LECTURES ON BASIC ALGEBRAIC GEOMETRY

VISHWAMBHAR PATI

Abstract. In these lectures, we will introduce some basic notions, developing the necessary algebra as we go along.

1. Motivation

1.1. **The Diophantine Problem.** Let us briefly look at a simple algebraic problem, one that has been around for centuries. Let $f(X,Y,Z)$ be a homogeneous polynomial of degree d , with integer coefficients. One would like to know if there are any solutions to the equation $f(X,Y,Z) = 0$ with $X,Y,Z \in \mathbb{Z}$. (For example, the Fermat problem asks whether such exist for $f(X,Y,Z) = X^d + Y^d - Z^d$ for $d > 2$). Note that $(0,0,0)$ is always a solution, and if $(a,b,c) \in \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ is a solution, so is (ma,mb,mc) for all $m \in \mathbb{Z}$, by the homogeneity of f. Thus it makes sense to consider only solutions of the kind $(a,b,c) \neq (0,0,0)$, and concern ourselves only with equivalence classes, denoted $[a:b:c]$, of *such* solutions, where the equivalence relation on the set $S = \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\setminus(0,0,0)$ is defined by $(a,b,c) \sim (ma,mb,mc)$ for all integers $m \neq 0$. There is also the obvious

Remark 1.1.1. Equivalence classes of solutions $[a:b:c] \in S/\sim$ to the homogeneous equation $f(X,Y,Z) = 0$ with $c \neq 0$ (resp. $a \neq 0$, resp. $b \neq 0$) are in 1-1 correspondence with rational solutions $(p,q) \in \mathbb{Q}\times\mathbb{Q}$ to the de-homogenised polynomial equation $f(X,Y,1) = 0$ (resp. $f(1,Y,Z) = 0$, resp. $f(X,1,Z) = 0$) in two variables.

It is clear that all the integral solutions to the problem when $d = 1$ can be enumerated. If $f(X,Y,Z) = lX+mY+nZ$ is a general degree one polynomial, all the rational solutions to, say the de-homogenised equation $f(X,Y,1) = 0$ are precisely the pairs $(p, \frac{-lp-n}{m})$ with $p \in \mathbb{Q}$. Similarly for the other two de-homogenised versions of $f(X,Y,Z)$.

For the case $d = 2$ (conics), one should first observe that there *need not be any non-trivial integral solutions.* For example, assume (a,b,c) is a solution to $f(X,Y,Z) = X^2+Y^2-3Z^2$. Since $\sqrt{3}$ is irrational, we can assume that a,b,c are all non-zero. We may also assume, by scaling away, that the greatest common divisor of a,b,c is 1. Since $a^2+b^2 = 3c^2$, we have a^2+b^2 congruent to 0 modulo 3. Now if a,b are any integers, a^2 and b^2 are congruent to 0 or 1 modulo 3, so that a^2+b^2 is congruent to 0 mod 3 iff both a and b are divisible by 3. This will mean that a^2+b^2 is divisible by 9, and hence c^2 is divisible by 3, so that c is also divisible by 3, contradicting that the greatest common divisor of a,b,c is 1.

In the degree 2 case however, there is a method of generating all the rational solutions to the de-homogenised equation say $g(X,Y) = f(X,Y,1) = 0$ *given one rational solution*, say $(p,q) \in \mathbb{Q}\times\mathbb{Q}$. Let us assume that $q \neq 0$.

This is a geometric method, given as follows. Join the point $P = (p,q)$ to the point $(t,0)$ by means of a straight line, which moves in time with the time parameter t (this is why we took $q \neq 0$, otherwise the line would be idle as the x-axis for all t !) keeping the point P fixed. For general t, this line will intersect the conic $g(X,Y) = 0$ in two points, one of which we know to be $P = (p,q)$. Let $Q(t) = (X_t, Y_t)$ be the other point where it intersects the conic. We note that for $Q(t)$ to lie on this line, we must have $(p-t)Y_t = q(X_t - t)$. Plug this equation for Y_t into the equation $g(X_t,Y_t) = 0$. We will then have a quadratic equation: $\alpha(t)X_t^2 + \beta(t)X_t + \gamma(t) = 0$ where $\alpha(t), \beta(t)$ and $\gamma(t)$ are rational functions of t (a rational function is a quotient of a polynomial in t by another non-zero polynomial in t.) Also, since $g(X,Y) = 0$ had integer coefficients, these rational functions in t have all rational coefficients. By well-known facts on quadratics, we have $p + X_t = \frac{-\beta(t)}{\alpha(t)}$, so that X_t also becomes a rational function of t with rational coefficients. Plugging into the above expression for Y_t, we have that Y_t is also a rational function of t with rational coefficients. We thus

have a *rational parametrisation* of our conic. Now all the points on $g(X,Y)=0$ with both coordinates rational are precisely (X_t, Y_t) with $t \in \mathbb{Q}$.

Exercise 1.1.2. Use the method of projection from the rational point $(0,1)$ on the conic $Y^2-X^2=1$ to obtain the rational parametrisation for it given by $X_t = \frac{2t}{1-t^2}$, $Y_t = \frac{1+t^2}{1-t^2}$. Use this to show that the Pythagorean triples: $\{[m^2-n^2 : 2mn : m^2+n^2]\}$ where $m, n \in \mathbb{Z}$ exhaust all the integral solutions to $X^2+Y^2=Z^2$ (upto permutations of X and Y.)

In passing, we note another application of the above parametrisation to the evaluation of definite integrals. Suppose we want a closed form solution to the indefinite integral:

$$\int (ax^2+bx+c)^{-\frac{1}{2}} dx$$

which maybe rewritten as $\int \frac{dx}{y}$, where $y^2 = ax^2+bx+c$. Let $g(x,y) = y^2 - ax^2 - bx - c$, and by the above method, find a rational parametrisation $x(t) = p(t)$, $y(t) = q(t)$, where both these functions are rational functions of t. Then $dx = p'(t)dt$ and our integral becomes : $\int \frac{p'(t)dt}{q(t)}$, which can be rewritten as the integral of a rational function in t, and integrated by the method of partial fractions. (Try it out for $a=1, b=0, c=1$, using the exercise above).

The story for $d=3$ changes completely. For example, in p. 7 of Shafarevic's book (Basic Algebraic Geometry), it is shown that the Fermat curve $X^d+Y^d=1$ cannot be rationally parametrised for $d>2$. Indeed, the entire theory of elliptic curves and elliptic integrals was born with the effort to evaluate the integral:

$$\int \frac{dx}{(ax^3+bx+c)^{1/2}}$$

the so called *elliptic integral* which arises when one solves the equations of motion of a pendulum without the small-amplitude approximation.

1.2. **Invariant Theory.** At the turn of the last century, Felix Klein sought to understand geometry by means of group theory, i.e. study the group of transformations under which the geometry remains invariant. For example, for Euclidean geometry, the corresponding group is the Motion Group, for hyperbolic geometry it is the group $PSL(2,\mathbb{R})$, and for the Minkowski space-time, the Poincare Group. In these cases, the original space is expressible as the quotient of the original group by a closed subgroup, and the groups listed above are all given by algebraic (polynomial) conditions on matrix coefficients in a suitable realisation inside a large-dimensional Euclidean space. So what sorts of objects does one get on taking a quotient like this, and what are a complete set of invariants on the quotient space to describe all possible functions on it ? To give a simple example, if one lets the permutation group S_n act on Euclidean n-space $\mathbb{R}^n$ by permutations of the coordinates, then the quotient space X is an algebraic object, and polynomial functions on $\mathbb{R}^n$ which descend to X are precisely the symmetric functions on $\mathbb{R}^n$,and it is well known that all symmetric polynomials are polynomials in the the elementary symmetric functions $\sigma_i(X_1, X_2, ..X_n)$, $i = 1, 2, ..., n$.

The objects of interest here are algebraic sets, which we define below:

Definition 1.2.1. Let k be a field, and let S be some subset of the polynomial ring in n variables, i.e. $k[X_1, X_2, ..X_n]$. The subset of k^n defined by:

$$V(S) := \{(a_1, ...a_n) \in k^n : f(a_1, ...a_n) = 0 \; \forall \; f \in S\}$$

is called an *affine algebraic set* . If $\langle S \rangle$ denotes the ideal generated by S in $k[X_1, X_2, ..X_n]$, clearly $V(S) = V(\langle S \rangle)$. If $S = \{f(X_1, ..X_n)\}$ is a singleton, $V(S)$ is denoted $V(f)$, and is called a *hypersurface* in k^n. More generally, if $S = \{f_1, .., f_m\}$ is a finite set, we denote $V(S)$ by $V(f_1, .., f_m)$. It will turn out by the Hilbert Basis Theorem in the next section that *all* algebraic sets are of the form $V(f_1, .., f_m)$.

Definition 1.2.2. Given a subset $Z \subset k^n$, we can define the *ideal of functions vanishing on* Z denoted $\mathfrak{I}(Z)$ inside the k-algebra $k[X_1, X_2, ..X_n]$ by:

$$\mathfrak{I}(Z) := \{f \in k[X_1, X_2, ..X_n] : f(a_1, ...a_n) = 0 \quad \forall \quad (a_1, ...a_n) \in Z\}$$

A natural question to ask is whether the correspondences $\mathfrak{I} \mapsto V(\mathfrak{I})$ and $Z \mapsto \mathfrak{I}(Z)$ are *bijective*. We will address this issue in §4, via the Hilbert Nullstellensatz.

We recall that if X is a compact Hausdorff space, the Banach algebra of continuous complex-valued functions $C(X)$ completely determines the space X upto homeomorphism. In fact, there is a 1-1 correspondence between closed ideals in $C(X)$ and closed subsets of X, and maximal ideals of $C(X)$ and points of X. Indeed, the set of maximal ideals of $C(X)$ (called the *maximal spectrum of* X) can be given a topology which makes it homeomorphic to X. That result is known as the Gelfand-Naimark Theorem, and can be looked up in most advanced analysis texts (e.g. Simmons, or Rudin).

In the situation of affine algebraic sets, the analogous facts are consequences of the Hilbert Nullstellensatz, as we shall see in §4. Towards defining the algebraic ring of functions on an affine algebraic set, we make the following definition:

Definition 1.2.3. Let $Z \subset k^n$ be an affine algebraic set, and let $\mathfrak{I}(Z)$ be the ideal in $k[X_1, X_2, ..X_n]$ as defined above. We define the *coordinate ring* $k[Z]$ of Z to be the quotient ring $k[X_1, X_2, ..X_n]/\mathfrak{I}(Z)$. This coordinate ring is obviously a k-algebra.

Since the restrictions of two polynomials $f,\ g \in k[X_1, .., X_n]$ to Z agree pointwise on Z iff their difference lies in $\mathfrak{I}(Z)$, the coordinate ring maybe viewed as the ring of all functions on Z which are restrictions of polynomials from the ambient space k^n, two such polynomial functions being identified if they agree pointwise on Z. Elements of this coordinate ring are called *regular functions* on Z, and the coordinate ring $k[Z]$ is sometimes called the *ring of regular functions on* Z.

Now, the central theme of invariant theory is the following. Suppose a group G acts algebraically on an affine algebraic set Z which has the coordinate ring $k[Z]$. To say G acts algebraically, for say, a finite group G, means that each element $g \in G$ induces a k-algebra automorphism of $k[Z]$. In this k-algebra $k[Z]$, there is then the subalgebra $k[Z]^G$ of functions that are G-invariant.

As an example, the polynomial ring $k[X_1, .., X_n]$ is the coordinate ring of the affine n-space $Z = k^n$. If we consider the action of the permutation group $G = S_n$ given by permutation of coordinates (viz. for a polynomial $f \in k[Z] = k[X_1, .., X_n]$, and $\sigma \in S_n$, we define $\sigma.f(X_1, .., X_n) = f(X_{\sigma^{-1}(1)}, .., X_{\sigma^{-1}(n)})$.), then $k[Z]^G$ is the subalgebra of symmetric polynomials. It is known to be generated as a k-algebra by the *elementary symmetric polynomials* $\sum_{i=1}^{n} X_i,\ \sum_{i\neq j=1}^{n} X_iX_j, ..., X_1X_2..X_n$. Now, can one realise this subalgebra as the coordinate ring of some affine algebraic set, call it Z/G? In this particular case, it is not too difficult to see that by viewing the affine space k^n as the space of all roots of all polynomial equations of the form $T^n + a_1T^{n-1} + ... + a_n$, the quotient space is precisely the space of all such polynomials, which is parametrised by the coefficients $(a_1, .., a_n)$, so that Z/G in this case is again k^n. The natural quotient map $Z \to Z/G$ is the map:

$$(\lambda_1, .., \lambda_n) \mapsto (-\sum_{i=1}^{n} \lambda_i,\ \sum_{i\neq j=1}^{n} \lambda_i\lambda_j, ..., (-1)^n\lambda_1\lambda_2..\lambda_n)$$

where the right side quite predictably consists of all the elementary symmetric functions in n variables.

For a general finite group, this issue is addressed in the section §5.3 in the sequel.

Even more generally, G could be an algebraic group, and one could again ask for a description of Z/G where Z is an affine algebraic group on which G acts algebraically. This consitutes the still fertile and deep area of algebraic geometry known as invariant theory.

2. Some Algebra

2.1. **Division.** We shall always be dealing with commutative rings with identity. Of course all ring homomorphisms will be required to preserve the identity element. We first need some facts on polynomial rings.

Proposition 2.1.1 (Weak Division Algorithm)**.** Let A be a ring, and let $A[X]$ be the polynomial ring in one variable over A. Let $f(X)$ and $g(X)$ be two polynomials in $A[X]$, of degrees m and n respectively. Let a be the coefficient of the highest degree term in g, and let $k = \max(m - n + 1, 0)$. Then there exist polynomials $q(X)$ and $r(X)$ in $A[X]$ such that :

$$a^k f(X) = q(X)g(X) + r(X)$$

where $r(X) = 0$ or $\deg r(X) < n = \deg g(X)$.

Proof: If $m - n + 1 < 0$, we may take $k = 0$ and $q(X) = 0$, with $r(X) = f(X)$. If $m - n + 1 \geq 0$, we can induct on this quantity $m - n + 1$. Clearly the induction starts because if $m - n + 1 = 0$, we make the same choices as above, namely, $k = q(X) = 0$, and $f(X) = r(X)$. Assume by induction that the result is proven for all r such that $r - n + 1 < m - n + 1$, i.e. $r < m$. Consider the polynomial

$$f_1(X) = af(X) - bX^{m-n}g(X)$$

where b is the leading coefficient of $f(X)$. This polynomial $f_1(X)$ has degree m_1 strictly less than m, and so applying induction:

$$a^l f_1(X) = q_1(X)g(X) + r_1(X)$$

where $l = m_1 - n + 1 < k = m - n + 1$, and $r_1 = 0$ or $\deg r_1 < n$. Substituting $f_1(X) = af(X) - bX^{m-n}g(X)$, we have :

$$a^{l+1} f(X) = (q_1(X) + ba^l X^{m-n})g(X) + r_1(X)$$

Now multiplying both sides by a^{k-l-1} , and by setting

$$q(X) = a^{k-l-1}(q_1(X) + ba^l X^{m-n}) \ ; \ r(X) = a^{k-l-1} r_1(X)$$

we have the result. □

Corollary 2.1.2 (Division Algorithm)**.** In the setting above, let $A = k$ a field. Then there exist polynomials $q(X)$ and $r(X)$ in $A[X]$ such that :

$$f(X) = q(X)g(X) + r(X)$$

where $r(X) = 0$ or $\deg r(X) < n = \deg g(X)$.

Proof: Just divide by a^k in the proposition above. □

Remark 2.1.3. An integral domain in which the division algorithm holds is called a *Euclidean Domain*, and a familiar example is the ring of integers $\mathbb{Z}$. By the last corollary, $k[X]$, where k is a field, is also an Euclidean domain. In a Euclidean domain, one can take greatest common divisors, and also prove unique prime factorisation. Unfortunately, the polynomial ring in several variables over a field is *not* an Euclidean domain. But it is something weaker, called a unique factorisation domain, which we shall discuss in the next section. In such a ring, one may still factorise uniquely into primes, take greatest common divisors, etc.

2.2. **Factorisation.** In this subsection, we look at factorisation in commutative rings. Necessarily, the account is very condensed, and the reader is urged to consult Jacobson's Basic Algebra, Zariski-Samuel's Commutative Algebra or Lang's Algebra for more details.

In this subsection A denotes an integral domain.

Definition 2.2.1 (Units, irreducibles, primes)**.** An element $a \neq 0$ in A is said to be a *unit* if there exists $b \in A$ such that $ab = 1$, i.e. a is invertible. An element $a \neq 0$ in A is said to be *irreducible* if $a = bc$ implies either b or c is a unit. This shows that the only divisors of an irreducible element a are units or a multiplied with a unit. An element $a \neq 0$ in A is said to be *prime* if for every $b, c \in A$ such that a divides bc, we have a divides b or a divides c. (We shall henceforth write $a|b$ to denote that a divides b).

It is an easy exercise to check that prime elements are always irreducible. However the converse is false. One can easily check that in the ring $A = \mathbb{Z}[\sqrt{5}]$, the element 2 is irreducible, but divides the product $(\sqrt{5}+1)(\sqrt{5}-1) = 4$ without dividing either of the factors $\sqrt{5} \pm 1$, and hence not a prime in A.

Definition 2.2.2 (Unique Factorisation Domain)**.** An integral domain A is called a *unique factorisation domain* (UFD) or a *factorial ring* if the following two conditions are satisfied:

(UFD1): If $a \neq 0$ is an element of A, then there exist irreducible elements p_i, and positive integers r_i for $i = 1, 2, ..n$ such that

$$a = up_1^{r_1} p_2^{r_2} .. p_n^{r_n}$$

where u is a unit.

(UFD2): Every irreducible element in A is prime.

From the conditions above, the reader can also easily check that in a UFD, the factorisation into irreducibles is unique, upto multiplication by units and ordering of the irreducible factors. We define, for a non- zero element $a \in A$, A a UFD, p a prime, the non-negative integer $v_p(a)$ by $v_p(a) = r$ if $p|a$ and r is the largest power of p dividing a, and $v_p(a) = 0$ if p does not divide a. Clearly

$$v_p(ab) = v_p(a) + v_p(b)$$

and

$$v_p(a+b) \geq \min(v_p(a), v_p(b))$$

To be consistent with the two properties above for v_p, one defines $v_p(0) = \infty$.

Thus, in a UFD, one may define their greatest common divisor as follows:

Definition 2.2.3. (Greatest common divisor in a UFD) Let A be a UFD and $a, b \in A$ be two non-zero elements. The *greatest common divisor (gcd)* of a and b, denoted (a, b), is :

$$(a, b) = \Pi_{p \text{ prime}}\, p^{r_p}$$

where $r_p = \min(v_p(a), v_p(b))$ and the product is finite since $r_p = 0$ for all but finitely many primes (=irreducibles). Note that greatest common divisors are unique upto multiplication by a unit.

Exercise 2.2.4. Show that an integral domain A is a UFD iff the following condition holds:

(**UFD**) If $a \neq 0$ is any element of A, then there exist irreducible elements p_i, and positive integers r_i for $i = 1, 2, ..n$ such that

$$a = up_1^{r_1} p_2^{r_2} .. p_n^{r_n}$$

where u is a unit. Further, if there is another such factorisation

$$a = vq_1^{s_1} q_2^{s_2} .. q_n^{s_n}$$

into irreducibles, then there exists a permutation σ such that $q_i = v_i p_{\sigma(i)}$ for some unit v_i, and $s_i = r_{\sigma(i)}$, for each $i = 1, 2, .., n$.

Exercise 2.2.5. Show that an integral domain A is UFD iff the following condition holds:

(**UFD'**) If $a \neq 0$ is any element of A, then there exist prime elements p_i, and positive integers r_i for $i = 1, 2, ..n$ such that

$$a = up_1^{r_1} p_2^{r_2} .. p_n^{r_n}$$

where u is a unit.

Remark 2.2.6. We saw above that $\mathbb{Z}[\sqrt{5}]$ is not a UFD. It is true that $\mathbb{Z}[\sqrt{d}]$ is *not a UFD* for $d \equiv 1 \mod 4$. This is because this ring fails to be *integrally closed in its quotient field* $\mathbb{Q}[\sqrt{d}]$ (see later section §4 for definitions, the Exercise 4.2.19 there.) On the other hand, for $d \equiv 2, 3 \mod 4$, it is unknown which are UFD's. It is however known that for $d < 0$, the only $\mathbb{Z}[\sqrt{d}]$ which is a UFD is when $d = -1$ or $d = -2$. (see Theorem 7.7 of Chapter 11 in Artin's *Algebra*).

An important subclass of UFD's are the so-called PID's, which are defined below.

Definition 2.2.7 (Principal Ideal Domains)**.** An integral domain A is said to be a *principal ideal domain (PID)* or *principal ring* if every ideal in A is a principal ideal, i.e. is generated by a single element.

It is easy to see that the ring of integers $\mathbb{Z}$ and the polynomial ring $k[X]$ in one variable over a field k are PID's, because of the Division Algorithm. Just take an ideal $\mathfrak{I}$ in either of these rings. Let $r \neq 0$ be an element in this ideal of least modulus (in the case of $\mathbb{Z}$) or least degree (in the case of $k[X]$). Then every other element $a \neq 0$ of this ideal is either divisible by r, or leaves a remainder r_1 of modulus (resp. degree) less than that of r. In the latter case, since a and r are in $\mathfrak{I}$, so is r_1. But this contradicts the choice of r. Thus every element in $\mathfrak{I}$ is divisible by r. Incidentally, there do exist PID's which are not Euclidean domains, but we needn't bother with them presently. We enumerate some facts on PID's below.

Proposition 2.2.8. Let A be a PID. Then every ascending chain of ideals:

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq ...\mathfrak{a}_k \subseteq \mathfrak{a}_{k+1} \subseteq .....$$

is eventually stationary.

Proof: Let $\mathfrak{a} = \cup_{i=0}^{\infty} \mathfrak{a}_i$, which is easily seen to be an ideal. Since A is a PID, we have an element $a \in A$ such that $\mathfrak{a} = \langle a \rangle$. Then $a \in \mathfrak{a}_n$ for some n, and thus we have $\mathfrak{a} \subseteq \mathfrak{a}_n$, which implies $\mathfrak{a}_j = \mathfrak{a}_n$ for all $j \geq n$. □

Proposition 2.2.9. If A is a PID, then for two non-zero elements a, b of A, their greatest common divisor $d = (a, b)$ exists, and is a generator of the ideal $\langle a, b \rangle$. It is unique upto multiplication by a unit.

Proof: Consider the ideal $\mathfrak{I} = \langle a, b \rangle$ generated by a and b. Since there exists a $d \in A$ such that $\mathfrak{I} = \langle d \rangle$, we have that $d = \lambda a + \mu b$, where $\lambda, \mu \in A$. This shows that any element dividing both a and b must divide d. On the other hand since a, b both belong to $\mathfrak{I} = \langle d \rangle$, d divides both a and b. Thus d is the required greatest common divisor. It is trivial to see that d is well-defined upto multiplication by a unit, because two generators of a principal ideal differ by a unit. □

Proposition 2.2.10. If A is a PID, then the condition UFD2 holds for A.

Proof: Let x be an irreducible element of A, and let $x \mid ab$. Let us assume that x does not divide a. Let $d = (x, a)$, the greatest common divisor guaranteed by the previous proposition. Since $d \mid x$ and x is irreducible, we have $d = ux$ or $d = v$, where u, v are units. In the former case x would divide a, contrary to assumption. Thus $d = v$. This means that $v = \lambda x + \mu a$, and mutliplying with v^{-1}, we have $1 = v^{-1}(\lambda x + \mu a)$, from which it follows that $b = v^{-1}(\lambda xb + \mu ab)$. Now since $x \mid ab$, we have that x divides the right hand side, so $x \mid b$. □

Corollary 2.2.11. Let A be a PID. An ideal $\mathfrak{a} = \langle x \rangle$ with $x \neq 0$ in A is maximal iff x is prime.

Proof: Let x be prime. Then if $\langle x \rangle \subseteq \langle y \rangle$, we have that y divides x. Since x is prime, we have y is a unit, or a unit times x. In the former case $\langle y \rangle = A$, and in the latter case $\langle x \rangle = \langle y \rangle$, showing that $\mathfrak{a} = \langle x \rangle$ is maximal. Conversely, suppose $\mathfrak{a} = \langle x \rangle$ is maximal, and $x \mid ab$ and that x does not divide a. Then the ideal generated by x and a, namely $\langle x, a \rangle$, strictly contains the maximal ideal $\mathfrak{a} = \langle x \rangle$. Thus $\langle x, a \rangle = A$, and we have $1 = \lambda x + \mu a$ which implies $b = \lambda xb + \mu ab$. Since $x \mid ab$ we have x divides the right hand side, and hence $x \mid b$. □

Proposition 2.2.12. If A is a PID, then A is a UFD.

Proof: We have already seen above that A satisfies (UFD2). It suffices to show the factorisation of a general non-zero element $x \in A$ into a unit times finitely many irreducibles. If x is prime, we are done. If not, by the previous proposition 2.2.11 the ideal $\langle x \rangle$ is not maximal, and is included in a maximal ideal $\langle p_1 \rangle$, so that p_1 is a prime by the previous proposition 2.2.11, and $\langle x \rangle \subset \langle p_1 \rangle$ implies p_1 is a prime divisor of x. Write $x = p_1 x_1$. Now apply the same reasoning to x_1 in place of x. We then have an ascending chain of ideals

$$\langle x \rangle \subset \langle x_1 \rangle \subset ....\langle x_n \rangle \subset ...$$

which must become stationary at some point, by the proposition 2.2.8 above. This proves UFD1, and the proposition. □

There are UFD's which are not PID's. For example, we shall see below that $\mathbb{Z}[X]$ is a UFD. However (exercise!), the ideal $\langle 2, X \rangle$ is not a principal ideal.

Definition 2.2.13. Let A be a UFD, and let $f(X) = a_0 + a_1 X + ...a_n X^n$ be a polynomial in $A[X]$. We define the *content of f*, denoted by $c(f)$ to be the greatest common divisor of $a_0, a_1, ..., a_n$. Note that $c(f)$ is defined upto multiplication by a unit. We say a polynomial $f(X)$ is a *primitive polynomial* if $c(f)$ is a unit.

Clearly every polynomial $f(X)$ maybe written uniquely as $c(f)f_1(X)$, where $f_1(X)$ is a primitive polynomial. We have the following :

Proposition 2.2.14 (Gauss' Lemma)**.** Let A be a UFD, and $f(X)$ and $g(X)$ be two polynomials in $A[X]$. Then :

$$c(fg) = c(f)c(g)$$

Proof: Write $f = c(f)f_1$ and $g = c(g)g_1$, where f_1 and g_1 are primitive. Then $fg = c(f)c(g)f_1g_1$. It suffices to show that f_1g_1 is a primitive polynomial. Let p be any prime factor dividing all the coefficients of f_1g_1. Let $f_1(X) = \sum_{i=0}^{n} a_i X^i$ and $g_1(X) = \sum_{i=0}^{m} b_i X^i$. Since f_1 and g_1 are primitive, there must be positive integers j and l such that $p \mid a_i$ for $0 \leq i \leq j-1$ but p does not divide a_j, and similarly $p \mid b_k$ for $0 \leq k \leq l-1$ but p does not divide b_l. Now note that the coefficient of X^{j+l} is of the form ($a_jb_l +$ terms divisible by p), by the above choice of j and l. Since p divides this coefficient, it must divide a_jb_l. Since p is prime, it must divide either a_j or b_l. This contradicts the choice of j and l. Hence f_1g_1 is primitive, and we are done. □

Proposition 2.2.15. Let A be a UFD and $b \neq 0$ be an element of A, and $f(X)$ be a polynomial in $A[X]$. Let g be a non-zero primitive polynomial such that $g \mid bf$. Then $g \mid f$.

Proof: $g \mid bf$ implies that $gh = bf$, which implies $c(g)c(h) = c(h) = c(b)c(f) = bc(f)$ by Gauss' lemma and primitivity of g. But this means that $b \mid c(h)$. Thus $h = c(h)h_1 = bH$, where H is some polynomial. Now substituting in $gh = bf$, we have $gH = f$, and the proposition follows. □

Corollary 2.2.16. Let A be a UFD, and Q denote its quotient field. If $f(X)$ is an irreducible polynomial in $A[X]$, then it is irreducible in $Q[X]$.

Proof: Write $f = gh$, with $g, h \in Q[X]$. Clearly, multiplying by the denominators occurring in the coefficients of g and h, we have $bf = GH$ where $G, H \in A[X]$, and $b \in A$. Write $G = c(G)G_1$, where G_1 is a primitive polynomial in $A[X]$ (since A is a UFD). Thus the primitive polynomial G_1 divides bf.

By the previous proposition 2.2.15, it follows that G_1 divides f in $A[X]$. Since f is irreducible in $A[X]$, G_1 must be a unit or a unit times f in $A[X]$. But it is easy to see that units in $A[X]$ are precisely the units in A, so $G_1 = u$ or $G_1 = uf$, where $u \in A$ is a unit in A. Since g is a non-zero multiple of G in $Q[X]$, and thus a unit times G_1 in $Q[X]$, we have that g is a unit or a unit times f in $Q[X]$, i.e., f is irreducible in $Q[X]$. The proposition follows. □.

Proposition 2.2.17. If A is a UFD, then $A[X]$ is also a UFD.

Proof: (UFD1) is easy. Write $f = c(f)f_1$, where f_1 is primitive. By factorising $c(f)$ into irreducibles in A which are also clearly irreducible in $A[X]$, we are reduced to considering the case of f primitive of degree greater than 0. If it is irreducible, we are done, or else it is factorisable as gh, where neither factor has degree 0 because f is primitive. Thus both g and h have degree strictly less than that of f, and are still of degree greater than 0. We are through by induction.

To show (UFD2), let p be an irreducible polynomial dividing a product fg, and let us assume p does not divide f. Consider the ideal $\mathfrak{a}$ generated by p and f. Let ϕ be the polynomial of least degree in $\mathfrak{a}$. By the weak division algorithm, proposition 2.1.1, we have $a^k f = b\phi + r$, where a is the leading coefficient of ϕ and the degree of r is strictly less than that of ϕ if $r \neq 0$. Since $a^k f - b\phi \in \mathfrak{a}$, the case $r \neq 0$ would contradict that ϕ has least degree in $\mathfrak{a}$, so $r = 0$. Thus $a^k f = bc(\phi)\phi_1$ where ϕ_1 is primitive. By the proposition 2.2.15 above, ϕ_1 divides f. Similarly, ϕ_1 divides p. Since p is irreducible, we have that ϕ_1 is either a unit, or a unit times p. The latter possibility would imply that $p \mid f$, since we have seen that $\phi_1 \mid f$, contradicting our assumption that p does not divide f. Thus ϕ_1 is a unit, and $\phi = c(\phi) := c \in A$. Also $c \in \mathfrak{a}$ implies $c = \alpha f + \beta p$, where $\alpha, \beta \in A[X]$. Then $cg = \alpha fg + \beta pg$. By assumption p divides the right hand side, so $p \mid cg$. Since p is irreducible, and therefore primitive, the proposition 2.2.15 implies that $p \mid g$. Hence $A[X]$ is a UFD. □

Corollary 2.2.18. If A is a UFD, $A[X_1, ...X_n]$ is a UFD.

