □

2.35 Theorem. *Let X be a affine variety and Y be a subvariety of X that is the zero set of an irreducible non-constant polynomial $f \in \Gamma(X)$. Then Y has codimension 1 in X.*

PROOF: Needs "Noether's Normalization Lemma". □

2.36 Corollary. *If $Y \subsetneqq X \subseteq \mathbb{A}^n$ has codimension r in X then there exist irreducible closed subsets $Y_1, \ldots, Y_r$ of X of codimension $1, \ldots, r$, respectively, such that $Y = Y_r \subsetneqq Y_{r-1} \subsetneqq \cdots \subsetneqq Y_1$.*

2.37 Corollary (Topological characterization of dimension). *The dimension of an affine variety X is the largest integer d for which there exists a chain of non-empty irreducible closed subsets*

$$X_0 \subsetneqq X_1 \subsetneqq \cdots \subsetneqq X_d = X$$

The dimension of a ring can be defined to be the length of the longest chain of prime ideals in that ring. By applying I to the chain above we see that the dimension of $\Gamma(X)$ is equal to $\dim X$, since each $I(X_i)$ is a prime ideal and the inclusions are strict, and any chain of prime ideals in $\Gamma(X)$ gives rise to a chain of irreducible closed subsets of X.

Remark. What is true when $\Bbbk$ is not algebraically closed or X is not irreducible?

1. If $X = X_1 \cup \cdots \cup X_r$ is a decompostion then we set $\dim X = \max_{1 \leq i \leq r} \{\dim X_i\}$
2. The quotient ring $\Bbbk[x_1, \ldots, x_n]/I(X)$ is well-defined for any field and any algebraic set X. However, it is an integral domain if and only if X is irreducible (whether or not $\Bbbk$ is algebraically closed).
3. Polynomial maps, pullbacks, *etc.* are all defined for any $\Bbbk$ and any X. In particular, if $\varphi : X \to Y$ is dominant then $\varphi^* : \Gamma(Y) \to \Gamma(X)$ is injective.
4. We need algebraic closure to say that $\mathscr{O}(X) = \Gamma(X)$.

3 Local Properties of Varieties

For this section, let X be an affine variety in $\mathbb{A}^n = \mathbb{A}^n(\Bbbk)$, where $\Bbbk$ is algebraically closed.

3.1 Properties of the Local Ring at a Point

Recall that $\Gamma(X)$ is the ring of polynomials on X, a domain, and $\Gamma(X) \cong \mathscr{O}(X)$ since $\Bbbk$ is algebraically closed. $\mathscr{O}_p(X)$ is the ring of rational functions that are regular at $p \in X$, a local ring. The unique maximal ideal is $M_p(X) = \{f \in \mathscr{O}_p(X) \mid f(p) = 0\}$. The ring of rational functions on X is denoted $\Bbbk(X)$ and we have $\Gamma(X) \subseteq \mathscr{O}_p(X) \subseteq \Bbbk(X)$.

3.1 Theorem. *$\Gamma(X)$ and $\mathscr{O}_p(X)$ are Noetherian.*

PROOF: Let $\pi : \Bbbk[x_1, \ldots, x_n] \to \Gamma(X)$ be the canonical projection. We know that for any ideal $J \subseteq \Gamma(X)$ that $\pi^{-1}(J)$ is an ideal and $\pi(\pi^{-1}(J)) = J$. If $J_1, J_2, \ldots$ were an ascending chain of ideals in $\Gamma(X)$ then the corresponding ascending chain of ideals $\pi^{-1}(J_1), \pi^{-1}(J_2), \ldots$ must terminate since the polynomial ring is Notherian. But this implies that $J_1, J_2, \ldots$ terminates as well.

Now consider an ideal $J \subseteq \mathcal{O}_p(X)$. Then $J \cap \Gamma(X)$ is an ideal of $\Gamma(X)$. Therefore it is finitely generated, say by $f_1, \ldots, f_r$. We shall show that these also generate J in $\mathcal{O}_p(X)$, which will show that $\mathcal{O}_p(X)$ is Noetherian. Let $f \in J$. Since f is regular at p there is a polynomial $b \in \Gamma(X)$ such that $b(p) \neq 0$ and $bf \in \Gamma(X)$. In fact, $bf \in J \cap \Gamma(X)$, so can be expressed as a linear combination of $f_1, \ldots, f_r$. Therefore f can be expressed as a linear combination of rational functions regular at p (this is seen by dividing by b). □

Notation. Let $R \subseteq S$ be two rings with identity and let $I \subseteq R$ be an ideal. IS denotes the ideal in S generated by I. Note that $I \subseteq IS$, but the inclusion may be strict.

Since $\Gamma(X) \subseteq \mathcal{O}_p(X)$ we have the following natural correspondence between the ideals

$$I \mapsto I\mathcal{O}_P(X) \qquad \text{and} \qquad J \cap \Gamma(X) \leftarrow J$$

Notice that $I\mathcal{O}_p(X) \mapsto I\mathcal{O}_p(X) \cap \Gamma(X) \supseteq I$, but the containment may be strict. This is not a one to one correspondence. Indeed, let I be the maximal ideal in $\Gamma(X)$ corresponding to the point $q \in X$. If $q \neq p$ then at least one of their coordinates differ, say the i^{th}. Then $x_i - q_i \in \Gamma(X)$ is a unit in $\mathcal{O}_p(X)$ (since $p_i - q_1 \neq 0$), implying that $I\mathcal{O}_p(X) = \mathcal{O}_p(X)$, so $I \subsetneq \Gamma(X) = I\mathcal{O}_p(X) \cap \Gamma(X)$.

Nonetheless, if I is a prime or radical ideal that is not maximal then $I = I\mathcal{O}_p(X) \cap \Gamma(X)$, giving a correspondence between non-maximal prime (or radical) ideals in $\Gamma(X)$ and prime (or radical) ideals in $\mathcal{O}_p(X)$. $I \subseteq \Gamma(X)$ maximal implies that $I\mathcal{O}_p(X) = \mathcal{O}_p(X)$ unless $I = M_p(X)$. $I \subseteq M_p(X)$ is prime if and only if $I = (I\mathcal{O}_p(X)) \cap \Gamma(X)$.

3.2 Multiple Points and Tangent Lines

Recall that we defined an affine plane curve to be the zero set in $\mathbb{A}^2$ of a polynomial $f \in \Bbbk[x, y]$. If this polynomial is reducible then its zero set may have more than one component. If $f = f_1^{m_1} \cdots f_r^{m_r}$ with $f_1, \ldots, f_r$ irreducible polynomials, then $V(f) = V(f_1) \cup \cdots \cup V(f_r)$. Moreover, if one of the multiplicities m_i is greater than 1, one loses information given by the equation of the curve by only considering its zero set. It is sometimes useful to keep track of multiplicities when considering the pole sets of rational function or intersections of varieties.

3.2 Definition. An *affine plane curve* is defined to be an equivalence class of polynomials in $\Bbbk[x, y]$, where $f \sim g$ if and only if $f = \lambda g$ for some $\lambda \in \Bbbk$.

Of course, if f is irreducible then the affine plane curve corresponding to f is $V(f)$, a variety in $\mathbb{A}^2$.

3.3 Definition. Let C be an affine plane curve in $\mathbb{A}^2$ given by $f \in \Bbbk[x, y]$ and let $p = (a, b) \in C$. p is said to be *smooth* (or *simple*) if and only if $\nabla f(a, b) \neq (0, 0)$. This is equivalent to the existence of a normal vector to the curve at p. In this case, there is a *tangent line* L to C at p given by $\nabla f(a, b) \cdot (x - a, y - b) = 0$. A point that is not smooth is called *singular* (or *mulitple*). A curve that is smooth at every point is called *non-singular*.

Remark. Partial differentiation of polynomials makes sense over any field, one just applies the normal rule of differentiation formally. In particular, the derivative of a polynomial is a polynomial.

3.4 Example.
1. $y - x^2$ is non-singular since its gradient is $(-2x, 1)$, which is never $(0, 0)$.
2. $y^2 - x^3$ has a singular point at $(0, 0)$ since its gradient is $(-3x^2, 2y)$ with is $(0, 0)$ at $(0, 0)$.
3. $r - \sin\theta$ (in polar coordinates) has a triple point. In Cartesian coordinates the curve is $(x^2 + y^2)^2 - 3x^2y + y^3$, which is seen to be singular at $(0, 0)$.
4. The double line $x^2 = 0$ is singular at every point on it.

3.5 Definition. The *tangent space* to C at $p = (a, b)$ is defined to be $T_p(C) = \{a \in \mathbb{A}^2 \mid \nabla f(a, b) \cdot v = 0\}$. $T_p = \mathbb{A}^2$ if and only if p is singular.

3.6 Theorem. *p is smooth if and only if* $\dim_{\Bbbk}(T_p(C)) = \dim C$.

3.7 Definition. A homogeneous polynomial of degree m is called an *m-form*.

Consider $M_p = \langle x, y\rangle$, the maximal ideal of $p = (0,0)$. Then $M_p^2 = \langle x^2, xy, y^2\rangle$, $M_p^3 = \ldots$, and the collection of all m-forms is M_p^m/M_p^{m+1}. These are all $\Bbbk$-vector spaces.

Let us fix the origin $p = (0,0)$ in $\mathbb{A}^2$. Then every 1-form is a differential form, *i.e.* a linear function that vanishes at $(0,0)$, which is isomorphic to $(\mathbb{A}^2)^*$.

Given any $g \in \Bbbk[x,y]$,

$$d_p g = \frac{\partial g}{\partial x}(p)x + \frac{\partial g}{\partial y}(p)y$$

the differential of g at $(0,0)$. This corresponds to the Jacobian matrix $[\frac{\partial g}{\partial x}(p), \frac{\partial g}{\partial y}(p)]$ in $(\mathbb{A}^2)^*$. It follows that $T_p(C) = \ker(d_p f)$, where C is given by f. There is a map $d_p : \Bbbk[x,y] \to (\mathbb{A}^2)^* : g \mapsto d_p g$. Since $d_p \alpha = 0$ for any constant polynomial α, we restrict this map to M_p. $d_p : M_p \to (\mathbb{A}^2)^*$ is linear, surjective, and $\ker(d_p) = M_p^2$. Therefore $M_p/M_p^2 \cong (\mathbb{A}^2)^*$.

Suppose that $C = V(f)$ passes through $p = (0,0)$. On $\Gamma(C)$, if $\overline{g} \in \Gamma(C)$ then $g = G + f \cdot H$ where $G, H \in \Bbbk[x,y]$. But $d_p\overline{g} = d_p G = d_p f \cdot H + f(p) \cdot d_p(H) = d_p G$. In particular, $d_p\overline{g}$ is independetnt of the choice of representative of $\overline{g}$, so d_p is well-defined on $\Gamma(C)$ and descends to the map $d_p : M_p \to (T_p(C))^*$, where M_p is the maximal ideal of p in $\Gamma(C)$. Hence $M_p/M_p^2 \cong (T_p(C))^*$.

Finally, on $\mathcal{O}_p(C)$, if $g \in \mathcal{O}_p(C)$ then $g = \frac{a}{b}$ where $b(p) \neq 0$. Therefore $d_p g = \frac{d_p a \cdot b(p) - a(p) \cdot d_p b}{b(p)^2}$. If $g \in M_p(C)$ then $g(p) = a(p) = 0$, so $d_p g = \frac{d_p a}{b(p)}$, so as before $d_p : M_p(C)/M_p^2(X) \cong (T_p(C))^*$, a $\Bbbk$-vector space dual to the tangent of C at p and is called the *cotangent space* of C at p.

3.8 Example.

1. Let C be the parabola $y - x^2$. C is smooth at every point and $\Gamma(C) = \Bbbk[t]$. Therefore at $p = (0,0)$, $M_p = \langle t\rangle$ and $M_p/M_p^2 = \{at \mid a \in \Bbbk\}$.
2. Let C be defined by $y^2 - x^3$, which is singular at the origin $p = (0,0)$. Here $\Gamma(C) = \Bbbk[x,y]/\langle y^2 - x^3\rangle$ and $M_p = \langle \overline{x}, \overline{y}\rangle$, while $M_p/M_p^2 = \{a\overline{x} + b\overline{y} \mid a, b \in \Bbbk\}$. Since this has dimension two, we know that p is a singular point.

3.9 Theorem. *Let C be a curve in $\mathbb{A}^2$ given by $f(x,y)$. Then $p \in C$ is smooth if and only if $M_p(C)$ is principal. In this case, $M_p = \langle t\rangle$, where $t = 0$ is the equation of any line through p that is not parallel to the tangent line of C at p.*

PROOF: Suppose that C is smooth at p. By making an appropriate affine transformation, we may assume that $p = (0,0)$ and that the tangent line at p is $y = 0$. Let us show that M_p is generated by $\overline{x}$. By the above assumptions $f(0,0) = 0$, so it has no constant term. That the tangent line at $(0,0)$ is $y = 0$ implies that the linear term in x also has coefficient 0. Therefore $f(x,y) = y +$ higher order terms. Grouping the terms with y, we get $f = yg - x^2 h$, where g is a unit in $\mathcal{O}_p(C)$ and $h \in \Bbbk[x]$. Taking residue classes, we get that $0 = \overline{f} = \overline{y}\,\overline{g} - \overline{x}^2\overline{h}$, so $\overline{y} = \overline{g}^{-1}\overline{h}\overline{x}^2$. Therefore $\overline{y} \in \langle\overline{x}\rangle$, so $M_p = \langle\overline{x}, \overline{y}\rangle = \langle\overline{x}\rangle$ is principal.