Proof: $A[X_1, ..., X_n] = A[X_1, ..., X_{n-1}][X_n]$ and induction. □

Exercise 2.2.19 (Eisenstein's Criterion for Irreducibility)**.** Prove that if $f(X) = \sum_{i=0}^{n} a_i X^i$ is a polynomial in $\mathbb{Z}[X]$, and $p \in \mathbb{Z}$ is a prime satisfying:

(i): p does not divide a_n.

(ii): $p \mid a_i$ for $i = 0, 1, .., n-1$.

(iii): p^2 does not divide a_0

then $f(X)$ is an irreducible polynomial in $\mathbb{Q}[X]$. If f is primitive, then it is irreducible in $\mathbb{Z}[X]$. As a corollary to this criterion, prove that the polynomial $1 + X + X^2 + ... + X^{p-1}$ is irreducible in $\mathbb{Q}[X]$. for p a prime. What happens if p is not a prime?

Exercise 2.2.20. Show that the only irreducible polynomials in $\mathbb{C}[X]$ are of degree ≤ 1, and the only irreducible polynomials in $\mathbb{R}[X]$ are of degree ≤ 1 or degree 2 polynomials with no real roots.

Exercise 2.2.21 (Power Series Rings)**.** Let A be a ring, and $A[[X]]$ denote the *ring of formal power series* in the variable X. That is, an element $f(X) \in A[[X]]$ is a formal expression

$$f(X) = \sum_{k=0}^{\infty} a_k X^k$$

with $a_k \in A$. Addition is defined in the obvious manner (coefficientwise), and multiplication of $f = \sum_{k=0}^{\infty} a_k X^k$ and $g = \sum_{k=0}^{\infty} b_k X^k$ by collecting coefficients, viz.

$$gh = \sum_{k=0}^{\infty} c_k X^k$$

where $c_k = \sum_{j+l=k} a_j b_l$. We leave it to the reader to make the analogous definition for the power series ring $A[[X_1, .., X_n]]$ in n-variables, and check that it is isomorphic to $A[[X_1, .., X_{n-1}]][[X_n]]$ in a canonical manner. Also note that the polynomial ring $A[X_1, .., X_n]$ is a subring of $A[[X_1, .., X_n]]$ via the natural inclusion.

Show that:

(i): If A is an integral domain, so is $A[[X]]$.

(ii): $f(X) = \sum_{k=0}^{\infty} a_k X^k$ is a unit in $A[[X]]$ iff a_0 is a unit in A. In particular, if $A = k$, a field, then the units in $k[[X]]$ are precisely the power series with non-zero constant term.

(iii): If $\mathfrak{m}$ is a maximal ideal in $A[[X]]$, then $X \in \mathfrak{m}$. (*Hint:* Show that $1 + aX$ is a unit for each $a \in A[[X]]$).

(iv): If $\mathfrak{m}$ is a maximal ideal in $A[[X]]$, then $\mathfrak{m}^c := \mathfrak{m} \cap A$ is a maximal ideal in A, and $\mathfrak{m}$ is generated by $\mathfrak{m}^c$ and X. (*Hint:* Use (iii) above to show that $\mathfrak{m}^c$ consists of precisely the constant terms of all the elements of $\mathfrak{m}$, and apply the canonical homomorphism $A[[X]] \to A$ sending each power series to its constant term.)

(v): Conclude that if A is a *local ring*, i.e., it has a unique maximal ideal $\mathfrak{m}$, then $A[[X]]$ is also a local ring (with unique maximal ideal $\langle \mathfrak{m}, X \rangle$). Since a field k is a local ring (with unique maximal ideal $\{0\}$), it follows that $k[[X]]$ is a local ring, and by induction, the power series ring $k[[X_1, .., X_n]]$ is also a local ring, with unique maximal ideal $\mathfrak{m} = \langle X_1, .., X_n \rangle$.

(vi): A local ring A whose maximal ideal satisfies

$$\bigcap_{k=1}^{\infty} \mathfrak{m}^k = \{0\}$$

is called a *complete local ring*. Show that if A is a complete local ring, then so is $A[[X]]$. Conclude that $k[[X_1, .., X_n]]$ is a complete local ring. Show that if $f, g \in k[[X_1, .., X_n]]$ satisfy $f \equiv g \pmod{\mathfrak{m}^k}$ for all $k \geq 1$, (where $\mathfrak{m} = \langle X_1, .., X_n \rangle$), then $f = g$. Note that determining $f \pmod{\mathfrak{m}^k}$ amounts to knowing all the terms in f of degree $\leq k - 1$.

Before we investigate factoriality in $k[[X_1, .., X_n]]$, k a field, we need a very important result which allows us to reduce many questions on formal power series to questions on polynomials. For notational convenience we shall denote by $f(0, 0, .., X_n)$ the power series in $k[[X_n]]$ which is the image of $f \in k[[X_1, .., X_n]]$ under the natural surjection

$$k[[X_1, .., X_n]] \to k[[X_1, .., X_n]]/\langle X_1, .., X_{n-1} \rangle = k[[X_n]]$$

Theorem 2.2.22 (Weierstrass Preparation Theorem)**.** Let $f \in k[[X_1, ..., X_n]]$ be a formal power series satisfying $f(0, 0, .., X_n) \neq 0$ in $k[[X_n]]$. Then there exists a unit $u \in k[[X_1, .., X_n]]$, an integer $d \geq 0$, and elements $b_i \in k[[X_1, .., X_{n-1}]]$ for $i = 0, .., d - 1$ such that:

$$f = u(X_n^d + b_{d-1} X_n^{d-1} + ... + b_0)$$

satisfying $b_i(0, .., 0) = 0$ in k for $0 \leq i \leq (d - 1)$. Further, this expression for f is unique.

Proof: For notational convenience, denote the ring $k[[X_1, .., X_{n-1}]]$ by A, and its unique maximal ideal $\langle X_1, .., X_{n-1} \rangle$ by $\mathfrak{m}$. Thus $f \in A[[X_n]]$, and we may write:

$$f = \sum_{k=0}^{\infty} a_k X_n^k$$

where $a_k \in A$ are formal power series in the variables $(X_1, .., X_{n-1})$.

Let $d \geq 0$ be the smallest integer m such that $a_m(0, .., 0) \neq 0$ in k. Clearly d exists since we have assumed $f(0, 0, .., X_n)$ is not identically 0. In the series expression of f above, it is the first coefficient a_m which is not in $\mathfrak{m}$, i.e. has a non-zero constant term.

Let us write $u = c_0 + c_1 X_n + ..c_j X_n^j + ...$ If we require u to be a unit, we must have c_0 a unit in A, by (ii) of 2.2.21. Thus c_0 is a unit modulo $\mathfrak{m}$.

We have to solve for b_i and c_j so that:

$$\begin{aligned} a_0 &= b_0c_0 \\ a_1 &= b_0c_1 + b_1c_0 \\ &\cdot \\ a_{d-1} &= b_0c_{d-1} + b_1c_{d-2} + ... + b_{d-1}c_0 \\ a_d &= b_0c_d + b_1c_{d-1} + ... + b_{d-1}c_1 + c_0 \\ &\cdot \\ a_{d+1} &= b_0c_{d+1} + b_1c_d + ... + b_{d-1}c_2 + c_1 \\ a_{m+d} &= b_0c_{m+d} + b_1c_{m+d-1} + ... + b_{d-1}c_{m+1} + c_m \text{ for all } \quad m \geq 0 \end{aligned}$$

By (vi) of the Exercise 2.2.21 above, to determine b_i and c_j for $i, j \geq 1$, it is enough to determine them modulo $\mathfrak{m}^r$ for every r. The left hand sides of the first d equations above are all $\equiv 0 \pmod{\mathfrak{m}}$, and since $c_0 \neq 0 \pmod{\mathfrak{m}}$, we have $b_0 \equiv 0 \pmod{\mathfrak{m}}$. Plugging in the second equation, we get $b_1 \equiv 0 \pmod{\mathfrak{m}}$, and then moving down the rest, we have $b_0, .., b_{d-1}$ are all $\equiv 0 \pmod{\mathfrak{m}}$. Plugging this into the remaining equations we obtain that $c_j \equiv a_{d+j} \pmod{\mathfrak{m}}$ for all $j \geq 0$. Thus all the b_i and c_j are determined $(\text{mod } \mathfrak{m})$.

Now suppose, we have inductively determined all the b_i and c_j $(\text{mod } \mathfrak{m}^r)$. We wish to determine them $(\text{mod } \mathfrak{m}^{r+1})$. Since $b_0 \equiv 0 \pmod{\mathfrak{m}}$, and we now know $c_0 \pmod{\mathfrak{m}^r}$, it is easy to see from the first equation $a_0 = b_0c_0$ that b_0 gets determined modulo $\mathfrak{m}^{r+1}$. Combining this with the facts that c_1 is already known $(\text{mod } \mathfrak{m}^r)$ and $b_0 \equiv 0 \text{ mod } \mathfrak{m}$, it again follows that b_0c_1 is determined $(\text{mod } \mathfrak{m}^{r+1})$. Plugging $c_0 \pmod{\mathfrak{m}^r}$, and $b_1 \pmod{\mathfrak{m}^r}$ in the second equation determines $b_1 \pmod{\mathfrak{m}^{r+1}}$. Proceeding down to the remaining equations upto the d-th one determines all the $b_j \pmod{\mathfrak{m}^{r+1}}$. By putting in these $b_j \pmod{\mathfrak{m}^{r+1}}$ in the $(d+1)$-th equation onwards determines all the $c_j \pmod{\mathfrak{m}^{r+1}}$. The induction is complete, and the existence of a factorisation as claimed is proved. The uniqueness is obvious, because d is uniquely determined by f, and the unit u is uniquely determined as the coefficient of X_n^d in any two such factorisations. Equating the coefficients of $X_n^{d-1}, ...,$ etc determines the b_j uniquely. □

Remark 2.2.23. The Weierstrass Preparation Theorem above crops up in many contexts, notably the theory of holomorphic functions of several complex variables. It reduces may questions on holomorphic functions of several variables into questions about polynomials. See, for example, the book of Gunning and Rossi entitled *Analytic Functions of Several Complex Variables* for the holomorphic version of 2.2.22.

Exercise 2.2.24. Let k be an infinite field, and let $f \neq 0$ be a formal power series in the ring $k[[X_1, .., X_n]]$. Show that we can make a linear non-singular change $X_i = \tau_i(Y_1, .., Y_n)$ of variables to $Y_1, .., Y_n$ such that the transformed power series

$$\widetilde{f}(Y_1, .., Y_n) := f(\tau_1(Y_1, .., Y_n), .., \tau_n(Y_1, .., Y_n)) \in k[[Y_1, .., Y_n]]$$

satisfies $\widetilde{f}(0, 0, .., Y_n) \neq 0$ in $k[[Y_n]]$.

Now we can prove that $k[[X_1, .., X_n]]$ is a UFD. We prove it below only for an infinite field, but it is true for all fields.

Proposition 2.2.25. Let k be an infinite field. The power series ring $k[[X_1, .., X_n]]$ is a UFD.

Proof: The case of $n = 1$ is trivial, because every element can be written as a unit times X^k, and from this it easily follows that $k[[X]]$ is a principal ideal domain (in fact, every ideal is a power of the unique maximal ideal $\mathfrak{m} = \langle X \rangle$). From the proposition 2.2.12, it follows that $k[[X]]$ is a UFD.

Inductively assume that $A := k[[X_1, .., X_{n-1}]]$ is a UFD. Let $f \in A[[X_n]] = k[[X_1, .., X_n]]$ be a non-zero element. In view of exercise 2.2.24, we may assume without loss of generality that $f(0, 0, .., X_n) \neq 0$.

By the Weierstrass Preparation Theorem 2.2.22, we may write:

$$f = ug$$

where $u \in A[[X_n]]$ is a unit, and g is a polynomial, lying in $A[X_n]$. Since A is a UFD by the induction hypothesis, so is the polynomial ring $A[X_n]$, by the proposition 2.2.18. Hence we may write:

$$g = vg_1^{s_1}g_2^{s_2}...g_r^{s_r}$$

where v is a unit in $A[X_n]$ (hence in A), and g_i are irreducible elements in $A[X_n]$. Thus f is factorised as:

$$f = uvg_1^{s_1}g_2^{s_2}...g_r^{s_r}$$

We claim that the polynomials $g_i \in A[X_n]$ continue to be irreducible in $A[[X_n]]$. This is because $f(0,..,X_n) \neq 0$ implies (since $A[[X_n]]$ is an integral domain) that $g_i(0,0,..,X_n) \neq 0$ for $i = 1,..,r$. If $g_i = G.H$ in $A[[X_n]]$, with $G, H \in A[[X_n]]$, it follows that $G(0,..,X_n) \neq 0$ and $H(0,..,X_n) \neq 0$.

Thus, by the Weierstrass Preparation Theorem 2.2.22 applied to G, H, we have that $G = u_1P$, $H = u_2Q$ for some units $u_i \in A[[X_n]]$ and $P, Q \in A[X_n]$. Thus:

$$g_i = wP.Q$$

where $w = u_1u_2$ is a unit. Since g_i is a polynomial in $A[X_n]$, the uniqueness assertion in the Weierstrass Preparation Theorem implies that one of P or Q is a unit in $A[[X_n]]$. So one of G or H is a unit in $A[[X_n]]$, proving our assertion that g_i are all irreducible in $A[[X_n]]$.

We now need to show that the factorisation of f above is unique. The factorisation $f = ug$ above, by 2.2.22, is unique, and the factorisation of $g \in A[X_n]$ into irreducibles is unique (upto units in A), since $A[X_n]$ is a UFD, so that the factorisation of f above is unique. By the exercise 2.2.4, the ring $k[[X_1,..,X_n]]$ is a UFD. □

Remark 2.2.26. The reader may wonder why one didn't adopt induction to show that $k[[X_1,..,X_n]]$ is a UFD as we did for polynomial rings. The reason is that there exist UFD's A such that $A[[X]]$ is *not* a UFD (see Lang, *Algebra*, p.). It is however known that if A is a PID, then $A[[X_1,..,X_n]]$ is a UFD. (See Bourbaki, *Commutative Algebra*). In particular $\mathbb{Z}[[X_1,..,X_n]]$ is a UFD, as is $k[T][[X_1,..,X_n]]$ for k a field. If A is a *discrete valuation ring* (viz. an integrally closed Noetherian domain with a unique non-zero prime-ideal), then again $A[[X_1,..,X_n]]$ is a UFD.

2.3. **Noetherian Modules and Rings.**

Definition 2.3.1. A module M over a ring A is said to be *Noetherian* if every A-submodule N of M is finitely generated. A ring is said to be *Noetherian* if it is Noetherian considered as a module over itself, i.e., if every ideal of A is finitely generated.

Proposition 2.3.2. For an A module M, the following conditions are equivalent:

(i): Every non-empty set $\{M_\alpha\}_{a\in\Lambda}$ of submodules of M has a maximal element.
(ii): Every ascending chain $M_0 \subseteq M_1 \subseteq M_2..... \subseteq M_n \subseteq ...$of submodules of M becomes eventually stationary.
(iii): M is Noetherian

Proof:
(i)⇒(ii)
Let $M_0 \subseteq M_1 \subseteq M_2..... \subseteq M_n \subseteq ....$ be an ascending chain of submodules of M. Then the family $\{M_i\}_{i=1}^{\infty}$ must have a maximal element, say N. Then $N = M_j$ for some j, and by maximality, $M_k \supseteq M_j = N$ for all $k \geq j$ implies that $M_k = M_j$ for all $k \geq j$.

(ii)⇒(iii)
Assume M is not Noetherian, so some submodule $N \subseteq M$ is not finitely generated. Then, we can choose a countable family of distinct elements $\{x_i\}_{i\in\mathbb{N}}$ of N, such that the chain of submodules of N,

$$\langle x_1\rangle \subseteq \langle x_1, x_2\rangle \subseteq ... \subseteq \langle x_1, x_2, ..., x_i\rangle \subseteq ...$$

is strictly ascending, and so does not become stationary, contradicting (ii).

(iii)⇒(i)

Let $\{M_\alpha\}_{a\in\Lambda}$ be a family of submodules of M . Order it by inclusion, and note that every totally ordered subfamily $\Gamma \subset \Lambda$ will have the submodule $N = \cup_{\alpha\in\Gamma} M_\alpha$, as an upper bound. We claim that $N = M_\gamma$, for some $\gamma \in \Lambda$, i.e. N is a member of this family Γ. By hypothesis M is Noetherian, so N is finitely generated, i.e. $N = \langle x_1, x_2, ..x_n\rangle$. Since Γ is totally ordered, there will exist an M_γ for some $\gamma \in \Gamma$, which contains all of the $\{x_i\}_{i=1}^n$. Clearly $N = M_\gamma$. This proves the claim. Now Zorn's Lemma proves that the family $\{M_\alpha\}_{a\in\Lambda}$ has maximal elements, and the proposition follows. □

Proposition 2.3.3. If M is a Noetherian module, then every quotient and submodule of M is Noetherian. If there is a short exact sequence :

$$0 \longrightarrow L \xrightarrow{i} M \xrightarrow{\pi} N \longrightarrow 0$$

of A-modules with L and N Noetherian, then M is Noetherian.

Proof: The first two assertions are clear by the definition.

Recall that the sequence above is said to be *exact* if $\operatorname{Im} i = \ker \pi$, i is injective and π is surjective. Now, for the second statement, let P be a submodule of M. Then $\pi(P)$ is finitely generated since it is a submodule of the Noetherian module N. Let $\{\pi(x_i)\}_{i=1}^n$ be a finite set of generators for $\pi(P)$, where $x_i \in P$. Since L is given to be Noetherian, so is its isomorphic image $i(L)$. Let $\{y_j\}_{j=1}^m$ be a finite set of generators for the submodule $P \cap i(L)$ of $i(L)$. Then, for $x \in P$, $\pi(x) = \sum_{i=1}^n a_i\pi(x_i)$, so that the element $x - \sum_{i=1}^n a_i x_i$ is in $P \cap \ker\pi = P \cap i(L)$, and is therefore equal to $\sum_{j=1}^m b_j y_j$ for some b_j. Thus P is generated by the $m + n$ elements $\{x_1, ...x_n, y_1...., y_m\}$, and the proposition is proved. □

Example 2.3.4. Every field is a Noetherian ring, as is every PID. So $\mathbb{Z}$, $k[X]$, $\mathbb{Z}[i]$ are all Noetherian rings.

Example 2.3.5. The ring $C([0, 1])$ of continuous real or complex valued functions is not Noetherian. The ideals:

$$\mathfrak{a}_m = \{f : f(x) = 0 \ \forall\ x \in [0, 1/m]\}$$

for $m \in \mathbb{N}$ is an ascending chain of ideals which is not stationary.

Proposition 2.3.6. Let A be a Noetherian ring, and M be a finitely generated A-module. Then M is a Noetherian module.

Proof: If M is generated by a single element, say x, then it is a quotient of the Noetherian module A, i.e. it is isomorphic to $A/\mathfrak{a}$ where the ideal $\mathfrak{a}$ is defined by :

$$\mathfrak{a} = \operatorname{Ann} x := \{a \in A : ax = 0\}$$

called the *annihilator* of x. Thus M is a quotient of the module A, which is a Noetherian module since it is a Noetherian ring. So it is Noetherian, by the first part of the proposition 2.3.3. Now proceed by induction on the number of generators, and the second part of proposition 2.3.3 about exact sequences. □

We now prove a very crucial result about polynomial rings:

Proposition 2.3.7 (Hilbert Basis Theorem)**.** If A is a Noetherian ring, then the polynomial ring $A[X]$ is also a Noetherian ring.

Proof: Let $\mathfrak{a}$ be an ideal in $A[X]$, and let $\mathfrak{I}$ be the ideal of A generated by all the leading coefficients of elements of $\mathfrak{a}$. Since A is Noetherian, there is a finite set of generators, say $\{a_i\}_{i=1}^n$, for $\mathfrak{I}$. Let $f_i(X)$ be a polynomial in $\mathfrak{a}$ with leading coefficient a_i for $i = 1, 2..., n$, and let r_i be the degree of $f_i(X)$.

Let $r = \max\{r_i : 1 \le i \le n\}$ and M be the $A-$submodule of $A[X]$ consisting of all polynomials of degree less than or equal to $(r-1)$ (i.e. $M = A+AX+...AX^{r-1}$). Since M is finitely generated, and A is Noetherian, we have that M is Noetherian,by proposition 2.3.6. Therefore the A-submodule $\mathfrak{a} \cap M$ of M is also finitely generated as an A-module, by proposition 2.3.3.

Let $\{t_j\}_{j=1}^m$ be a set of generators for this A-module $\mathfrak{a} \cap M$. We claim that the set $S = \{f_1, f_2, .., f_n, t_1, .., t_m\}$ generates $\mathfrak{a}$. If $f(X)$ is any polynomial in $\mathfrak{a}$ of degree less than or equal to $r-1$, then $f(X)$ lies in $\mathfrak{a} \cap M$ and hence is an A-linear combination of the elements t_j. Therefore, assume that $\deg(f) \geq r$. We induct on $k = \deg(f)$. Write $f(X) = aX^k + ... + a_0$. We have $a \in \mathfrak{I}$, so $a = \sum_{i=1}^n \lambda_i a_i$. Consider the element :

$$g(X) = f(X) - \sum_{i=1}^{n} \lambda_i X^{k-r_i} f_i.$$

which makes sense since $k \geq r \geq r_i$ for $i = 1, 2, ..n$. Since f, and f_i all belong to $\mathfrak{a}$, this element $g(X)$ also belongs to $\mathfrak{a}$. On the other hand its leading coefficient is $(a - \sum_{i=1}^n \lambda_i a_i) = 0$. Thus $\deg(g) < \deg(f)$, and by induction hypothesis, $g(X)$ belongs to the ideal generated by S. Also, so does $\sum_{i=1}^n \lambda_i X^{k-r_i} f_i$, and hence so does $f(X)$, and we are done. □

Corollary 2.3.8. If A is Noetherian, so is $A[X_1, ...X_n]$, by induction on the number of variables and the proposition above. If k is a field, $k[X_1, ...X_n]$ is a Noetherian ring.

Definition 2.3.9. Let k be a field. We say a k-algebra A is of *finite type* if A is generated as a k-algebra by finitely many elements $\{y_1, y_2, ...y_n\}$. That is, every element of A is a finite $k-$linear combination (not necessarily unique) of elements in the set

$$\{y_1^{r_1} y_2^{r_2} ... y_n^{r_n} : \ r_i \in \mathbb{Z}_+\}$$

Clearly, a k-algebra of finite type is the quotient of a polynomial ring $k[X_1, ...X_n]$, and hence we have the

Corollary 2.3.10. Every k-algebra of finite type is Noetherian.

Proof:
Let A be a k-algebra of finite type, generated by $\{y_i\}_{i=1}^n$, and let $\pi : k[X_1, ...X_n] \to A$ be the k-algebra homomorphism defined by $\pi(X_i) = y_i$. If $\mathfrak{a}$ is an ideal in A, verify that $\pi^{-1}(\mathfrak{a})$ is an ideal in the polynomial ring $k[X_1, ...X_n]$, and hence generated as an ideal by finitely many polynomials $\{f_i(X_1, ...X_n)\}_{i=1}^m$. It is clear that $\mathfrak{a} = \pi\pi^{-1}(\mathfrak{a})$ is generated as an A-ideal by $\pi(f_i) = f_i(y_1, ..., y_n)$. □

Example 2.3.11. It is possible for a Noetherian ring to contain a *non*-Noetherian subring. By the above corollary, the polynomial ring $k[X, Y]$ in two variables is Noetherian. However, consider $A \subset k[X, Y]$ to be the k-subalgebra generated by the infinitely many elements $X, XY, XY^2, ..., XY^i, ...$ Then if we define the chain of ideals $\mathfrak{a}_i = \langle X, XY, .., XY^i \rangle$, we see that $\mathfrak{a}_{i+1}$ strictly contains $\mathfrak{a}_i$ for all i, and this ascending chain does not become stationary. Thus A is not Noetherian. Also, in particular, by the above Corollary 2.3.10, A is not a k-algebra of finite type, even though it is a subalgebra of $k[X, Y]$, which is a k-algebra of finite type.

We now look at the Noetherian-ness of power series rings (see the Exercise 2.2.21 for the definitions).

Proposition 2.3.12. Let A be a Noetherian ring. Then the ring of formal power series $A[[X]]$ is a Noetherian ring.

Proof: Let $\mathfrak{a} \subset A[[X]]$ be an ideal. For $j = 0, 1, ...,$ define

$$\mathfrak{q}_j := \{a \in A : \ \exists \ f \in \mathfrak{a} \text{ with } f = aX^j + ...\text{higher order terms}\}$$

(Compare with the proof of 2.3.7, where we considered the ideal of *leading* coefficients, i.e. coefficients of the degree terms). It is easy to check that $\mathfrak{q}_j$ is an ideal, and since $Xf \in \mathfrak{a}$ for $f \in \mathfrak{a}$, it follows that:

$$\mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subseteq ... \subseteq \mathfrak{q}_j \subseteq \mathfrak{q}_{j+1} ....$$

is an ascending chain of ideals in A. By (ii) of the proposition 2.3.2, this chain becomes eventually stationary, which implies $\mathfrak{q}_j = \mathfrak{q}$ for all $j \geq r$.

Since A is Noetherian, $\mathfrak{q}$ is finitely generated, so let $\{a_1, .., a_m\}$ be a set of generators for $\mathfrak{q}$. Let $f_1, .., f_m \in \mathfrak{q}_r = \mathfrak{q}$ such that $f_j = a_j X^r + ..$(higher order terms).

For any power series $f = a_0 + a_1 X + ..a_j X^j + ..$, define the *order* of f by

$$\text{ord}(f) = \min\{k : a_k \neq 0\}$$

We claim that each $f \in \mathfrak{a}$ with $\text{ord}(f) \geq r$ is in the ideal $\langle f_1, .., f_m \rangle \subset \mathfrak{a}$. For let

$$f = b_r X^r + ...$$

be an element of $\mathfrak{a}$. Then $b_r \in \mathfrak{q}_r = \mathfrak{q}$, and we can write $b_r = \sum_{j=1}^m \lambda_{0j} a_j$, where $\lambda_{0j} \in A$. Then we have:

$$f - \sum_{j=1}^m \lambda_{0j} f_j = b_{r+1} X^{r+1} + ...$$

which is in $\mathfrak{a}$, so that $b_{r+1} \in \mathfrak{q}_{r+1} = \mathfrak{q}$. Again write $b_{r+1} = \sum_{j=1}^m \lambda_{1j} a_j$, and note that

$$f - \sum_{j=1}^m \lambda_{0j} f_j - \sum_{j=1}^m \lambda_{1j} X f_j = b_{r+2} X^{r+2} ....$$

That is,

$$f - \sum_{j=1}^m (\lambda_{0j} + \lambda_{1j} X) f_j = b_{r+2} X^{r+2} + ...$$

Proceeding inductively, we find that

$$f = \sum_{j=1}^m (\lambda_{0j} + \lambda_{1j} X + ..\lambda_{ij} X^i + ...) f_j$$

which proves our claim.

Now let $a_{j1}, .., a_{jm_j}$ be a set of generators for $\mathfrak{q}_j$ for $j = 0, 1, .., r-1$. Let $f_{j1}, .., f_{jm_j}$ be elements of $\mathfrak{q}_j$ such that:

$$f_{jl} = a_{jl} X^j + ...\text{(higher order terms)} \quad \text{for } \ 1 \leq l \leq m_j, \ \ 0 \leq j \leq r-1$$

Now if $f = b_0 + ..$ is *any* element of $\mathfrak{a}$, $b_0 \in \mathfrak{q}_0$, and we can write $b_0 = \sum_{l=1}^{m_0} \mu_{0l} a_{0l}$, with $\mu_{0l} \in A$. Then the element:

$$f - \sum_{l=1}^{m_0} \mu_{0l} f_{0l}$$

has order ≥ 1, and can be written as:

$$f - \sum_{l=1}^{m_0} \mu_{0l} f_{0l} = b_1 X + ...$$

and since this element is in $\mathfrak{a}$, we have $b_1 \in \mathfrak{q}_1$. Proceeding by the inductive method outlined above, we will finally have

$$\text{ord}\left(f - \sum_{j=0}^{r-1} \sum_{l=1}^{m_j} \mu_{jl} f_{jl} \right) \ \geq \ r$$

with $\mu_{jl} \in A$. In view of the claim in the previous paragraph, this implies that $\mathfrak{a}$ is generated by the finite set:

$$S = \{f_{jl} : \ 0 \leq j \leq r-1, \ 1 \leq l \leq m_j\} \cup \{f_1, .., f_m\}$$

Thus $\mathfrak{a}$ is finitely generated, and $A[[X]]$ is Noetherian.

□

Corollary 2.3.13. Let k be a field. Then the power series ring $k[[X_1, .., X_n]]$ is Noetherian.

Proof: Apply the proposition above, inducting on n. □.

Here are some additional exercises on polynomials, power series, Noetherian rings and modules.

Exercise 2.3.14. Let $k[X]$ be the polynomial ring in one variable over a field k. Prove that the principal ideal $\langle f(X)\rangle$ is a maximal ideal iff f is irreducible ($\Leftrightarrow$ f is prime).

Exercise 2.3.15. For A an integral domain, consider the following conditions:

(i): Every ascending chain of *principal ideals*:

$$\langle a_1\rangle \subset \langle a_2\rangle .... \subset \langle a_n\rangle \subset ....$$

becomes stationary.

(ii): Every $a \neq 0$ in A can be factorised as a unit times finitely many irreducibles.

Show that the condition (i) implies the condition (ii). In particular, if A is a Noetherian integral domain, then every element factorises as a product of a unit and irreducibles. Thus the "key" condition for A to be UFD is the condition UFD2.

What about (ii) $\Rightarrow$ (i)?

Exercise 2.3.16. For the power series ring $k[[X]]$ in one variable, prove that the division algorithm holds. (*Hint:* Consider the function $\delta(f) = \text{ord}(f)$, where $\text{ord}(f)$, the *order of* f is defined in the proof of Proposition 2.3.12.)

Exercise 2.3.17. Let A be a Noetherian ring and $f : A \to B$ be a ring homomorphism. We may make B an A-module via f, i.e. define $a.b := f(a)b$. Suppose that B is finitely generated as an A-module, with this A-module structure. Then show that B is a Noetherian ring.

Exercise 2.3.18. Let $f : A \to B$ be a ring homomorphism, with A Noetherian. Consider B as an A-algebra via f, as in the previous exercise. Suppose B is an A- algebra of finite type (i.e. is a quotient of some polynomial algebra $A[X_1, .., X_n]$). Again show that B is a Noetherian ring.

Exercise 2.3.19. Let A be a Noetherian ring, and let $f : A \to A$ be a surjective ring homomorphism. Then show that f is also injective. Similarly, show that if $f : M \to M$ is a surjective module homomorphism of a Noetherian A-module M, then f is injective. (*Hint*: Consider the sequence of ideals (resp. submodules) $\ker f \subset \ker f^2 \subset ... \subset \ker f^n \subset ...$)

Exercise 2.3.20 (Germs of analytic functions)**.** Let $k = \mathbb{C}$, and consider the subring of $\mathbb{C}[[X]]$ defined by:

$$\mathcal{O}_{0,an} = \{f = \sum_{n=0}^{\infty} a_n X^n : \limsup_{n\to\infty} \mid a_n \mid^{1/n} < \infty\}$$

This subring is called the *ring of germs of holomorphic functions at* 0, and represents all holomorphic functions whose Taylor expansions are convergent in a neighbourhood of 0 (by using the Taylor expansion). Show that $\mathcal{O}_{0,an}$ is also a local ring, with unique maximal ideal $\mathfrak{m}$ consisting of all functions vanishing at 0 (i.e. those with zero constant term). Is it a Euclidean domain? A PID? A UFD? Upto units, what are the irreducibles of $\mathcal{O}_{0,an}$?

There is an obvious analogous ring (of *germs of real analytic functions at* 0 with $k = \mathbb{R}$. Check that the analogous properties hold there.

Exercise 2.3.21 (Germs of smooth functions)**.** Define the *germ* of a smooth real (resp. complex) valued smooth function at 0 to be the equivalence class $[f, W]$ where W is a neighbourhood of 0 and f is smooth on W. The equivalence class is defined by $[f, W] = [g, V]$ iff there exists a neighbourhood $U \subset V \cap W$ with $f_{|U} = g_{|U}$. Prove that the collection of real (resp. complex) germs of smooth functions at 0 is a local ring, and not Noetherian. What are the irreducible elements of this ring? Is it a UFD? Is it a subring of $\mathbb{R}[[X]]$ (resp. $\mathbb{C}[[X]]$) as in the previous exercise? What is the story for "smooth" above replaced by "continuous" ?

Exercise 2.3.22. Show that $\mathbb{Q}[[X]]$ is not contained in the quotient field of $\mathbb{Z}[[X]]$. (*Hint*: Consider the element $\sum_{i=1}^{\infty} X^i/p_i$, where p_i is the i-th prime). What is the quotient field of $\mathbb{Z}[[X]]$?

3. Algebraic Sets

Let k be a field in whatever follows.

3.1. **The Zariski Topology.**

Proposition 3.1.1. Let $X = V(\mathfrak{a})$ be an affine algebraic set in k^n. Then

$$X = V(f_1, ..f_m) = \cap_{i=1}^m V(f_i)$$

where $\{f_i(X_1, ...X_n)\}_{i=1}^m$ is any set of generators for the ideal $\mathfrak{a}$. Thus every affine algebraic set is defined by finitely many equations, and is a finite intersection of hypersurfaces.

Proof: Clear from the Hilbert Basis Theorem 2.3.7 of the last section. □

Proposition 3.1.2 (The Zariski Topology)**.** We have the following:

(i): If $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are two ideals in $A = k[X_1, ...X_n]$, then :

$$V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) = V(\mathfrak{a}_1 \cap \mathfrak{a}_2)$$

(ii): If $\{\mathfrak{a}_\alpha\}_{\alpha \in \Lambda}$ is a family of ideals in $A = k[X_1, ...X_n]$, then

$$V(\Sigma_{\alpha \in \Lambda} \mathfrak{a}_\alpha) = \cap_{\alpha \in \Lambda} V(\mathfrak{a}_\alpha)$$

(iii): $V(A) = V(\{1\}) = \phi$
(iv): $V(0) = k^n$

Proof:
We prove only (i), leaving the rest to the reader. Since $\mathfrak{a}_1$ and $\mathfrak{a}_2$ both contain $\mathfrak{a}_1 \cap \mathfrak{a}_2$ we clearly have $V(\mathfrak{a}_1 \cap \mathfrak{a}_2) \supset V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2)$. On the other hand, if $(a_1, ...a_n) \notin V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2)$, then there are polynomials $f_i(X_1, ...X_n) \in \mathfrak{a}_i$, where $i = 1, 2$, such that $f_i(a_1, ...a_n) \neq 0$. Then $f_1 f_2$ is a polynomial in $\mathfrak{a}_1 \cap \mathfrak{a}_2$, which does not vanish at $(a_1, ...a_n)$, and hence $(a_1, ...a_n) \notin V(\mathfrak{a}_1 \cap \mathfrak{a}_2)$. □

Thus the family of subsets:

$$\{V(\mathfrak{a}) \subset k^n : \mathfrak{a} \text{ an ideal in } k[X_1, ...X_n]\}$$

satisfies the axioms for closed sets of a topology on k^n called the *Zariski topology* on k^n. If $k = \mathbb{F}$ (:= $\mathbb{R}$ or $\mathbb{C}$), it is clear that a Zariski closed subset of $\mathbb{F}^n$ is closed in the classical (Euclidean metric) topology on $\mathbb{F}^n$, since polynomials are continuous in this classical topology on and algebraic sets are common zero sets of these. However, the Zariski topology is much coarser, as we shall see shortly.

Example 3.1.3. If $n = 1$, the Zariski closed subsets of $k^n = k$ are precisely the finite subsets of k, i.e. the Zariski topology is the cofinite topology, since polynomials in one variable have only finitely many zeros !

Example 3.1.4. If $n = 2$, the Zariski closed subsets of k^2 are k^2, the empty set, and all algebraic curves, and their arbitrary intersections. The reader should convince herself that this is *not* the product topology of Zariski topology on k with itself, which is strictly coarser.

Notation : 3.1.5 (Affine n-space over k)**.** The set k^n with this topological structure, coming from the Zariski topology, will be denoted $\mathbb{A}^n(k)$, and called *n-dimensional affine space over k*. $\mathbb{A}^1(k)$ is called the *affine line* and $\mathbb{A}^2(k)$ is called the *affine plane*.

Proposition 3.1.6. Let $Y \subset \mathbb{A}^n(k)$ be any subset, and let $\mathfrak{I}(Y)$ be the ideal of polynomials $f \in k[X_1, ...X_n]$ vanishing on Y (see definition 1.2.2). Then the algebraic set $V(\mathfrak{I}(Y))$ is the Zariski closure $\overline{Y}$. In particular, for a closed subset $Y \subset \mathbb{A}^n(k)$, we have $V(\mathfrak{I}(Y)) = Y$.

Proof: It is clear that $V(\mathfrak{I}(Y))$ is a Zariski closed subset of $\mathbb{A}^n(k)$ containing Y, and hence $\overline{Y} \subset V(\mathfrak{I}(Y))$. On the other hand suppose $p = (a_1, ...a_n) \notin \overline{Y}$. Then there exists a Zariski closed set $V(\mathfrak{a}) \supset Y$, which excludes p, and hence there is a polynomial $f \in \mathfrak{a}$ such that $f(p) \neq 0$. Now $V(\mathfrak{a}) \supseteq Y$ implies that $f(q) = 0$ for all $q \in Y$. Thus $f \in \mathfrak{I}(Y)$. Hence $p \notin V(\mathfrak{I}(Y))$. □

We can induce the Zariski topology from $\mathbb{A}^n(k)$ to any Zariski closed subset, i.e. any algebraic set $X \subset \mathbb{A}^n(k)$. If, for example, X is an algebraic set, and $\mathfrak{I} = \mathfrak{I}(X)$ is the corresponding ideal, then by the last proposition 3.1.6, we have $X = V(\mathfrak{I})$. Thus the collection :

$$\{Z \cap X : \ Z \text{ closed in } \mathbb{A}^n(k)\}$$

is precisely the collection:

$$\{V(\mathfrak{a} + \mathfrak{I}) : \mathfrak{a} \text{ an ideal in } k[X_1, ...X_n]\}$$

of Zariski closed subsets of X. If we define, for an ideal $\mathfrak{b}$ in $k[X] = k[X_1, ...X_n]/\mathfrak{I}$ (=the coordinate ring of X as defined in 1.2.3) the set $V(\mathfrak{b}) := V(\pi^{-1}(\mathfrak{b}))$ where π is the quotient homomorphism from the polynomial ring $k[X_1, ...X_n]$ to the coordinate ring $k[X]$, then the above collection of closed sets in the induced Zariski topology on X is just the collection:

$$\{V(\mathfrak{b}) : \mathfrak{b} \text{ an ideal in } k[X]\}$$

This is clear in view of the definition 1.2.3 and the fact that the natural surjection π from $k[X_1, ...X_n]$ to $k[X]$ sets up a 1-1 correspondence between ideals in $k[X]$ and ideals in $k[X_1, ...X_n]$ containing $\mathfrak{I}$, and that $\mathfrak{a} + \mathfrak{I}$ is the most general ideal containing $\mathfrak{I}$

Exercise 3.1.7. Show that any infinite subset of $\mathbb{A}^1(k)$ is Zariski dense in it. Let $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$. Show that the graph of the exponential function, i.e. the set $\{(z, e^z) : z \in \mathbb{K}\}$ is Zariski dense in $\mathbb{A}^2(\mathbb{K})$.

Exercise 3.1.8. Show that if $\mathfrak{a} \subset \mathfrak{b}$ are ideals in $k[X_1, .., X_n]$, then $V(\mathfrak{a}) \supset V(\mathfrak{b})$. Similarly, if $X \subset Y$ are any two subsets in $\mathbb{A}^n(k)$, then $\mathfrak{I}(X) \supset \mathfrak{I}(Y)$.

The proposition 3.1.6 above says that if we start with an algebraic (Zariski closed) subset $Y \subset \mathbb{A}^n(k)$, compute its ideal $\mathfrak{I}(Y)$, and then compute the closed set $V(\mathfrak{I}(Y))$ defined by this ideal, then we recover Y. Clearly it would be desirable to also start with an ideal $\mathfrak{a} \subset k[X_1, .., X_n]$ and compute the ideal $\mathfrak{I}(V(\mathfrak{a}))$, and compare it with $\mathfrak{a}$. This is the statement of the Hilbert Nullstellensatz, which will be proved in the course of the next two sections. Before that, we need to understand the notion of prime ideals, and the related notion of the radical of an ideal, which is addressed in the next section.

4. More Algebra

4.1. **Prime Ideals.**

Definition 4.1.1. Let A be a ring with 1, commutative, as usual. We say an ideal $\mathfrak{p}$ in A is a *prime ideal* if $\mathfrak{p} \neq A$ and, for each pair of elements $x, y \in A$ such that $xy \in \mathfrak{p}$, either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

Note that this is equivalent to saying that $A/\mathfrak{p}$ is a non-zero integral domain. Note that $\{0\}$ is a prime ideal iff A is an integral domain. Since $\mathfrak{m}$ is a maximal ideal iff $A/\mathfrak{m}$ is a (non-zero!) field, it is clear that every maximal ideal is a prime ideal. *We emphasize that maximal and prime ideals are always, by definition, proper ideals of A.*

Exercise 4.1.2. Show that a principal ideal $\langle x \rangle$ in a ring is prime iff x is not a unit and a prime element of A. If A is a UFD (e.g. a polynomial ring over a field k), then the $\langle x \rangle$ is prime iff x is a non-unit and irreducible. Thus an ideal generated by a single irreducible polynomial of degree greater than zero in a polynomial ring $k[X_1, .., X_n]$ is prime. Show that if A is a PID, every non-zero ideal is prime iff it is maximal. Show that the ideal generated by $X^2 + 1$ in $\mathbb{R}[X]$ is maximal (hence prime), but the ideal generated by $X^2 + 1$ in $\mathbb{C}[X]$ is not maximal (hence not prime). Find all the maximal ideals in $\mathbb{R}[X]$.

Exercise 4.1.3. If $\mathfrak{p} \supset \prod_{i=1}^{m} \mathfrak{a}_i$ for some ideals $\mathfrak{a}_i \subset A$, then $\mathfrak{p} \supset \mathfrak{a}_i$ for some i. In particular, if $\mathfrak{p}$ is a prime ideal such that $\mathfrak{p} \supset \cap_{i=1}^{m} \mathfrak{a}_i$, then $\mathfrak{p} \supset \mathfrak{a}_i$ for some i.

Exercise 4.1.4. If $\cup_{i=1}^{m} \mathfrak{p}_i \supset \mathfrak{a}$ for some prime ideals $\mathfrak{p}_i$ and some ideal $\mathfrak{a}$ in a ring A, then $\mathfrak{p}_i \supset \mathfrak{a}$ for some i. (Note that for $m = 2$, the primeness assumption on $\mathfrak{p}_i$ is not necessary, the result is true in general. For $m \geq 3$, use induction, and the primeness of the $\mathfrak{p}_i$.)

Definition 4.1.5. Let A be as above, and let $\mathfrak{a}$ be an ideal in A. We define the *radical of* $\mathfrak{a}$, denoted $\sqrt{\mathfrak{a}}$ by

$$\sqrt{\mathfrak{a}} = \{x \in A : x^k \in \mathfrak{a} \text{ for some } k \geq 1\}$$

which is easily checked to be an ideal. An ideal $\mathfrak{a}$ is said to be a *radical ideal* if $\sqrt{\mathfrak{a}} = \mathfrak{a}$. For example, a prime ideal is clearly a radical ideal.

The *nilradical* of A is defined as the radical of the zero ideal, and denoted by $\text{nil}(A)$.

Exercise 4.1.6. Let A be a UFD. Show that a proper principal ideal $\langle x \rangle$ in A is a radical ideal iff x factors into a product of distinct primes.

Exercise 4.1.7. Show that for a subset $S \subset \mathbb{A}^n(k)$, k a field, the ideal $\mathfrak{I}(S)$ in $k[X_1, .., X_n]$ is a radical ideal.

Proposition 4.1.8. Let A be any ring. The nilradical $\text{nil}(A)$ of A is the intersection of all the prime ideals of A.

Proof: Clearly the nilradical $= \sqrt{\{0\}}$, is the ideal of all the nilpotent elements of A. If $x \in \text{nil}(A)$, then $x^k = 0$ belongs to every prime ideal of A, and by the definition of a prime ideal, so does x. Conversely, assume $x \notin \text{nil}(A)$, so that no positive power of x is zero. Let

$$\Sigma = \{\mathfrak{I} : \mathfrak{I} \text{ is an ideal containing no power of } x\}$$

Clearly $\{0\} \in \Sigma$ so Σ is a non-empty collection, which can be partially ordered by inclusion. Let $\{\mathfrak{I}_\alpha\}_{\alpha \in \Lambda}$ be a totally ordered subset of Σ. It is clear that $\cup_{\alpha \in \Lambda} \mathfrak{I}_\alpha$ is an ideal which is an upper bound for this chain. So, by Zorn, Σ has a maximal element, say $\mathfrak{I}$. We claim that $\mathfrak{I}$ is a prime ideal. For let us assume $a \notin \mathfrak{I}$, and $b \notin \mathfrak{I}$. Then the ideal $\mathfrak{I} + Aa$ is an ideal strictly containing $\mathfrak{I}$, and hence not in Σ. Thus $x^r \in \mathfrak{I} + Aa$. Similarly

$x^s \in \mathfrak{I} + Ab$. Thus $x^{r+s} \in \mathfrak{I} + Aab$. Thus $\mathfrak{I} + Aab \notin \Sigma$, which implies $\mathfrak{I} + Aab \neq \mathfrak{I}$, and hence $ab \notin \mathfrak{I}$. Hence $\mathfrak{I}$ is a prime ideal not containing x, and the proposition is proved. □.

Corollary 4.1.9. If A is any ring and $\mathfrak{a}$ an ideal in A, then

$$\sqrt{\mathfrak{a}} = \cap\{\mathfrak{p} \text{ prime ideal} : \ \mathfrak{p} \supset \mathfrak{a}\}$$

Proof: Apply the above proposition to $A/\mathfrak{a}$, noting that prime ideals in this ring lift to exactly to prime ideals in A that contain $\mathfrak{a}$. □

Definition 4.1.10. The collection of all prime ideals of a ring A is called the *prime spectrum* of A and denoted $\operatorname{Spec} A$. The collection of all maximal ideals of A is called the *maximal spectrum* of A, and denoted $\operatorname{Spm} A$.

Exercise 4.1.11. Let $f : A \to B$ be a ring homomorphism. Show that there is an induced map of prime spectra:

$$\begin{aligned} f^* : \operatorname{Spec} B &\to \operatorname{Spec} A \\ \mathfrak{p} &\mapsto f^{-1}\mathfrak{p} \end{aligned}$$

Give an example of a ring homomorphism $f : A \to B$ and a maximal ideal $\mathfrak{m} \subset B$ such that $f^{-1}\mathfrak{m}$ is not a maximal ideal of A.

Exercise 4.1.12.

(i): Let $\mathfrak{a}$ be an ideal in a Noetherian ring. Show that $\left(\sqrt{\mathfrak{a}}\right)^n \subset \mathfrak{a}$ for some $n \geq 1$.

(ii): Let $f(X) = \sum_{i=0}^{\infty} a_i X^i$ be a formal power series in the power series ring $A[[X]]$, where A is a Noetherian ring. Show that a_i nilpotent for each i implies that f is nilpotent.

(iii): Give an example of a ring A whose nilradical is not nilpotent (Note: an ideal $\mathfrak{a}$ is said to be nilpotent if there exists an n such that $\mathfrak{a}^n = \{0\}$).

We will return to further facts on prime ideals later.

4.2. **Integral Dependence.** We need a new algebraic notion here. To motivate it geometrically, let us consider the following example. Let $C = V(XY - 1) \subset \mathbb{C}^2$ be the hyperbola in $\mathbb{C}^2$. Thus the coordinate ring $k[C] = k[X, Y]/\langle XY - 1\rangle$. Consider also the line $L_1 = V(Y)$, the x-axis. Let $\pi : C \to L_1$ be the map $\pi(x, y) = x$, the projection onto the first coordinate. The following facts are clear:

(i): $\pi^{-1}(a) = \{(a, a^{-1})\}$ for $a \neq 0$, whereas $\pi^{-1}(0) = \phi$, so π is not surjective.

(ii): The inverse image of each closed disc around the origin $\{x :| x |\leq \varepsilon\}$ in L_1 is unbounded, i.e. the map π is not a proper map (with respect to the classical topologies on C and L_1).

Now let us change the line, and use the line $L_2 = V(X - Y)$, the diagonal in $\mathbb{C}^2$, and project from C to L_2. That is, define

$$\begin{aligned} \tau : C &\to L_2 \\ (x, y) &\mapsto \frac{1}{2}(x + y) \end{aligned}$$

It is convenient, now, to introduce new coordinates $z = \frac{1}{2}(x + y)$ and $w = \frac{1}{2}(x - y)$, so that $x = z + w$, and $y = z - w$. Then C can be rewritten as $V(Z^2 - W^2 - 1)$ and $\tau(z, w) = z$. Now note that :

(i): $\tau^{-1}(a) = \{(a, \pm\sqrt{a^2-1})\}$ (in the new coordinate system) for all $a \in L_2$, i.e. the map τ is surjective. The fibre $\tau^{-1}(a)$ has two points for $a \neq 0$, and one point for $a = \pm 1$.

(ii): With respect to the classical topologies on C and L_2, the inverse image $\tau^{-1}(K)$ of every compact subset K of L_2 is compact, i.e. τ is a proper map.

Let us try to see what is going on, algebraically. In the first instance, the map $\pi : C \to L_1$ induces the ring homomorphism $\pi^* : k[L_1] \to k[C]$ between the coordinate rings, taking a polynomial function $f \in k[L_1]$ to the function $\pi \circ f \in k[C]$. More precisely, if we write:

$$k[L_1] = k[X,Y]/\langle Y \rangle = k[X], \;\; k[C] = k[X,Y]/\langle XY - 1 \rangle$$

and denote the functions $X \pmod{\langle XY-1\rangle}$ and $Y \pmod{\langle XY-1\rangle}$ in $k[C]$ as x and y respectively, the homomorphism $\pi^* : k[L_1] \to k[C]$ is just the natural inclusion:

$$k[X] \hookrightarrow k[X,Y]/\langle XY - 1 \rangle$$

taking X to x. Note that in the right hand coordinate ring, the element y satisfies the equation $xy - 1 = 0$, whose coefficients are in $k[X]$, but whose leading coefficient, viz. x, is not 1. We now make the following:

Definition 4.2.1. We call a polynomial *monic* if the coefficient of the leading (degree) term is 1.

Thus y *does not* satisfy a monic polynomial with coefficients in $k[X]$.

In the second situation, the homomorphism $\tau^* : k[L_2] \to k[C]$ is just the inclusion of rings:

$$k[Z] \hookrightarrow k[Z,W]/\langle Z^2 - W^2 - 1 \rangle$$

taking Z to $z := Z \pmod{\langle Z^2 - W^2 - 1\rangle}$. In this case, the function w, which is defined by $w = W \pmod{\langle Z^2 - W^2 - 1\rangle}$ *does satisfy* the monic degree 2 polynomial equation $z^2 - w^2 - 1 = 0$, with coefficients in the subring $k[Z] = k[L_2]$.

This paves the way for the next

Definition 4.2.2. An inclusion of rings $B \supset A$ is called a *ring extension*. Let $B \supset A$ be a ring extension. An element $y \in B$ is said to be *integral over* A if y satisfies a monic polynomial with coefficients in A. A ring extension $B \supset A$ is said to be an *integral extension* if every element in B is integral over A.

Note that whenever we have a ring extension $B \supset A$, B is an A-module in a natural fashion.

Example 4.2.3. From the discussion above, the element $y \in k[C]$ is not integral over $k[X] = k[L_1]$, but the element $w = \frac{1}{2}(x + y)$ in $k[C]$ is integral over the subring $k[Z] = k[L_2]$.

Example 4.2.4. The element $\sqrt{5}$ in $\mathbb{Z}[\sqrt{5}]$ is integral over the subring $\mathbb{Z}$. In fact, the reader may easily prove (by squaring $y = m + n\sqrt{5}$ and eliminating $\sqrt{5}$ between y and y^2) that every such element y in $\mathbb{Z}[\sqrt{5}]$ is integral over the subring $\mathbb{Z}$. Thus the ring extension $\mathbb{Z}[\sqrt{5}] \supset \mathbb{Z}$ is an integral extension.

Example 4.2.5. The element $y = \frac{1+\sqrt{5}}{2}$ in $\mathbb{Q}[\sqrt{5}]$ is integral over the subring $\mathbb{Z}$, and satisfies the famous monic polynomial $y^2 - y - 1 = 0$.

Exercise 4.2.6. Show that if $A \subset B$ is an integral extension of rings, and $\mathfrak{b} \subset B$ is an ideal, then the extension

$$A/(\mathfrak{b} \cap A) \subset B/\mathfrak{b}$$

is also an integral extension.

Example 4.2.7. In the ring extension $\mathbb{Q} \supset \mathbb{Z}$, no element in $\mathbb{Q} \setminus \mathbb{Z}$ is integral over $\mathbb{Z}$. This is because of the following proposition.

Proposition 4.2.8. Let A be a UFD, and K be the quotient field of A (which is denoted $Q(A)$). Then if $y \in K$ is integral over A, y belongs to A.

Proof:

Let $y \in K$ be written as $\frac{p}{q}$ where p, q are relatively coprime (that is, $\gcd(p,q) = 1$). If y is integral over the subring A, there is a monic polynomial equation:

$$\left(\frac{p}{q}\right)^n + a_1\left(\frac{p}{q}\right)^{n-1} + ..a_n = 0$$

where $a_i \in A$. Multiply the equation by q^{n-1}, and transpose all terms from the second one on to the right hand side to get :

$$\frac{p^n}{q} = -a_1p^{n-1} - a_2qp^{n-2} - .... - a_nq^{n-1}$$

which shows that q divides p^n in A. A being a UFD, any irreducible (prime) factor of q would therefore divide p^n, and hence p, contradicting that $\gcd(p,q) = 1$. Thus q is a unit in A, and has an inverse $u \in A$, and $y = \frac{p}{q} = up$ is in A. □

The above proposition gives a handy way of showing that various rings are *not* UFD's. For example, $\mathbb{Z}[\sqrt{5}]$ is not a UFD, because its quotient field is $\mathbb{Q}[\sqrt{5}]$, and the element $\frac{1+\sqrt{5}}{2}$ in $\mathbb{Q}[\sqrt{5}]$, which is integral over $\mathbb{Z}[\sqrt{5}]$ (in fact even over $\mathbb{Z}$) is not in $\mathbb{Z}[\sqrt{5}]$. We know this fact already, of course.

Corollary 4.2.9. Denote the quotient field of $k[X_1, ...X_n]$ by $k(X_1, ...X_n)$. By the proposition 2.2.17 and the proposition above, it follows that if a rational function $\frac{p(X_1,...X_n)}{q(X_1,...X_n)} \in k(X_1, ..., X_n)$ satisfies a monic relation whose coefficients are polynomials, then this rational function is itself a polynomial.

Definition 4.2.10. We say that a module M over a ring A is *faithful* if $aM = \{0\}$ for $a \in A$ implies that $a = 0$. That is, the *annihilator ideal* of M defined by:

$$\text{Ann } M := \{a \in A : \ aM = \{0\}\}$$

is the zero ideal in A.

We now state several equivalent conditions for integrality of an element.

Proposition 4.2.11. Let $B \supset A$ be a ring extension, and let $y \in B$. Then the following are equivalent:

(i): y is integral over A.

(ii): The smallest subring of B containing A and y, which is denoted $A[y]$ (caution: this is *not* the polynomial ring over A in one variable, y may satisfy non-trivial relations) is finitely generated as an A-module.

(iii): There exists a subring $R \subset B$ such that $A[y] \subset R$ and R is a finitely generated A-module.

(iv): There exists a faithful $A[y]$-module M which is finitely generated as an A-module.

Proof:

(i)⇒ (ii)

For, let $y \in B$ be integral over A, and let

$$y^n + a_1y^{n-1} + ...a_n = 0$$

with $a_i \in A$, be the monic polynomial relation over A which y satisfies. Then $y^n = -(a_1y^{n-1} + ...a_n)$, and the higher powers y^r for $r \geq n$ can, by induction, all be written as A-linear combinations of $1, y, y^2, ...y^{n-1}$. Since the elements of $A[y]$ are precisely finite A-linear combinations of powers of y, it follows that every element of $A[y]$ is a finite A-linear combination of $1, y, y^2, ..y^{n-1}$. Thus $A[y] = A + Ay + ...Ay^{n-1}$, and is a finitely generated A-module.

(ii)⇒(iii) Take $R = A[y]$.

(iii)⇒(iv) Let $M = R$. M is then clearly a faithful $A[y]$ module since $A[y]$ is a subring of R, and any element of $A[y]$ annihilating all of R would have to annihilate 1, and thus be zero.

(iv)⇒(i)

We need a monic polynomial relation for y. Since M is an $A[y]$-module, and hence the map $y.\_$ (multiplication by y) maps M to M and is A-linear. M is given to be finitely generated over A, so let $\{x_1, x_2, ..x_n\}$ be a set of generators of M as an A-module. Then clearly we have the relations:

$$y.x_i = \Sigma_{j=1}^n a_{ij}x_j \ \ ; 1 \leq i, j \leq n,\ a_{ij} \in A$$

Now one has Cramer's Rule, which holds in any commutative ring :

$$\det T.\mathbf{1} = T^{adj}T$$

for any matrix $T = [T_{ij}]$, and T^{adj} is the transpose of the matrix of cofactors and $\mathbf{1}$ is the identity matrix. Apply this to $T = y\mathbf{1} - A$, with entries from the ring $A[y]$, where $A = [a_{ij}]$. Then we have the matrix identity:

$$\det(y\mathbf{1} - A)\mathbf{1} = (y\mathbf{1} - A)^{adj}(y\mathbf{1} - A)$$

However, the matrix $y\mathbf{1} - A$ kills all the generators x_i of M, and hence acts as the zero operator on M. Thus $\det(y\mathbf{1} - A).\mathbf{1}$ acts as the zero operator on M. Since M is faithful, it follows that $\det(y\mathbf{1} - A) = 0$. But this is a monic relation for y with coefficients being polynomials in the entries a_{ij} of the matrix A, i.e., elements of the ring A. Thus (iv) implies (i). □

Corollary 4.2.12. Let $B \supset A$ be a ring extension, and let y_1, y_2 be elements of B which are integral over A. Then the elements $y_1 + y_2$ and y_1y_2 are integral over A. Taking $y_2 = a \in A$, we have ay_1 is integral over A for all $a \in A$.

Proof:

By (ii) of the last proposition, $A[y_1] = Az_1 + ...Az_n$ and $A[y_2] = Aw_1 + ...Aw_m$. We claim that $A[y_1, y_2] = \Sigma_{i,j}Aw_iz_j$. This is because any power $y_1^r = \Sigma_j a_j z_j$ for some $a_j \in A$, and similarly $y_2^s = \Sigma_i b_i w_i$ for some $b_i \in A$. Thus the product $y_1^r y_2^s = \Sigma a_j b_i w_i z_j$, so any A-linear combination of monomials $y_1^r y_2^s$, i.e. any element of $A[y_1, y_2]$, is an A-linear combination of the mn elements w_iz_j. Thus our claim is established and $A[y_1, y_2]$ is finitely generated as an A-module. Now the subrings $A[y_1+y_2]$ and $A[y_1y_2]$ of B are contained in $R = A[y_1, y_2]$, which is finitely generated, so by (iii) of the last proposition, $y_1 + y_2$ and y_1y_2 are integral over A. □

Corollary 4.2.13. If $B \supset A$ is a ring extension, and $\{y_i\}_{i=1}^n$ is a collection of elements with y_i integral over A for each i, then the subring $A[y_1, ..., y_n]$ of B is an integral extension of A.