Conversely, if the maximal ideal is principal then $M_p = \langle t\rangle$, so that $M_p^2 = \langle t^2\rangle$ and $M_p/M_p^2 = \{at \mid a \in \Bbbk\}$, which is a one dimensional $\Bbbk$-vector space. This implies that C is smooth at p. □

3.10 Corollary. *If p is smooth and $M_p = \langle t\rangle$ then any function in $\mathcal{O}_p(C)$ can be expressed as a power series in t.*

PROOF: Let $g \in \mathcal{O}_p(C)$ and set $\alpha_0 = g(p)$. Then $g_1 = g - \alpha_0 \in M_p = \langle t\rangle$. Since $M_p/M_p^2 = \{at \mid a \in \Bbbk\}$, $g_1 = t(\alpha_1 +$ higher order terms). Continuing, $g_2 = g - \alpha_1 - \alpha_1 t \in M_p^2$, so $g_2 = (b_1 t + \cdots)(b_2 t + \cdots) = \alpha_2 t^2 + \cdots$. This leads to an expression $g = \alpha_0 + \alpha_1 t + \alpha_2 t^2 + \cdots \in \Bbbk[[t]]$. □

3.11 Definition. A *discrete valuation ring (DVR)* is a PID that is not a field and that has a unique maximal ideal (*i.e.* is *local*). Equivalently, a DVR is a local Noetherian ring whose maximal ideal is principal.

By 3.9, at any smooth point p on C, $\mathcal{O}_p(C)$ is a DVR. DVR's have the following important property. If R is a DVR with maximal ideal $M = \langle t \rangle$, then an non-zero element $z \in R$ can be expressed as uniquely as $t^n u$ where n is a non-negative integer and u is a unit. (If z is not a unit then $z \in M$, so $z = z_1 t$. By induction we get a sequence $z_i = z_{i+1} t$ of elements that generate an ascending chain of ideals. Since R is Noetherian this chain ends, say at z_n, so $z = t^n u$. Finally, suppose $t^n u = t^m v$. Then $t^{n-m} = vu^{-1}$, a unit, which implies that $n = m$ and $u = v$.) This gives a *valuation* on R, $n = \operatorname{ord} z$. There is also an induced order on the field of fractions, given by $\operatorname{ord} \frac{a}{b} = \operatorname{ord} a - \operatorname{ord} b$.

The local ring $\mathcal{O}_p(C)$ is said to be a valuation ring of the function field $\Bbbk(C)$. More generally, if $K/\Bbbk$ is any field extension over $\Bbbk$, set $C_K =$ set of all valuation rings in $K/\Bbbk$. Then an *abstract nonsingular curve* is defined as an (open) subset of C_K.

3.12 Definition. One can define the tangent line by considering its intersection with the curve. Let us first define the *intersection multiplicity* of a line L with the curve C, given by f, at the point p. Without loss of generality, we can assume that $p = (0,0)$ and $f(0,0) = 0$, otherwise simply translate. Therefore, since $f(0,0) = 0$, the polynomial f does not have a constant term. Moreover, L is a line through the origin given by the equation $v_2 x - v_1 y = 0$, where $v = (v_1, v_2)$ is a direction vector of L. Then the intersection of L and C is the zero set of the single variable polynomial $g(t) = f(tv_1, tv_2) = t^m p(t)$, with $p(0) \neq 0$. We set m to be the *intersection* muliplicity of L and C. L is *tangent* to C if $m \geq 2$.

3.13 Example. For $C : y - x^2$ and $L : (v_1 t, v_2 t)$, $f(v_1 t, v_2 t) = t(v_2 - t v_1)$, so L is tangent to C if and only if v_2 is zero (and v_1 is not).

In general, if $f = f_m + f_{m+1} + \cdots + f_d$, where each f_i is an i-form and $f_m \neq 0$, and m is minimal. Note that since $f_i = a_0 x^i + a_1 x^{i-1} y + \cdots + a_i y^i$, we have $f_i(v_1 t, v_2 t) = t^i f_i(v_1, v_2)$. Therefore the intersection multiplicity is at least m, since $g(t) = f(v_1 t, v_2 t) = t^m [f_m(v_1, v_2) + \cdots + t^{d-m} f_d(v_1, v_2)]$. Thus if $m \geq 2$ then every line through p is tangent to C at p. However, there are "preferred" tangent lines. If the muliplicity of L is at least $m+1$ then L is called a *tangent direction*. In particular, this means that $f_m(v_1, v_2) = 0$, so $v_2 x - v_1 y$ is a linear factor if f_m.

3.14 Example.

1. For $C : y - x^2$ again, the decomposition is $(y) + (-x^2)$, and $y = 0$ is the tangent direction (line).
2. For $C : y^2 - x^3$, the decomposition is $(y^2) + (-x^3)$, and the tangent direction is again $y = 0$, but this time it has multiplicity 2.
3. For $C : y^2 - x^2 - x^3$, the decomposition is $(y^2 - x^2) + (-x^3)$, and the tangent directions are $y - x = 0$ and $y + x = 0$.

The tangent directions are the tangent lines of the (smooth) components of the curve in a neighbourhood of $p = (0,0)$. If the multiplicity of the tangent direction is 1, it is called *simple*, otherwise *double*, *triple*, *etc*. Moreover, a singular point is called an *ordinary double point* if is has 2 distinct tangent directions. In general, if a singular piont has multiplicity m then it is called *ordinary* if it has m distinct tangent directions.

3.15 Example. For $C : r = \sin 3\theta$ (the same curve as $(x^2 + y^2)^2 - 3x^2 y + y^3 = 0$) has a triple ordinary point since $-3x^2 y + y^3 = y(y - \sqrt{3}x)(y + \sqrt{3}x)$. There are 3 tangent lines $y = 0$, $y = \sqrt{3}x$, and $y = -\sqrt{3}x$ at the origin.

If p is not smooth on C, one can still describe regular functions at p in terms of power series, except that in this case the power series expression may not be unique. Indeed, $M_p(C) = \langle \overline{x}, \overline{y} \rangle$ with $\overline{x}$ and $\overline{y}$ algebraically independent (since $f = f_m + \cdots + d_d$ with $m \geq 2$) and $M_p / M_p^2 = \{a\overline{x} + b\overline{y} \mid a, b \in \Bbbk\}$, so $\dim_{\Bbbk} M_p / M_p^2 = 2$.

3.16 Theorem. *Let $p = (0,0)$ be a point on the irreducible curve C, given by f. Then*

$$m_p(f) = \dim_{\Bbbk}(M_p^r / M_p^{r+1})$$

for all sufficiently large r. In particular, the multiplicity of f at p only depends on the local ring $\mathcal{O}_p(C)$.

Any curve has at most a finite number of singular points (because they are solutions to $\nabla f = 0$). Singularities can be removed by a process called *blowing up*.

3.3 Non-Singular Varieties

3.17 Definition. Let $X = V(f) \subseteq \mathbb{A}^n$, where f is an irreducible polynomial. Then X is *non-singular* (or *smooth*) at a point $p \in X$ if $\nabla f(p) \neq 0$. The *tangent space* is $T_p(X) = \{v \in \mathbb{A}^n \mid \nabla f(p) \cdot v = 0\}$.

If p is smooth thne T_p is a hyperplane, so that $\dim_{\Bbbk}(T_p(X)) = n - 1 = \dim X$. Otherwise $T_p(X) = \mathbb{A}^n$, so p is smooth if and only if $\dim_{\Bbbk}(T_p(X)) = \dim X$. On the intersection of irreducible hypersurfaces in $\mathbb{A}^3$, $C = V(f) \cap V(g)$, C is non-singular at p if and only if there are unique tangent planes to $V(f)$ and $V(g)$ at p and these planes are not parallel. In other words, the Jacobian of f and g must have rank 2. The tangent line to C at p will then be the intersection of these planes.

3.18 Definition. In general, if X is an r-dimensional variety in $\mathbb{A}^n$ whose ideal is generated by $f_1, \ldots, f_s$, we define the Jacobian matrix of $f_1, \ldots, f_s$ at p to be

$$\mathrm{Jac}(f_1, \ldots, f_s)(p) = \left[\frac{\partial f_i}{\partial x_j}(p) \right]_{s \times n}$$

Moreover, $T_p = \ker(\mathrm{Jac}(f_1, \ldots, f_s)(p))$, the tangent space of X at p. X is *smooth* at p if and only if $\dim_{\Bbbk}(T_p(X)) = \dim X = r$, which happens if and only if $\mathrm{rank}(\mathrm{Jac}(f_1, \ldots, f_s)(p)) = n - r$.

This definition also makes sense for reducible algebraic sets. One simply gets more singular points, *e.g.* point in the intersection of components may be singular.

3.19 Example.
1. $V(x^2 + x^3 - y^2) \subseteq \mathbb{A}^3$ has a double line of singularities at $z = 0$.
2. The cone $x^2 + y^2 = z^2$ has a singular point at $(0,0,0)$ since the Jacobian is $\begin{bmatrix} 2x & 2y & -2z \end{bmatrix}$, which is the zero matrix at the origin.

One can show that this definition of smoothness (non-singularity) is independent of the choice of generators of the ideal of the variety. In particular, it depends only on the local ring at p. Again, $M_p(X)/M_p(X)^2$ is a $\Bbbk$-vector space of 1-forms, the *cotangent space*, and $T_p(X) = (M_p/M_p^2)^*$. By this definition, the tangent space is sometimes known as the *Zariski tangent space*. The definition of smoothness is the same.

3.4 Blowing-Up Singularities

3.20 Definition. The *graph* of a rational function $f : X \subseteq \mathbb{A}^n \to Y \subseteq \mathbb{A}^m$ is the closure of

$$W = \{(x, f(x)) \mid x \in X\} \subseteq X \times Y$$

with respect to the induced Zariski topology from $\mathbb{A}^{n+m}$.

3.21 Definition. The *local blow-up* of $\mathbb{A}^n$, denoted $\widetilde{\mathbb{A}^n}$ is the graph of a projection from a point $p \in \mathbb{A}^n$ onto a hyperplane in $\mathbb{A}^n$.

For $n = 2$, $p = (0,0)$, and the line $x = 1$, the line L through the origin and a point $(x,y) \in \mathbb{A}^n$ is (xt, yt) (for $t \in \Bbbk$). The intersection of this line with $x = 1$ is $(1, \frac{y}{x})$, as long as $x \neq 0$. This gives the rational map $\pi : \mathbb{A}^2 \to \mathbb{A}^1 \cong V(x-1) : (x,y) \mapsto \frac{y}{x}$ (here π is defined on $U = \mathbb{A}^2 \setminus V(x)$). The blow-up is $\widetilde{\mathbb{A}^2} = \{(x,y,u) \mid u = \frac{y}{x}\} = V(y - ux) \subseteq \mathbb{A}^3$. There is a natural projection $P : \widetilde{\mathbb{A}^2} \to \mathbb{A}^2 : (x,y,u) \mapsto (x,y)$.

What's going on here? u is the slope of the line through the origin and (x,y). We call $P^{-1}(0,0) = \{(0,0,u) \mid u \in \Bbbk\} \cong \mathbb{A}^1$ the *exceptional curve*. When $x \neq 0$, $P^{-1}(x,y) = \{(x,y,\frac{y}{x})\}$, so P is off of the y-axis in $\mathbb{A}^2$. $P^{-1}(0,y) = \varnothing$ if $y \neq 0$ (this will change in projective space). Finally, the image of P is $(\mathbb{A}^2 \setminus V(x)) \cup \{(0,0\}$, which is dense in $\mathbb{A}^2$, so P is a dominant rational map. In fact, P is a birational equivalence of $\mathbb{A}^2$ with $\widetilde{\mathbb{A}^2}$.

3.22 Definition. If X is a variety, the *blow-up* (or *proper transform*) of X at $p = (0,0)$, denoted $\widetilde{X}$, is (the irreducible algebraic set) $\overline{P^{-1}(X \setminus \{(0,0)\}}$.

3.23 Example.
1. Consider $X = V(y^2 - x^3)$. The Jacobian of X is $\begin{bmatrix} 3x^3 & 2y \end{bmatrix}$, which is rank zero at $(0,0)$. Therefore X has a singularity at $(0,0)$.

   Notice that $P^{-1}(X) = V(y^2 - x^3, y - xu)$, an algebraic set, and its irreducible components are $V(x,y) \cup V(x = u^2, y = u^3)$. But $V(x,y)$ is the exceptional curve. The other component is the twisted cubic, which is smooth because $\left[\begin{smallmatrix} 1 & 0 & 2u \\ 0 & 1 & 3u^2 \end{smallmatrix}\right]$ is rank 2 everywhere. Here $\widetilde{X}$ is the twisted cubic, so the singularity disappears.
2. Let $X = V(y^2 - x^3 - x^2)$, so now $(0,0)$ is a multiple point. $P^{-1}(X \setminus \{(0,0)\}) = V(x - (u^2+1), y - u(u^2+1))$ which is non-singular.