Proof: By applying the argument of the last corollary inductively, $A[y_1, ..., y_n]$ is a finitely generated A-submodule of B. If $y \in A[y_1, ..., y_n]$, then $A[y] \subset A[y_1, ..., y_n]$, and by (iii) of the last proposition, y is integral over A. □

Corollary 4.2.14. If $B \supset C \supset A$ is a tower of ring extensions such that B is an integral extension of C, and C is an integral extension of A, then B is an integral extension of A.

Proof: Let $y \in B$. Let $y^n + c_1y^{n-1} + ...c_n = 0$ be a monic polynomial relation for y over C, i.e., $c_i \in C$. Then this becomes a monic relation for y over $A[c_1, ..c_n]$. Thus $A[c_1, ..c_n, y]$ is a finitely generated $A[c_1, ..c_n]$-module, i.e., there exist elements $\{z_j\}_{j=1}^m$ in $A[c_1, ..c_n, y]$ such that $A[c_1, ..c_n, y] = \Sigma_{j=1}^m A[c_1, ..c_n]z_j$. By the last corollary, since c_i are integral over A, $A[c_1, ..c_n]$ is a finitely generated A-module, so that $A[c_1, ..c_n] = \Sigma_{k=1}^r Aw_k$. Thus $A[c_1, ..c_n, y] = \Sigma_{j,k}Aw_kz_j$ is a finitely generated A-module, and since $A[y] \subset A[c_1, ..c_n, y]$, by (iii) of the last proposition, y is integral over A. □

Definition 4.2.15. Let $B \supset A$ be a ring extension. We define the *integral closure* of A in B to be the set :

$$\overline{A} = \{y \in B : y \text{ is integral over } A\}$$

By the corollary 4.2.12 above, it is a subring of B. By definition, $\overline{A} \supset A$ is an integral extension.

Proposition 4.2.16. Let $B \supset A$ be a ring extension. Then $\overline{A}$ is the largest integral extension of A contained in B. Further $\overline{A}$ is integrally closed in B. In other words, the integral closure (in B) $\overline{\overline{A}} = \overline{A}$.

Proof: We have already remarked that $\overline{A}$ is an integral extension of A. If $y \in B$ is integral over $\overline{A}$, then $\overline{A}[y] \supset \overline{A}$ is an integral extension. Also $\overline{A} \supset A$ is an integral extension. By corollary 4.2.14 above, $\overline{A}[y] \supset A$ is an integral extension, so y is integral over A. Thus $y \in \overline{A}$, proving the proposition. □

Definition 4.2.17 (Integral closure, normal domains)**.** The *integral closure* of a domain A, (when no overring B is specified) is understood to be the integral closure of A in the quotient field $Q(A)$ of A. Similarly, saying that a domain is integrally closed without specifying an overring means that it is integrally closed in its quotient field.

An integrally closed domain is often called a *normal domain*, and the integral closure $\overline{A}$ of a domain A inside its quotient field is called its *normalisation*.

So, for example, a UFD is a normal domain by the Proposition 4.2.8.

Definition 4.2.18. An element $\alpha \in \mathbb{C}$ which satisfies a monic polynomial with integer coefficients is called an *algebraic integer*. By the previous Proposition 4.2.16, algebraic integers are elements of the integral closure of $\mathbb{Z}$ in the overring $\mathbb{C}$, and hence the set of algebraic integers is a normal domain inside $\mathbb{C}$.

Exercise 4.2.19 (Quadratic integers and number fields)**.** An algebraic integer α is said to be a *quadratic integer* if it satisfies a monic degree 2 polynomial in $\mathbb{Z}[X]$ which is irreducible in $\mathbb{Z}[X]$. Prove that:

(i): If α is a quadratic integer, then it is of the form $\frac{1}{2}(m+n\sqrt{d})$ where $m, n \in \mathbb{Z}$, and $d \in \mathbb{Z}$ is a square-free integer. (A square-free integer d is one which satisfies $v_p(d) = 0$ or 1 for all primes p).

(ii): For d a square-free integer, the set

$$\mathbb{Q}[\sqrt{d}] := \mathbb{Q}[X]/\langle X^2 - d\rangle = \{r + s\sqrt{d} : r, s \in \mathbb{Q}\}$$

is a field, and is called a *quadratic number field*. If $d < 0$, we call it an *imaginary quadratic number field*.

(iii): For d as above, show that every element of

$$\mathbb{Z}[\sqrt{d}] := \{m + n\sqrt{d} \in \mathbb{Q}[\sqrt{d}] : m, n \in \mathbb{Z}\}$$

is integral over $\mathbb{Z}$, by explicitly writing down a monic quadratic equation for the element $(m + n\sqrt{d})$.

(iv): Since d is square free, we have $d \equiv 1, 2, 3 \mod 4$. Show that if $d \equiv 1 \mod 4$, then the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{d}]$ is the subring $\{\frac{1}{2}(m + n\sqrt{d}) : m, n \in \mathbb{Z},\ m \equiv n \mod 2\} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

In particular, $\mathbb{Z}[\sqrt{d}]$ is *not a normal domain for* $d \equiv 1 \mod 4$*, and hence cannot be a UFD.* (We already stated this in the Remark 2.2.6, now we have a proof.)

(v): If d is square free, and $d \equiv 2, 3 \mod 4$, show that $\mathbb{Z}[\sqrt{d}]$ is integrally closed in $\mathbb{Q}[\sqrt{d}]$.
The integral closure of $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{d}]$ is called the *ring of integers* in $\mathbb{Q}[\sqrt{d}]$.

Remark 4.2.20 (Normal domains which are not UFD's)**.** The above exercise completely determines the ring of integers A_d in the quadratic number field $\mathbb{Q}[\sqrt{d}]$. Note that A_d is precisely the normalisation (=integral closure) of $\mathbb{Z}[\sqrt{d}]$. It is natural to ask which A_d's are UFD's. From the Theorem 7.7 of Chapter 11 in Artin's *Algebra*, one learns that for the *imaginary* quadratic number fields $\mathbb{Q}[\sqrt{d}]$ $(d < 0)$, the only ones which are UFD's are for $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$ (a deep theorem in number theory). Hence for any $d < 0$ which is not in the above list, A_d is a normal domain, but not a UFD. For $d > 0$, the complete answer to which A_d's are UFDs is unknown !

Now we need to prove a most important lemma called Noether Normalisation. Recall the Definition 2.3.9 of a k-algebra of finite type, where k is a field as usual. We make some definitions first.

Definition 4.2.21. Let A be a k-algebra. We say that a subset $S \subset A$ is *k-algebraically independent* or simply *algebraically independent*, if there does not exist any polynomial relation with coefficients in k among any of the elements of S. That is, if there is a finite subset $F = \{s_1, ..., s_n\} \subset S$, and a polynomial $p(X_1, ..., X_n) \in k[X_1, ..., X_n]$, such that $p(s_1, ..., s_n) = 0$, then p is the 0 polynomial. If S is a singleton $\{s\}$, we say s is *transcendental* over k. A set which is not k-algebraically independent is called *k-algebraically dependent*, and if the singleton set x is k-algebraically dependent, we say it is *algebraic over k*.

Example 4.2.22. In the ring $\mathbb{R}$, which is a $\mathbb{Q}$-algebra (not of finite type, since it has uncountable dimension as a $\mathbb{Q}$-vector space), the set $\{\pi\}$ is $\mathbb{Q}$-algebraically independent (viz. π is transcendental), though this is a non-trivial fact. Also, it is known that e is transcendental over $\mathbb{Q}$. On the other hand, $\sqrt{2}$ is algebraic over $\mathbb{Q}$. Hence the sets $\{e, \sqrt{2}\}$ or $\{\pi, \sqrt{2}\}$ are k-algebraically *dependent*.

Remark 4.2.23. If A is a k-algebra, and the subset $\{y_i\}_{i=1}^n$ is algebraically independent over k iff the k-subalgebra $k[y_1, y_2, .., .y_n]$ of A generated by the $y_i's$ is isomorphic to the polynomial ring $k[X_1, ..., X_n]$ under the k-algebra homomorphism $X_i \mapsto y_i$. For, by definition, the kernel of this k-algebra homomorphism is an isomorphism onto its image iff it has no kernel, which is equivalent to demanding that y_i are k-algebraically independent.

Proposition 4.2.24 (The Noether Normalisation Lemma)**.** Let A be a k-algebra of finite type. Then there exists a k-algebraically independent subset $\{y_1, ..., y_n\}$ in A such that the extension:

$$A \supset k[y_1, ..., y_n]$$

is an integral extension. (Note: n could be $= 0$, in which case $k[y_1, ..., y_n]$ is just k.)

Proof: The proof is by induction on the number of algebra generators for A. Suppose A is singly generated as a k-algebra, say $A = k[y]$ for some $y \in A$, then we have:

$$A = k[X]/\langle f(X)\rangle$$

where $f(X)$ is the generator of the kernel ideal of the natural surjective k-algebra homomorphism $k[X] \to A$ taking X to y (this kernel ideal is singly generated since $k[X]$ is a PID). Thus $f(y) = 0$. If $f(X)$ is the identically zero polynomial, then y is transcendental, and the ring extension $A \supset k[y]$ is integral, since it is an equality, and the required extension. If $f(X) \neq 0$ in $k[X]$, then by multiplying with the inverse of the leading coefficient, we may take f to be monic, and thus $k[y] \supset k$ becomes an integral extension, with $f(y) = 0$ being the monic relation of integrality for y over k. By Corollary 4.2.13, it is an integral extension.

Now assume, by induction, that we have the result for all k-algebras generated by $m-1$ elements, and assume $A = k[y_1, ...y_m]$. Again, if $y_1, ..., y_m$ are k-algebraically independent we take, as above, the ring extension $A \supset k[y_1, ...y_m]$, which is an equality, and hence an integral extension. If $y_1, ..., y_m$ is not a k-algebraically independent set, we must have some polynomial $f(X_1, ..., X_m) \in k[X_1, ..., X_m]$ which gives a non-trivial relation, i.e. $f(y_1, ...y_m) = 0$. We have to create some new elements $\{z_i\}_{i=2}^m$, which are $m-1$ in number, such that this equation becomes a monic equation for y_1 with coefficients in $k[z_2, ..., z_m]$. To this end define :

$$z_i = y_i - y_1^{r_i};\ \text{for } i = 2, 3..., m$$

where the positive integers r_i for $i = 2, 3, ..m$ are to be chosen as follows. Let us consider the subset :

$$\Gamma = \{\mathbf{b} = (b_1, ..., b_m) \in (\mathbb{Z}_+)^m : \text{the monomial } X_1^{b_1} X_2^{b_2} ..X_m^{b_m} \text{ occurs in} f\}$$

which is a finite set. For $\mathbf{b}, \mathbf{c} \in \Gamma$, with $\mathbf{b} \neq \mathbf{c}$, the subset $V(\mathbf{b}, \mathbf{c}) = \{\mathbf{x} \in \mathbb{R}^m : \mathbf{x}.\mathbf{b} = \mathbf{x}.\mathbf{c}\}$ is a hyperplane in $\mathbb{R}^m$ whose intersection, if non-empty, with the plane $\{1\} \times \mathbb{R}^{m-1}$ is an affine subspace of dimension $m-2$. The finite union of the above hyperplanes, i.e., $V = \cup\{V(\mathbf{b}, \mathbf{c}) : \mathbf{b} \neq \mathbf{c} \in \Gamma\}$ thus intersects $\{1\} \times \mathbb{R}^{m-1}$ in a finite union of $(m-2)$-dimensional affine subspaces of $\{1\} \times \mathbb{R}^{m-1}$, and if we choose a lattice point (exercise: prove

that such points exist) $\mathbf{r} = (1, r_2, .., r_m) \in \{1\} \times (\mathbb{Z}_+)^{m-1}$ outside this union, we have $\mathbf{r}.\mathbf{b} \neq \mathbf{r}.\mathbf{c}$ for all $\mathbf{b} \neq \mathbf{c}$ in Γ. This is the required choice of r_i for the equations above.

Thus the positive integers $\{\mathbf{r}.\mathbf{b} : \mathbf{b} \in \Gamma\}$ are all distinct, and there will be an $\mathbf{a} \in \Gamma$ such that $\mathbf{r}.\mathbf{a} > \mathbf{r}.\mathbf{c}$ for all $\mathbf{c} \in \Gamma$ such that $\mathbf{c} \neq \mathbf{a}$. Now substitute $y_i = z_i + y_1^{r_i}$ for $i \geq 2$ in the polynomial relation $f(y_1, ...y_m) = 0$, to get

$$f(y_1, z_2 + y_1^{r_2}, ..., z_m + y_1^{r_m}) := g(y_1, z_2, ...z_m) = 0$$

A typical monomial term $\lambda_{\mathbf{b}} y_1^{b_1} y_2^{b_2} ... y_m^{b_m}$ in f changes to

$$\lambda_{\mathbf{b}} y_1^{b_1 + r_2 b_2 + ... r_m b_m} + (\text{terms involving } z_i)$$

where $\mathbf{b} = (b_1, ..., b_m) \in \Gamma$. By the choice of $\mathbf{r}$ and $\mathbf{a}$, the term containing the highest power of y_1 in $g(y_1, z_2, ...z_m)$ is $\lambda_{\mathbf{a}} y_1^{a_1 + r_2 a_2 + ... r_m a_m}$, and on dividing by $\lambda_{\mathbf{a}} \in k$, $\lambda_{\mathbf{a}}^{-1} g(y_1, z_2, ...z_m) = 0$ is the required monic polynomial relation showing that y_1 is integral over $k[z_2, ..., z_m]$. Thus:

$$A = k[y_1, ..., y_m] = k[y_1, z_2, ..., z_m] \supset k[z_2, ..., z_m]$$

is an integral extension.

Now, by the induction hypothesis, this last ring being generated by $m - 1$ algebra generators, there is a subring $k[w_1, ..., w_r]$ with $\{w_j\}$ being k-algebraically independent, and with $k[z_2, ..., z_m] \supset k[w_1, ..., w_r]$ an integral extension. By the Proposition 4.2.14 above, $A \supset k[w_1, ..., w_r]$ is an integral extension and we are done. □

Remark 4.2.25. If we assume that the field k in the proposition above is *infinite*, a simpler proof can be given. We first make the observation that if $F \in k[X_2, .., X_m]$ is any non-zero polynomial in $m - 1$ variables, then there exists a point $(a_2, .., a_m) \in \mathbb{A}^{m-1}(k)$ such that $F(a_2, .., a_m) \neq 0$. This is obvious for the 1-variable case, since non-zero polynomials in 1-variable have only finitely many roots. In general, write :

$$F(X_2, .., X_m) = \Sigma_{j=1}^{d} f_j(X_2, .., X_{m-1}) X_m^j$$

and, by induction, find a point $(a_2, ..., a_{m-1})$ such that the coefficient of the degree term does not vanish at this point, i.e. $f_d(a_2, .., a_{m-1}) \neq 0$. Then choose a_m to be any element in k outside the set of roots of the single variable polynomial $F(a_2, ..., a_{m-1}, X_m)$. Now, to return to the proof of the Normalisation lemma, proceed as before by induction, and get the polynomial $f(y_1, ..., y_m) = 0$, as before. But now, we make the *linear* change of variables :

$$z_i = y_i - a_i y_1 \text{ for } 2 \leq i \leq m$$

where a_i are chosen as follows. Let $F(X_1, ..., X_m)$ be the highest degree homogeneous term (of degree d, say) in the polynomial $f(X_1, .., X_m)$. Choose $(a_2, .., a_m)$ so that $F(1, a_2, ...a_m) = \lambda \neq 0$, which is possible by the observation above. Verify that on substituting $y_i = z_i + a_i y_1$ for $2 \leq i \leq m$, the equation $f(y_1, ...y_m) = 0$ transforms to the equation :

$$\lambda y_1^d + \Sigma_{j=0}^{d-1} H_j(z_2, ... z_m) y_1^j = 0.$$

Multiplying by $\lambda^{-1} \in k$, we have the required fact that y_1 is integral over $k[z_2, .., z_m]$. Then the rest of the proof is as before.

Proposition 4.2.26. Let $B \supset A$ be an integral extension with B an integral domain. Then B is a field iff A is a field.

Proof: Let A be a field, and let $y \in B$. By hypothesis, there is a relation

$$y^n + a_1 y^{n-1} + ... a_n = 0$$

where $a_i \in A$. Since B is a domain, we may assume without loss of generality that $a_n \neq 0$, and since A is a field, we may multiply the equation above by $-a_n^{-1}$, transpose the last term to the right hand side to get :

$$y(-a_n^{-1} y^{n-1} - a_1 a_n^{-1} y^{n-2} - ..... - a_{n-1} a_n^{-1}) = 1$$

which shows that the inverse of y is the term in brackets.

Conversely, suppose B is a field, and $a \in A \setminus \{0\}$. Then there exists an inverse $a^{-1} \in B$, since B is a field. We claim it is actually in A. For, by the fact that a^{-1} is integral over A, there is a monic polynomial relation:

$$(a^{-1})^n + a_1(a^{-1})^{n-1} + ... + a_n = 0$$

Multiply the entire equation by a^{n-1} and transpose all but the first term to the right hand side to get $a^{-1} = -(a_1 + a_2a^1 + ...a_na^{n-1})$. Since the right hand side is clearly in A, a^{-1} is in A. Hence A is a field. □

Remark 4.2.27. We note that the integral extension $k \subset B$ where k is a field and $B = k[X]/\langle X^2 \rangle$, shows that the result above is false if one drops the assumption that B is an integral domain.

Here are some additional exercises on prime ideals, integral dependence and integral closure.

Exercise 4.2.28 (I.S. Cohen)**.** Let A be a ring in which all *prime ideals* are finitely generated. Show that A is Noetherian. (*Hint:* Assume that there exist non-finitely generated ideals, so the set Σ of non-finitely generated ideals is non-empty. Apply Zorn's Lemma to this set to get a maximal element $\mathfrak{a} \in \Sigma$. Claim that this maximal element must be a prime ideal. Now suppose $x \notin \mathfrak{a}$. Prove that there exists a finitely generated ideal $\mathfrak{b} \subset \mathfrak{a}$ such that $\mathfrak{b} + Ax = \mathfrak{a} + Ax$. For any two ideals $\mathfrak{a}, \mathfrak{c}$ in a ring, define:

$$\mathfrak{a}/\mathfrak{c} := \{z \in A : \ y\mathfrak{c} \subset \mathfrak{a}\}$$

Show that $\mathfrak{a}/\mathfrak{c}$ is always an ideal, and contains $\mathfrak{a}$. Also show that in the above situation $\mathfrak{a} = \mathfrak{b} + x.(\mathfrak{a}/Ax)$. If $y \notin \mathfrak{a}$, show that the ideal $(\mathfrak{a}/Ax)$ strictly contains $\mathfrak{a}$, and is therefore finitely generated. Conclude that xy cannot be in $\mathfrak{a}$, and hence $\mathfrak{a}$ is a prime ideal.

Exercise 4.2.29. Show that the inclusion of rings $k[X] \subset k[[X]]$ is not an integral ring extension.

The following few exercises are a rapid primer on field extensions, and easily follow by reformulating the Propositions 4.2.11, 4.2.12, 4.2.13, 4.2.14, 4.2.16, together with some other purely elementary considerations. For more details on these matters, the reader may consult Zariski-Samuel's *Commutative Algebra*, Vol. 1, Ch. II.

Exercise 4.2.30 (Algebraic Field Extensions)**.** If $k \subset K$ is an inclusion of fields, we call it a *field extension*. If S is a subset of K, $k(S)$ denotes the smallest subfield of K containing k and S.

Show that, for an element $x \in K$, the following are equivalent :

(i): There is a unique irreducible monic polynomial $f \in k[X]$ such that $f(x) = 0$ (called the *minimal monic polynomial* of x).

(ii): x is algebraic over k (see definition 4.2.21).

(iii): x integral over k.

(iv): $k[x]$, the k-subalgebra of K generated by k and x, is a finite dimensional k-vector space.

(v): $k[x]$ is contained in a k-subalgebra L of K with $\dim_k L < \infty$.

(vi): $k[x]$ is the smallest subfield of K containing k and x, i.e. $k[x] = k(x)$.

Exercise 4.2.31 (More on Algebraic Field Extensions)**.** The field extension $k \subset K$ is said to be an *algebraic field extension* if every element in K is algebraic over k, viz. if $k \subset K$ is an integral extension. If every element of $K \setminus k$ is transcendental over k, we say $k \subset K$ is a *transcendental extension*. We say that it is a *finite field extension* if the vector space dimension $\dim_k K < \infty$. This number is denoted $[K : k]$ and called the *degree* of the extension $k \subset K$. Show that :

(i): If $k \subset K$ is a field extension with $x \in K$ algebraic over k, then $\dim_k k[x] = n$, where n is the degree of the minimal monic polynomial f of x.

(ii): If $k \subset K$ is a finite field extension, then it is an algebraic extension.

(iii): If $k \subset L$ and $L \subset K$ are finite field extensions, then so is $k \subset K$, and that the degree of this extension is given by:

$$[K : k] = [K : L][L : k]$$

(iv): If x_i for $i = 1, 2, .., n$ are elements of K algebraic over k, then $k[x_1, .., x_n]$ is a field, and the field extension $k \subset k[x_1, .., x_n]$ is a finite algebraic extension. If $k \subset L$ and $L \subset K$ are any two (not necessarily finite) algebraic extensions, then $k \subset K$ is also an algebraic extension.

(v): If $k \subset K$ is any field extension, the integral closure of k in K, call it L, is an algebraic extension of k. Show L is the largest algebraic extension of k contained in K, and that the extension $L \subset K$ is a transcendental extension. Thus every field extension of k can be decomposed into a two step extension, the first algebraic and the second transcendental.

Exercise 4.2.32. Let $A \subset B$ be an integral extension of domains. Show that $Q(A) \subset Q(B)$ is an algebraic extension of their respective quotient fields.

Exercise 4.2.33 (Algebraic Closure of a Field)**.** Let k be a field.

(i): For $f \in k[X]$ an irreducible polynomial of degree $d > 0$, show that the ring $K = k[X]/\langle f \rangle$ is an algebraic field extension of k with $[K : k] = d$, and containing a root of f (namely x, the image of X in K). Show that if L is any field extension of k containing a root α of f, then the subfield $k(\alpha)$ of L is isomorphic to K. Thus, the process above is the minimal way of "adjoining a root" of a given irreducible polynomial to k, and the above construction shows that every irreducible polynomial with coefficients in k certainly has a root in *some* algebraic extension of k.

(ii): Order the family :

$$\{L : k \subset L \text{ is an algebraic extension}\}$$

by inclusion, and show that a chain L_α in this chain has the upper bound $\cup_\alpha L_\alpha$. Conclude, using Zorn's Lemma that there is a maximal element $\overline{k}$ in this family, which is therefore an algebraic extension of k. It is called *the algebraic closure* of k.

(iii): Show that $\overline{k}$ is algebraically closed, i.e. if L is an algebraic extension of $\overline{k}$, then $L = \overline{k}$. Equivalently, every polynomial f with coefficients in $\overline{k}$ has a root in $\overline{k}$, and hence breaks up into a product of linear factors.

For example: the algebraic closure of $\mathbb{R}$ is $\mathbb{C}$, a fact which is known as the Fundamental Theorem of Algebra. It can be proved using the Liouville Theorem complex analysis or some elementary algebraic topology. The algebraic closure $\overline{\mathbb{Q}}$ is called *the field of algebraic numbers*, and has countable vector space dimension over $\mathbb{Q}$, and hence a countable set, and thus much smaller than $\mathbb{C}$. Elements of $\mathbb{C} \setminus \overline{\mathbb{Q}}$ are the *transcendental numbers*, such as π or e (again, non-trivial facts to prove!).

(iv): Every proper field extension of an algebraically closed field is a transcendental extension.

Exercise 4.2.34 (Transcendence bases and transcendental extensions)**.** Let k be a field, and $k \subset K$ be a field extension in whatever follows. We say that a subset $S \subset K$ is a *k-transcendence set* if the elements are k-algebraically independent (see definition 4.2.21). We say that a k-transcendence set $S \subset K$ is a *transcendence base* for K over k (or k-transcendence base) if the extension $k(S) \subset K$ is algebraic. (Here $k(S)$ denotes the smallest subfield of K containing k and S). Prove the following:

(i): The set $\{X_1, .., X_n\}$ is a k-transcendence base for the extension $k \subset k(X_1, .., X_n)$ (this last field is defined as the quotient field of the polynomial ring $k[X_1, .., X_n]$, and is called the *field of rational functions in n-variables* over k).

(ii): If $T \subset K$ is a k-transcendence set, then there exists a transcendence base S for K over k containing T. (Apply Zorn's lemma to the family of all transcendence sets containing T).

(iii): If there exists a k-transcendence base S for K with $\text{card}(S) = n < \infty$, then every k-transcendence base for K has cardinality n, and this number is called the *transcendence degree* of K over k and denoted $\text{tr deg}_k K$. (Hint: Let $S = \{x_i\}_{i=1}^n$, and $T = \{y_\alpha\}$ be another transcendence base. Assume that T has cardinality $> n$. Choose some $y_1 \in T$, and noting that it is algebraic over $k(S)$, get an irreducible polynomial relation $f(y_1, x_1, .., x_n) = 0$, i.e. the minimal monic polynomial for y_1 over $k(x_1, .., x_n) = k(S)$. Since y_1 is transcendental over k, it follows that some x_i, say x_1, actually occurs in f. Now write f in powers of x_1 as:

$$f(y_1, x_1, .., x_n) = f_0(y_1, x_2, .., x_n) + f_1(y_1, x_2, .., x_n)x_1 + ...f_d(y_1, x_2, .., x_n)x_1^d = 0 \quad (1)$$

Now no irreducible factor of the polynomial $f_d(Y_1, X_2, .., X_n)$ can vanish at $(y_1, x_2, .., x_n)$, because $f(Y_1, x_1, .., x_n)$ is the unique irreducible polynomial satisfied by y_1 over $k(x_1, .., x_n)$. Thus $f_d(y_1, x_2, .., x_n) \neq 0$, and the relation (1) above shows that x_1 is algebraic over $k(y_1, x_2, .., x_n)$. Hence K is algebraic over $k(y_1, x_2, .., x_n)$. Now proceed with $y_2 \in T$, until one has K algebraic over $k(y_1, .., y_n)$, and thus arrive at the contradiction that any y_j with $j \neq 1, 2, .., n$ is k- algebraically dependent on $y_1, .., y_n$. Thus $\text{card}(T) \leq \text{card}(S)$. Similarly, $\text{card}(S) \leq \text{card}(T)$. The proof is similar to the proof that all bases of a finite dimensional vector space have the same cardinality.)

(iv): Let $k \subset L \subset K$ be a tower of field extensions, with K algebraic over L. Show that $\text{tr deg}_k L = \text{tr deg}_k K$.

(v): If $k \subset L \subset K$ is a tower of field extensions, all of finite transcendence degree, then show that:

$$\text{tr deg}_k L = \text{tr deg}_L K + \text{tr deg}_k L$$

(Contrast with multiplicativity of degrees of finite algebraic extensions.)

Exercise 4.2.35. Let $k = \mathbb{R}$, and let K be the quotient field of the formal power series ring $\mathbb{R}[[X]]$ (see the exercise 2.2.21 for the definition). Show that $\text{tr deg}_{\mathbb{R}} K = \infty$. (Hint: Construct a set S of exponential functions of the kind $e^{\alpha X}$ with α ranging in a suitable infinite set such that S is a $\mathbb{R}$-transcendence set.)

5. Hilbert's Nullstellensatz

We recall the question raised earlier in the subsection on algebraic sets, i.e., if $\mathfrak{I}$ is an ideal in $k[X_1, ..., X_n]$, k a field, then how does $\mathfrak{I}(V(\mathfrak{I}))$ compare with $\mathfrak{I}$? For one thing, we noted in Exercise 4.1.7 that the ideal $\mathfrak{I}(V(\mathfrak{I}))$ is a radical ideal, whereas the ideal $\mathfrak{I}$ need not have been radical. So it is natural to expect $\mathfrak{I}(V(\mathfrak{I}))$ to be just the smallest radical ideal containing $\mathfrak{I}$, i.e. $\sqrt{\mathfrak{I}}$. (Compare with the situation of $C([0,1])$, where the ideal of continuous functions vanishing on the common zero set of an ideal $\mathfrak{I}$ in $C([0,1])$ turns out to be the closure of that ideal in the sup-norm topology).

The Hilbert Nullstellensatz says that this expectation is realised, when the field k is algebraically closed.

5.1. **The Weak Nullstellensatz.** We first prove the weak nullstellensatz.

Proposition 5.1.1. Let k be an algebraically closed field, and $\mathfrak{m}$ be a maximal ideal in $k[X_1, ..., X_n]$. Then there exists an $(a_1, ..., a_n) \in \mathbb{A}^n(k)$ such that:

$$\mathfrak{m} = \langle X_1 - a_1, ..., X_n - a_n \rangle$$

Thus maximal ideals in the polynomial ring in n variables over k are in 1-1 correspondence with points in $\mathbb{A}^n(k)$. In the notation of 4.1.10, $\mathrm{Spm}(k[X_1, .., X_n])$ is $\mathbb{A}^n(k)$, as a set.

Proof: Let $\mathfrak{m}$ be a maximal ideal in $k[X_1, ..., X_n]$, which is a k-algebra of finite type. Then $k[X_1, ..., X_n]/\mathfrak{m}$ is also a k-algebra of finite type, and also a field. Call it K. By Noether's Normalisation lemma, there exists a subset $S = \{y_i\}_{i=1}^r$ such that $K \supset k[y_1, ..., y_r]$ is an integral extension. By the Proposition 4.2.26 of the previous section, since K is a field, so is $k[y_1, ..., y_r]$. Since the latter is a polynomial ring in r variables, it can only be a field if $r = 0$. Thus $k[y_1, ..., y_r] = k$, and $K \supset k$ is an integral extension. Thus every element $y \in K$ satisfies a monic polynomial over k, and is hence algebraic over k. But k is algebraically closed, so $y \in k$. Thus $K = k$. Let τ be the quotient map :

$$k[X_1, ..., X_n] \to K = k$$

and let us denote $\tau(X_i) = a_i \in k$. By definition, $\tau(X_i - a_i) = 0$, so that $(X_i - a_i) \in \mathfrak{m}$ for $i = 1, 2, .., n$. Thus $\langle X_1 - a_1, ..., X_n - a_n \rangle \subset \mathfrak{m}$. On the other hand, the ideal $\langle X_1 - a_1, ..., X_n - a_n \rangle$ is clearly maximal. This follows by using the first order "Taylor formula", i.e. for any polynomial $f(X_1, ..., X_n)$ we have:

$$f(X_1, ..., X_n) = f(a_1, ..., a_n) + \Sigma_{j=1}^n h_j(X_1, ..., X_n)(X_j - a_j)$$

where h_j are some polynomials. This is obtained by writing:

$$f(X_1, ..., X_n) = f(a_1 + (X_1 - a_1), ..., a_n + (X_n - a_n))$$

and expanding each monomial in f binomially. So for every polynomial $f \in k[X_1, .., X_n]$ we have:

$$f(X_1, ..., X_n) \equiv f(a_1, ..., a_n) \in k \qquad (\mathrm{mod}\ \langle X_1 - a_1, ..., X_n - a_n \rangle)$$

so that this ideal $\langle X_1 - a_1, ..., X_n - a_n \rangle$ is maximal.

Thus $\mathfrak{m} = \langle X_1 - a_1, ..., X_n - a_n \rangle$, and we are done. □

Proposition 5.1.2 (Weak Nullstellensatz for general k)**.** If K is a k-algebra of finite type which is a field, then K is a finite algebraic extension of k. Thus, if $\mathfrak{m}$ is a maximal ideal in a k-algebra A of finite type, then the quotient $A/\mathfrak{m}$ is a finite algebraic field extension of k.

Proof: Because K is a k-algebra of finite type, it is an integral extension of some $k[y_1, ..., y_r]$ by Noether normalisation and, as in the proof above, $k[y_1, ..., y_r]$ must be a field and r must be 0. Thus K is an integral extension of k, and hence an algebraic extension. If we let $\{x_i\}_{i=1}^n$ denote the algebra generators of K over k, we have $K = k[x_1, ..., x_n]$, where all the x_i are integral, and so by (ii) of Proposition4.2.11, and Proposition 4.2.14, we have K is a finitely generated k-module, i.e., a k-vector space of finite dimension, so a finite algebraic extension of k. The second part is clear by considering $K = A/\mathfrak{m}$. □

Exercise 5.1.3. Show that the above Proposition 5.1.2 is equivalent to the following statement: Let A be a k-algebra of finite type. Then every embedding $\phi : k \to L$ with L algebraically closed extends to a ring homomorphism $\psi : A \to L$.

Exercise 5.1.4. This exercise yields another consequence of the weak nullstellensatz for a general field k which is not necessarily algebraically closed.

(i): Let K be a field, and let $K \subset L$ be an algebraic extension. Show that if A is a K-subalgebra of L, then A is a field.

(ii): Let k be a field (not necessarily algebraically closed) and K its algebraic closure. Show that there is a 1-1 correspondence between k-algebra homomorphisms $f : k[X_1, .., X_n] \to K$, and points $(a_1, .., a_n) \in L^n$ where $L \subset K$ is some finite extension of k, depending on f.

(iii): Let k, K be as in (ii) above. If $A = k[X_1, .., X_n]/\mathfrak{a}$ is a k-algebra of finite type, then show that there is a $1-1$ correspondence between k-algebra homomorphisms $f : A \to K$, and points $(a_1, .., a_n) \in V_L(\mathfrak{a})$ where L is a finite algebraic extension of k (depending on f). (*Note*: We define the set:

$$V_L(\mathfrak{a}) := \{(a_1, .., a_n) \in L^n : h(a_1, .., a_n) = 0 \text{ for all } h \in \mathfrak{a}\}$$

The points of $V_L(\mathfrak{a})$ are called the *L-rational points of* $V(\mathfrak{a})$.)

Corollary 5.1.5. The rational function field $k(X_1, .., X_n)$ in n variables, for $n \geq 1$, is not a k-algebra of finite type.

Proof: If it were so, the Proposition 5.1.2 would imply that $k(X_1, .., X_n)$ is an algebraic extension of k, contradicting the fact that it is a transcendental extension of k (of transcendence degree n). □.

Corollary 5.1.6. Let $A = k[X_1, ..., X_n]/\mathfrak{a}$ be a k-algebra of finite type, where k is algebraically closed. Then maximal ideals in A are in 1-1 correspondence with points in $V(\mathfrak{a})$.

Proof: Let $\mathfrak{n}$ be a maximal ideal in A, so that $A/\mathfrak{n}$ is a k-algebra of finite type, which is also a field. Again, by the argument in the weak nullstellensatz above, this field has to be k. Let $\tau : k[X_1, ..., X_n] \to A$ be the quotient map. Then $\mathfrak{m} = \tau^{-1}(\mathfrak{n})$ satisfies the relation : $k[X_1, ..., X_n]/\mathfrak{m} \simeq A/\mathfrak{n} = k$, so that $\mathfrak{m}$ is a maximal ideal in $k[X_1, ..., X_n]$. By the Proposition 5.1.1 above, $\mathfrak{m} = \langle X_1 - a_1, ..., X_n - a_n\rangle$, for some $(a_1, ..., a_n) \in \mathbb{A}^n(k)$. Also $\mathfrak{m}$ contains the ideal $\mathfrak{a}$.

Thus we have that $V(\langle X_1 - a_1, .., X_n - a_n\rangle) \subset V(\mathfrak{a})$. But we saw above that $V(\langle X_1 - a_1, .., X_n - a_n\rangle) = (a_1, .., a_n)$. So it follows that $(a_1, ...a_n) \in V(\mathfrak{a})$. Conversely, if $(a_1, .., a_n) \in V(\mathfrak{a})$, $f(a_1, ..., a_n) = 0$ for all $f \in \mathfrak{a}$. Thus $f \in \langle X_1 - a_1, .., X_n - a_n\rangle$, so that $\mathfrak{a} \subset \mathfrak{m}$. □

Next, we have a couple of further consequences of the various nullstellensatzes above.

Proposition 5.1.7. Let $\phi : A \to B$ be a k-algebra homomorphism, with A and B k-algebras of finite type. If $\mathfrak{m}$ is a maximal ideal in B, then $\mathfrak{n} = \phi^{-1}(\mathfrak{m})$ is a maximal ideal in A

Proof: We note that since $\mathfrak{m}$ is maximal, it is prime, and hence so is $\mathfrak{n} = \phi^{-1}(\mathfrak{m})$. Thus $A/\mathfrak{n}$ is an integral domain, and the induced homomorphism $\overline{\phi} : A/\mathfrak{n} \to B/\mathfrak{m}$ is an injective k-algebra homomorphism. In fact we have $k \subset A/\mathfrak{n}$, and so by Proposition 5.1.2 above, $K = B/\mathfrak{m}$ is an integral extension of k. Thus it is also an integral extension of the integral domain $A/\mathfrak{n}$. By Proposition 4.2.26, $A/\mathfrak{n}$ is a field, and so $\mathfrak{n} = \phi^{-1}(\mathfrak{m})$ is maximal in A. □

Remark 5.1.8. We note here that the above result is *false* if we drop the finiteness assumption on the algebras. For example, $\phi : \mathbb{Q}[\pi] \subset \mathbb{R}$ is an inclusion of $\mathbb{Q}$-algebras, though $\mathbb{R}$ is not a $\mathbb{Q}$-algebra of finite type. The 0-ideal is maximal in $\mathbb{R}$, but $\phi^{-1}(0) = (0)$ is not maximal in $\mathbb{Q}[\pi]$, since this algebra is not a field (it is isomorphic to $\mathbb{Q}[X]$, the polynomial ring over $\mathbb{Q}$ in one variable.

Geometrically, one interprets the Proposition 5.1.6 to mean that the points in $V(\mathfrak{a})$ are precisely the maximal ideals in its coordinate ring $A = k[X_1, .., X_n]/\mathfrak{a}$. Similarly, one interprets the statement of Proposition 5.1.7 to mean that an algebra homomorphism of two coordinate rings gives a map (in the opposite direction) of the two algebraic sets: the image of a point is obtained by taking the inverse image of the corresponding maximal ideal.

So one has the following:

Proposition 5.1.9. Let k be algebraically closed, and $X \subset \mathbb{A}^n(k)$ and $Y \subset \mathbb{A}^m(k)$ be algebraic sets, with coordinate rings $k[X] = k[X_1, .., X_n]/\mathfrak{I}(X)$ and $k[Y] = k[X_1, .., X_m]/\mathfrak{I}(Y)$ respectively. Each k-algebra homomorphism $\phi : k[Y] \to k[X]$ uniquely defines a set map:

$$\phi^* : X \to Y$$

Such maps $\phi^* : X \to Y$ will be called *k-morphisms* or simply *morphisms* from X to Y.

Proof: We have seen from Proposition 5.1.6 that the set X is in bijective correspondence with the maximal spectrum $\operatorname{Spm} k[X]$, and likewise for Y. For $x \in X$, corresponding to the maximal ideal $\mathfrak{m}_x$, define $\phi^*(x) = y$ where $y \in Y$ is the point corresponding to the ideal $\mathfrak{n}_y = \phi^{-1}(\mathfrak{m}_x)$ (a maximal ideal by 5.1.7 above). Note that $\mathfrak{n}_y$ is the ideal of all regular functions on Y that vanish at y, and $\phi^{-1}(\mathfrak{m}_x) = \mathfrak{n}_y$ merely says that the composite function $f \circ \phi^*$ is a regular function on X vanishing at x iff f is a regular function on Y vanishing at $y = \phi^*(x)$. □

Example 5.1.10 (Morphisms of affine spaces)**.** If $X = \mathbb{A}^n(k)$ and $Y = \mathbb{A}^m(k)$, then a morphism $\phi^* : \mathbb{A}^n(k) \to \mathbb{A}^m(k)$ corresponds precisely to a k-algebra homomorphism of polynomial rings:

$$\phi : k[Y_1, .., Y_m] \to k[X_1, ..., X_n]$$

Such a k-algebra homomorphism is clearly determined uniquely by the images $\phi(Y_i)$, which is a polynomial $f_i(X_1, .., X_n) \in k[X_1, .., X_n]$. If $a := (a_1, .., a_n) \in \mathbb{A}^n(k)$ is a point, then the Taylor formula implies that:

$$f_i(X_1, .., X_n) - f_i(a_1, .., a_n) = \sum_{j=1}^{n} (X_j - a_j) h_{ij}(X_1, .., X_n) \in \mathfrak{m}_a \qquad i = 1, , , m$$

Define the point $b := (f_1(a_1, .., a_n), .., f_m(a_1, .., a_n))$. The above relation reads as:

$$\phi(Y_i) - b_i \in \mathfrak{m}_a, \quad i = 1, ..., m$$

Since ϕ is a k-algebra homomorphism, $\phi(b_i) = b_i$, so we have:

$$\phi(Y_i - b_i) \in \mathfrak{m}_a, \quad i = 1, ..., m$$

so that $(Y_i - b_i) \in \phi^{-1}(\mathfrak{m}_a)$ for $i = 1, .., m$. This implies that $\mathfrak{m}_b = \phi^{-1}(\mathfrak{m}_a)$, or equivalently, $b = \phi^*(a)$. Thus the set map $\phi^* : \mathbb{A}^n(k) \to \mathbb{A}^m(k)$ is just the expected map $(a_1, .., a_n) \mapsto (f_1(a_1, .., a_n), ..., f_m(a_1, .., a_n))$

Thus morphisms of affine spaces are just coordinate-wise polynomial maps. Clearly these are far fewer than all set maps. For example the set map $\mathbb{C} \to \mathbb{C}$ given by $a \mapsto e^a$ is not a morphism.

5.2. **The Strong Nullstellensatz.** This is a bit of a misnomer, since it is actually equivalent to the "weak nullstellensatz" stated above. First we need the :

Proposition 5.2.1. If A is a k-algebra of finite type, then for any ideal $\mathfrak{a} \subset A$,

$$\sqrt{\mathfrak{a}} = \cap\{\mathfrak{m} : \mathfrak{m} \text{ is maximal } \supset \mathfrak{a}\}$$

Proof: By arguing with $A/\mathfrak{a}$, we may assume that $\mathfrak{a} = 0$. Thus we need to show that $\sqrt{\{0\}}$ (which is the same as $\mathrm{nil}(A)$ by Proposition 4.1.8 in §4) is also the intersection of all the *maximal* ideals in A (which is also called the *Jacobson radical* of A, denoted $\mathrm{Jac}(A)$).

Since every maximal ideal is prime (and Proposition 4.1.8), it follows that $\mathrm{nil}(A) \subset \mathrm{Jac}(A)$. Suppose $a \in A$ such that $a \notin \mathrm{nil}(A)$. Then there is a prime ideal $\mathfrak{p}$ such that $a \notin \mathfrak{p}$. Let $x \neq 0$ denote the image of a in $B := A/\mathfrak{p}$ under the quotient homomorphism $\pi : A \to B$. Note B is an integral domain since $\mathfrak{p}$ is prime and also a k-algebra of finite type. Since it is a domain, it has a nontrivial quotient field $Q(B)$. Consider the inclusion of k-algebras of finite type: $B \subset B[\frac{1}{x}]$, where $B[\frac{1}{x}]$ denotes the smallest subring of $Q(B)$ containing B and $\frac{1}{x}$. Let $\mathfrak{m}$ be a maximal ideal in $B[\frac{1}{x}]$. Since x is invertible in $B[\frac{1}{x}]$, $x \notin \mathfrak{m}$. By the Proposition 5.1.7 above, $\mathfrak{n} = B \cap \mathfrak{m}$ is maximal in B, and does not contain x. Now $\pi^{-1}(\mathfrak{n})$ is a maximal ideal in A which does not contain a. Thus $a \notin \mathrm{Jac}(A)$. (This trick of producing ideals in B not containing an element x by taking inverse images of ideals in $B[\frac{1}{x}]$ is called the *Rabinowitch Trick*). □

Remark 5.2.2. In a general ring, the nilradical is strictly contained in the Jacobson radical. For example, in the power series ring $k[[X]]$, the nilradical is $\{0\}$, but the Jacobson radical is $\langle X \rangle$. In particular $k[[X]]$ is not a k-algebra of finite type.

Proposition 5.2.3 (Hilbert's Nullstellensatz)**.** Let k be an algebraically closed field. Then the following are equivalent:

(i): The weak nullstellensatz

(ii): If $\mathfrak{a}$ is an ideal in $k[X_1, .., X_n]$, then $\mathfrak{I}(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.

(iii): If $f_1, ..., f_m$ are polynomials in $k[X_1, ..., X_n]$ such that $V(f_1, .., f_m) = \phi$, then there exist elements $\{g_i\}_{i=1}^m$ in $k[X_1, ..., X_n]$ such that $\Sigma_{i=1}^m g_i f_i = 1$.

Proof: (i)$\Longrightarrow$(ii)

In view of the Proposition 5.2.1 above, it suffices to prove that

$$\mathfrak{I}(V(\mathfrak{a})) = \cap\{\mathfrak{m} : \mathfrak{m} \text{ is maximal } \supset \mathfrak{a}\}$$

for an ideal $\mathfrak{a}$ in $k[X_1, ..., X_n]$ when k is algebraically closed. By (i) $\mathfrak{m}$ is maximal in $k[X_1, .., X_n]$ iff $\mathfrak{m} = \langle X_1 - a_1, ..., X_n - a_n \rangle$, the ideal of all polynomial functions which vanish at some point $(a_1, .., a_n) \in \mathbb{A}^n(k)$, and such a maximal ideal contains $\mathfrak{a}$ iff every $f \in \mathfrak{a}$ vanishes at $(a_1, .., a_n)$ (recall the Taylor formula in the proof of the weak nullstellensatz above), i.e, if $(a_1, ..., a_n) \in V(\mathfrak{a})$. Thus the intersection

$$\cap\{\mathfrak{m} : \mathfrak{m} \text{ is maximal } \supset \mathfrak{a}\}$$

is precisely the ideal of all polynomials which vanish at each point of $V(\mathfrak{a})$, which is by definition $\mathfrak{I}(V(\mathfrak{a}))$. Thus $\sqrt{\mathfrak{a}} = \mathfrak{I}(V(\mathfrak{A}))$

(ii)$\Rightarrow$(iii)

Let $\{f_1, .., f_m\}$ be elements of $k[X_1, .., X_n]$ such that $V(f_1, ..., f_m) = \phi$. Then clearly we have $\mathfrak{I}(V(f_1, ..., f_m)) = k[X_1, ..., X_n]$. Thus $\sqrt{\langle f_1, ..., f_m \rangle} = A$, and so $1 \in \langle f_1, ..., f_m \rangle$, i.e., $1 = \sum_{i=1}^m g_i f_i$.

(iii)$\Rightarrow$(i)

Let $\mathfrak{m}$ be a maximal ideal in $k[X_1, .., X_n]$. Then let $f_1, ..., f_m$ be ideal generators of $\mathfrak{m}$, by Proposition 2.3.7. If $V(f_1, ..., f_m) = \phi$, we would have $1 \in \mathfrak{m}$ by (iii), a contradiction. So there exists a point $(a_1, ..., a_n) \in$

$V(f_1,..,f_m)$. Thus $f_i(a_1,..,a_n) = 0$ for all $i = 1,...,m$, implying that $f_i \in \langle X_1 - a_1,...,X_n - a_n\rangle$. Hence $\mathfrak{m} \subset \langle X_1 - a_1,...,X_n - a_n\rangle$. However, since $\mathfrak{m}$ is maximal, we must have $\mathfrak{m} = \langle X_1 - a_1,...,X_n - a_n\rangle$. This proves the proposition. □

5.3. **Localisation.** We now need the notion of localisation of a ring, which is a generalisation of the construction of the quotient field of an integral domain. The idea is to invert certain elements which are non-zero.

Definition 5.3.1. Let A be a commutative ring with 1, and let S be a *multiplicative set* in A. i.e. :

(i): $0 \notin S$, $1 \in S$

(ii): $a, b \in S \Rightarrow ab \in S$.

Define the *localisation* $S^{-1}A$ of A at S as follows: On the set $A \times S$, define the equivalence relation: $(a, s) \sim (a_1, s_1)$ if there exists a $t \in S$ such that $t(as_1 - a_1 s) = 0$ (verify that this is an equivalence relation). Denote the equivalence class of (a, s) as $\frac{a}{s}$. Make the set of these equivalence classes a ring by declaring $\frac{a}{s} + \frac{a_1}{s_1} = \frac{as_1+a_1s}{ss_1}$, and $\frac{a}{s}.\frac{a_1}{s_1} = \frac{aa_1}{ss_1}$. Again, verify that these operations are well defined, and that there is a natural homomorphism:

$$\begin{array}{ccc} A & \to & S^{-1}A \\ a & \mapsto & \frac{a}{1} \end{array}$$

Example 5.3.2. If $f \in A$ is not a nilpotent element, then the set $\{f^k\}_{k=0}^{\infty}$ is a multiplicative set. In this case $S^{-1}A$ is denoted by A_f. If A is a domain, this is the subring $A[\frac{1}{f}]$ generated by A and $\frac{1}{f}$ inside the quotient field $Q(A)$ of A.

Example 5.3.3. If $\mathfrak{p}$ is a *prime* ideal in any ring A, then the set $S = A \setminus \mathfrak{p}$ is a multiplicative set, and we define the ring $A_{\mathfrak{p}} := S^{-1}A$, which, by abuse of language is called the *localisation of A at $\mathfrak{p}$* , though it should be called the localisation of A at $A \setminus \mathfrak{p}$.

Remark 5.3.4. The natural homomorphism $A \to S^{-1}A$ *may not be injective* in general. For example, if we take $A = \mathbb{Z}_6$ and $S = \{\overline{1}, \overline{3}\}$ (verify that this is a multiplicative set), then under the natural homomorphism $\mathbb{Z}_6 \to S^{-1}\mathbb{Z}_6$, the element $\overline{2}$ goes to 0, since $\overline{3}.\overline{2} = 0$, showing that $\frac{\overline{2}}{\overline{1}} = 0$ in $\mathrm{S}^{-1}\mathbb{Z}_6$. (Exercise: compute $S^{-1}\mathbb{Z}_6$). Of course, the natural map $A \to S^{-1}A$ is injective if and only if no element of S is a zero-divisor. In particular, if A is an integral domain.

Example 5.3.5. If A is a domain and $S = A \setminus \{0\}$, then $S^{-1}A$ is just $Q(A)$, the quotient field of A. More generally, for an arbitrary ring A, if $S = \{x : x \text{ is not a zero-divisor}\}$, then $S^{-1}A$ is the *total quotient ring* (or *total ring of fractions*) of A. In this ring, every possible element which can be inverted, is inverted. By the above, the natural map of a general ring A to its total quotient ring is an inclusion.

Exercise 5.3.6 (Rabinowitch trick again)**.** Let S be a multiplicative set in a ring A, and let $f : A \to S^{-1}A$ denote the natural homomorphism. Show that if $\mathfrak{q}$ is a proper ideal (resp. prime ideal) in $S^{-1}A$, then $f^{-1}\mathfrak{a}$ is a proper ideal (resp. prime ideal) in A which is disjoint from S. In particular, for every *maximal ideal* $\mathfrak{m} \subset S^{-1}A$, the ideal $f^{-1}(\mathfrak{m})$ is a prime ideal in A avoiding S. (The particular case of $S = \{1, x, x^2, .., x^n, ..\}$ is the Rabinowitch trick used earlier in the proof of Proposition 5.2.1).

Exercise 5.3.7. Let A be any ring, and let D be the set of zero-divisors (and note that 0 is included in D). Show that for every $x \in D$, there is a prime ideal $\mathfrak{p} \subset D$ which contains x. Conclude that the set D is a union of prime ideals. Conclude that if $D \neq \{0\}$ in a ring A, then there exist prime ideals in A consisting entirely of zero-divisors.

Exercise 5.3.8 (Rings of continuous functions)**.** Consider the ring $A = C([0,1])$ of continuous complex-valued functions on the closed interval $[0,1]$. Note that A is a complete normed linear space (Banach space) over $\mathbb{C}$ with the sup norm

$$\|f\| := \sup_{x \in [0,1]} | f(x) |$$

Prove that:

(i): For each $a \in [0,1]$, the ideal:

$$\mathfrak{m}_a := \{f \in C([0,1]) : \ f(a) = 0\}$$

is a maximal ideal.

(ii): Show that if $\mathfrak{a} \subset A$ is an ideal, then the set:

$$V(\mathfrak{a}) = \{x \in [0,1] : f(x) = 0 \ \text{ for all } \ f \in \mathfrak{a}\}$$

is a closed set. Show that $\mathfrak{a} \subset \mathfrak{b}$ iff $V(\mathfrak{a}) \supset V(\mathfrak{b})$.

(iii): Show that if $\mathfrak{a}$ is a maximal ideal in A, then there exists a point $a \in [0,1]$ with $\mathfrak{a} = \mathfrak{m}_a$.

(iv): Show that for each closed subset $C \subset [0,1]$, the ideal:

$$\mathfrak{I}(C) := \{f \in A : f_{|C} \equiv 0\}$$

is an ideal in A. Check that it is a *norm-closed ideal*. That is, if $\|f_n - f\|_\infty \to 0$ for a sequence $f_n \in \mathfrak{I}(C)$, then $f \in \mathfrak{I}(C)$.

(v): For any subset $S \subset [0,1]$ show that $V(\mathfrak{I}(S)) = \overline{S}$. Show that for any ideal $\mathfrak{a} \subset A$, $\mathfrak{I}(V(\mathfrak{a}) = \bar{\mathfrak{a}}$, where the closure on the right is the closure in the norm $\|-\|_\infty$.

(vi): Show that $f \in A$ is a zero-divisor iff $V(f)$ has a non-empty interior.

(vii): Show by using the last two exercises that there exist prime ideals in A which are not maximal.

Exercise 5.3.9. Show that in the ring $A_\mathfrak{p}$, there is a *unique* maximal ideal, namely the ideal :

$$\mathfrak{p}A_\mathfrak{p} = \left\{ \frac{x}{s} : \ x \in \mathfrak{p} \text{ and } s \in A \setminus \mathfrak{p} \right\}$$

Definition 5.3.10. A ring with a unique maximal ideal is called a *local* ring. For example, the formal power series ring $k[[X_1, ..., X_n]]$ is a local ring, for any formal power series is invertible iff it has non-zero constant term, i.e., iff it lies outside the (clearly maximal) ideal $\langle X_1, ..., X_n \rangle$, which is therefore the unique maximal ideal. For a local ring A, the localisation $A_\mathfrak{m}$ at the unique maximal ideal $\mathfrak{m}$ is isomorphic to the original ring via the natural homomorphism $A \to A_\mathfrak{m}$ defined in 5.3.1 above.

We have one last fact, which is a universal property of localisations.

Proposition 5.3.11 (Universal property of localisations)**.** Let A be a ring, and $S \subset A$ be a multiplicative set. Let $\theta : A \to S^{-1}A$ denote the natural map introduced in Definition 5.3.1.

(i): If $f : A \to B$ is a ring homomorphism such that $f(s)$ is invertible (i.e. a unit) for each $s \in S$, then there is a unique homomorphism $\widetilde{f} : S^{-1}A \to B$ such that the diagram:

$$\begin{array}{ccc} A & & \\ & \overset{f}{\searrow} & \\ \theta \downarrow & & B \\ & \underset{\widetilde{f}}{\nearrow} & \\ S^{-1}A & & \end{array}$$

commutes.

(ii): If $f : A \to B$ is a homomorphism of rings, and $\mathfrak{p} \subset A$, $\mathfrak{q} \subset B$ are prime ideals such that $f^{-1}\mathfrak{q} \subset \mathfrak{p}$, then there is a unique homomorphism $\widetilde{f} : A_{\mathfrak{p}} \to B_{\mathfrak{q}}$ such that the diagram:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \theta_1 \downarrow & & \downarrow \theta_2 \\ A_{\mathfrak{p}} & \xrightarrow{\widetilde{f}} & B_{\mathfrak{q}} \end{array}$$

commutes.

Proof: For (i), define $\widetilde{f}(\frac{a}{s}) = f(a)f(s)^{-1}$. It is trivial to check that this definition is independent of representative chosen for $\frac{a}{s}$. With this definition of $\widetilde{f}$, we have $(\widetilde{f} \circ \theta)(a) = \widetilde{f}(\frac{a}{1}) = f(a)$, so the diagram commutes as claimed.

For (ii) note that the hypothesis implies that $f(A \setminus \mathfrak{p}) \subset B \setminus \mathfrak{q}$, and θ_2 maps this last set into invertible elements of $B_{\mathfrak{q}}$. Apply (i) to the map $\theta_2 \circ f$. □

Exercise 5.3.12. Here are a few simple exercises about localisation:

(i): Compute $S^{-1}A$ for $A = k[X, Y]/\langle XY \rangle$ and $S = \{1, x, x^2, ..., \}$, where x is the image of X in A.

(ii): Show that the natural map $\theta : A \to S^{-1}A$ is an isomorphism iff every element of S is a unit.

(iii): Let f be a non-nilpotent element in a ring A, and $S = \{1, f, f^2, ..\}$. Using the universal property (i) of Proposition 5.3.11, prove that the localisation $S^{-1}A$ is isomorphic to the ring $A[X]/\langle Xf - 1 \rangle$.

(iv): Compute the coordinate ring $k[X]$ of the hyperbola $X = V(X_1X_2 - 1) \subset \mathbb{A}^2(k)$.

One can extend the notion of localisation to A-modules as well. More precisely:

Definition 5.3.13. Let S be a multiplicative set in a ring A, and let M be an A-module. One can also localise this module at S, by defining an equivalence relation on $M \times S$ just as before, viz. $(m, s) \sim (m_1, s_1)$ iff there exists a $t \in S$ such that $t(s_1m - sm_1) = 0$ in M. Again, the equivalence classes are denoted by $\frac{m}{s}$ where $m \in M$ and $s \in S$, and the set of all these equivalence classes is denoted by $S^{-1}M$, and called the *localisation of M at S*. It is easily checked to be an abelian group, and an $S^{-1}A$ module by defining the addition and scalar multiplication in the obvious manner. Thus it makes sense to define $S^{-1}\mathfrak{a}$ for an ideal $\mathfrak{a}$ in A, and for example, the ideal $\mathfrak{p}\ A_{\mathfrak{p}}$ defined above is nothing but $S^{-1}\mathfrak{p}$ with $S = A \setminus \mathfrak{p}$. If M is an A-module, and $\mathfrak{p}$ a prime ideal in A, the localisation of M at the multiplicative set $S = A \setminus \mathfrak{p}$ is denoted $M_{\mathfrak{p}}$.

Exercise 5.3.14. If

$$0 \to L \to M \to N \to 0$$

is an exact sequence of A-modules, show that the sequence :

$$0 \to S^{-1}L \to S^{-1}M \to S^{-1}N \to 0$$

is an exact sequence of $S^{-1}A$-modules.

Proposition 5.3.15. If $B \supset A$ is an integral ring extension, then for S a multiplicative set in A (which also makes it a multiplicative subset of B), $S^{-1}B \supset S^{-1}A$ is an integral ring extension.

Proof: Let $\frac{b}{s}$ be an element of $S^{-1}B$ and let $b^n + a_1 b^{n-1} + ...a_n = 0$ be a monic polynomial relation for b over A. Divide this equation by s^n and get :

$$\left(\frac{b}{s}\right)^n + \frac{a_1}{s}\left(\frac{b}{s}\right)^{n-1} + ...\frac{a_n}{s^n} = 0.$$

as the monic relation for $\frac{b}{s}$ over $S^{-1}A$. □

We next have a crucial proposition about "lifting" prime ideals in integral extensions.

Proposition 5.3.16 (The Going-up Theorem of Cohen-Seidenberg)**.** Let $A \subset B$ be an integral ring extension. Then, for each prime ideal $\mathfrak{p} \subset A$, there is a prime ideal $\mathfrak{p}_1 \subset B$ such that $\mathfrak{p}_1 \cap A = \mathfrak{p}$. (*Notation*: We say that the ideal $\mathfrak{p}_1$ *lies over* $\mathfrak{p}$. That is, the natural map $\operatorname{Spec} B \to \operatorname{Spec} A$ defined by $\mathfrak{q} \mapsto \mathfrak{q} \cap A$ is surjective, with the prime ideal $\mathfrak{p}_1 \subset B$ lying in the fibre of the prime ideal $\mathfrak{p} \subset A$).

Proof: Let us first do an easy case. Suppose A is a local ring, i.e. A has a unique maximal ideal, and also assume that $\mathfrak{p}$ is this maximal ideal. Let $\mathfrak{p}_1$ be *any* maximal ideal in ideal in B. We claim $\mathfrak{p}_1 \cap A = \mathfrak{p}$. This is because $B/\mathfrak{p}_1 \supset A/A \cap \mathfrak{p}_1$ is also an integral extension. Since $B/\mathfrak{p}_1$ is a field, so is $A/A \cap \mathfrak{p}_1$, by Proposition 4.2.26, and hence $\mathfrak{p}_1 \cap A$ is maximal. Since $\mathfrak{p}$ is the unique maximal ideal of A, this forces $\mathfrak{p}_1 \cap A = \mathfrak{p}$. Hence we are done in this easy case.