Remark.
1. If one blows up $\mathbb{A}^2$ using the projection from $(0,0)$ onto $y = 1$ then $\widetilde{\mathbb{A}^2} = V(x - yu) \subseteq \mathbb{A}^3$.
2. Since any line in $\mathbb{A}^2$ can be transformed into $x = 1$ by and affine transformation, we see that all blowups are isomorphic.

3.24 Definition. In general, the *(local) blow-up* of $\mathbb{A}^n$ at $(0,\ldots,0)$ is defined as

$$\widetilde{\mathbb{A}^n} = V(x_2 - u_1 x_1, \ldots, x_n - u_{n-1} x_1)$$

It is obtained as the graph of the projection from $(0,\ldots,0)$ onto the hyperplane $x_i = 1$, where $\{x_1,\ldots,x_n\}$ are coordinates in $\mathbb{A}^n$ and $\{u_1,\ldots,u_{n-1}\}$ are coordinated in $\mathbb{A}^{n-1}$. If $X \subseteq \mathbb{A}^n$ is a variety, the *blow-up* of X is

$$\widetilde{X} = \overline{P^{-1}(X \setminus \{(0,\ldots,0)\})}$$

where $p : \widetilde{\mathbb{A}^n} \to \mathbb{A}^n$ is the natural projection.

Remark.
1. A blow-up is also known as a σ*-process* or a *monomial transformation*.
2. Once can show that by performing repreated blow-ups on a curve X at singular points, one eventually gets a non-singular curve, called the *desingularization* of X. Note that the desingularization of X is birational to X. This process is known as *resolving the singularities* of X.

4 Projective Space

4.1 Projective Varieties

4.1 Definition. Projective n-space is $\mathbb{P}^n = \mathbb{P}^n(\Bbbk) = (\mathbb{A}^{n+1} \setminus \{(0,\ldots,0)\})/\Bbbk^*$. Given a point $p \in \mathbb{P}^n$, if $(x_1,\ldots,x_{n+1})$ is any representative of the equivalence class then we write $p = [x_1 : \cdots : x_{n+1}]$, a *homogeneous coordinate*.

Remark.
1. $\mathbb{P}^n$ can be thought of as the collection of all one dimensional subspaces of the vector space $\mathbb{A}^{n+1}$.

2. $\mathbb{P}^n$ may be thought of as $n+1$ copies of affine n-space. Indeed, for each $i = 1, \dots, n+1$, the set

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

is isomorphic to $\mathbb{A}^n$ *via* $[x_1 : \cdots : x_{n+1}] \mapsto (\frac{x_1}{x_i}, \dots, \hat{x}_i, \dots, \frac{x_{n+1}}{x_i})$. In particular, $\mathbb{A}^n$ can be considered as a subspace of $\mathbb{P}^n$, where the inclusion is $\mathbb{A}^n \cong U_{n+1} \subseteq \mathbb{P}^n$.

For each i, define $H_i = \{[x_1 : \cdots : x_{n+1}] \mid x_i = 0\} = \mathbb{P}^n \setminus U_i$, a *hyperplane*, which can be identified with $\mathbb{P}^{n-1}$. In particular, H_{n+1} is often denoted H_∞ and is called the *hyperplane at infinity*. Then $\mathbb{P}^n = U_{n+1} \cup H_\infty \cong \mathbb{A}^n \cup \mathbb{P}^{n-1}$.

4.2 Example. 1. $\mathbb{P}^0 = \{\infty\}$ is a single point.

2. $\mathbb{P}^1 = \mathbb{A}^1 \cup \mathbb{P}^0 = \mathbb{A}^1 \cup \{\infty\}$, the one point compactification of $\mathbb{A}^1$.

3. $\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$, where the copy of $\mathbb{P}^1$ here is often called the *line at infinity*.

Curves in $\mathbb{A}^n$ correspond to curves in $\mathbb{P}^n$ since we can identify $\mathbb{A}^n$ with U_{n+1}. That is, the curve $f(x_1, \dots, x_n) = 0$ is identified with the curve $f(\frac{x_1}{x_{n+1}}, \dots, \frac{x_n}{x_{n+1}}) = 0$ in $\mathbb{P}^n$. In particular, the line $ax + by + c = 0$ in $\mathbb{A}^2$ corresponds to the line $ax + by + cz = 0$ in $\mathbb{P}^2$. If we have distinct parallel lines in $\mathbb{A}^2$ then they will intersect at $[b : -a : 0]$ in $\mathbb{P}^2$.

If $f \in \Bbbk[t_1, \dots, t_{n+1}]$ and $p \in \mathbb{P}^n$ then $f(p) = 0$ implies that $f(\lambda x_1, \dots, \lambda x_{n+1}) = 0$ for every $\lambda \in \Bbbk^*$. If $f = f_m + \cdots + f_d$ is a decomposition of f into i-forms f_i, then

$$0 = f(\lambda x_1, \dots, \lambda x_{n+1}) = \lambda^m f_m(x_1, \dots, x_{n+1}) + \cdots + \lambda^d f_d(x_1, \dots, x_{n+1})$$

Since $\lambda \neq 0$ and $\Bbbk$ is algebraically closed (hence infinite), this implies that each coefficient of this polynomial in λ is zero. Therefore $f(\lambda x_1, \dots, \lambda x_{n+1}) = 0$ if and only if $f_m(x_1, \dots, x_{n+1}) = \cdots = f_d(x_1, \dots, x_{n+1}) = 0$.

4.3 Definition. If $S \subseteq \Bbbk[t_1, \dots, t_{n+1}]$ is any set of polynomials then

$$V(S) := \{[x_1 : \cdots : x_{n+1}] \in \mathbb{P}^n \mid f(p) = 0 \text{ for all } f \in S\} = V(T)$$

where T is the set of homogeneous components of the polynomials in S. A *(projective) algebraic set* in $\mathbb{P}^n$ is the zero set of a set of homogeneous polynomials in $\Bbbk[t_1, \dots, t_{n+1}]$.

Notice that, up to powers of t_{n+1}, factoring a form $f \in \Bbbk[t_1, \dots, t_{n+1}]$ is the same as factoring $\frac{f}{t_{n+1}^d}$ where $d = \deg f$. Indeed, $\frac{f}{t_{n+1}^d}$ may simply be thought of as a polynomial of degree at most d in variables $\frac{t_1}{t_{n+1}}, \dots, \frac{t_n}{t_{n+1}}$. In particular, if $f \in \Bbbk[x, y]$ is a form then, since $\Bbbk$ is algebraically closed, f factors into a product of linear factors. *e.g.*

$$f(x, y) = y^3 + 2xy^2 + 4x^2y + 8x^3 = y^3(1 + 2(\tfrac{x}{y}))(1 + 4(\tfrac{x}{y})^2) = (y + 2x)(2x + iy)(2x - iy)$$

4.4 Theorem. *In $\mathbb{P}^1(\Bbbk)$, the algebraic sets are $\varnothing$, finite sets of points, and $\mathbb{P}^1$.*

PROOF: Clearly $\varnothing = V(1)$, $\mathbb{P}^1 = V(0)$ and $\{[a : b]\} = V(bx - ay)$. Conversely, let $X = V(T)$ where $T \subseteq \Bbbk[x, y]$ is a set of homogeneous polynomials. Then if $T = \varnothing$ or T only consists of constant polynomials, then $X = \varnothing$ or $X = \mathbb{P}^1$. Otherwise, there is a non-constant homogeneous polynomial $f \in T$. Then f factors into a product of linear factors $f = (\alpha_1 x + \beta_1 y) \cdots (\alpha_d x + \beta_d y)$, so $V(f) = \{[\beta_1 : -\alpha_1], \dots, [\beta_d : -\alpha_d]\}$, a finite set of points. $X \subseteq V(f)$, so X is at most a finite set of points. □

4.5 Proposition. *The algebraic sets form the closed sets for a topology on $\mathbb{P}^n$. Namely*

1. *The union of two algebraic sets is an algebraic set.*

2. *The intesection of a collection of algebraic sets is algebraic.*
3. *$\varnothing$ and $\mathbb{P}^1$ are algebraic.*

4.6 Definition. The topology given by taking the closed sets to be the algebraic sets is again known as the *Zariski topology* on $\mathbb{P}^n$. A non-empty closed subset of $\mathbb{P}^1$ is *irreducible* if it cannot be expressed as the union of two proper closed subsets.

Remark. For example, $\mathbb{P}^1$ is irreducible. As before, any algebraic set can be decomposed uniquely as a finite union of irreducible algebraic sets. For each $i = 1, \ldots, n+1$, $H_i = V(x_i)$ is a closed set and $U_i = \mathbb{P}^n \setminus H_i$ is an open set. Therefore $\{U_i\}_{i=1}^{n+1}$ is a (finite) open cover of $\mathbb{P}^n$.

4.7 Definition. A *(projective algebraic) variety* (or *projective variety*) is an irreducible algebraic set in $\mathbb{P}^n$ with the induced Zariski topology.

4.2 Homogeneous Ideals

4.8 Definition. An ideal $I \subseteq \Bbbk[x_1, \ldots, x_n]$ is called *homogeneous* if and only if whenever $f \in I$ and $f = f_m + \cdots + f_d$ is the decomposition of f into homogeneous components, then $f_i \in I$ for each $i = m, \ldots, d$.

4.9 Example. 1. $\langle x^2 \rangle \subseteq \Bbbk[x]$ is homogeneous.
2. $I = \langle x^2 + x \rangle \subseteq \Bbbk[x]$ since $x \notin I$.

4.10 Lemma. *An ideal I is homogeneous if and only if I is generated by homogeneous polynomials.*

PROOF: Trivial. □

4.11 Proposition. *Let I and J be homogeneous ideals. Then $I + J$, $I \cap J$, and IJ are homogeneous ideals. Also, $\sqrt{I}$ is a homogeneous ideal.*

PROOF: Exercise. □

Remark. For any $Y \subseteq \mathbb{P}^n$, $I(Y)$, the *ideal* of Y, is defined as in the affine case. It turns out that $I(Y)$ is radical and homogeneous. Indeed, for any $f \in I(Y)$, $f(p) = 0$ for each $p \in Y$. Thus, if $f = f_m + \cdots + f_d$ is the decomposition of f into homogeneous polynomials then $f_i(p) = 0$ for each $i = m, \ldots, d$, so each i-form is in $I(Y)$, which implies that $I(Y)$ is homogeneous.

We therefore have the following correspondence.

$$\text{algebraic sets in } \mathbb{P}^n \longleftrightarrow \text{radical homogeneous ideals in } \Bbbk[t_1, \ldots, t_{n+1}]$$

We will see that is correspondence is almost one to one.

Notation. V_a and I_a refer to V and I in affine space, while V_p and I_p refer to V and I in projective space.

4.12 Definition. Let $\theta : \mathbb{A}^{n+1} \setminus \{0\} \to (\mathbb{A}^{n+1} \setminus \{0\})/\Bbbk^* = \mathbb{P}^n$ so that $\theta(x_1, \ldots, x_{n+1}) \mapsto [x_1 : \cdots : x_{n+1}]$. Given a subset $Y \subseteq \mathbb{P}^n$, we define $C(Y) = \theta^{-1}(Y) \cup \{(0, \ldots, 0\}$. $C(Y)$ is the *projective cone* over Y.

4.13 Proposition.

1. *If $Y \neq \varnothing$ then $I_a(C(Y)) = I_p(Y)$.*
2. *If $I \subseteq \Bbbk[t_1, \ldots, t_{n+1}]$ is homogeneous such that $V_a(I) \neq \varnothing$ then $C(V_p(I)) = V_a(I)$.*

4.14 Proposition.

1. *If $T_1 \subseteq T_2$ are sets of homogeneous polynomials then $V_p(T_2) \subseteq V_p(T_1)$.*
2. *If $Y_1 \subseteq Y_2 \subseteq \mathbb{P}^n$ then $I_p(Y_2) \subseteq I_p(Y_1)$.*
3. *For any two subsets $Y_1, Y_2 \subseteq \mathbb{P}^n$, $I_p(Y_1 \cup Y_2) = I_p(Y_1) \cap I_p(Y_2)$.*
4. *For any $Y \subseteq \mathbb{P}^n$, $V_p(I_p(Y)) = \overline{Y}$, the closure of Y in the Zariski topology.*

4.15 Theorem (Projective Nullstellenzatz). *Let $I \subseteq \Bbbk[t_1, \ldots, t_{n+1}$ be a homogeneous ideal.*

1. *$V_p(I) = \varnothing$ if and only if there exists $N \in \mathbb{N}$ such that I contains every form of degree at least N.*
2. *If $V_p(I) \neq \varnothing$ then $I_p(V_p(I)) = \sqrt{I}$.*

PROOF: The following statements are equivalent.

$$\begin{aligned} V_p(I) = \varnothing &\iff V_a(I) = \varnothing \text{ or } \{(0, \ldots, 0)\} \\ &\iff V_a(I) \subseteq \{(0, \ldots, 0)\} \\ &\iff \langle t_1, \ldots, t_{n+1} \rangle = I_a(\{(0, \ldots, 0)\}) \subseteq I_a(V_a(I)) = \sqrt{I} \end{aligned}$$

Therefore $t_i^{m_i} \in I$ for some $m_i \in \mathbb{N}$. Let $m = \max m_1, \ldots, m_{n+1}$, so that $t_i^m \in I$ for all i. Then $V_p(I) = \varnothing \iff \langle t_1, \ldots, t_{n+1} \rangle^N \subseteq I$ for some $N \geq m$ This last statement holds if and only if any form of degree at least N is contained in I.