To do the general case we have to consider the localisation $A_\mathfrak{p}$ of A at $\mathfrak{p}$. Again, by an abuse of notation, we denote the $A_\mathfrak{p}$-module $S^{-1}B$ by $B_\mathfrak{p}$, where $S = A \setminus \mathfrak{p}$ ($\mathfrak{p}$ is not a prime ideal in B !). Since $A_\mathfrak{p}$ is a local ring, with the maximal ideal being $S^{-1}\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$, by the easy case above, there exists an ideal $\mathfrak{n}$ in $B_\mathfrak{p}$ such that $\mathfrak{n} \cap A_\mathfrak{p} = S^{-1}\mathfrak{p}$.

Let us consider the commutative diagram:

$$\begin{array}{ccc} i : A & \to & A_\mathfrak{p} \\ \downarrow & & \downarrow \\ j : B & \to & B_\mathfrak{p} \end{array}$$

where the vertical maps are inclusions. Let $\mathfrak{p}_1 = j^{-1}(\mathfrak{n})$. We claim that $\mathfrak{p}_1 \cap A = \mathfrak{p}$.

Since $\mathfrak{n} \supset S^{-1}\mathfrak{p}$ we have :

$$\mathfrak{p}_1 = j^{-1}(\mathfrak{n}) \supset j^{-1}(S^{-1}\mathfrak{p}) = j^{-1}(\mathfrak{p}A_\mathfrak{p}) \supset \mathfrak{p}$$

so that $\mathfrak{p}_1 \cap A \supset \mathfrak{p}$.

On the other hand, let $b \in \mathfrak{p}_1 \cap A$. Then, $\frac{b}{1} \in \mathfrak{n} \cap A_\mathfrak{p} = S^{-1}\mathfrak{p}$. Thus $\frac{b}{1} = \frac{p}{s}$ for some $p \in \mathfrak{p}$ and $s \in A \setminus \mathfrak{p}$. Thus $t(bs - p) = 0$, for some $t \in S = A \setminus \mathfrak{p}$. Since $0 \in \mathfrak{p}$ and $\mathfrak{p}$ is prime, $bs - p \in \mathfrak{p}$. Since $p \in \mathfrak{p}$, this means $bs \in \mathfrak{p}$, and since $s \notin \mathfrak{p}$, it follows that $b \in \mathfrak{p}$. Thus $\mathfrak{p}_1 \cap A = \mathfrak{p}$, and we are done. □

Exercise 5.3.17. Do the Exercise 4.2.29 using the Going-up Theorem 5.3.16 above.

Lemma 5.3.18. Let $A \subset B$ be an integral extension of rings. Let $\mathfrak{q}_1 \subset \mathfrak{q}_2$ be prime ideals of B such that $\mathfrak{p}_1 := \mathfrak{q}_1 \cap A = \mathfrak{p}_2 := \mathfrak{q}_2 \cap A$. Then $\mathfrak{q}_1 = \mathfrak{q}_2$.

Proof: We note that with the given hypotheses, the extension

$$A_1 := A/\mathfrak{p}_1 \subset B_1 := B/\mathfrak{q}_1$$

is an integral extension of domains, and the prime ideal $\mathfrak{q} := \mathfrak{q}_2/\mathfrak{q}_1$ in B_1 satisfies the relation $\mathfrak{q} \cap A_1 = \{0\}$. We need to show that $\mathfrak{q} = \{0\}$. So it is enough to prove that:

$A \subset B$ is an integral extension of domains, and $\mathfrak{q}$ is a prime ideal of B with $\mathfrak{p} = \mathfrak{q} \cap A = \{0\}$, then $\mathfrak{q} = \{0\}$

Since A is a domain, the set $S = A \setminus \{0\}$ is a multiplicative set, and $S^{-1}A$ is precisely the quotient field of A. Also, by the Proposition 5.3.15, the extension of domains

$$Q(A) = S^{-1}A \subset S^{-1}B$$

is an integral extension of domains. But since $Q(A)$ is a field, it follows by the Proposition 4.2.26 that $S^{-1}B$ is a field. Since $S^{-1}\mathfrak{q}$ is an ideal in $S^{-1}B$, it must be either all of $S^{-1}B$ or $\{0\}$. It cannot be all of $S^{-1}B$, because then we would have that $1 = a/s$ for some $a \in \mathfrak{q}$ and $s \neq 0$ in A, and since B is a domain, this would imply that $a = s \neq 0$, i.e. $0 \neq s \in \mathfrak{q} \cap A = \{0\}$, a contradiction. So $S^{-1}\mathfrak{q} = \{0\}$. Again, since B is an integral domain, this means $\mathfrak{q} = \{0\}$ and the lemma is proved. □

Remark 5.3.19. In the above Lemma 5.3.18, one cannot drop the restriction that all the ideals be *prime*. For example, with $A = k$ and $B = k[x]/\langle x^2 \rangle$, we see that for $\mathfrak{q}_1 = \langle x \rangle$ and $\mathfrak{q}_2 = \{0\}$, we have $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A = \{0\}$. However, $\mathfrak{q}_1 \neq \mathfrak{q}_2$, the reason being that $\mathfrak{q}_2 = \{0\}$ is *not* a prime ideal in B, since B is not a domain.

Corollary 5.3.20 (Going-up Theorem 2)**.** Let $A \subset B$ be an integral extension of rings, and let

$$\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset .... \subset \mathfrak{p}_n$$

be an ascending chain of prime ideals in A . Then there exists an ascending chain of prime ideals in B

$$\mathfrak{q}_1 \subset \mathfrak{q}_2 \subset ... \subset \mathfrak{q}_n$$

with $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for all i. Furthermore, $\mathfrak{q}_i = \mathfrak{q}_{i+1}$ iff $\mathfrak{p}_i = \mathfrak{p}_{i+1}$.

Proof: Inductive application of the Theorem 5.3.16 to the integral extensions $A/\mathfrak{p}_i \subset B/\mathfrak{q}_i$ yields the ideal $\mathfrak{q}_{i+1}$. The last assertion follows immediately from Lemma 5.3.18. □

Here are some additional exercises on this section.

Exercise 5.3.21. Let A be a domain and $\mathfrak{p}$ a prime ideal in A. Show that $A \subset A_{\mathfrak{p}}$ is an integral extension iff $A = A_{\mathfrak{p}}$. (*Hint:* First show that $\mathfrak{p}$ must be a maximal ideal in A, and then show that it must be the *only* maximal ideal in A, i.e. A must be a local ring).

Exercise 5.3.22. Prove that the polynomial ring in one variable $k[T]$ is not isomorphic to $k[X,Y]/\langle Y^2 - X^3 \rangle$ as a k-algebra. (*Hint:* One is integrally closed in its quotient field, and the other is not). Show that the morphism of the affine line to the cubic cusp defined by:

$$\begin{aligned} \mathbb{A}^1(k) &\rightarrow V(Y^2 - X^3) \subset \mathbb{A}^2(k) \\ t &\mapsto (t^2, t^3) \end{aligned}$$

is a bijective morphism, but *not* an isomorphism of algebraic sets. (That is, there is no morphism which is an inverse of this morphism). Thus a morphism of algebraic sets which is a bijection as a set map *need not be an isomorphism* of algebraic sets! This is in sharp contrast to most algebraic objects like groups, rings, fields, vector spaces etc.

Exercise 5.3.23. If k is *not* algebraically closed, prove that every closed subset of $\mathbb{A}^n(k)$ can be expressed as $V(G)$ for some polynomial $G \in k[X_1, .., X_n]$. That is, every algebraic subset of $\mathbb{A}^n(k)$ can be defined by a *single* equation. (*Hint*: For $n = 1$, this fact is true for arbitrary k. So assume $n \geq 2$. First construct a polynomial $F_r \in k[T_1, .., T_r]$ (where $r \geq 2$)) whose only zero is the origin. Since k is not algebraically closed, find a monic polynomial $f(T) = T^m + a_1 T^{m-1} + ...a_m \in k[T]$ which has no roots in k. Prove that the only zero of $F_2(X_1, X_2) := \sum_{0 \leq i \leq m} a_i T_1^i T_2^{m-i}$ in $\mathbb{A}^2(k)$ is $(0,0)$. Inductively define $F_r(T_1, .., T_r) = F_2(F_{r-1}(T_1, .., T_{r-1}), T_r)$ and show that its only zero in $\mathbb{A}^r(k)$ is $(0, .., 0)$. Now let $X = V(f_1, .., f_r)$ be any closed subset of $\mathbb{A}^n(k)$. Set

$$G(X_1, .., X_n) = F_r(f_1(X_1, .., X_n), ..., f_r(X_1, .., X_n))$$

where F_r is the polynomial constructed above. For example, in the case of $k = \mathbb{R}$, we could set $f(T) = 1 + T^2$, leading to $F_2(T_1, T_2) = T_1^2 + T_2^2$, and more generally $F_r(T_1, .., T_r) = T_1^2 + .. + T_r^2$, and so $G = \sum_{i=1}^r f_i^2$ does the job).

Exercise 5.3.24. Let G be a finite group of automorphisms of a ring B, and let

$$A = B^G := \{b \in B : \ \sigma(b) = b \ \ \forall \ \ \sigma \in G\}$$

Show that:

(i): The ring extension $A \subset B$ is an integral extension (*Hint:* For an element $x \in B$, note that x satisfies the monic polynomial $f(X) = \prod_{\sigma \in G}(X - \sigma(x))$.)

(ii): Let $\mathfrak{p} \subset A$ be a prime ideal, and let:

$$S_{\mathfrak{p}} = \{\mathfrak{q} \in \operatorname{Spec} B : \ \mathfrak{q} \cap A = \mathfrak{p}\}$$

be the set of all prime ideals in A "lying over"$\mathfrak{p}$. Show that G acts transitively on $S_{\mathfrak{p}}$ (and hence $S_{\mathfrak{p}}$ has finite cardinality. *Hint:* Let $\mathfrak{q}_1, \mathfrak{q}_2 \in S_{\mathfrak{p}}$. For each $x \in \mathfrak{q}_1$, note that $\prod_\sigma(\sigma(x)) \in \mathfrak{q}_1 \cap B^G = \mathfrak{p} \subset \mathfrak{q}_2$. By the primeness of $\mathfrak{q}_2$, it follows that $\sigma(x) \in \mathfrak{q}_2$ for some $\sigma \in G$. Thus $\mathfrak{q}_1 \subset \cup_{\sigma \in G}\sigma(\mathfrak{q}_2$. Now use Exercise 4.1.4 and lemma 5.3.18 to conclude that $\mathfrak{q}_1 = \sigma\mathfrak{q}_2$.)

Exercise 5.3.25. Determine which of the following k-algebras (all are domains) are integrally closed:

(i): $k[X, Y]/\langle XY - 1\rangle$.

(ii): $k[X, Y]/\langle Y^2 - X^3\rangle$.

(iii): $k[X, Y]\langle Y^2 - X^2(X + 1)\rangle$.

Exercise 5.3.26. Let $A \subset B$ be an integral extension of rings. Show that if $\mathfrak{q} \subset B$ is a prime ideal of B lying over a maximal ideal $\mathfrak{m} \subset A$, then $\mathfrak{q}$ is a maximal ideal of B. Thus the natural map $\operatorname{Spec} B \to \operatorname{Spec} A$, which is a surjection, continues to be a surjection $\operatorname{Spm} B \to \operatorname{Spm} A$.

Exercise 5.3.27. Give an example of an integral ring extension $A \subset B$ such that B is not a finitely generated A-module.

6. Topology of Affine Algebraic Sets

In this section, we will translate algebra into geometry. *We will henceforth always assume that the field k is algebraically closed, unless explicitly stated otherwise.*

6.1. **An equivalence of categories.** The following proposition is obvious from the Proposition 5.2.3.

Proposition 6.1.1. Let k be algebraically closed, as per our assumption above. The correspondences $\mathfrak{a} \mapsto V(\mathfrak{a})$ and $Z \mapsto \mathfrak{I}(Z)$ set up a one-one correspondence between *radical ideals* of $k[X_1, .., X_n]$ and closed algebraic subsets of $\mathbb{A}^n(k)$.

Proof: Follows immediately from Propositions 5.2.3 and 3.1.6 that for a radical ideal $\mathfrak{a}$, we have $\mathfrak{I}(V(\mathfrak{a})) = \mathfrak{a}$ and for a closed algebraic subset Z of $\mathbb{A}^n(k)$, we have $V(\mathfrak{I}(Z)) = Z$, so the two correspondences above are inverses of each other. □

Definition 6.1.2. We call a ring A *reduced* if $\operatorname{nil} A = \{0\}$, i.e., the only nilpotent element in A is 0.

If $Z = V(\mathfrak{a})$ is a closed set, by replacing $\mathfrak{a}$ by its radical $\sqrt{\mathfrak{a}}$, we may as well assume that $\mathfrak{a}$ is a radical ideal, and equal to $\mathfrak{I}(Z)$. Thus in this case, there are no non-zero nilpotents in the coordinate ring $k[Z] = k[X_1, X_2, ..., X_n]/\mathfrak{a}$ of Z, and the coordinate ring of an affine closed set is a reduced k-algebra of finite type. It is obvious that a reduced k-algebra of finite type is the quotient of some polynomial ring $k[X_1, .., X_n]$ by a radical ideal. (This is, of course, not a unique representation, and will change if we change the algebra generators of the k-algebra.) Thus every reduced k-algebra of finite type is the coordinate ring of some affine closed set. The elements of the coordinate ring $k[Z]$ are called *regular functions* on Z. If $Z \in \mathbb{A}^n(k)$, then these are precisely the functions on Z which are restrictions of polynomials on $\mathbb{A}^n(k)$.

Going back to rings of continuous complex valued functions, it is known that every abelian, unital C^*-algebra (i.e. a Banach algebra with conjugation which satisfies a norm relation) arises as $C(X)$ for some compact hausdorff space X. In the Gelfand-Naimark theory for a compact hausdorff topological space X, one can reconstruct X and its topology from the ring of continuous complex valued functions $C(X)$. In algebraic geometry, the role of continuous functions is taken by regular functions,i.e. elements of the coordinate ring. Thus, one would analogously like to reconstruct Z with its Zariski topology from the reduced k-algebra of finite type given by the coordinate ring $k[Z]$. To this end, we have the following proposition:

Proposition 6.1.3. If $Z = V(\mathfrak{a})$ is an algebraic subset of $\mathbb{A}^n(k)$, where $\mathfrak{a}$ is a radical ideal in $k[X_1, .., X_n]$, then Z is in 1-1 correspondence with the *maximal spectrum*

$$\operatorname{Spm} k[Z] = \{\mathfrak{m} : \mathfrak{m} \text{ is a maximal ideal in } k[Z]\}$$

of the coordinate ring $k[Z] = k[X_1, .., X_n]/\mathfrak{a}$. Further, the family of Zariski-closed subsets of Z corresponds to the family of subsets:

$$\{\widetilde{V}(\mathfrak{b}) : \mathfrak{b} \text{ an ideal in } k[Z]\}$$

of $\operatorname{Spm} k[Z]$, where we define:

$$\widetilde{V}(\mathfrak{b}) := \{\mathfrak{m} : \mathfrak{m} \text{ is a maximal ideal in } k[Z] \text{ containing } \mathfrak{b}\}$$

Conversely, given a reduced k-algebra A of finite type, $\operatorname{Spm} A$ is a topological space, and homeomorphic to some algebraic set Z in some $\mathbb{A}^n(k)$ with its Zariski topology, and A is recovered as its coordinate ring $k[Z]$.

Proof: The first part of the proposition is clear from the Proposition 5.1.6 (weak nullstellensatz), and we remark here in passing that for a general (not necessarily radical) ideal $\mathfrak{a}$ in $k[X_1, .., X_n]$, a maximal (in fact even prime) ideal $\mathfrak{m}$ contains $\mathfrak{a}$ iff it contains $\sqrt{\mathfrak{a}}$, and hence the sets $\operatorname{Spm} k[X_1, .., X_n]/\sqrt{\mathfrak{a}}$, and $\operatorname{Spm} k[X_1, .., X_n]/\mathfrak{a}$ and the set:

$$\{\mathfrak{m} \subset k[X_1, .., X_n] : \mathfrak{m} \text{ is maximal} \supset \mathfrak{a}\}$$

are all in bijective correspondence. To check the statements about the topologies, let

$$p : k[X_1, .., X_n] \to k[X_1, .., X_n]/\mathfrak{a}$$

be the quotient homomorphism. Note that, $\mathfrak{b}$ is an ideal in $k[Z] = k[X_1, .., X_n]/\mathfrak{a}$ iff the inverse image $\mathfrak{b}_1 = p^{-1}(\mathfrak{b})$ is an ideal in $k[X_1, .., X_n]$ containing $\mathfrak{a}$, and $\mathfrak{m}$ is a maximal ideal in $k[Z]$ containing $\mathfrak{b}$ iff its inverse image $p^{-1}(\mathfrak{m})$ is a maximal ideal in $k[X_1, .., X_n]$ containing $\mathfrak{b}_1 = p^{-1}(\mathfrak{b})$. Thus the mapping $\mathfrak{m} \mapsto p^{-1}(\mathfrak{m})$ giving

the bijection between $\mathrm{Spm}(k[X_1,..,X_n]/\mathfrak{a}) \to V(\mathfrak{a})$ takes the set $\widetilde{V}(\mathfrak{b})$ to the closed subset $V(p^{-1}(\mathfrak{b})) \subset V(\mathfrak{a})$. For the converse statement, just write a representation of A as $A = k[X_1,..,X_n]/\mathfrak{a}$, where $\mathfrak{a}$ is a radical ideal in $k[X_1,..,X_n]$. By definition, the coordinate ring of $Z = V(\mathfrak{a})$ is the reduced k-algebra A. This proves the proposition. □

Let A, B be reduced k-algebras of finite type, and $\psi : A \to B$ be a k-algebra homomorphism. We define a map:

$$\begin{aligned} \psi^* : \mathrm{Spm}\, B &\to \mathrm{Spm}\, A \\ \mathfrak{m} &\mapsto \psi^{-1}(\mathfrak{m}) \end{aligned}$$

By the Proposition 5.1.7, $\psi^{-1}(\mathfrak{m})$ is a maximal ideal in A. It is easily verified that $(\psi^*)^{-1}(\widetilde{V}(\mathfrak{b})) = \widetilde{V}(\langle\psi(\mathfrak{b})\rangle)$, where $\langle\psi(\mathfrak{b})\rangle$ is the ideal generated by $\psi(\mathfrak{b})$ in B, so that ψ^* is continuous with respect to the Zariski topologies on $\mathrm{Spm}\, A$ and $\mathrm{Spm}\, B$.

Let Z_1, Z_2 be algebraic sets. We recall from the Proposition 5.1.9 that a map $\phi : Z_1 \to Z_2$ is a *morphism* if $\phi = \psi^*$ for some k-algebra homomorphism $\psi : k[Z_2] \to k[Z_1]$.

Remark 6.1.4 (Morphisms *versus* Zariski continuous maps)**.** Though morphisms between algebraic sets are continuous with respect to their Zariski topologies by definition (and the Proposition 6.1.3 above), *not all Zariski continuous maps are morphisms.* For example, if $k = \mathbb{C}$, any bijection from $\mathbb{C}$ to itself is continuous with respect to the Zariski topologies (=cofinite topologies), whereas the only morphisms from $\mathbb{C}$ to itself are polynomial maps, by Example 5.1.10.

We need one last lemma before we state the main proposition of this subsection.

Lemma 6.1.5. We have the following:

(i): Let k be an arbitrary field (not necessarily algebraically closed). Let A be a *reduced* k-algebra of finite type. For $f \in A$, $f = 0$ iff $f = 0 \pmod{\mathfrak{m}}$ for all $\mathfrak{m} \in \mathrm{Spm}\, A$.

(ii): Let k be an algebraically closed field. If $\phi, \psi : A \to B$ are both k-algebra homomorphisms of *reduced* k-algebras of finite type, then $\phi = \psi$ iff $\phi^* = \psi^* : \mathrm{Spm}\, B \to \mathrm{Spm}\, A$.

Proof: For (i), the only if part is obvious. So assume $f = 0 \pmod{\mathfrak{m}}$ for all $\mathfrak{m} \in \mathrm{Spm}\, A$. This means $f \in \cap\{\mathfrak{m} : \mathfrak{m} \in \mathrm{Spm}\, A\}$. But this last intersection is exactly $\mathrm{nil}\, A$, by Proposition 5.2.1 (which is true for an arbitrary field). Since A is reduced, $\mathrm{nil}\, A = 0$, and hence $f = 0$.

The only if part of (ii) is obvious again. So assume that $\phi^* = \psi^* : \mathrm{Spm}\, B \to \mathrm{Spm}\, A$. This means that $\psi^{-1}\mathfrak{m} = \phi^{-1}\mathfrak{m}$ for all $\mathfrak{m} \in \mathrm{Spm}\, B$. By the fact that $\phi^{-1}\mathfrak{m} \in \mathrm{Spm}\, A$, and ϕ is a k-algebra homomorphism, the map:

$$\overline{\phi} : A/\phi^{-1}\mathfrak{m} \to B/\mathfrak{m}$$

is precisely the identity map $k \to k$. Thus for each $x \in A$, we have

$$x \pmod{\phi^{-1}\mathfrak{m}} = \overline{x} = \overline{\phi}(\overline{x}) = \phi(x) \pmod{\mathfrak{m}} \quad \text{for all } \mathfrak{m} \in \mathrm{Spm}\, B$$

Similarly,

$$x \pmod{\psi^{-1}\mathfrak{m}} = \overline{x} = \overline{\psi}(\overline{x}) = \psi(x) \pmod{\mathfrak{m}} \quad \text{for all } \mathfrak{m} \in \mathrm{Spm}\, B$$

Since $\psi^{-1}\mathfrak{m} = \phi^{-1}\mathfrak{m}$ for all $\mathfrak{m} \in \mathrm{Spm}\, B$, it follows that $x \pmod{\phi^{-1}\mathfrak{m}} = x \pmod{\psi^{-1}\mathfrak{m}}$ for all $\mathfrak{m} \in \mathrm{Spm}\, B$. By the two equations above, this means that $\phi(x) = \psi(x) \pmod{\mathfrak{m}}$ for all $\mathfrak{m} \in \mathrm{Spm}\, B$ and all $x \in A$. By the part (i) above, this implies $\phi(x) = \psi(x)$ for all $x \in A$, i.e. $\phi \equiv \psi$. The lemma follows. □

Remark 6.1.6. (i) of the above Lemma is false if A is not assumed to be reduced. For example, if $A = k[X]/\langle X^2\rangle$, and we denote the image of X in A by x, then $\operatorname{Spm} A$ is $\{\langle x\rangle\}$, and clearly $x \pmod{\langle x\rangle} = 0$ even though $x \neq 0$.

Similarly (ii) fails if we don't assume A and B reduced (Exercise, using the example above). It *also* fails if we don't assume k to be algebraically closed. For example, setting $A = B = \mathbb{Q}[i]$, a $\mathbb{Q}$-algebra of finite type which happens to be a field, we have $\operatorname{Spm} A = \operatorname{Spm} B = \{0\}$. Clearly the identity map and the complex-conjugation map are distinct $\mathbb{Q}$-algebra homomorphisms, but both induce the identity map on $\operatorname{Spm} A$.

Proposition 6.1.7. Let $\mathcal{A}lg_{red}(k)$ be the category of *reduced* k-algebras of finite type with morphisms being k-algebra homomorphisms, and let $\mathcal{Z}ar$ be the category of all closed algebraic sets, with morphisms as defined in Proposition 5.1.9. Consider the functor:

$$\begin{aligned} F : \mathcal{Z}ar &\to \mathcal{A}lg_{red}(k) \\ Z &\mapsto k[Z] \end{aligned}$$

For a morphism $\phi^* : Z \to Y$, we define $F(\phi^*) = \phi : k[Y] \to k[Z]$, which makes sense by (ii) of Lemma 6.1.5.

Then:

(i): For each reduced k-algebra of finite type $A \in \mathcal{A}lg_{red}(k)$, there exists a $Z \in \mathcal{Z}ar$ such that $A = k[Z]$. (*Note*: This Z is *not* unique, but is determined upto isomorphism in $\mathcal{Z}ar$ as will follow from (iii) below.)

(ii): If two reduced k-algebras of finite type A and B are thus realised as $k[Y]$ and $k[X]$ respectively, then each k-algebra homomorphism $\phi : A \to B$ is realised as $F(f)$ for some uniquely determined morphism $f : X \to Y$ in $\mathcal{Z}ar$.

(iii): Algebraic sets X and Y in $\mathcal{Z}ar$ are isomorphic in $\mathcal{Z}ar$ iff $F(X) = k[X]$ and $k[Y]$ are isomorphic in $\mathcal{A}lg_{red}(k)$.

(iv): For each $Z \in \mathcal{Z}ar$, Z is homeomorphic to $\operatorname{Spm} F(Z)$, with the topology defined as in Proposition 6.1.3.

Thus the categories $\mathcal{Z}ar$ and $\mathcal{A}lg_{red}(k)$ may be viewed as "equivalent categories".

Proof: For (i), note that $A \in \mathcal{A}lg_{red}(k)$ implies $A = k[X_1, .., X_n]/\mathfrak{a}$ for some radical ideal $\mathfrak{a}$, which implies that $A = k[Z]$ for $Z := V(\mathfrak{a}) \subset \mathbb{A}^n(k)$. Since this expression of A as a quotient of a polynomial algebra is not unique, Z is not unique.

(ii) follows immediately from the definition of a morphism in Proposition 5.1.9, (by taking $f := \phi^*) : X \to Y$, and of course (ii) of the preceding Lemma 6.1.5 which says that this $\phi^* : X \to Y$ uniquely pins down ϕ.

The "if" part of (iii) is trivial noting that $\phi^*\psi^* = (\psi\phi)^*$ and $\mathrm{id}^* = \mathrm{id}$. For the only if part note that if $\phi^* : X \to Y$ and $\psi^* : Y \to X$ are morphisms which are inverses of each other, then $(\psi\phi)^*$ and $(\phi\psi)^*$ are identity maps of Y and X respectively. By (ii) of Lemma 6.1.5, this implies that $\psi\phi$ and $\phi\psi$ are both identity maps of $k[Y]$ and $k[X]$ respectively. Thus $k[Y]$ and $k[X]$ are isomorphic.

(iv) follows directly from the Proposition 6.1.3. The proposition follows. □

Exercise 6.1.8. Let $\psi^* : X \to Y$ be a morphism of affine algebraic sets. Show that $\psi : k[Y] \to k[X]$ is injective, iff ψ^* has Zariski dense image in Y. Similarly show that if ψ is a surjective map, then ψ^* is injective. What about the converse ?

The Exercise 5.3.22 shows that bijective morphisms of affine algebraic sets are not necessarily isomorphisms, i.e. do not necessarily induce isomorphisms of coordinate rings.

6.2. **Noether Normalisation Lemma Revisited.** We can now reformulate the Noether Normalisation Lemma in geometric terms.

Proposition 6.2.1. Let $Z = V(\mathfrak{a})$ be an affine algebraic subset of $\mathbb{A}^n(k)$, where k is an algebraically closed field, $\mathfrak{a}$ a radical ideal in $k[X_1, ..., X_n]$. Then there exists a morphism $\pi : Z \to \mathbb{A}^r(k)$ which is surjective and has finite fibres. If $k = \mathbb{C}$, then π is also a proper map, with respect to the classical topologies on Z and $\mathbb{C}^r$.

Proof: Let x_i denote the coordinate functions (= image of X_i) in the coordinate ring $k[Z] = k[X_1, ..., X_n]/\mathfrak{a}$. By the Noether Normalisation lemma, there is a subalgebra $k[y_1, .., y_r]$ of the coordinate ring $k[Z] = k[X_1, ..., X_n]/\mathfrak{a}$ such that the inclusion :

$$k[X_1, ..., X_n]/\mathfrak{a} \supset k[y_1, .., y_r]$$

is an integral extension, and the elements y_i are k-algebraically independent in $k[Z]$. Thus $k[y_1, .., y_r] = k[\mathbb{A}^r(k)]$.

Let $Y_1, .., Y_r$, which are polynomial functions of $X_1, .., X_n$, be elements of $k[X_1, .., X_n]$ which map to $y_1, .., y_r$ respectively under the quotient map $p : k[X_1, .., X_n] \to k[X_1, ..., X_n]/\mathfrak{a}$. Define :

$$\begin{aligned} \pi : \mathbb{A}^n(k) &\to \mathbb{A}^r(k) \\ (a_1, .., a_n) &\mapsto (Y_1(a_1, .., a_n), ..., Y_r(a_1, .., a_n)) \end{aligned}$$

In other words, $\pi = i^*$, where $i : k[y_1, .., y_r] \hookrightarrow k[Z]$ is the inclusion. Clearly π is continuous with respect to the Zariski topology since it is a morphism. By its definition above, it also continuous with respect to the classical topology if $k = \mathbb{C}$.

By the Exercise 6.1.8 above, π is surjective. We need to show the last two finiteness/properness statements.

For these assertions, note that $\{x_j\}_{j=1}^n$ are elements of $k[Z]$ which are integral over $k[y_1, .., y_r]$, so there are monic polynomial relations :

$$x_j^{n_j} + a_{j1}(y_1, .., y_r)x_j^{n_j - 1} + ..a_{jn_j}(y_1, .., y_r) = 0$$

for $j = 1, 2, ..n$, where $a_{ji}(y_1, .., y_r) \in k[y_1, .., y_r]$. For a fixed $(y_1, .., y_r) = (b_1, .., b_r)$, this is a polynomial with coefficients in k, so has only finitely many roots. Thus the fibre of π is finite. If $k = \mathbb{C}$, then as $(y_1, .., y_r)$ ranges in a compact set in $\mathbb{C}^r$, each coefficient $a_{ji}(y_1, .., y_r)$, which is polynomial and so continuous with respect to the classical topology, also ranges in some compact subset of $\mathbb{C}$, so the roots of all the above monic polynomials also range in some compact subsets of $\mathbb{C}$. (All roots of a monic polynomial $x^n + a_1x^{n-1} + ..a_n = 0$ with complex coefficients have modulus less or equal to $\max\{1, \Sigma_{i=1}^n \mid a_i \mid\}$, a fact which crucially depends on the monicity of the polynomial !). So the inverse image $\pi^{-1}(K) \subset Z$ of a compact subset $K \subset \mathbb{C}^r$ is compact, and π is proper. This proves the proposition. □

6.3. **An application: Invariant Theory for Finite Groups.** For reasons to be explained in the next section, an affine algebraic set X whose coordinate ring $k[X]$ is an integral domain is called an *irreducible* algebraic set. The quotient field of this integral domain is denoted by $k(X)$, and is called the *field of rational functions on* X.