For the second assertion, $I_p(V_p(I)) = I_a(C(V_p(I)) = I_a(V_a(I)) = \sqrt{I}$ by the affine nullstellenzatz. □

We therefore have the following one to one correspondence.

$$\text{radical homogeneous ideals } I \text{ with } V_p(I) \neq \varnothing \longleftrightarrow \text{non-empty algebraic sets in } \mathbb{P}^n$$

The empty algebraic set is usually thought of as corresponding to $\langle t_1, \ldots, t_{n+1} \rangle$. We expect to have a one to one correspondence between irreducible algebraic sets and homogeneous ideals in $\Bbbk[t_1, \ldots, t_{n+1}]$. Notice that a homogeneous ideal I is prime if and only if the primality condition holds for pairs of forms. (*i.e.* I is prime if and only if for any forms f and g then $fg \in I$ implies $f \in I$ or $g \in I$.)

4.16 Proposition. *Let $Y \subseteq \mathbb{P}^n$ be an algebraic set. Then Y is irreducible if and only if $I(Y)$ is prime.*

PROOF: Suppose that Y is irreducible. Let f and g be forms such that $fg \in I(Y)$. Then $Y \subseteq V(f) \cup V(g)$, so $Y = (Y \cap V(f)) \cup (Y \cap V(g))$. Therefore, since Y is irreducible, $Y = Y \cap V(f)$ or $Y = Y \cap V(g)$, so $f \in I(Y)$ or $g \in I(Y)$, which implies that $I(Y)$ is prime since it is homogeneous. The proof of the converse is as in the affine case. □

4.17 Example.

1. $\mathbb{P}^n$ is irreducible since $\mathbb{P}^n = V(\langle 0 \rangle)$.
2. If f is an irreducible homogeneous polynomial then $\langle f \rangle$ is homogeneous and prime, implying that its zero set $V(f)$ is irreducible. Such algebraic sets are called *hypersurfaces*.
3. We have the one to one correspondence

$$\text{homogeneous prime ideals } I \text{ such that } I \neq \langle t_1, \ldots, t_{n+1} \rangle \longleftrightarrow \text{varieties in } \mathbb{P}^n$$

4. $Y = V(x^2 + y^2 + 2yz) \subseteq \mathbb{P}^2$ is irreducible since $f = z^2((\frac{x}{z})^2 + (\frac{y}{z})^2 + 2(\frac{y}{z}))$ which is z^2 times an irreducible polynomial in $\frac{x}{z}$ and $\frac{y}{z}$, hence irreducible.

4.18 Lemma. *Y is irreducible if and only if its projective cone $C(Y)$ is irreducible.*

PROOF: Y is irreducible if and only if $I_p(Y) = I_a(C(Y))$ is prime, and this occurs if and only if $C(Y)$ is irreducible.□

4.19 Example. $Y = V_p(x - y, x^2 - yz) \subseteq \mathbb{P}^2$ is not irreducible since $C(Y) = V_a(x - y, x^2 - yz)$ is the union of two lines through the origin in $\mathbb{A}^3$. Indeed, Y is the corresponding two points in $\mathbb{P}^2$.

4.3 Regular and Rational Functions

4.20 Definition. Let $I \subseteq \Bbbk[t_1, \ldots, t_{n+1}]$ be a homogeneous ideal. Let $\Gamma = \Bbbk[t_1, \ldots, t_{n+1}]/I$. A residue class $\overline{f} \in \Gamma$ is said to be a *form of degree* d if there exists a form f of degree d in $\Bbbk[t_1, \ldots, t_{n+1}]$ whose residue class is $\overline{f}$.

4.21 Proposition. *Every element $\overline{f} \in \Gamma$ may be written uniquely as $\overline{f}_m + \cdots + \overline{f}_d$, where each $\overline{f}_i$ is a form of degree i.*

PROOF: Suppose that $\overline{f} = \overline{f}_m + \cdots + \overline{f}_d = \overline{g}_m + \cdots + \overline{g}_d$. Then $\sum_i (\overline{f}_i - \overline{g}_i) = 0$, which implies that $\sum_i (f_i - g_i) \in I$, so $f_i - g_i \in I$ since I is homogeneous. Therefore $\overline{f}_i = \overline{g}_i$ for each i. □

4.22 Definition. Let $Y \subseteq \mathbb{P}^n$ be a projective variety, so that $I(Y)$ is prime and homogeneous. Then

$$\Gamma_H(Y) = \Bbbk[t_1, \ldots, t_{n+1}]/I(Y)$$

is a domain, called the *homogeneous coordinate ring*.

Note that, unlike in the affine case, the elements of $\Gamma_H(Y)$ cannot be considered a functions unless they are constant. Indeed, if $f \in \Gamma_H(Y)$ defines a function on Y then $f(\lambda t_1, \ldots, \lambda t_{n+1}) = f(t_1, \ldots, t_{n+1})$ for all $\lambda \in \Bbbk^*$. *i.e.*, if and only if $f(\lambda t_1, \ldots, \lambda t_{n+1}) = \lambda^d f(t_1, \ldots, t_{n+1})$, where $d = \deg f$ and $\lambda \in \Bbbk^*$, which happens if and only if f is constant.

One also defines $\Bbbk_H(Y)$, the *homogeneous function field*, as the quotient field of $\Gamma_H(Y)$. This time, the only elements of $\Bbbk_H(Y)$ that define functions on Y are of the form $\frac{f}{g}$ where $f, g \in \Gamma_H(Y)$ are of the same degree. We can then define $\Bbbk(Y)$ to be the collection $\{\frac{f}{g} \mid f, g \in \Gamma_H(Y) \text{ are of the same degree}\}$. $\Bbbk(Y)$ is the *function field of* Y, whose elements are the *rational functions on* Y. We have

$$\Bbbk \subseteq \Bbbk(Y) \subseteq \Bbbk_H(Y) \qquad \text{but} \qquad \Gamma_H(Y) \not\subseteq \Bbbk(Y)$$

If $p \in Y$ and $f \in \Bbbk(Y)$ then we say that f is *defined* (or *regular*) at p if there exist forms $a, b \in \Gamma_H(Y)$ of the same degree such that $b(p) \neq 0$ (??) and $f = \frac{a}{b}$. Also, the set of points where f is not defined is called the *pole set*.

4.23 Proposition.

1. *The pole set of a rational function is algebraic.*
2. *A rational function is regular at every point in Y if and only it is constant.*

As in the affine case, one defines the local ring $\mathcal{O}_p(Y)$ of regular functions at $p \in Y$ with maximal ideal $M_p(Y)$. A rational function is completely determined by its restriction to an open set $U \subseteq Y$. In particular, if we consider $Y = Y \cap Y_{n+1}$ then $\Bbbk(Y) \cong \Bbbk(Y \cap U_{n+1})$ (considered over $\mathbb{A}^n$) and $\mathcal{O}_p(Y) \cong \mathcal{O}_p(Y \cap U_{n+1})$. We define $\dim Y$ to be the transcendence degree of $\Bbbk(Y)$ over $\Bbbk$. For example, $\dim \mathbb{P}^n = n$ since $\Bbbk(\mathbb{P}^n) \cong \Bbbk(U_{n+1}) \cong \Bbbk(\mathbb{A}^n)$

Remark.

1. In general, for $Y = V_p(f_1, \ldots, f_r) \subseteq \mathbb{P}^n$, let $Y|_{U_{n+1}} = V_a(f_1(t_1, \ldots, t_n, 1), \ldots, f_r(t_1, \ldots, t_n, 1))$. Then $\mathcal{O}_p(Y) \cong \mathcal{O}_p(Y|_{U_{n+1}})$, so that local questions about Y can be reduced to local questions about the restriction $Y|_{U_{n+1}} \subseteq \mathbb{A}^n$.
2. Let $X \subseteq \mathbb{A}^n \cong U_{n+1}$ be a variety and $I = I_a(X)$ be its ideal in $\Bbbk[t_1, \ldots, t_n]$. We define $\overline{I}^p$ to be the ideal in $\Bbbk[t_1, \ldots, t_{n+1}]$ generated by $\{t_{n+1}^d f(\frac{t_1}{t_{n+1}}, \ldots, \frac{t_n}{t_{n+1}}) \mid f \in I, d = \deg f\}$. Then I is prime if and only if $\overline{I}^p$ is prime. From this, define $\overline{X}^p = V_p(\overline{I}^p)$, the *projective closure* of X in $\mathbb{P}^n$; it is the smallest algebraic set in $\mathbb{P}^n$ that contains X. For example, if $X = V_a(yx - 1)$ then $\overline{X}^p = V_p(xy - z^2)$. Finally, it can be shown that $\overline{X}^p|_{U_{n+1}} = X$.

4.4 Varieties, Morphisms, and Rational Maps

4.24 Definition. A *quasi-affine variety* is defined to be any open subset of an affien variety. Similarily, a *quasi-projective variety* is an open subset of a projective variety.

Since any non-empty open subset of an irreducible space is irreducible, quasi-affine and quasi-projective varieties are irreducible, where *irreducibility* is defined as for algebraic sets.

4.25 Example. 1. $\mathbb{A}^1 \setminus \{0\}$
2. $GL(n,\Bbbk) = \{A \in M_n(\Bbbk) \mid \det A \neq 0\} \subseteq \mathbb{A}^{n^2}$
3. $U_i \subseteq \mathbb{P}^n$

Varieties are endowed with the induced Zariski topology. Regular and rational functions are defined as in the affine and projective cases.

4.26 Definition. Let X and Y be varieties. A *morphism* from X to Y is a function $\varphi : X \to Y$ such that φ is continuous and for every open set subset $V \subseteq Y$ and for every regular function $f : V \to \Bbbk$, the composition $f \circ \varphi : \varphi^{-1}(V) \to \Bbbk$ is regular. (This is analogous to requiring that the components of φ are regular functions.) The composition of two morphisms is a morphism, and if a morphism is bijective and its inverse is a morphism, we call it an *isomorphism*.

4.27 Example. 1. If X and Y are affine varieties then morphims are simply polynomial maps.
2. $\varphi : \mathbb{A}^1 \setminus \{0\} \to V(xy-1) \subseteq \mathbb{A}^2 : t \mapsto (t, \frac{1}{t})$ is an isomorphism since each component is regular on $\mathbb{A}^1 \setminus \{0\}$.
3. Inclusions and projections are morphisms.
4. Affine and projective coordinate changes are isomorphisms. (A projective coordinate change must map every line through the origin in $\mathbb{A}^{n+1}$ to a line in $\mathbb{A}^{n+1}$, so it is given by an $(n+1) \times (n+1)$ matrix, *i.e.* 1-forms.)
5. $\varphi : X = \mathbb{P}^1 \to Y = V_p(y^2 - xz) \subseteq \mathbb{P}^2 : [u : v] \mapsto [u^2 : uv : v^2]$ is an isomorphism. Clearly it is onto, and it is one to one since we are in projective space. The inverse is a morphism since restricting to $u \neq 0$ (*i.e.* U_1) $\varphi : [u : v] \mapsto [u : v : \frac{v^2}{u}]$, and if $v \neq 0$ then $\varphi : [u : v] \mapsto [\frac{u^2}{v} : u : v]$.

Remark. 1. Quasi-affine varieties are not necessarily affine varieties.
2. If X and Y are two isomorphic (quasi-)projective varieties then this does not necessarily imply that $\Gamma_H(X) \cong \Gamma_H(Y)$. *e.g.* $\mathbb{P}^1 \cong V_p(y^2 - xz)$ but $\Gamma_H(\mathbb{P}^1) = \Bbbk[u,v]$ while $\Gamma_H(V_p(y^2 - xz)) = \Bbbk[x,y,z]/\langle y^2 - xz \rangle$.