Let G be a finite group acting *regularly* on an irreducible affine algebraic set X, i.e., for each $g \in G$, the left translation L_g is a regular morphism from X to X, with regular inverse $L_{g^{-1}}$. Thus it induces a natural k-algebra automorphism $L_g^* : k[X] \to k[X]$, given by $L_g^* f = f \circ L_{g^{-1}}$ for $f \in k[X]$. For notational convenience, we will denote $L_g^* f$ by $g.f$. Assume that the characteristic of the field k is not divisible by $|G|$. We would like to make the quotient set X/G an affine algebraic set by describing its coordinate ring. Finally, we want the natural quotient map $\pi : X \to X/G$ to be a surjective morphism with finite fibres.

It is clear that if any regular function h on the to-be X/G is composed with π, which is to be a regular morphism, then this composite will be forced to be a regular function on X which will be constant on each orbit, i.e. a function which is invariant under the action $h \mapsto g.h$ of G on $k[X]$. Conversely, we would like every such G-invariant regular function on X to descend to the quotient X/G, in keeping with the universal property of any quotient object in any category.

Introduce the *averaging operator*:

$$\begin{aligned} A : k[X] &\to k[X] \\ f &\mapsto \frac{1}{|G|}\sum_{g\in G} g.f \end{aligned}$$

which makes sense since $\mathrm{char}(k)$ does not divide $|G|$. It is clear that A maps $k[X]$ onto the *G-invariant subalgebra* defined by:

$$k[X]^G := \{f \in k[X] : g.f = f \text{ for all } g \in G\}$$

Of course, A is not a ring homomorphism, but is easily checked to be a $k[X]^G$-module endomomorphism of $k[X]$. Let $\{y_i\}_{i=1}^n$ be a set of k-algebra generators for $k[X]$ (for example, the coordinate functions, if X is realised as isomorphic to an affine closed subset of $\mathbb{A}^n(k)$). Let us denote $d := |G|$.

Consider the single variable polynomial of degree d:

$$P_i(T) = \Pi_{g\in G}(T - g.y_i)$$

This is a monic polynomial in T whose coefficients are the elementary symmetric polynomials in the roots $\{g.y_i\}_{g\in G}$. G acts on this set of roots by permutations, so all the coefficients $\{a_{ij}\}_{j=1}^d$ of this polynomial are in the invariant subalgebra $k[X]^G$. Also note $P_i(y_i) = 0$. Hence all algebra generators y_i of $k[X]$ are integral over $k[X]^G$, and it follows that the inclusion homomorphism $j : k[X]^G \hookrightarrow k[X]$ is an integral extension.

We now claim that $k[X]^G$ is a k-algebra of finite type. Look at the set:

$$S = \{A(y_1^{i_1}...y_n^{i_n}) : i_j \leq d-1 \ \forall\ 1 \leq j \leq n\} \cup \{a_{ij} : 1 \leq j \leq d;\ 1 \leq i \leq n\}$$

We claim that S is a set of k-algebra generators of $k[X]^G$. For, if $f = f(y_1, .., y_n)$ is any element of $k[X]^G$, by using the monic relations $P_i(y_i) = 0$, we can convert it into a polynomial in a_{ij} and y_i such that only powers of y_i which occur in f are $\leq d-1$. That is $f = \Sigma\lambda_{JI}a_J y^I$ where $\lambda_{JI} \in k$, a_J is a monomial in a_{ij}, $y^I = y_1^{i_1}..y_n^{i_n}$ with $i_r \leq d-1$ for all $1 \leq r \leq n$. Since $f \in k[X]^G$, $f = Af = \Sigma\lambda_{JI}a_J A(y^I)$, (since A is $k[X]^G$ linear, and $a_J \in k[X]^G$. This shows that S generates $k[X]^G$ as a k-algebra.

Since $k[X]^G$ is a subalgebra of $k[X]$, it is also an integral domain, and by the Proposition 6.1.3, it is the coordinate ring of an irreducible affine closed set which we denote by X/G. Since the injection $j : k[X]^G \subset k[X]$ is an integral extension, it induces a finite surjective map $j^* : X \to X/G$, which is the required regular quotient map, which we will denote by π. It is a finite map by definition.

Those who are familiar with finite Galois extensions will note that the inclusion of the corresponding function fields, namely the field extension $k(X) \supset k(X)^G$ is a Galois extension of degree $\mid G \mid$. This is by the fundamental theorem of Galois theory. Also, the case of $G = S_n$ acting by permutations on k^n, is the classical one considered by Galois in his work on the solvability of equations. If one views k^n as the space of all roots of monic polynomials of degree n, with G acting by permutation of these roots, the space $(k^n)^G$ is interpreted as the space of all monic polynomials of degree n, the quotient map $\pi : k^n \to (k^n)^G$ simply maps $(x_1, ..., x_n)$ to the monic polynomial $\prod_{i=1}^n(X - x_i)$. If one identifies the space of monic polynomials of degree n with k^n, the polynomial $f(X) = X^n + \Sigma_{i=1}^n a_i X^{n-i}$ being identified with $(a_1, .., a_n)$, we clearly have

$$\pi(x_1, .., x_n) = (-\sigma_1(x_1, .., x_n), .., (-1)^n\sigma_n(x_1, .., x_n))$$

where the elementary symmetric functions σ_i are a set of k-algebra generators for $k[X]^G$. Finally, we note that for a monic polynomial f of degree n, $\pi^{-1}(f)$ consists of all permutations of the n-roots of f, and if f is a monic polynomial with distinct roots, the cardinality of this fibre $\pi^{-1}(f)$ is $n\,!$. If it does not have distinct roots, the fibre will have cardinality $\frac{n\,!}{d_1\,!..d_k\,!}$ where d_i is the multiplicity of the $i-th$ (distinct) root. The degenerate polynomials $f(X) = (X - a)^n$ will have singleton fibres. Since k is algebraically closed, every fibre is non-empty. The subset of polynomials whose fibres have cardinality strictly less than $n\,!$ constitutes a closed subset of $X^G = k^n$, namely, the hypersurface defined by the vanishing of the discriminant (defined as $\prod_{i\neq j}(x_i - x_j)$ for the polynomial $f(X) = \prod_{i=1}^n(X - x_i)$. It can be expressed as a polynomial in the coefficients σ_i of f. For example, in the case of $n = 2$, the discriminant is $\sigma_1^2 - 4\sigma_2$.)

6.4. **Noetherian Spaces, irreducibility.**

Definition 6.4.1. A topological space Z is said to be *Noetherian* if every descending chain of closed sets:

$$...C_{i+1} \subset C_i ... \subset C_1 \subset C_0 = Z$$

becomes stationary, i.e., there exists an N such that $C_j = C_{j+1}$ for all $j \geq N$.

Proposition 6.4.2. An algebraic set with its Zariski topology is Noetherian.

Proof:

Let $...C_{j+1} \subset C_j \subset ....Z$ be a descending chain of closed subsets of Z. The sequence of ideals

$$\mathfrak{I}(C_j) := \{f \in k[Z] : \ f_{|C_j} \equiv 0\}$$

is an ascending chain of ideals in the Noetherian ring $k[Z]$ (by Proposition 2.3.7) and thus becomes stationary. Since C_j are Zariski closed, $C_j = \widetilde{V}(\mathfrak{I}(C_j))$, and the descending chain above becomes stationary. □

Definition 6.4.3. We call a space *quasicompact* if every open covering of it has a finite subcovering.

Usually such spaces are called compact. But Bourbaki, and other mathematicians of the French school, included hausdorffness in their notion of compactness. So, for purely historical reasons, algebraic geometry conventions dictate that such spaces be called quasicompact, since most spaces in the Zariski topology are not hausdorff.

Corollary 6.4.4. Every open subset of a Noetherian topological space Z is quasicompact.

Proof: Let U be an open subset of Z, and let us assume that $\{U_\alpha\}_{\alpha \in \Lambda}$ is an open covering of U with no finite subcovering. Then it is possible to find a sequence of opens $\{U_{\alpha_i}\}_{i=1}^{\infty}$ such that the open subsets $V_k = \cup_{i=1}^{k} U_{\alpha_i}$ satisfy $V_k \subset V_{k+1}$ is a proper inclusion. Thus the complements $C_k = V_k^c$ give a strictly descending chain of closed sets which is never stationary, which contradicts that Z is Noetherian. □

Corollary 6.4.5. In a Noetherian topological space, every intersection of closed sets is a finite intersection.

Proof: If not, one easily obtains a strictly descending chain of closed sets. □

Definition 6.4.6. A topological space Z is said to be *irreducible* if it cannot be expressed as the union of two *proper* closed subsets. That is, if $Z = C_1 \cup C_2$, with C_i closed, then $Z =$C$_1$ or $Z = C_2$.

Remark 6.4.7. Clearly, an irreducible space is connected, but not conversely. The algebraic set defined by the union of the coordinate axes $V(XY) \subset \mathbb{C}^2$ is connected, but expressible as $V(X) \cup V(Y)$ and thus not irreducible.

Proposition 6.4.8. If $\mathfrak{p}$ is a prime ideal in any commutative ring, and $\mathfrak{p} \supset \mathfrak{a}\mathfrak{b}$ for some ideals $\mathfrak{a}$, $\mathfrak{b} \subset A$, then $\mathfrak{p} \supset \mathfrak{a}$, or $\mathfrak{p} \supset \mathfrak{b}$. In particular if a prime ideal $\mathfrak{p} \supset \mathfrak{a} \cap \mathfrak{b}$, then $\mathfrak{p} \supset \mathfrak{a}$ or $\mathfrak{p} \supset \mathfrak{b}$. More generally, if $\mathfrak{p} \supset \prod_{i=1}^{n} \mathfrak{a}_i$ for some ideals $\mathfrak{a}_i$ in A, then $\mathfrak{p} \supset \mathfrak{a}_j$ for some j. In particular, if $\mathfrak{p} \supset \cap_{i=1}^{n} \mathfrak{a}_i$, then $\mathfrak{p} \supset \mathfrak{a}_j$ for some j.

Proof: This was the Exercise 4.1.3, but here's the proof anyway. Suppose $\mathfrak{p} \not\supset \mathfrak{a}$ and $\mathfrak{p} \not\supset \mathfrak{b}$. Then let $a \in \mathfrak{a} \setminus \mathfrak{p}$ and $b \in \mathfrak{b} \setminus \mathfrak{p}$. Then $ab \in \mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$, which contradicts that $\mathfrak{p}$ is prime. The second assertion follows since $\mathfrak{a} \cap \mathfrak{b} \supset \mathfrak{a}\mathfrak{b}$. The third assertion follows by induction. The last follows since $\cap_{i=1}^{n} \mathfrak{a}_i \supset \prod_{i=1}^{n} \mathfrak{a}_i$. □

Proposition 6.4.9. An algebraic set $V(\mathfrak{a}) \subset \mathbb{A}^n(k)$ is irreducible iff $\sqrt{\mathfrak{a}}$ is a prime ideal in $k[X_1, .., .X_n]$. Equivalently, for a reduced k-algebra of finite type, Spm(A) is irreducible iff A is an integral domain.

Proof:
Let A denote $k[X_1, .., X_n]$. Assume $\sqrt{\mathfrak{a}}$ is prime. Let $V(\mathfrak{a}) = C_1 \cup C_2$, where C_i are closed subsets, and hence equal to $V(\mathfrak{a}_i)$ for $i = 1, 2$. Thus $V(\mathfrak{a}) = V(\mathfrak{a}_1 \cap \mathfrak{a}_2)$, so that by the nullstellensatz $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{a}_1 \cap \mathfrak{a}_2} \supset \mathfrak{a}_1 \cap \mathfrak{a}_2$. By the previous proposition, $\sqrt{\mathfrak{a}} \supset \mathfrak{a}_1$ or $\sqrt{\mathfrak{a}} \supset \mathfrak{a}_2$. Thus $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}}) \subset V(\mathfrak{a}_1) = C_1$ or $V(\mathfrak{a}_2) = C_2$, which implies $V(\mathfrak{a}) = C_1$ or C_2.

Conversely, assume $V(\mathfrak{a})$ is irreducible, and let $fg \in \sqrt{\mathfrak{a}}$. Then $V(fg) = V(f) \cup V(g) \supset V(\mathfrak{a})$, so that :

$$V(\mathfrak{a}) = (V(f) \cap V(\mathfrak{a})) \cup (V(g) \cap V(\mathfrak{a})) = V(\mathfrak{a} + Af) \cup V(\mathfrak{a} + Ag)$$

By irreducibility, either $V(\mathfrak{a}) = V(\mathfrak{a} + Af)$ or $V(\mathfrak{a}) = V(\mathfrak{a} + Ag)$, which implies $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{a} + Af} \supset \mathfrak{a} + Af$ or $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{a} + Ag} \supset \mathfrak{a} + Ag$. In the first case $f \in \sqrt{\mathfrak{a}}$, and in the second $g \in \sqrt{\mathfrak{a}}$, showing that $\sqrt{\mathfrak{a}}$ is prime.

The second assertion follows immediately from the Proposition 6.1.3. □

Proposition 6.4.10. Every algebraic set is a finite union of irreducible closed sets.

Proof: Fix an n, and let Σ be the collection of all algebraic subsets $Z \subset \mathbb{A}^n(k)$ which are *not* finite unions of closed irreducibles. We claim that $\Sigma = \phi$.

Assume $\Sigma \neq \phi$. Order it by inclusion. We claim that every chain $\Lambda = \{Z_\alpha\}$ in Σ has a lower bound. Let $Z = \cap_\alpha Z_\alpha$. By the Corollary 6.4.5 above, $Z = \cap_{\alpha \in F} Z_\alpha$, where F is a finite set. Since Λ is a chain, $Z = Z_\gamma$ where Z_γ is the smallest element of the finite family $\{Z_\alpha\}_{\alpha \in F}$. Thus $Z \in \Sigma$.

By Zorn's lemma, Σ has a minimal element Z, say. We claim that Z is irreducible. For if $Z = C_1 \cup C_2$, with C_i closed and both proper subsets of X, by the minimality of X in Σ, it follows that C_1 and C_2 are not members of Σ, and hence both are finite unions of closed irreducible sets, which means that Z is also a finite union of closed irreducibles, contradicting that $Z \in \Sigma$. Thus Z is irreducible, and since it is closed, this means $Z \notin \Sigma$, which is again a contradiction. Thus Σ is empty, and the assertion is proved. □

Remark 6.4.11. In the above proposition, if we express an algebraic set $Z = \cup_{i=1}^k Z_i$, where Z_i are irreducible algebraic sets, and make the union *irredundant* (i.e. $Z_i \not\subset Z_j$ for $i \neq j$), then the sets Z_j are uniquely determined upto a permutation, and called the *irreducible components of* Z. The proof is an easy exercise.

Corollary 6.4.12. Let $\mathfrak{a}$ be an ideal in $k[X_1, ..., X_n]$. Then there exist prime ideals $\{\mathfrak{p}_i\}_{i=1}^k$ such that $\sqrt{\mathfrak{a}} = \cap_{i=1}^k \mathfrak{p}_i$ and $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ for $i \neq j$. Further, this collection of primes is uniquely determined.

Proof: Consider $Z = V(\mathfrak{a})$. By the Propositions 6.4.9 and 6.4.10, it follows that $V(\mathfrak{a}) = \cup_{i=1}^k V(\mathfrak{p}_i) = V(\cap_{i=1}^k \mathfrak{p}_i)$, from which it follows that $\sqrt{\mathfrak{a}} = \sqrt{\cap_{i=1}^k \mathfrak{p}_i} = \cap_{i=1}^k \sqrt{\mathfrak{p}_i} = \cap_{i=1}^k \mathfrak{p}_i$. The uniqueness assertion follows from the Remark 6.4.11 above. □

The corollary above is a purely algebraic statement about polynomial rings, even though geometric ingredients went into proving it. In the special case that $\mathfrak{a} = \langle f \rangle$, i.e., a principal ideal, the corollary above can be deduced from the unique prime factorisation in $k[X_1, .., X_n]$ proved in Proposition 2.2.17. Thus the above corollary should be viewed as a way of factorising radical *ideals* into prime factors. There is thing called "primary decomposition" in arbitrary Noetherian rings which is the most general avatar of prime factorisation, and we shall encounter it later.

Remark 6.4.13. Usually, one is used to decomposing elements into *products* of primes, so it would seem natural to seek expressions of arbitrary ideals as ideal products of prime ideals. We note that for a prime ideal $\mathfrak{p}$

$$\mathfrak{p} \supset \prod_{i=1}^n \mathfrak{a}_\mathfrak{i} \Leftrightarrow \mathfrak{p} \supset \mathfrak{a}_i \text{ for some } i \Leftrightarrow \mathfrak{p} \supset \cap_{i=1}^n \mathfrak{a}_i$$

(by 6.4.8) which implies (by 4.1.9) that the radical of a product of ideals is the same as the radical of their intersection, for a radical ideal (or equivalently, a closed algebraic set), the statement of the last corollary is true with intersection of prime ideals replaced by the *radical* of their product.

Incidentally, there are radical ideals in the world which cannot be expressed as a *product* of prime ideals. Consider the:

Example 6.4.14. Let $\mathfrak{a} = \langle XZ, YZ, XY\rangle \subset k[X,Y,Z]$. It is easily verified that:

$$\mathfrak{a} = \langle X, Y\rangle \cap \langle Y, Z\rangle \cap \langle Z, X\rangle$$

and each of the three ideals on the right is prime. Thus $\mathfrak{a}$ is a radical ideal. However the product of the three prime ideals on the right is the ideal:

$$\langle X^2Y, XY^2, X^2Z, XZ^2, Y^2Z, YZ^2\rangle$$

which is strictly contained in $\mathfrak{a}$.

Exercise 6.4.15. Let X be an affine closed set with irreducible components $\{X_i\}_{i=1}^m$. Then show that the coordinate ring $k[X]$ is a k-subalgebra of $\oplus_{i=1}^m k[X_i]$ (which is a reduced k-algebra in a natural manner by coordinate-wise operations). Determine the coordinate ring of $k[Z]$ where $Z = V(XY) \subset \mathbb{A}^2(k)$ as a subalgebra of $k[X] \oplus k[Y]$.

Exercise 6.4.16.

(i): In the polynomial ring $k[X,Y,Z]$, compute the radical of the ideal $\mathfrak{a} = \langle XY^2, Y^2Z\rangle$.

(ii): Write down the decomposition of $V(\mathfrak{a})$ ($\mathfrak{a}$ being the ideal in (i) above) into its irreducible components.

Exercise 6.4.17. Let $X = \cup_{i=1}^m X_i$ be the irredundant decomposition of an affine algebraic set X, and let $x \in X_i \setminus (\cup_{j\neq i} X_j)$. Show that there exists a regular function $f \in k[X]$ which satisfies $f(x) \neq 0$, and $f_{|X_j} \equiv 0$ for all $j \neq i$.

Now we would like to define a convenient basis for the open subsets of an algebraic set Z.

Proposition 6.4.18. Let $Z \in \mathbb{A}^n(k)$ be an algebraic set, and $k[Z]$ its coordinate ring. Then for $f \in k[Z]$, define the subset

$$D(f) = \{p \in Z : f(p) \neq 0\}$$

Then $D(f)$ is an open subset of Z, called a *principal open set* or *basic open set* of Z. The collection of principal open sets

$$\{D(f) :\ f \in k[Z]\}$$

is a basis for the Zariski topology on Z. In fact, for any open set $U \subset Z$, one may write:

$$U = \cup_{i=1}^m D(f_i)$$

where $f_i \in k[Z]$ are some regular functions. Finally, $Z = \cup_{i=1}^m D(f_i)$ iff there exist $h_i \in k[Z]$ such that $\sum_{i=1}^m h_i f_i = 1$.

Proof: By the Proposition 6.1.3, the set $\widetilde{V}(f) \subset Z$ is a closed subset of Z, and $D(f)$ is its complement, so it is open. If U is an open subset of Z, then $U = Z \setminus \widetilde{V}(\mathfrak{b})$, for some ideal $\mathfrak{b} \subset k[Z]$. Since $k[Z]$ is Noetherian, we have $\mathfrak{b} = \langle f_1, .., f_m\rangle$, so that $\widetilde{V}(\mathfrak{b}) = \cap_{i=1}^m \widetilde{V}(f_i)$, which implies that $U = \cup_{i=1}^m D(f_i)$.

For the last statement, note that $Z = \cup_{i=1}^m D(f_i)$ iff $\widetilde{V}(\langle f_1, .., f_m\rangle) = \phi = \widetilde{V}(\langle 1\rangle)$, and this happens iff the radical $\sqrt{\mathfrak{b}}$ of the ideal $\mathfrak{b} := \langle f_1, .., f_m\rangle$ is the whole ring $k[Z]$. This, in turn, happens iff $1 \in \mathfrak{b}$, i.e. iff $1 = \sum_{i=1}^m h_i f_i$. The proposition follows. □

We have already defined regular functions on an affine algebraic set X as the elements of the coordinate ring $k[X]$. Our next aim is to define the local ring at a point $x \in X$, as well as the ring of regular functions on an open set $U \subset X$. First we observe the following easy fact about localisations.

Proposition 6.4.19. Let A be an integral domain, and let $K = Q(A)$ denote its quotient field. For a prime ideal $\mathfrak{p}$, we denote the localisation $S^{-1}A$ at the multiplicative set $S = A \setminus \mathfrak{p}$ by $A_\mathfrak{p}$ (see Definitions 5.3.1 and 5.3.3). Clearly $A_\mathfrak{p} \subset K$ for each prime ideal $\mathfrak{p}$ of A. Then we have:

$$A = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} A_\mathfrak{p} = \bigcap_{\mathfrak{m} \in \operatorname{Spm} A} A_\mathfrak{m}$$

where the intersections on the right are taken in K.

Proof: Since A is a domain, it sits inside all its localisations, so it is clear that A is contained in the two intersections on the right. Also since $\operatorname{Spm} A \subset \operatorname{Spec} A$, it follows that

$$\bigcap_{\mathfrak{p} \in \operatorname{Spec} A} A_\mathfrak{p} \subset \bigcap_{\mathfrak{m} \in \operatorname{Spm} A} A_\mathfrak{m}$$

Thus it is enough to prove that inside K, we have:

$$\bigcap_{\mathfrak{m} \in \operatorname{Spm} A} A_\mathfrak{m} \subset A$$

So let $f \in K$ be an element of the left hand side. Then, for each $\mathfrak{m} \in \operatorname{Spm} A$, we have the following equality in K:

$$f = \frac{a_\mathfrak{m}}{b_\mathfrak{m}}$$

with $b_\mathfrak{m} \in A \setminus \mathfrak{m}$. Consider the ideal in A defined by:

$$\mathfrak{a} := \langle b_\mathfrak{m} \rangle_{\mathfrak{m} \in \operatorname{Spm} A}$$

If this ideal $\mathfrak{a}$ is a proper ideal of A, there will be a maximal ideal $\mathfrak{n}$ of A containing it. But then $\mathfrak{n} \in \operatorname{Spm} A$, and so $b_\mathfrak{n} \in \mathfrak{a}$. It follows that $b_\mathfrak{n} \in \mathfrak{n}$, contradicting that $b_\mathfrak{n} \in A \setminus \mathfrak{n}$. It follows that $\mathfrak{a}$ must be A. In particular, there exist elements $b_i \in A \setminus \mathfrak{m}_i$, for $\mathfrak{m}_i \in \operatorname{Spm} A$, $i = 1, 2, .., r$, such that $1 = \sum_{i=1}^r h_i b_i$, for some $h_i \in A$. Thus

$$f = \sum_{i=1}^r h_i b_i f = \sum_{i=1}^r h_i a_i$$

since $f = \frac{a_i}{b_i}$ for each i. But the element on the right hand side above is clearly in A, which proves our assertion and the proposition follows. □

6.5. **Local rings and regular functions on open sets.** We have already defined regular functions on X to be elements of the coordinate ring $k[X]$. It will be useful to define other kinds of functions, which are regular at a point, or on an open subset, etc.

Definition 6.5.1 (Local ring at a point)**.** Let X be an affine closed set, with the reduced affine coordinate ring $k[X]$. For a maximal ideal $\mathfrak{m}_x$ corresponding to the point $x \in X$, the localisation $k[X]_{\mathfrak{m}_x}$ (in the sense of Example 5.3.3) is called the *local ring of X at x*. This local ring will be denoted by $\mathcal{O}_{X,x}$. Its unique maximal ideal is $\mathfrak{m}_x \mathcal{O}_{X,x}$, sometimes denoted by abuse of notation as $\mathfrak{m}_x$. An element in this local ring is a quotient $\frac{f}{g}$, where $g \in k[X] \setminus \mathfrak{m}_x$, i.e. $g(x) \neq 0$. The image of a regular function $f \in k[X]$, viz. the element $\frac{f}{1} \in \mathcal{O}_{X,x}$ is denoted f_x, and called the *germ of f at x*. This germ f_x *is not be confused with* $f(x) \in k$. An element of $\mathcal{O}_{X,x}$ is said to be a function *regular at x*.

Definition 6.5.2 (Function field of an irreducible affine algebraic set)**.** If $X \subset \mathbb{A}^n(k)$ is an *irreducible* closed algebraic set with $X = V(\mathfrak{p})$ where $\mathfrak{p} \subset k[X_1, .., X_n]$ is a prime ideal, its coordinate ring $k[X] = k[X_1, .., X_n]/\mathfrak{p}$ is an *integral domain*. The quotient field $Q(k[X])$ makes sense, and is called the *field of rational functions on X*, or *function field of X*, and denoted $k(X)$. An element of $k(X)$ can be written as $\frac{f}{g}$ where $g \neq 0$ in $k[X]$, i.e. g does not vanish identically on X. In this situation of X irreducible, each local ring $\mathcal{O}_{X,x}$ is a subring of $k(X)$.

Example 6.5.3. For $X = \mathbb{A}^n(k)$, the function field is $k(X) = k(X_1, X_2, .., X_n)$, the field of rational functions in n-variables.

We remark here that although the coordinate ring $k[X]$ of X is a quotient of the polynomial coordinate ring $k[X_1, .., X_n]$ of $\mathbb{A}^n(k)$, the function field $k(X)$ of X generally bears no relation to the function field $k(X_1, .., X_n)$ of $\mathbb{A}^n(k)$.

We now list some immediate facts about these local rings.

Proposition 6.5.4 (Some facts on $\mathcal{O}_{X,x}$ and $k(X)$)**.**

(i): There is an evaluation map $\epsilon_x : \mathcal{O}_{X,x} \to k$, sending $\frac{f}{g}$ to $\frac{f(x)}{g(x)}$, which is a k-algebra homomorphism. Its kernel is precisely the unique maximal ideal $\mathfrak{m}_x\mathcal{O}_{X,x}$ (= the ideal localisation $S^{-1}\mathfrak{m}_x$ at the multiplicative set $S = k[X] \setminus \mathfrak{m}_x$). $\mathfrak{m}_x\mathcal{O}_{X,x}$ is therefore the ideal of functions in $\mathcal{O}_{X,x}$ which vanish at x.

(ii): If $f, g \in k[X]$, and $f(x) = g(x)$ for all $x \in X$, then $f = g$. In particular, if the germs $f_x = g_x$ in $\mathcal{O}_{X,x}$ for all $x \in X$, then $f = g$.

(iii): If $f : X \to Y$ is a morphism of affine algebraic sets, induced by the k-algebra homomorphism $f^* : k[Y] \to k[X]$ of their coordinate rings, then for each $x \in X$, there is an induced homomorphism of local rings denoted:

$$f_x^* : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$$

which satisfies $\epsilon_x \circ f_x^* = \epsilon_{f(x)}$. Thus $(f_x^*)^{-1}(\mathfrak{m}_x) = \mathfrak{m}_{f(x)}$, where $\mathfrak{m}_x$ and $\mathfrak{m}_{f(x)}$ are the unique maximal ideals of $\mathcal{O}_{X,x}$ and $\mathcal{O}_{Y,f(x)}$ respectively.

(iv): Let $f : X \to Y$ be a morphism as in (iii), and X and Y be *irreducible*. Further assume that the homomorphism $f^* : k[Y] \to k[X]$ is *injective*. Then we have an induced injection of function fields $f^* : k(Y) \to k(X)$.

(v): If X is irreducible, we have:

$$\bigcap_{x \in X} \mathcal{O}_{X,x} = k[X], \quad \bigcup_{x \in X} \mathcal{O}_{X,x} = k(X)$$

where the intersection and union are taken inside the function field $k(X)$.

Proof: To see (i), observe that there is the evaluation homomorphism $\epsilon_x : k[X] \to k[X]/\mathfrak{m}_x = k$. Also it maps every element of the multiplicative set $k[X] \setminus \mathfrak{m}_x$ to $k \setminus \{0\}$, i.e. invertible elements in k. Thus by (i) of the Proposition 5.3.11, there is a homomorphism $\mathcal{O}_{X,x} \to k$, which we also denote ϵ_x, satisfying $\epsilon_x(f_x) = \epsilon_x(f) = f(x)$. For a typical element $\frac{f}{g} \in \mathcal{O}_{X,x}$, with $g \notin \mathfrak{m}_x$ (i.e. $g(x) \neq 0$) we have $\epsilon_x(\frac{f}{g}) = \frac{f(x)}{g(x)} \in k$. The second statement of (i) is clear.

To see (ii), note that $f(x) = g(x)$ for all $x \in X$ means that $f - g \in \cap_{x \in X}\mathfrak{m}_x$. The right hand side is the nilradical of $k[X]$ by the Proposition 5.2.1, which is $\{0\}$ since $k[X]$ is reduced. Thus $f = g$. Since $f_x(x) = f(x)$ for all $x \in X$, the second assertion of (ii) is clear.

To see (iii), note that the inverse image $(f^*)^{-1}\mathfrak{m}_x \subset k[X]$ is $\mathfrak{m}_{f(x)} \subset k[Y]$ (by the Proposition 5.1.7 in §5). Now we apply (ii) of the Proposition 5.3.11 to get a homomorphism $\widetilde{f^*} : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ of the corresponding localised rings. We will also denote this homomorphism by f^*, for notational simplicity.

Since f^* is injective, and $\mathcal{O}_{X,x}$ and $\mathcal{O}_{Y,f(x)}$ are domains, the inverse image of the prime ideal $\{0\}$ in $\mathcal{O}_{X,x}$ is the prime ideal $\{0\}$ in $\mathcal{O}_{Y,f(x)}$. Now (iv) is immediate from (ii) of the Proposition 5.3.11.