4.28 Proposition. *Every point p on a variety X has a neighbourhood that is isomorphic to an affine variety.*

PROOF: If X is affine then there is nothing to prove. If X is projective then consider $X \cap U_i$, where $p \in U_i$. If X is quasi-affine then consider the projective closure of X. Therefore we may assume that X is quasi-projective and $p \in X \cap U_{n+1}$. Since X is quasi-prijective, $X = \tilde{Y} \setminus \tilde{Y}_1$ for some projective variety $\tilde{Y}$ and algebraic set $\tilde{Y}_1 \subseteq \tilde{Y}$. Thus $X \cap U_{n+1} = Y \cap Y_1$, where $Y = \tilde{Y} \cap U_{n+1}$ is a variety in $U_{n+1} \cong \mathbb{A}^n$ and $Y_1 = \tilde{Y}_1 \cap U_{n+1}$ is an algebraic subset. Since $p \in Y \setminus Y_1$, there is a polynomial f in n variables such that $f \equiv 0$ on Y_1 and $f(p) = 0$. Consider $V(f) \cap Y$ and let $D(f) = Y \setminus (V(f) \cap Y)$, the open neighbourhood of p in Y, which is isomorphic to an affine variety. Indeed, suppose that $Y = V(g_1, \ldots, g_m) \subseteq \mathbb{A}^n$ and $\mathbb{A}^n$ has coordinates $x_1, \ldots, x_n$. We define $Z := V(g_1, \ldots, g_m, x_{n+1}f - 1) \subseteq \mathbb{A}^{n+1}$. Then X is isomorphic to $D(f)$ via projection (which has inverse $\varphi : Z \to D(f) : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_n, (f(x_1, \ldots, x_n))^{-1})$). Therefore the neighbourhood $D(f)$ of p is isomorphic to the affine variety $Z \subseteq \mathbb{A}^{n+1}$. □

Remark. 1. In proof of local properties, one can always assume that X is an affine variety.
2. Singular points are defined as in the affine case by using the restrictions to these open sets.

3. For any variety X, $\dim X$ is the transcendence degree of $\Bbbk(X)$ over $\Bbbk$. Since $\Bbbk(X) \cong \Bbbk(U)$ for any open neighbourhood of a point p, we have that $\dim X = \dim U$. In particualr, if $\dim X = m$ then any point p has a neighbourhood that is isomorphic to any m-dim affine variety.

4.29 Definition. A *rational map* between two varieties X and Y is defined as an equaivalence class of pairs (U, φ), where U is an open set and $\varphi : U \to Y$ is a morphism. The equivalence is defined as

$$(U, \varphi) \sim (V, \psi) \iff \varphi|_{U \cap V} = \psi|_{U \cap V}$$

One defines dominance and birational equivalence as in the affine case. We have $X \sim Y$ if and only if $\Bbbk(X) \cong \Bbbk(Y)$.

Remark.
1. A variety is called *rational* if it is birational to $\mathbb{A}^n$ or $\mathbb{P}^n$, for some n.
2. One can prove that any variety X of dimension r is birational to a hypersurface on $\mathbb{P}^{r+1}$. In particular, any curse is birational to a projective plane curve.
3. An example of a birational equivalence that is not an isomorphism is the blow-up $\widetilde{\mathbb{P}^n}$ of $\mathbb{P}^n$, which is a subvariety of $\mathbb{P}^n \times \mathbb{P}^{n-1}$. It is defined by $V(x_i y_j - x_j y_i) \subseteq \mathbb{P}^n \times \mathbb{P}^{n-1}$, where $x_1, \ldots, x_{n+1}$ are coordinates in $\mathbb{P}^n$ and $y_1, \ldots, y_n$ are coordinates on $\mathbb{P}^{n-1}$. As in the affine case, one uses the blow-up to resulve singularities.

5 Projective Plane Curves

5.1 Bézout's Theorem and Intersection Multiplicity

A projective plane curve is a hypersurface in $\mathbb{P}^2$ that may have multiple components. It is the zero set of a non-constant form $f \in \Bbbk[x, y, z]$ and is defined uniquely up to a constant multiple.

5.1 Definition. A *projective plane curve* is defined to be an equivalence calss of non-constant forms in $\Bbbk[x, y, z]$, where $f \sim g$ if and only if $f = \lambda g$ for some $\lambda \in \Bbbk$. The *degree* of a curves is the degree of the form defining it. Curves of degree 1, 2, 3, and 4 are called *lines*, *conics*, *cubics*, and *quartics*, respectively.

If f is irreducible then the projective curve defined by f is the projective variety $V(f) \subseteq \mathbb{P}^2$. Let $U_x = \{[x : y : z] \mid x \neq 0\}$ and define U_y and U_z similarily. These three sets are an open cover of $\mathbb{P}^2$. Consider a plane curve C defined by f. If $p \in C$ is contained in $C \cap U_x$ then define $\mathcal{O}_p(C) = \mathcal{O}_p(C \cap U_x) = \mathcal{O}_p(V(f(1, y, z))$, and similar definitions are made for U_y and U_z. In particular, we have seen that the multiplicity of a point on an affine curve only depends on the local ring. We therefore define the multiplicity of $p \in C$ as $m_p(C) = m_p(C \cap U_x)$ (or whichever U p happens to lie in). Moreover, if p is smooth then $\mathcal{O}_p(C)$ is a DVR.

5.2 Theorem (Bézout). *The number of points of intersection (counted with respect to multiplicity) of two distinct projective plane curves equals the product of their degrees.*

Since intersection is a local property, we assume for now that C and D are two curves in $\mathbb{A}^2$.

5.3 Definition. Two plane curves C and D *intersect properly* at $p \in \mathbb{A}^2$ if C and D do not have a common component passing through p. They *intersect transversally* at $p \in \mathbb{A}^2$ if they are both smooth at p and have distinct tangent lines at p.

5.4 Example.
1. $y = x$ and $y = x^2$ intersect transversally at $(0, 0)$.
2. $y = x^2$ and $y = -x^2$ do not intersect transversally at $(0, 0)$ since $y = 0$ is tangent to both at $(0, 0)$.

Consider the two plane curves $C = V(f)$ and $D = V(g)$. Let $p \in C \cap D$. We define $I(p, C \cap D)$ to be the *intersecton multiplicity*, which is the multiplicity of vanishing of g at p on C. Let us suppose that C is smooth at p, so that we can assume, without loss of generality, that C is irreducible. Then $\mathcal{O}_p(C)$ is a DVR and $M_p(C) = \langle t \rangle$ for some $t \in \mathcal{O}_p(C)$, so that every element of $\mathcal{O}_p(C)$ can be expressed uniquely as a power series in t. Therefore $\overline{g} = ut^m$, where u is a unit in $\mathcal{O}_p(C)$ and $I(p, C \cap D) = m = \text{ord}_p^C(\overline{g})$. If g has f as a factor, so that C is a component of D, then $\overline{g} \equiv 0 \in \mathcal{O}_p(C)$ and $I(p, C \cap D) = \infty$. Otherwise, if f and g do not have a common factor (so that C and D intersect properly at p) then $1 \leq I(p, C \cap D) < \infty$. If f and g do have a common zero, so that C and D do not intersect at p, then $\overline{g}$ is a unit in $\mathcal{O}_p(C)$, and its order is zero.

$I(p, C \cap D)$ is invariant under affine coordinate changes since $\mathcal{O}_p(C)$ is invariant under such changes. Intersection number depends only on the residue class of g in $\mathcal{O}_P(C)$. Consequently, if $E = V(g + f \cdot h)$ then $I(p, C \cap D) = I(p, C \cap E)$. If D has more than one component, say $D = D_1 \cup D_2$, so that $g = g_1 g_2$, then

$$I(p, C \cap D) = \text{ord}_p^C(\overline{g}_1 \overline{g}_2) = \text{ord}_p^C(\overline{g}_1) + \text{ord}_p^C(\overline{g}_2) = I(p, C \cap D_1) + I(p, C \cap D_2)$$

The intersection multiplicity is additive. If C and D intersect transversaly at p then $I(p, C \cap D) = 1$. Indeed, since C and D have distinct tangent lines at p, we can use the tangent line of g at p as a generator of $M_p(C)$. Therefore $\overline{f} = ut$, where u is a unit in $\mathcal{O}_p(C)$. If D is not smooth at p and does not have a common tangent direction with C then any tangent direction of D can be used as a generator of $M_p(C)$. Moreover $\overline{g} = ut^m$, where $m = m_p(D)$, and $I(p, C \cap D) = m_p(D) m_p(C)$.

5.5 Example.
1. If $C = V(y^2 - x^3 - x)$ and $D = V(x + y)$ then C and D are both smooth at $(0, 0)$. They have distinct tangent lines $V(x)$ and $V(x + y)$, respectively, so they intersect tansversally at $(0, 0)$ with intersection multiplicity 1.
2. If $C = V(y^2 - x^3 - x^2)$ and $D = V(x + y)$ then D is smooth at $(0, 0)$ by C is not. C has tangent directions $V(y + x)$ and $V(y - x)$. Note that $f = -x^3 + (y - x)g$, so $\overline{f} = -\overline{x}^3$ in $\mathcal{O}_p(D)$. Since $V(x)$ is not the tangent line to D at $(0, 0)$, we set $t = \overline{x}$, so that $\overline{f} = -t^3 \in \mathcal{O}_p(D)$, giving $I(p, C \cap D) = \text{ord}_p^D(\overline{f}) = 3$.

Suppose again that C is smooth at p, so that $M_p(C) = \langle t \rangle$ and $\overline{g} = ut^m$, for some unit $u \in \mathcal{O}_p(C)$. Then $\mathcal{O}_p(C)/\langle \overline{g} \rangle = \mathcal{O}_p(C)/\langle t^m \rangle$, which is the polynomials of degree less than m, a $\Bbbk$-vector space of dimension m. It is possible to define $I(p, C \cap D) = \dim_{\Bbbk}(\mathcal{O}_p(C)/\langle \overline{g} \rangle)$. Also, if we shrink the curve to a neighbourhood U where f and g only intersect at p, then $\mathcal{O}_p(C)/\langle \overline{g} \rangle \cong \mathcal{O}_p(C \cap U)/\langle \overline{g} \rangle$ and $\mathcal{O}_p(C \cap U) \cong \mathcal{O}_p(U)/\langle f \rangle$. Therefore $\mathcal{O}_p(C)/\langle \overline{g} \rangle \cong \mathcal{O}_p(U)/\langle f, g \rangle \cong \mathcal{O}(\mathbb{A}^2)/\langle f, g \rangle$. Therefore we see that $I(p, C \cap D) = \dim_{\Bbbk}(\mathcal{O}(\mathbb{A}^2)/\langle f, g \rangle)$. In particular, we see that $I(p, C \cap D)$ is symmetric in C and D.

We require that the intersection multiplicity of any two curves in $\mathbb{A}^2$ to satisfy the following properties.

5.6 Proposition.

1. *$I(p, C \cap D)$ is a non-negative integer if C and D intersect properly, and it is ∞ if C and D have a common component passing through p.*
2. *$p \notin C \cap D$ if and only if $I(p, C \cap D) = 0$.*
3. *$I(p, C \cap D)$ is invariant under affine corrdinate change.*
4. *It is symmetric, $I(p, C \cap D) = I(p, D \cap C)$*
5. *$I(p, C \cap D) = 1$ if and only if C and D intersect transversally at p, otherwise $I(p, C \cap D) \geq m_p(C) m_p(D)$ with equality holding if they do not have common tangent directions at p.*
6. *It is additive, $I(p, (C_1 \cup C_2) \cap D) = I(p, C_1 \cap D) + I(p, C_2 \cap D)$.*
7. *$I(p, C \cap D) = I(p, C \cap E)$ for any curve $E = V(g + f \cdot h)$.*

5.7 Theorem. *There exists a unique intersection number $I(p, C \cap D)$, defined for all plane curves and all points $a \in \mathbb{A}^2$, satisfying the above proposition. It is given by $I(p, C \cap D) = \dim_{\Bbbk}(\mathcal{O}_p(\mathbb{A}^2)/\langle f, g \rangle)$, where $C = V(f)$ and $D = V(g)$.*

PROOF: Uniqueness comes from the construction. One therefore only has to show that $\dim_{\Bbbk}(\mathscr{O}_p(\mathbb{A}^2)/\langle f,g\rangle)$ satisfies these properties. □

5.8 Example. 1. Let $C = V(y^2 - x^3)$ and $D = V(y - x^2)$. In this case $C \cap D = \{(0,0),(1,1)\}$ and D is smooth. C is not smooth at the origin. C and D do not intersect transversally at the origin and have common tangent direction $V(y)$. They do intersect transversally at $(1,1)$, so $I((1,1), C \cap D) = 1$. Since D is smooth at the origin, let us express f modulo g. $f = y^2 - x^3 = x^3(x-1) \pmod g$, so we will take $V(x)$ to be the generator of $M_{(0,0)}(D)$. Then $\overline{f} = x^3 u$, so $I((0,0), C \cap D) = \operatorname{ord}^D_{(0,0)}(\overline{f}) = 3$. Note that the sum of the intersection multiplicities is $1 + 3 = 4 < 6$. This is because C and D are in $\mathbb{A}^2$ and would intersect at ∞ in $\mathbb{P}^2$.

Let $I = \langle f,g\rangle \subseteq \Bbbk[x,y]$. Recall that $I(p, C \cap D) = \dim_{\Bbbk}(\mathscr{O}_p(\mathbb{A}^2)/I\mathscr{O}_p(\mathbb{A}^2))$. Globally,

$$\Bbbk[x,y]/I = \Bbbk[x,y]/\langle y - x^2, y^2 - x^3\rangle = \{a_0 + a_1 x + a_2 x^2 + a_3 x^3 \mid a_i \in \Bbbk\}$$

a $\Bbbk$-vector spaced of dimension $4 = 3{+}1$.

2. Let $C = V((x^2+y^2)^2 + 3x^2y - y^3)$ and $D = V((x^2+y^2)^3 - 4x^2y^2)$. The tangent directions at the origin are $V(y)$ and $V(y \pm \sqrt{3}x)$ for C and $V(x)$ and $V(y)$ for D. Therefore we have to rewrite the equations in such a way as to obtain distinct tangent directions. $g = (x^2+y^2)f + yh$, where $h = -3f + yq$, where $q = 5x^2 - 3y^2 + 4y^3 + 4x^2y$, which does not have $V(y)$ as a tangent direction. Thus $g = y^2 q \pmod f$, so that $V(g)$ has at least 3 components $V(y)$, $V(y)$, and $V(q)$. Thus $I((0,0), C \cap D) = 2I((0,0), C \cap V(y)) + I((0,0), C \cap V(q)) = 14$.

The first example suggests the following theorem.

5.9 Theorem. *Let C and D be two plane curves that are given by the polynomials f and g. Suppose that f and g do not have a common factor, so that C and D do not have a common component, and $C \cap D = \{p_1, \ldots, p_m\}$. If $I = \langle f,g\rangle$ then $\sum_i I(p_i, C \cap D) = \dim_{\Bbbk}(\Bbbk[x,y]/I)$.*

This is a direct consequence of the following.

5.10 Theorem. *If $I \subseteq \Bbbk[x,y]$ such that $V(I) = \{p_1, \ldots, p_m\}$ then*

$$\Bbbk[x,y] \cong \mathscr{O}_{p_1}(\mathbb{A}^2)/I\mathscr{O}_{p_1}(\mathbb{A}^2) \times \cdots \times \mathscr{O}_{p_m}(\mathbb{A}^2)/I\mathscr{O}_{p_m}(\mathbb{A}^2)$$

PROOF: Any element of $\Bbbk[x,y]/I$ can be viewed as an element of $\mathscr{O}_{p_i}(\mathbb{A}^2)/I\mathscr{O}_{p_i}(\mathbb{A}^2)$. Indeed, if $\overline{H}_1 = \overline{H}_2$ in $\Bbbk[x,y]/I$ then $H_1 = H_2 + h$ for some $h \in I \subseteq I\mathscr{O}_{p_i}(\mathbb{A}^2)$, so $H_1 \equiv H_2 \pmod{I\mathscr{O}_{p_i}(\mathbb{A}^2)}$. We therefore have a well-defined homomorphism $\varphi_i : \Bbbk[x,y]/I \to \mathscr{O}_{p_i}(\mathbb{A}^2)/I\mathscr{O}_{p_i}(\mathbb{A}^2)$ which induces the homomorphism

$$\varphi : \Bbbk[x,y]/I \to \prod_{i=1}^{m} \mathscr{O}_{p_i}(\mathbb{A}^2)/I\mathscr{O}_{p_i}(\mathbb{A}^2) : h \mapsto (\varphi_1(h), \ldots, \varphi_m(h))$$

This is actually an isomorphism. We need only to prove that φ is bijective.

We can find $E_1, \ldots, E_m \in \Bbbk[x,y]$ such that if $e_i = \overline{E}_i \in \Bbbk[x,y]/I$ then $e_i e_j = 0$ if $i \neq j$ and $\sum_i e_i = 1$. Let us assume that I is radical, so that $V(I) = \{p_1, \ldots, p_m\}$ (the proof is similar in the general case). One constructs the set of polynomials $\{E_1, \ldots, E_m\}$ as follows. Choose a polynomial F_i such that $F_i(p_i) \neq 0$ and $F_i(p_j) = 0$ for $i \neq j$. Set $E_i = \frac{1}{F_i(p_i)} F_i$. Then $E_i E_j$ vanishes at every point of $V(I)$ if $i \neq j$, so $e_i e_j = 0$ in $\Bbbk[x,y]/I$. Furthermore, $I = \sum_i E_i$ vanishes at every point, so $\sum_i e_i = 1$. Now since $E_i(p_i) \neq 0$, e_i is a unit in $\mathscr{O}_{p_i}(\mathbb{A}^2)/I\mathscr{O}_{p_i}(\mathbb{A}^2)$ and $\varphi_i(e_i)\varphi_i(e_j) = \varphi_i(e_i e_f) = 0$ if $i \neq j$. Whence $\varphi_i(e_j) = 0$ when $i \neq j$, so $\varphi(e_i) = (0, \ldots, 0, 1, 0, \ldots, 0)$. Finally, if

$G \in \Bbbk[x,y]$ is such that $G(p_i) \neq 0$ then there is $T \in \Bbbk[x,y]$ such that $\overline{TG} = e_i$, since $(1-G)E_i \in I$ and we set $T = \frac{1}{G(p_i)}E_i$.

Now if $\varphi(h) = 0$ then $\varphi_i(h) = 0$ for every i and $h \in I\mathcal{O}_{p_i}(\mathbb{A}^2)$ for all i. In particular, this means that $s_i h \in I$ for some $s_i \in \Bbbk[x,y]/I$ such that $s_i(p_i) \neq 0$. Moreover, there is $t_i \in \Bbbk[x,y]/I$ such that $t_i s_i = e_i$. Thus $h = h(\sum_i e_i) = \sum_i t_i s_i h = 0$.

Let $z = \prod \overline{a}_i/s_i$ where $s_i(p_i) \neq 0$. Take t_i as above, and note that $\varphi(\sum_i a_i t_i e_i) = z$, so φ is onto. □

Remark. To find the intersection multiplicity at p of curves in $\mathbb{P}^2$, one simply has to restrict the curvesto an open affine set containing p and compute the "affine" intersection multiplicity.

5.2 Proof of Bézout's Theorem

Let us begin by proving that any two projective plane curves intersect at a point. We need a technical lemma.

5.11 Lemma. *Let $R = \Bbbk[x,y,z]$ and R_d be the set of forms of degree d in R.*

1. *R_d is a $\Bbbk$-vector space of dimension $\frac{1}{2}(d+1)(d+2)$.*
2. *Let f and g be forms in R of degrees m and n, respectively. If f and g do not have a common factor then for $d \geq m+n$*
$$\dim(\langle f,g\rangle_d) = \dim R_d - mn$$
where $\langle f,g\rangle_d = \langle f,g\rangle \cap R_d =$ forms of degree d in $\langle f,g\rangle$.

PROOF: There are $\frac{1}{2}(d+1)(d+2)$ monomials of degree d, and these form a basis for R_d.

There is a surjective homomorphism $\psi : R_{d-m} \times R_{d-n} \mapsto \langle f,g\rangle_d : (a,b) \to af + bg$ whose kernel consists of pairs (a,b) such that $af + bg = 0$, of $af = -bg$. Since f and g do not have common factors, $a = cg$ and $b = -cf$, for some form $c \in R_{d-m-n}$. Thus $\ker\psi \cong R_{d-m-n}$, and $\dim_{\Bbbk}(\langle f,g\rangle_d) = \dim_{\Bbbk} R_{d-m} + \dim_{\Bbbk} R_{d-n} - \dim_{\Bbbk} R_{d-m-n} = \frac{1}{2}(d+1)(d+2) - mn$. □

5.12 Proposition. *Any two projective plane curves intersect in at least one point.*

PROOF: Let C and D be two projective plane curves that do not have a common component. Then C and D are given by homogeneous polynomials f and g in $R = \Bbbk[x,y.z]$ that do not have a common factor. By the above lemma, if $d \geq m+n$ then $\dim_{\Bbbk}(R_d \cap \langle f,g\rangle) = \dim_{\Bbbk} R_d - mn$. Let us assume that C and D do not intersect, so that $V_p(\langle f,g\rangle) = V_p(f) \cap V_p(g) = C \cap D = \varnothing$. By the projective Nullstellenzatz, $\langle f,g\rangle$ contains all forms of degree at least N, for some integer N. Let $d = \max\{N, m+n\}$. Then $R_d \subseteq \langle f,g\rangle$, so that $R_d = R_d \cap \langle f,g\rangle$, a contradiction.□

5.13 Corollary. *If C and D are two projective plane curves that do not have a common component then $C \cap D$ is a (non-empty) finite set of points.*

PROOF: If $C = V_p(f)$ and $D = V_p(g)$ for homogeneous polynomials $f, g \in \Bbbk[x,y,z]$ then $C \cap D = V_p(f) \cap V_p(g)$ is a non-empty proper algebraic subset of $V_p(f) = C$. The restriction to the affine open sets U_x, U_y, and U_z is then a proper algebraic subset of the affine curves $C \cap U_x$, $C \cap U_y$, and $C \cap U_z$, implying that $C \cap D$ is finite. □

Remark.
1. To find intersection points of projective plane curves, one just has to solve the systems $\{f = 0, g = 0, z = 0\}$ and $\{f = 0, g = 0, z = 1\}$ (indepedently), and discard the trivial solution $[0:0:0]$.
2. Not every two projective plane curves intersect at infinity, *i.e.* at a point with z-coordinate 0.

Let $R = \Bbbk[x,y,z]$, R_d be the set of d-forms in R. Let f and g be forms that do not have a common factor, and set $\Gamma = R/\langle f,g\rangle$ and let Γ_d be the set of d-forms in Γ, where a d-form in Γ is a residue class that can be represented by a d-form. Also, one can identify the d-forms in Γ with $R_d/\langle f,g\rangle_d$. We therefore see that Γ_d is a $\Bbbk$-vector space of dimension $\dim_{\Bbbk}(\Gamma_d) = \dim_{\Bbbk}(R_d) - \dim_{\Bbbk}(\langle f,g\rangle_d) = \dim_{\Bbbk}(R_d) - (\dim_{\Bbbk}(R_d) - mn) = mn$ when $d \geq m+n$. If h is a form in R, then $h(x,y,1)$ is the *restriction* of h to U_z. We denote $\Gamma_* = \Bbbk[x,y]/\langle f(x,y,1), g(x,y,1)\rangle$. If $F \in \Bbbk[x,y]$ has degree r then $z^r F(\frac{x}{z}, \frac{y}{z})$ is an r-form in R. Also, if f is a d-form in R then $f = z^d f(\frac{x}{z}, \frac{y}{z}, 1)$.

PROOF (OF BÉZOUT'S THEOREM): Let C and D be two curves in $\mathbb{P}^2$ given by the forms f and g that do not have a common factor. Let $m = \deg f$ and $n = \deg g$. We have to show that C and D intersect in mn points, counting multiplicity. Since C and D do not have a common component, they intersect in a finite set of points. We may therefore assume, after an appropriate projective coordinate change of coordinates, that none of the intersection points lie on the line at infinity $z = 0$. In particular, z does not divide both f and g. Moreover,

$$\sum_{p\in C\cap D} I(p, C\cap D) = \sum_{p\in C\cap D} I(p, V_a(f(x,y,1))\cap V_a(g(x,y,1))) = \dim_{\Bbbk}(\Bbbk[x,y]/\langle f(x,y,1), g(x,y,1)\rangle = \dim_{\Bbbk}(\Gamma_*)$$

We therefore have to prove that the dimension of Γ_* is mn. This is done by showing that $\Gamma_* \cong \Gamma_d$ as $\Bbbk$-vector spaces, for some $d \geq m+n$.

Notice that $\Gamma_d \cong \Gamma_{d+r}$ for all $r \geq 0$ via $\alpha : \Gamma_d \to \Gamma_{d+r} : \overline{h} \mapsto \overline{z^r h}$. Γ_d and Γ_{d+r} are $\Bbbk$-vector spaces of the same dimension, so α is an isomorphism for all $r \geq 0$ since it is injective. Indeed, if $\alpha(\overline{h}) = \overline{z^r h} = 0$ then $z^r h = af + bg$ for forms $a, b \in R$. Since z does not divide both f and g, z^r must divide both a and b. Therefore $h = a'f + b'g$ for some forms $a', b' \in R$, and $\overline{h} = 0$, proving injectivity. Consider now the homomorphism

$$\varphi : \Gamma_d \to \Gamma_* : \overline{h} \mapsto \overline{h(x,y,1)}$$

φ is well-defined since if $\overline{h}_1 = \overline{h}_2$ then $h_1 = h_2 + af + bg$ for some $a, b \in R$, so that $h_1(x,y,1) = h_2(x,y,1) + af(x,y,1) + bg(x,y,1)$, so the residue classes of the restrictions are equal. Suppose that $\overline{h(x,y,1)} = 0$ in Γ^*. Then $h(x,y,1) = Af(x,y,1) + Bg(x,y,1)$ for some $A, B \in \Bbbk[x,y]$. For large enough t, $a = z^{t-m}A(\frac{x}{z}, \frac{y}{z})$ and $b = z^{t-n}B(\frac{x}{z}, \frac{y}{z})$ are both forms. Whence $z^{t-d}h = z^t h(\frac{x}{z}, \frac{y}{z}, 1) = af + bg$, so $\overline{z^{t-d}h} = 0$, so $\overline{h} = 0$ by injectivity. Therefore φ is one to one. Let $H \in \Bbbk[x,y]$ and $s = \deg H$. Let $N = \max\{s, d\}$. Then $h = z^N H(\frac{x}{z}, \frac{y}{z})$ is a form of degree at least d. Therefore, by the isomorphism α, $\overline{h} = \overline{z^r h_d}$ for some d-form h_d and some postive integer r. Note that $H(x,y) = h(x,y,1) = h_d(x,y,1)$, so $H = \varphi(\overline{h}_d)$ and φ is onto. Therefore $\Gamma_* = \Gamma_d$. □

5.14 Corollary. *If C and D do not have a common component then*

$$\sum_{p\in C\cap D} m_p(C)m_p(D) \leq \sum_{p\in C\cap D} I(p, C\cap D) = mn$$

5.15 Corollary. *If C and D meet in mn distinct points then these points are all smooth points of C and D.*

5.16 Corollary. *If C and D have more than mn points in common then they have a common component.*

5.3 Divisors

5.17 Definition. Let C be a non-singular projective curve. A *divisor* on C is a formal sum $D = \sum_{p\in C} n_p p$, where $n_p \in \mathbb{Z}$ and $n_p = 0$ for all but finitely many $p \in C$.

Let $D = \sum_{p\in C} n_p p$ and $D' = \sum_{p\in C} m_p p$ be two divisors. If $n_p = 0$ for all $p \in C$ then we write $D = 0$; the *zero divisor*. The *sum* of divisors is defined coordinatewise, *i.e.* $D + D' = \sum_{p\in C}(n_p + m_p)p$. The set of all divisors on C is an Abelian group under addition. The *degree* of a divisor is $\deg D := \sum_{p\in C} n_p$, the sum of the coefficients. If $n_p \geq m_p$ for all $p \in C$ then we write $D \geq D'$. If $D \geq 0$ then D is called *effective* (or *positive*).

Remark.
1. For general varieties, divisors are defined as formal sums of irreducible hypersurfaces (*i.e.* subvarieties of codimension 1). They have the same properties as above.
2. The homomorophism $\deg : D(X) \to \mathbb{Z}$ shows that the collection of divisors of degree 0 is a subgroup $D_0(X)$ of $D(X)$.

5.18 Definition. Suppose that C is a projective plane curve of degree m and $G \in \Bbbk[x,y,z]$ is an m-form that does not vanish on all of C. We define the *divsor of* G as $\operatorname{div}(G) = \sum_{p\in C} \operatorname{ord}_p^C(\overline{G})p = \sum_{p\in C} I(p, C \cap V_p(G))p$

By Bézout's Theorem, $\operatorname{div}(G)$ has degree mn. For any $f \in \Bbbk(C)$, we define the *divisor of* f as $\operatorname{div}(f) = \sum_{p\in C} \operatorname{ord}_p^C(f)p$. Since f and $\frac{1}{f}$ both have algebraic pole sets, f has at most a finite number of zeroes and poles on C, so that $\operatorname{div}(f)$ is a well-defined divisor. If we let $(f)_0 = \sum_{\operatorname{ord}_p^C(f)>0} \operatorname{ord}_p^C(f)p =$ *divisor of zeroes* and $(f)_\infty = \sum_{\operatorname{ord}_p^C(f)<0} -\operatorname{ord}_p^C(f)p =$ *divisor of poles*. Then $\operatorname{div}(f) = (f)_0 - (f)_\infty$. Note that $\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g)$ and $\operatorname{div}(f^{-1}) = -\operatorname{div}(f)$.

5.19 Example.
1. If f is constant (and non-zero) then $\operatorname{div}(f) = 0$.
2. Let $C = \mathbb{P}^1 = \{[x : y : 0]\} \subseteq \mathbb{P}^2$ and $f = \frac{y}{x}$. Then $(f)_0 = \operatorname{div}(y) = [1 : 0 : 0]$ and $(f)_\infty = \operatorname{div}(x) = [0 : 1 : 0]$, so $\operatorname{div}(f) = [1 : 0 : 0] - [0 : 1 : 0]$.
3. Let $C = V_p(y - x)$ and $f = \frac{G}{H}$ where $G = y^3 - x^2z$ and $H = xyz$. Then $(f)_0 = \operatorname{div}(G) = 2[0 : 0 : 1] + [1 : 1 : 1]$ and $(f)_\infty = \operatorname{div}(H) = [1 : 1 : 0] + 2[0 : 0 : 1]$, so $\operatorname{div}(f) = [1 : 1 : 1] - [1 : 1 : 0]$.

The divisor of a rational function is called *principal*; the set of all principal divisors, $P(C)$, forms a subgroup of $D(C)$.

5.20 Proposition. *For any $f \in \Bbbk(C)$, $\operatorname{div}(f)$ is a divisor of degree 0, so that rational functions have the same number of zeroes as poles, counting multiplicity. In particular, this means that $P(C)$ is a subgroup of $D_0(C)$.*

PROOF: If $f = \frac{a}{b}$, where a and b are forms of the same degree m in $\Gamma_H(C)$. These forms can be represented by m-forms A and B in $\Bbbk[x,y,z]$. Then $\operatorname{div}(f) = \operatorname{div}(A) - \operatorname{div}(B)$, and by Bézout's Theorem $\operatorname{div}(A)$ and $\operatorname{div}(B)$ each have degree mn if C has degree n. □

Remark. Note all divisors of degree zero are principal. We will see that this is true on smooth rational curves, but not on elliptic curves or (smooth) curves of higher genus.

5.21 Corollary. *Let $f \in \Bbbk(C)$ be non-zero. The following are equivalent.*

1. $\operatorname{div}(f) \geq 0$
2. *f is a constant function.*
3. $\operatorname{div}(f) = 0$.

PROOF: If $\operatorname{div}(f) \geq 0$ then f has no poles and therefore must either be the constant zero function or have no zeros. If f is non-zero then $f = \frac{G}{H}$, where G and H are forms of the same degree. Since f has no poles, H has no zeros, so G and H are both forms of degree zero, a constant. □

5.22 Corollary. *Let $f, g \in \Bbbk(C)$, both non-zero. Then* $\operatorname{div}(f) = \operatorname{div}(g)$ *if and only if $f = \lambda g$ for some constant $\lambda \in \Bbbk$.*

PROOF: $\operatorname{div}(f) - \operatorname{div}(g) = 0$, so $\operatorname{div}(fg^{-1}) = 0$, which implies that fg^{-1} is a constant. □

5.23 Definition. Two divisors D and D' are said to be linearly equivalent if $D' = D + \operatorname{div}(f)$ for some rational function $f \in \Bbbk(C)$, *i.e.* if $D - D' \in P(C)$, and we write $D \equiv D'$. The *Picard group* is $\operatorname{Pic}(C) = D(C)/P(C)$.

Notice that if $D \equiv D'$ then $\deg D = \deg D'$. $\operatorname{Pic}^m(C)$ is defined to be the component of $\operatorname{Pic}(C)$ consisting of elements of degree m. In particular, $\operatorname{Pic}^0(C) = D_0(C)/P(C)$. Notice that $\operatorname{Pic}^0(C)$ can be thought of as a measure of how badly $P(C)$ fails to include all divisors.

5.24 Example. Let C be a line in $\mathbb{P}^2$, so that $C \cong \mathbb{P}^1$. Then $\mathrm{Pic}^0(C) \cong 0$. Indeed, we have to prove that any two points $p, q \in C$ are linearly equivalent. Let L be a line in $\mathbb{P}^2$ through p different from C, and let L' be a line through q other than C. Then L and C and L' and C inThen L and C itntersect transversely at p, and p is the only point of intersection. Same for L' and C concerning q. Then $\mathrm{div}(L) = p$ and $\mathrm{div}(L') = q$, so $p - q = \mathrm{div}(L/L')$, so $p \equiv q$.

5.25 Definition. Fix $p_0 \in C$ and define $\phi_c : C \to \mathrm{Pic}^0(C) : p \mapsto p - p_0$.

The map ϕ_C can be used to define addition on the curve. Given $p, q, r \in C$, we say that $p + q = r$ if and only if $\phi_C(p) + \phi_C(q) = \phi_C(r)$.

We therefore have that if C is any projective plane curve isomorphic to $\mathbb{P}^1$, then $\mathrm{Pic}(C) = \mathbb{Z}$ and $\mathrm{Pic}^0(C) = 0$. The same is true for any smooth rational projective plane curve because of the following proposition.

5.26 Proposition. *Any rational smooth projective plane curve is isomorphic to* $\mathbb{P}^1$.

This is an immediate consequence of the following theorem.

5.27 Theorem. *A rational map $\varphi : C \to \mathbb{P}^2$, where C is a projective plane curve, is regular at every smooth point of C.*

PROOF: Suppose that the smooth point $p \in C$ lies in the affine piece $C \cap U_z$ and has affine coordinates (x, y). We can write the rational map φ as $(x, y) \to [\varphi_1 : \varphi_2 : \varphi_3]$ for some rational functions φ_i on C. Note that one can always find a polynomial g such that the $g\varphi_i$ are forms of the same degree. One may therefore assume that the φ_i's are homogeneous polynomials of the same degree, giving a well-defined expression of φ wherever the φ_i's are not simultaneously zero. Since $p \in C$ is a smooth point of C, $\mathcal{O}_p(C)$ is a DVR and $M_p(C) = \langle t \rangle$ for some $t \in \mathcal{O}_p(C)$. Now, each φ_i is regular at p, so that $\varphi_i = t^{k_i} u_i$ for some integer $k_i \geq 0$ and a unit u_i. Suppose without loss of generality that k_1 is the smallest. Then $\phi = [u_1 : t^{k_2 - k_1} u_2 : t^{k_3 - k_1} u_3]$ is a well-defined map at p, since $u_1(p) \neq 0$. Thus ϕ is regular at p and it agrees with φ on C. □

Therefore, if C is a smooth projective plane curve then every rational map from C to $\mathbb{P}^2$ is a morphism, implying that rational maps between smooth plane curves are morphisms. Thus, any two birationl smooth projective plane curves are in fact isomorphic.

5.28 Proposition. *If C is a smooth rational projective plane curve then* $\mathrm{Pic}^0(C) = 0$.

5.29 Proposition. *If C is a smooth curve in $\mathbb{P}^2$ of degree 2 then* $\mathrm{Pic}^0(C) = 0$.

PROOF: Let $p, q \in C$. We want to show that $p \equiv q$. Let L be a line passing through p and not q. Then L is given by a 1-form h and by Bézout's Theorem, since C has degree 2, $\mathrm{div}(h) = p + r$, where $r \neq q$. Let L' be a line passing through q and r. Then if L' is given by the 1-form h', since C has degree 2, $\mathrm{div}(h') = q + r$. Thus $\mathrm{div}(h/h') = p - q$, which implies that $p \equiv q$. □

5.30 Theorem. *Let C be a smooth curve in $\mathbb{P}^2$. Then C is rational if and only if* $\mathrm{Pic}^0(C) = 0$.

PROOF: We have already proved the forward implication. Suppose that $\mathrm{Pic}^0(C) = 0$. We have to show that $C \sim \mathbb{P}^1$. It is enough to show that $\Bbbk(C) \cong \Bbbk(\mathbb{P}^1) \cong \Bbbk(\mathbb{A}^1) = \Bbbk(t)$. Let $p, q \in C \cap U_2$. Then since $\mathrm{Pic}^0(C) = 0$, $p \equiv q$ and there is $\alpha \in \Bbbk(C)$ such that $\mathrm{div}(\alpha) = p - q$. Note that α be thought of as a rational map $\psi : C \to \mathbb{A}^1 : s \mapsto \alpha(s)$. Also, for $\varphi \in \Bbbk(t)$, $\psi^*(f) = f(\alpha)$, and this is a bijection. Indeed, $\psi^*(f) = 0$ implies that $f(\alpha) = 0$, which happens if and only if $f = 0$ since α is non-constant. The image of $\Bbbk(t)$ in $\Bbbk(C)$ is $\Bbbk(\alpha)$. We must show that $\Bbbk(\alpha) = \Bbbk(C)$. We claim that if $r \in C \cap U_2$ is such that $r \neq q$ then there is $\beta \in \Bbbk(C)$ such that $\mathrm{div}(\beta) = r - q$ and $\beta \in \Bbbk(\alpha)$. Since $r \neq q$, α is defined at r. Let $a = \alpha(r)$. If $F, G \in \Bbbk[x, y, z]$ are forms of the same degree such that $\alpha = \frac{F}{G}$, set

$\beta = \frac{F-aG}{G} \in \Bbbk(\alpha)$. Then β is defined at r and $\beta(r) = 0$. We would like to show that $\operatorname{div}(\beta) = q - r$. Note that β is not everywhere zero, otherwise $\alpha = a$ on all of C, which is impossible since $\operatorname{div}(\alpha) \neq 0$. Since $\deg(\operatorname{div}(\beta)) = 0$ and $\beta(r) = 0$, it is sufficient to show that $(\beta)_\infty = q = (\alpha)_\infty$. This follows from the fact that any pole of β is a pole of α (prove this as an exercise).

Now let $\gamma \in \Bbbk(C)$. Then if $\operatorname{div}(\gamma) = \sum_{i=1}^m r_i - s_i$ then one can fine $g, h \in \Bbbk(\alpha)$ such that $\operatorname{div}(g) = \sum_{i=1}^m r_i - m_q$ and $\operatorname{div}(h) = \sum_{i=1}^m s_i - m_q$. Therefore $gh^{-1} \in \Bbbk(\alpha)$ and $\operatorname{div}(gh^{-1}) = \operatorname{div}(g) - \operatorname{div}(h)$, implying that γ is a constant multiple of gh^{-1} and $\gamma \in \Bbbk(\alpha)$. □

Remark. If there are distinct points p and q such that $p \equiv q$ then C is rational. Indeed, if such points exist then there is a rational map $\alpha \in \Bbbk(C)$ such that $\operatorname{div}(\alpha) = p - q$, which can be used, as in the proof of the above theorem, to define an isomorphism $\Bbbk(X) \cong \Bbbk(\mathbb{P}^1)$.

5.31 Corollary. *If C is a smooth projective plane curve of degree 1 or 2 then C is rational.*

It follows from this corollary that we must look at smooth curves of degree at least 3 to find a non-rational curve.

5.32 Definition. An isomorphism from a variety to itself is called and *automorphism*.

5.33 Proposition. *Any non-identity automorphism of $\mathbb{P}^1$ has at most two fixed points. In particular, if a smooth curve in $\mathbb{P}^2$ admits an automorphism with more than two fixed points then it is not rational.*

PROOF: Notice that $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$ is the one point compactification of $\mathbb{A}^1$. Whence any automorphism of $\mathbb{P}^1$ can be thought of as a rational map $\mathbb{P}^1 \to \mathbb{A}^1$ whose poles get mapped to ∞. In this case, $\alpha = \frac{F}{G}$, with $F, G \in \Bbbk[x, y]$, of the same degree. F and G split into linear factors, and we may assume that they have no common factors. Thus there are no removeable singularities and $\operatorname{div}(F) = (\alpha)_0$ and $\operatorname{div}(G) = (\alpha)_\infty$. Since α is an automorphism, $(\alpha)_0$ is a single point, implying that F and G are both 1-forms. If we write $F = ax + by$ and $G = cx + dy$ then we may write $\alpha : [x : y] \to [ax + by : cx + dy]$ (where $ad - bc \neq 0$, since otherwise there are x and y such that $ax + by = 0 = cx + dy$). Now if $[x : y]$ is a fixed point then $[x : y] = [ax + by : cx + dy]$, so

$$\lambda x = ax + by$$
$$\lambda y = cx + dy$$

a system which has exactly two linearly independent solutions. □

5.34 Theorem. *Let C be a smooth curve of degree 3 in $\mathbb{P}^2$. Suppose that $p, q \in C$ are such that $p \equiv q$. Then $p = q$, and C is not rational.*

PROOF: Let L be a line in $\mathbb{P}^2$ through p. Since C has degree 3, L intersects C in $p + r_1 + r_2$, where r_1 and r_2 may be equal to p. Since two points define a line and C is smooth, if there is a line L' that intersects C through r_1 and r_2, then $L' = L$ and $p = q$. Suppose that C is given by $F \in \Bbbk[x, y, z]$ and L is given by the 1-form $F_1 \in \Bbbk[x, y, z]$. Since $p \equiv q$ there are forms $G, H \in \Bbbk[x, y, z]$ of the same degree such that $\operatorname{div}(G/H) = p - q$, *i.e.* $\operatorname{div}(H) = \operatorname{div}(G) - p + q$. Then $\operatorname{div}(HF_1) = \operatorname{div}(H) + \operatorname{div}(F_1) = \operatorname{div}(G) + (q + r_1 + r_2)$ In particular, for any $r \in C$, we have $ord_r^C(\overline{HF_1}) > ord_r^C(\overline{G})$. Suppose that all points where $ord_r^C(\overline{G}) > 0$ do not lie at infinity, *i.e.* C and $V_p(G)$ do not intersect at infinity. Therefore $ord_r^{C \cap U_z}(\overline{HF_1}(x, y, 1)) \geq ord_v^{C \cap U_z}(\overline{G}(x, y, 1))$ on $C \cap U_z$, so that $\overline{HF_1}(x, y, 1)/\overline{G}(x, y, 1) \in \mathcal{O}_r(C \cap U_x)$. This implies that $\overline{HF_1}(x, y, 1) = 0$ in $\mathcal{O}_r(C \cap U_z)/\langle \overline{G}(x, y, 1) \rangle \cong \mathcal{O}_r(\mathbb{A}^2)/\langle \overline{F}(x, y, 1), \overline{G}(x, y, 1) \rangle$ for all $r \in C \cap U_z$. Whence $\overline{HF_1}(x, y, 1) = 0$ in $\Bbbk[x, y]/\langle \overline{F}(x, y, 1), \overline{G}(x, y, 1) \rangle \cong \prod_r \mathcal{O}_r(\mathbb{A}^2)/\langle \overline{F}(x, y, 1), \overline{G}(x, y, 1) \rangle$. It follows that there are forms $A, B \in \Bbbk[x, y, z]$ such that, for some d, $z^d HF_1 = AF + BG$. Mulitplication by high enough powers of z is injective on $\Bbbk[x, y, z]$, so $HF_1 = A'F + B'G$. Therefore $\operatorname{div}(HF_1) = \operatorname{div}(B'G)$ since $F = 0$ on C, so $\operatorname{div}(B') = q + r_1 + r_2$. Therefore B' is a 1-form since C has degree 3, so $V_p(B')$ is a line L' (as above), so $p = q$. □

5.4 Elliptic Curves

5.35 Definition. An *elliptic curve* over $\Bbbk$ is a smooth curve E that is birational to a smooth projective plane curve of degree 3, together with a point p_0 on E.

We will therefore think of elliptic curves as being smooth degree 3 curves in $\mathbb{P}^2$; they are therefore given by 3-forms in $\Bbbk[x,y,z]$. After an appropriate coordinate change, a 3-form in giving a smooth curve can be written as

$$y^2x + b_1xyz + b_2yz^2 = x^3 + a_1x^2z + a_2xz^2 + a_3z^3$$

(smoothness imposed that certain coefficients are non-zero). We may also assume that $p_0 = [0:1:0]$. This is the standard form which is called the *Weierstraß form*.

Remark.
1. E only has one points at infinity, and it is $[0:1:0]$ (notice that if $z=0$ then $x=0$). Whence p_0 has multiplicity 3 since E has degree 3.
2. If the characteristic of $\Bbbk$ is not two then after completing the square in y and transforming, we may write the curve as $y^2z = x^3 + a_1x^2z + a_2xz^2 + a_3z^3$. On the affine piece $U_z = \{z \neq 0\}$, E is given by $y^2 - p(x)$, where $p(x) = x^3 + a_1x^2 + a_2x + a_3$. The Jacobian is hence $\begin{bmatrix} -p'(x) & 2y \end{bmatrix}$. If p and p' have a common root x_0 then the point $(x_0, 0)$ is on $E \cap U_z$ and the Jacobian is zero at that point. Since E is assumed to be smooth it must be the case that p has no repeated roots.
3. Notice that the automorphism of E given by $[x:y:z] \mapsto [x:-y:z]$ has fixed points whereever $y=0$.

Let E be a smooth curve of degree 3 in $\mathbb{P}^2$ with a fixed point p_0 such that the line at infinity $z=0$ intersects E in $3p_0$ (so the tangent line to E at p_0 is $z=0$). Consider $\phi_E : E \to \mathrm{Pic}^0(E) : p \to p - p_0$.

5.36 Theorem. *ϕ_E is a bijection, so that $E \cong \mathrm{Pic}^0(E)$.*

PROOF: If $p,q \in E$ are such that $p - p_0 \equiv q - p_0$ then $p \equiv q$, so by the above theorem $p = q$. Therefore ϕ_E is injective. If L is a line in $\mathbb{P}^2$ then it intersects E in three points p,q,r (which may not be distinct). We have $p+q+r \equiv 3p_0$ since if H gives L then $\mathrm{div}(H/z) = \mathrm{div}(H) - \mathrm{div}(z) = p+q+r-3p_0$. For every point $p \in E$ there is a point r such that $p + r \equiv 2p_0$ since there is a line through p and p_0 which must intersect E at another point, r. Let $D \in \mathrm{Pic}^0(E)$. Then $D = \sum_i p_i - q_i = \sum_i (p_i - p_0) - \sum_i (p_i - p_0)$. For every q_i there is r_i such that $(q_i - p_0) \equiv -(r_i - p_0)$, so that $D = \sum_i (p_i - p_0) + \sum_i (r_i - p_0) = \sum_{j=1}^{m} s_j - p_0$ (after possibly some cancellation). If $m = 1$ then we are done. If $m = 2$ then $D \equiv s_1 + s_2 - 2p_0$, but there is L through s_1 and s_2, which will intersect E at some t, giving $s_1 + s_2 + t \equiv 3p_0$, so $D \equiv p_0 - t = -(t - p_0) \equiv p - p_0$ for some p. Clearly we are done by induction. □

The group structure on E is induced by the group structure on $\mathrm{Pic}^0(E)$, namely for $p,q \in E$, $p + q = \phi_E^{-1}((p - p_0) + (q - p_0))$. In particular, each point $p \in E$ has an inverse $-p = \phi_E^{-1}(-(p - p_0))$, and p_0 is the zero of E.

5.37 Example. For the elliptic curve $y^2z = x^3 - 5x^2z$ over $\mathbb{C}$, $p = [0:0:1]$, and $q = [-1:-2:1]$, notice that $p,q \in U_z$, so we may consider the affine plane curve $y^2 = x^3 - 5x^2$. Then the line L through p and q is $y = 2x$, and L intersects the curve at $r = [5:10:1]$. Therefore $p + q$ is the third intersection point of the line joining $p_0 = [0:1:0]$ and r, so $p + q = [5:-10:1]$. Notice that $2p = p + p = p_0$, so p is a torsion point.

5.38 Definition. Let (E, p_0) be an elliptic curve. A point p on E is an *n-torsion point* if $np = p_0$.

Remark.
1. Elliptic curves are examples of algebraic groups that are not matrix groups. They are in fact *Abelian varieties*, connected projective algebraic groups.
2. If C is a smooth curves in $\mathbb{P}^2$ of genus greater than 1, then $\mathrm{Pic}^0(C)$ is a g-dimensional abelian variety.

3. Recall that if C is a smooth curve in $\mathbb{P}^2$ of degree one or two then $C \cong \mathbb{P}^1$, via picking distinct points $p, q \in C$ and 1-forms H and H' such that $\operatorname{div}(H/H') = p - q$, which induces the map $x \mapsto [H(x) : H'(x)]$. If C is smooth of degree 3, then such an isomorphism does not exists. Nonetheless, one has a two to one map. Suppose that the characteristic is not 2 and C has Weierstraß model $y^2z = x^3 + a_1x^2z + a_2xz^2 + a_3z^3$, and fixed point $p_0 = [0 : 1 : 0]$. Then we have the map $[x : y : z] \mapsto [x : -y : z]$, which has 4 fixed points, the 2-torsion points. Moreover, the map

$$C \subseteq \mathbb{P}^2 \to \mathbb{P}^1 \subseteq \mathbb{P}^2 : [x : y : z] \mapsto [x : 0 : z]$$

is a surjective two to one map from C to $\mathbb{P}^1$. Therefore any elliptic curve is a double cover of $\mathbb{P}^1$. Given this map, one can show that $\Bbbk(C)$ is a Galois extension of $\Bbbk(\mathbb{P}^1)$.

For $\Bbbk = \mathbb{C}$, fix $\tau \in \mathbb{C}$ such that $\tau \notin \mathbb{R}$. Let $\Lambda = \{m + n\tau \mid m, n \in \mathbb{Z}\}$, a lattice. Notice that $\mathbb{C}/\Lambda \cong S^1 \times S^1$, the torus. An *elliptic function (with respect to Λ)* is a merophic function $f(z)$ such that $f(z+\omega) = f(z)$ for any $\omega \in \Lambda$. Such functions are often called *doubly periodic*. Moreover, these functions descend to (well-defined) functions on the torus $\mathbb{C}/\Lambda$. One of the most important elliptic functions is the Weierstraß $\wp$-function, defined by

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

This series converges for all $z \notin \Lambda$ and is elliptic. Its derivative is

$$\wp'(z) = \sum_{\omega \in \Lambda} \frac{-2}{(z-\omega)^3}$$

which is another elliptic function. Any sum, difference, product, or ratio of elliptic functions is again elliptic, so that the set of all elliptic functions forms a field.

5.39 Theorem. *The field of elliptic functions for a given lattice Λ is generated over $\mathbb{C}$ by the associated Weierstraß $\wp$-function and its derivative $\wp'$. They satisfy the algebraic relation $(\wp')^2 = 4\wp^3 - g_2\wp - g_3$, where $g_2 = 60\sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^4}$ and $g_3 = 140\sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^6}$.*

Thus, if we define the mapping $\varphi : \mathbb{C} \to \mathbb{P}^2(\mathbb{C}) : z \mapsto [\wp(z) : \wp'(z) : 1]$ (and sends poles to $[0 : 1 : 0]$ we obtain a holomorphic map whose image is the smooth cubic E given by $y^2z = 4x^3z - g_2xz^2 - g_3z^3$. This map descends to an isomorphism $\varphi : \mathbb{C}/\Lambda \to E \subseteq \mathbb{P}^3$. Therefore, over $\mathbb{C}$, elliptic curves are isomorphic to complex tori, which can always be expressed as $\mathbb{C}/\Lambda$ for some lattice Λ.