The first part of (v) follows from the Proposition 6.4.19. The second part follows by observing that if $\frac{f}{g} \in k(X)$, with $g \neq 0$ in $k[X]$, then there exists a point $x \in X$ such that $g(x) \neq 0$. This is because the intersection of all the maximal ideals in $k[X]$ is the nilradical of $k[X]$ (by Proposition 5.2.1), which is $\{0\}$, since $k[X]$ is a domain. Thus the element $\frac{f}{g}$ lies in $\mathcal{O}_{X,x}$. This proves the proposition. □

Remark 6.5.5. The part (v) of the last proposition says that every rational function on an irreducible affine algebraic set X is regular at some point, and a rational function that is regular at each point of x is a regular function on X.

Remark 6.5.6. The requirement that k be algebraically closed is crucial. The reader can easily construct an example of a function $f \in k[\mathbb{A}^1(k)] = k[T]$, k a finite field, with $f(x) = 0$ for all $x \in \mathbb{A}^1(k)$ but $f \neq 0$. (Exercise: If k is an infinite but not algebraically closed, and $f \in k[X_1, .., X_n]$ satisfies $f(x) = 0$ for all $x \in \mathbb{A}^n(k)$, is it true that $f = 0$?)

Exercise 6.5.7. Describe the local ring $\mathcal{O}_{Z,0}$ of the pair of intersecting lines $Z := V(XY) \subset \mathbb{A}^2(k)$.

Exercise 6.5.8. Using the map $\phi : \mathbb{A}^1(k) \to V(Y^2 - X^3)$ given by $t \mapsto (t^2, t^3)$, describe the local ring $\mathcal{O}_{Z,0}$ of the plane cusp $Z := V(Y^2 - X^3)$ at the origin as a subring of $k(t)$.

Proposition 6.5.9 (Regular functions on open sets)**.** Let X be an irreducible affine algebraic set, and $f \in k[X]$ be a regular function on X. Let $D(f) \subset X$ denote the principal open set of points at which f does not vanish (see the Proposition 6.4.18). Then we have:

$$\bigcap_{x \in D(f)} \mathcal{O}_{X,x} = (k[X])_f$$

inside the function field $k(X)$. The intersection on the left side is precisely the set of functions regular at each point of $D(f)$, and denoted by $k[D(f)]$. An element of $k[D(f)]$ is said to be a *regular function on* $D(f)$.

Proof: First note that a maximal ideal $\mathfrak{n}$ in $k[X]_f$ is of the form $\mathfrak{n} = S^{-1}\mathfrak{m}$, where S is the multiplicative set $S := \{1, f, f^2, .., f^m, ..\}$, and $\mathfrak{m}$ is a maximal ideal in $k[X]$ disjoint from S (See Exercise 5.3.6). On the other hand $\mathfrak{m}$ a maximal ideal in $k[X]$ implies $\mathfrak{m} = \mathfrak{m}_x$ for some $x \in X$ by the weak Nullstellensatz (Corollary 5.1.6). Further $S \cap \mathfrak{m} = \phi$ iff $f \notin \mathfrak{m}_x$ iff $f(x) \neq 0$ iff $x \in D(f)$. Thus the maximal spectrum of $k[X]_f$ is precisely:

$$\operatorname{Spm} k[X]_f = \{\mathfrak{n} : \mathfrak{n} = S^{-1}\mathfrak{m}_x : x \in D(f)\}$$

Finally, for $x \in D(f)$, since $S = \{1, f, f^2, ..\} \subset k[X] \setminus \mathfrak{m}_x$, it also follows easily that for $x \in D(f)$ and $\mathfrak{n} = S^{-1}\mathfrak{m}_x \in \operatorname{Spm} k[X]_f$:

$$(k[X]_f)_{\mathfrak{n}} = \left(S^{-1}k[X]\right)_{S^{-1}\mathfrak{m}_x} = k[X]_{\mathfrak{m}_x} = \mathcal{O}_{X,x}$$

Now we apply the second equality of the Proposition 6.4.19 to the domain $A = k[X]_f$ (whose quotient field is the same as that of $k[X]$, viz. $k(X)$) to conclude that:

$$k[X]_f = \cap_{\mathfrak{n} \in \operatorname{Spm} k[X]_f} (k[X]_f)_{\mathfrak{n}} = \cap_{x \in D(f)} \mathcal{O}_{X,x}$$

which proves our proposition. (Note that the proof of the last statement of Proposition 6.4.18 is just a special case of this proof by setting $f = 1$). □

Corollary 6.5.10. Let $U \subset X$ be open, with X irreducible as above. Then the subalgebra $k[U] \subset k(X)$ of rational functions which are regular on U (i.e. at each point of U) can be described as the intersection:

$$\cap_{i=1}^{n} k[X]_{f_i}$$

where $U = D(f_1) \cup D(f_2) ... \cup D(f_n)$ is an expression for U as a union of finitely many basic open sets (see Proposition 6.4.18). By the proposition above, the subalgebra $k[U]$ consists of all functions in $k(X)$ which are regular at each point $x \in U$, and in particular, the expression above for $k[U]$ holds for *every* expression of U as a union of principal opens $D(f_i)$.

Proof: Clear from the foregoing proposition. □

Exercise 6.5.11. Let X be an affine algebraic set with an irredundant decomposition $X = \cup_{i=1}^{m} X_i$ into irreducible affine closed sets. Let $x \in X_i \setminus (\cup_{j \neq i} X_j)$. Then show that the natural (restriction) homomorphism:

$$\mathcal{O}_{X,x} \to \mathcal{O}_{X_i,x}$$

is an isomorphism. That is, the local ring at a point x lying in a unique irreducible component X_i "sees" only that irreducible component. (*Hint:* Surjectivity of this homomorphism is easy. For injectivity, one needs to construct a regular function which does not vanish at x, and vanishes identically on all X_j for $j \neq i$, which was the assertion of Exercise 6.4.17.)

Exercise 6.5.12. Consider the plane curve $Z := V(Y^2 - X^2(X-1))$ (called the *cubic node*).

(i): Show that Z is irreducible and hence $k[Z]$ is a domain.

(ii): Denote the images of X and Y in the coordinate ring $k[Z]$ by x and y respectively. Show that the rational functions $y^2/x \in k(Z)$ and $y^2/x^2 \in k(Z)$ are regular functions on Z.

(iii): Show that the rational function y/x is not a regular function. Show using this fact that $k[Z]$ is not integrally closed, and in particular, not a UFD.

Exercise 6.5.13. Let X be an *irreducible* affine algebraic set. Show that every non-empty open subset $U \subset X$ is Zariski-dense in X.

Exercise 6.5.14. Let X be an irreducible affine algebraic set, and assume that X has a covering by basic open sets, viz., $X = \cup_{i=1}^{n} D(f_i)$ for some regular functions $f_i \in k[X]$. Show that the intersection:

$$\cap_{i=1}^{n} k[X]_{f_i} = k[X]$$

where $k[X]_{f_i}$ denotes the localisation of $k[X]$ at the multiplicative set $\{1, f_i, f_i^2, ..., \}$, and the intersection above is taken in the function field $k(X)$ of X. Conclude that if a rational function $f \in k(X)$ is regular on each $D(f_i)$, then it is a regular function on X.

6.6. **Affine Algebraic Varieties.** Let X be an irreducible affine algebraic set, with the coordinate ring $k[X]$. In the Corollary 6.5.10 of the last subsection, we have seen how to define the ring $k[U]$ of functions regular on U as a subring of the function field $k(X)$. These regular functions on open sets U have the following property:

Proposition 6.6.1 (The sheaf of regular functions)**.** Let $X \subset \mathbb{A}^n(k)$ be an *irreducible* affine algebraic set. For each Zariski open subset $U \subset X$, we define $\mathcal{O}(U) = k[U]$. We set $\mathcal{O}(\phi) = \{0\}$. Then:

(i): For each open subset $U \subset X$, and each $x \in U$ there is a natural k-algebra homomorphism:

$$\begin{aligned} \rho_{U,x} : \mathcal{O}(U) &\to \mathcal{O}_{X,x} \\ f &\mapsto f_x \end{aligned}$$

mapping a function to its *germ* at x.

(ii): For $U \subset X$ an open set, and a regular function $f \in \mathcal{O}(U)$, $f = 0$ iff $\rho_{U,x}(f) = 0$ for each $x \in U$. That is, a function regular on an open set U is uniquely determined by its germ at each point.

(iii): For each pair of Zariski open subsets $V \subset U$ of X are natural (*restriction*) ring homomorphisms:

$$\begin{aligned} \rho_{U,V} : \mathcal{O}(U) &\to \mathcal{O}(V) \\ f &\mapsto f_{|V} \end{aligned}$$

mapping f to its restriction. These satisfy the compatibility conditions:

(a): For all opens $W \subset V \subset U$, we have $\rho_{V,W} \circ \rho_{U,V} = \rho_{U,W}$. The homomorphism $\rho_{U,U} : \mathcal{O}(U) \to \mathcal{O}(U)$ is the identity map.

(b): For any $x \in V \subset U$, U, V open subsets of X, $\rho_{V,x} \circ \rho_{U,V} = \rho_{U,x}$.

(c): (*Patching of functions*) If $G \in \mathcal{O}(U)$ and $H \in \mathcal{O}(V)$ are functions satisfying $\rho_{U,U\cap V}(G) = \rho_{V,U\cap V}(H)$, then there exists a unique $F \in \mathcal{O}(U \cup V)$ such that $\rho_{U\cup V,U}(F) = G$ and $\rho_{U\cup V,V}(F) = H$.

Proof: Since $\mathcal{O}(U) = \cap_{x\in U}\mathcal{O}_{X,x}$, it follows that there is a natural inclusion:

$$\mathcal{O}(U) \hookrightarrow \mathcal{O}_{X,x}$$

which is precisely the homomorphism $\rho_{U,x}$. This gives (i).

(ii) is now trivial, since all the maps $\rho_{X,x}$ are inclusions. Indeed, it is worth remarking that if $f \in \mathcal{O}(U)$, and $\rho_{U,x}f = 0$ for *any single* $x \in U$, then $f = 0$ in $\mathcal{O}(U)$, since the map $\rho_{X,x}$ is an inclusion. This seems a bit puzzling, but can be understood as follows. Write $f \in \mathcal{O}(U)$ as $f = g/h \in k(X)$, where g, $h \in k[X]$, and $h \neq 0$. Then $hf = g$ in $\mathcal{O}(U)$, and all the functions $f, g, h \in \mathcal{O}(U)$. Assuming $\rho_{U,x}f = 0$, apply $\rho_{U,x}$ to this equation to obtain that $\rho_{U,x}(g) = 0$, where g also denotes $g_{|U}$. This means $\alpha.g = 0$ in $k[X]$ for some $\alpha \in k[X] \setminus \mathfrak{m}_x$. That is, $\alpha(x) \neq 0$. Hence $X = V(\alpha) \cup V(g)$, with $V(\alpha) \neq X$ since $x \notin V(\alpha)$. The irreducibility of X implies that $X = V(g)$, so that $g \equiv 0$, and hence $f = 0$.

For (iii), let $V \subset U$ be open subsets of X. By the Proposition 6.4.18, we have:

$$\mathcal{O}(U) = \cap_{x\in U}\mathcal{O}_{X,x} \subset \cap_{x\in V}\mathcal{O}_{X,x} = \mathcal{O}(V)$$

and this natural inclusion map is the restriction map $\rho_{U,V}$. The assertion (a) now follows easily, since composites of inclusions are inclusions, and the inclusion of $\mathcal{O}(U)$ into itself is the identity map of $\mathcal{O}(U)$.

Part (b) is also trivial, since all maps concerned are inclusions. To see the patching condition (c), we first note that by expressing V as a finite union of basic opens, it boils down to proving it for $V = D(g) \neq \phi$, $U \neq \phi$ arbitrary. So suppose we have $U = \cup_{i=1}^{m} D(g_i)$, and $V = D(g)$. Note that since X is irreducible, $U \neq \phi$ implies U is dense in X (by Exercise 6.5.13), as is $D(g)$, if it is non-empty. Consequently, $U \cap D(g)$ is non-empty.

Let $G \in \mathcal{O}(U)$, so that $G = f_i/g_i^r$ for each i. (We may choose the largest r among the exponents of all denominators, and make a common exponent for the denominators.) Also let $H = f/g^r \in \mathcal{O}(D(g)) = k[X]_g$. The fact that $\rho_{U,U\cap D(g)}(G) = \rho_{D(g),U\cap D(g)}(H)$ implies that applying $\rho_{U\cap D(g),x}$ to both sides produces the same germ. By the part (b), this implies that $H_x = G_x$ for all $x \in U \cap D(g)$. This means that for each $x \in U \cap D(g)$ the following equations hold in $k[X]$:

$$h_x(f_i g^r - f\, g_i^r) = 0$$

for some $h_x \in k[X] \setminus \mathfrak{m}_x$, and each $i = 1, 2, .., m$. Since $h_x \notin \mathfrak{m}_x$, we have $h_x(x) \neq 0$, and since $k[X]$ is a domain by the irreducibility of X, we have:

$$f_i(x)g^r(x) - f(x)\, g_i^r(x) = 0 \quad 1 \leq i \leq m, \quad x \in U \cap D(g)$$

Since $U \cap D(g)$ is non-empty and open, it is Zariski dense in X (by Exercise 6.5.13), and so it follows that:

$$f_i(x)g^r(x) = f(x)\, g_i^r(x) \quad 1 \leq i \leq m \quad \text{for all } \ x \in X$$

Again this implies that for each i, the regular function $f_i g^r - f g_i^r \in \cap_{x\in X}\mathfrak{m}_x = \{0\}$. Thus, in $k(X)$, we have the identity:

$$\frac{f_1}{g_1^r} = ... = \frac{f_i}{g_i^r} = ... = \frac{f}{g^r}$$

If we call this rational function F, we have that $F = G$ on U and $F = H$ on $D(g)$, and hence F is regular at each point of $U \cup D(g)$. It is therefore the required regular function in $\mathcal{O}(U \cup D(g))$. The uniqueness of F follows by (ii) above. This proves the proposition. □

Definition 6.6.2. Let X be a topological space. A *sheaf of rings* $\mathcal{F}$ on X is an association of a ring $\mathcal{F}(U)$ to each open set $U \subset X$. For every pair of opens $V \subset U$, there is the restriction map $\rho_{UV} : \mathcal{F}(U) \to \mathcal{F}(V)$ which is a ring homomorphism. Furthermore, these restriction homomorphisms are required to satisfy (a) and (c) of (iii) in Proposition 6.6.1. Likewise, one may define sheaves of abelian groups, k-algebras, k-vector spaces etc. The *stalk* of the sheaf $\mathcal{F}$ at a point $x \in X$, denoted $\mathcal{F}_x$ is defined as:

$$\mathcal{F}_x = \lim_{\to} \mathcal{F}(U)$$

where the direct limit is taken over the directed set of neighbourhoods $\mathcal{U}(x)$ of x ordered by $U < V$ if $U \supset V$, and the maps of the direct system being the restriction maps ρ_{UV}. (For more on these matters, the reader may consult a book on Sheaf Theory, or Hartshorne's *Algebraic Geometry*).

The sheaf on an irreducible affine algebraic set X defined above in Proposition 6.6.1 is called the *structure sheaf of* X, and denoted $\mathcal{O}_X$, or simply $\mathcal{O}$, if no confusion is likely.

Exercise 6.6.3 (Sheaf of continuous functions)**.** The reader may similarly construct, for a topological space X, the *structure sheaf of continuous functions on* X. For $U \subset X$ open $\mathcal{O}(U)$ is defined as the ring of continuous functions on the set U, and the local ring $\mathcal{O}_{X,x}$ is the *ring of germs of continuous functions at* x. It consists of equivalence classes $\langle f, U\rangle$, where U is an open neighbourhood of x, and the equivalence relation is given by $\langle f, U\rangle = \langle g, V\rangle$ iff there exists a $W \subset U \cap V$ such that $f_{|W} = g_{|W}$. It is precisely the localisation of $\mathcal{O}(X) = C(X)$ at the maximal ideal $\mathfrak{m}_x = \{f : f(x) = 0\}$, and is therefore a local ring. The maps $\rho_{U,V}$ are defined by restriction, and $\rho_{U,x}$ is the map taking a function f continuous on U to the germ $\langle f, U\rangle$. All the assertions above are easily checked in this situation by usual facts about patching of continuous functions etc. The reader may similarly construct the sheaf of smooth functions on a smooth (differentiable) manifold X.

Definition 6.6.4 (Affine algebraic varieties)**.** A topological space X, together with a sheaf of rings $\mathcal{F}_X$, such that each *stalk* $\mathcal{F}_{X,x}$ is a local ring, is called a *locally ringed space*. A locally ringed space $(X, \mathcal{F}_X)$ is called an *affine algebraic variety over* k if there is an irreducible affine algebraic set Y, and a homeomorphism $h : X \to Y$, and an isomorphism h^* of $\mathcal{F}_X$ with the natural structure sheaf of k-algebras $\mathcal{O}_Y$ of Y defined in the Proposition 6.6.1 above. That is, for each $U \subset X$ open, there should be an isomorphism of rings $h^*_U : \mathcal{F}_X(U) \simeq \mathcal{O}_Y(h(U))$, compatible with all the restrictions $\rho_{U,V}$ on both sides.

The reason for doing all this is to free the definition of an affine algebraic set from the ambient affine space it sits inside. The important object attached to an affine variety is the structure sheaf, which determines it completely. The ambient affine space is not important.

Exercise 6.6.5. Show that a basic open set $D(f)$ of an irreducible affine algebraic set X is an affine algebraic variety. (In fact, if $X \subset \mathbb{A}^n(k)$, then one can make $D(f)$ isomorphic to a closed subset $Y \subset \mathbb{A}^{n+1}(k)$. That is, there is a bijection between $h : D(f) \to Y$, which is a homeomorphism of Zariski topologies, and such that for any open set $W \subset D(f)$ and its image $h(W) \subset Y$, the rings of regular functions $\mathcal{O}_X(W)$ and $\mathcal{O}_Y(h(W))$ are isomorphic as k-algebras. (*Hint:* See part (iii) of the Exercise 5.3.12.)

In particular, by viewing the group $\mathrm{GL}(n, k)$ as the principal open set $D(\det)$ inside the affine space $M(n, k) = \mathbb{A}^{n^2}(k)$, we have that $\mathrm{GL}(n, k)$ is an affine algebraic variety.

Remark 6.6.6 (Open subsets of affines need not be affine)**.** There are open subsets of affine varieties which are not affine. For example, the open set $U := \mathbb{A}^2(k) \setminus \{(0, 0)\}$ (or for that matter the complement of the origin in $\mathbb{A}^n(k)$ for all $n \geq 2$) are not isomorphic to any affine algebraic set. The reason is as follows. Let $X = \mathbb{A}^2(k)$. We first claim that $\mathcal{O}_X(U) = k[X, Y]$. Let $V := D(X)$ and $W := D(Y)$ be the principal open subsets of $\mathbb{A}^2(k)$ defined by the coordinate functions. Clearly $U = V \cup W$. By our earlier generalities, $\mathcal{O}_X(U) \subset \mathcal{O}_X(V) \cap \mathcal{O}_X(W)$. If $r \in k(X)$ is in $\mathcal{O}_X(U)$, it follows, since $\mathcal{O}_X(V) = k[X, Y]_X$ and $\mathcal{O}_X(W) = k[X, Y]_Y$, that $r = X^{-m} f(X, Y)$ on $D(X)$ and $r = Y^{-n} g(X, Y)$ on $D(Y)$. Thus at each point of $V \cap W = D(XY)$, we have:

$$Y^n f(X, Y) = X^m g(X, Y)$$

Again, both sides are regular functions on all of $X = \mathbb{A}^2(k)$, and $D(XY)$ is non-empty, open and hence Zariski dense in the irreducible X, so the above equality holds on all of $\mathbb{A}^2(k)$, i.e. is an equality in $k[X,Y]$. Since $k[X,Y]$ is a UFD, and X and Y are irreducible, we have that Y^n divides $g(X,Y)$ and X^m divides $f(X,Y)$. Thus $r = X^{-m}f(X,Y) = Y^{-n}g(X,Y)$ is a polynomial in X,Y, viz., an element in $k[X,Y]$. The claim follows.

We already know that for an affine algebraic set X, points of X are in 1-1 correspondence with maximal ideals by the Corollary 5.1.6 of the Weak Nullstellensatz. Now if the open set U above were an affine variety, the maximal ideal $\mathfrak{n} := \langle X, Y\rangle$ in $k[U] = k[X,Y]$ would correspond to (functions vanishing at) some point $(a,b) \in U$. But for $p = (a,b) \in U$, the maximal ideal $\mathfrak{m}_p$ corresponding to p is $\langle X - a, Y - b\rangle$, which is not $\mathfrak{n}$ for any $p \in U$.

6.7. **Birational Equivalence.**

Definition 6.7.1. Closed irreducible algebraic sets whose function fields are k-isomorphic (i.e. as field extensions of k) are said to be *birationally equivalent*. Clearly algebraic varieties which are isomorphic are birationally equivalent. But birational equivalence is much weaker than isomorphism, as the following example shows.

Example 6.7.2 (The cubic cusp)**.** Consider $Y := V(Y^2 - X^3) \subset \mathbb{A}^2(k)$, and $X = \mathbb{A}^1(k)$. We have the natural map:

$$\begin{aligned} \phi : X &\to Y \\ t &\mapsto (t^2, t^3) \end{aligned}$$

The corresponding homomorphism between coordinate rings is:

$$\begin{aligned} \phi^* : k[Y] = \frac{k[X,Y]}{\langle Y^2 - X^3 \rangle} &\to k[X] = k[T] \\ x &\mapsto T^2 \\ y &\mapsto T^3 \end{aligned}$$

where x and y are the images of X and Y in the quotient ring on the left. The map between the function fields $k(Y) \to k(X)$ induced by ϕ^* is an isomorphism, with inverse map $t \mapsto \frac{y}{x}$. However, $\phi^* : k[Y] \to k[X]$ is not an isomorphism, as was noted in Exercise 5.3.22 (the reader can check that y/x is integral over $k[Y]$, but not in it, so $k[Y]$ is not a normal domain). So there can be no k-algebra isomorphism between these rings.

We shall see more examples in the next section on plane algebraic curves. However, we can assert the following:

Proposition 6.7.3. Let X and Y be two irreducible affine algebraic sets which are birationally isomorphic. Then there exist non-empty Zariski open (and hence Zariski dense) subsets $U \subset X$ and $V \subset Y$ such that the rings of regular functions $\mathcal{O}_X(U)$ and $\mathcal{O}_Y(V)$ are isomorphic. In fact, if we restrict the structure sheaves $\mathcal{O}_X$ (resp. $\mathcal{O}_Y$) to U (resp. V) and call them $\mathcal{O}_U$ (resp. $\mathcal{O}_V$), then $(U, \mathcal{O}_U)$ is isomorphic to $(V, \mathcal{O}_V)$ as a locally ringed space.

Proof: Let $k[X]$ be generated as a k-algebra by some regular functions $x_1, .., x_m$ (e.g. coordinate functions, if $X \subset \mathbb{A}^m(k)$), and $k[Y]$ by the regular functions $y_1, .., y_n$. If $\theta : k(Y) \to k(X)$ is an isomorphism, we may write:

$$\theta(y_i) = \frac{f_i(x_1, ..., x_m)}{g_i(x_1, .., x_m)}, \qquad 1 \leq i \leq n$$

and also

$$\theta^{-1}(x_j) = \frac{p_j(y_1, ..., y_n)}{q_j(y_1, .., y_n)}, \qquad 1 \leq j \leq m$$

where $f_i, g_i \in k[X]$ and $p_j, q_j \in k[Y]$ are some regular functions.

Let

$$U_1 = (\cap_{i=1}^n D(f_i g_i)) = (\cap_{i=1}^n D(g_i)) \cap (\cap_{i=1}^n D(f_i))$$

Then θ maps y_i, and hence $k[Y]$ into $\mathcal{O}_X(U_1)$. In particular, $\theta(p_j)$ and $\theta(q_j) \in \mathcal{O}_X(U_1)$ for each $j = 1, .., m$. Now

$$\begin{aligned} \theta(p_j) &= p_j(\theta(y_1), .., \theta(y_n)) = p_j(f_1/g_1, .., f_n/g_n) \\ &= \frac{P_j(x_1, .., x_m)}{g^I} \end{aligned}$$

where $I = (i_1, .., i_n)$ is some multiindex, and g^I denotes the monomial $g_1^{i_1} ... g_n^{i_n}$. Similarly,

$$\theta(q_j) = \frac{Q_j(x_1, .., x_m)}{g^I}$$

(Note that we can choose a common denominator g^I for all the $\theta(p_j)$'s and $\theta(q_j)$'s, by taking the largest of the exponents for each g_i occurring in all of these expressions, and multiplying and dividing by a suitable positive power of g_i) Now let U be the open set $U_1 \cap (\cap_j D(P_j Q_j))$. Then, we have the following:

(i): For each $j = 1, .., m$, the rational functions P_j and Q_j are regular functions on U, not vanishing anywhere on U. Hence they are invertible elements of $\mathcal{O}_X(U)$.

(ii): For each $i = 1, .., n$, the functions $f_i(x_1, .., x_m)$ and $g_i(x_1, .., x_m)$ are regular and everywhere non-vanishing on U. Thus they are also invertible elements of $\mathcal{O}_X(U)$.

By repeating the above mutatis mutandis for θ^{-1}, and defining V_1 and V analogously, we obtain that

$$\theta^{-1}(f_i) = \frac{F_i(y_1,..,y_n)}{q^J};\ \ \theta^{-1}(g_i) = \frac{G_i(y_1,..,y_n)}{q^J}$$

Furthermore,

(iii): For each $i = 1,..,n$, the functions F_i and G_i are regular functions on V, not vanishing anywhere on V. Hence they are invertible elements of $\mathcal{O}_Y(V)$.

(iv): For each $j = 1,..,m$, the functions $p_j(y_1,..,y_n)$ and $q_j(y_1,..,y_n)$ are regular and everywhere non-vanishing on V. Thus they are also invertible elements of $\mathcal{O}_Y(V)$.

By definition of U, $g_i^{-1} \in \mathcal{O}_X(U)$, and thus θ maps $k[Y]$ into $\mathcal{O}_X(U)$. Now $\mathcal{O}_Y(V)$ is the localisation of $k[Y]$ at the multiplicative set generated by

$$S_Y = \{p_j, q_j, F_i, G_i\}_{1\leq i\leq n;\ 1\leq j\leq m}.$$

Now $\theta(p_j) = \frac{P_j}{g^I}$ and $\theta(q_j) = \frac{Q_j}{g^I}$, and we have P_j, Q_j and g_j invertible elements of $\mathcal{O}_X(U)$, by (i) and (ii) above. Hence $\theta(p_j)$ and $\theta(q_j)$ are invertible in $\mathcal{O}_X(U)$. Also note that $F_i = q^J\theta^{-1}(f_i)$ implies $\theta(F_i) = \theta(q^J)f_i$, and since $\theta(q_j)$ is invertible in $\mathcal{O}_X(U)$ for each j (by the last line), and f_i are invertible in $\mathcal{O}_X(U)$ by (ii) above, it follows that $\theta(F_i)$ is invertible in $\mathcal{O}_X(U)$ for each i. Similarly, $\theta(G_i)$ is invertible in $\mathcal{O}_X(U)$ for each i.

By the universal property of localisations (see Proposition 5.3.11, (i)), we have that θ defines a map $\mathcal{O}_Y(V) \to \mathcal{O}_X(U)$. Interchanging the roles of θ and θ^{-1}, U and V, X and Y, and using (iii) and (iv) above, we similarly obtain that θ^{-1} maps $\mathcal{O}_X(U)$ into $\mathcal{O}_Y(V)$. Since θ and θ^{-1} are inverses of each other all over the respective function fields, the maps θ and θ^{-1} above give an isomomorphism of $\mathcal{O}_X(U)$ with $\mathcal{O}_Y(V)$ and the proposition is proved. □

Definition 6.7.4. An affine algebraic variety X is said to be *rational* if it is birationally equivalent to affine n-space $\mathbb{A}^n(k)$, for some n. That is, its function field $k(X)$ is isomorphic to the field $k(x_1,..,x_n)$ of rational functions in n-variables. We saw in the Example 6.7.2 that the cusp is a rational curve. In the next section, we will encounter some non-rational varieties.

We close with some additional exercises on this section.

Exercise 6.7.5. Let X be an irreducible algebraic set. Define the system of neighbourhoods of x by

$$\mathcal{U}(x) = \{U \subset X :\ U \text{ is open and contains } x\}$$

Show that:

$$\mathcal{O}_{X,x} = \cup_{U\in\mathcal{U}(x)}\mathcal{O}(U)$$

where the union is taken inside the function field $k(X)$ of X. Hence show that if there is a system of ring homomorphisms into a ring R:

$$\{f_U : \mathcal{O}(U) \to R\}_{U\in\mathcal{U}(x)}$$

satisfying $f_V \circ \rho_{UV} = f_U$ for all $U, V \in \mathcal{U}(x)$ with $V \subset U$, then there exists a unique homomorphism $f_x : \mathcal{O}_{X,x} \to R$ satisfying $f_x \circ \rho_{U,x} = \rho_U$ for all $U \in \mathcal{U}(x)$. (This universal property, by the way, is the definition of the direct limit, and shows that

$$\mathcal{O}_{X,x} = \varinjlim \mathcal{O}(U)$$

and $\mathcal{O}_{X.x}$ is therefore the stalk of the structure sheaf $\mathcal{O}_X$.)

Exercise 6.7.6. Show that the cubic node $X := V(Y^2 - X^2(X-1)) \subset \mathbb{A}^2(k)$ is birationally equivalent to $\mathbb{A}^1(k)$ (i.e. is a rational curve). Determine the largest Zariski open subsets $U \subset X$ and $V \subset \mathbb{A}^1(k)$ which satisfy $\mathcal{O}_X(U) \simeq \mathcal{O}_{\mathbb{A}^1(k)}(V)$.

Exercise 6.7.7. Show that an irreducible plane conic is a rational curve. (See §1.1. Note that an irreducible plane conic is defined to be $V(f) \subset \mathbb{A}^2(k)$ where $f \in k[X,Y]$ is an irreducible polynomial of degree 2.)

7. A brief detour into plane curves

7.1. **Generalities.** In this section, let $k = \mathbb{C}$, just to be specific, though much of what we say holds good for any algebraically closed field.

Definition 7.1.1. A *plane algebraic curve* is just $V(f)$ for f a polynomial in $k[X, Y]$. We say it is *irreducible* if X is an irreducible algebraic set $\Leftrightarrow$ the ideal $\langle f \rangle$ is prime $\Leftrightarrow$ the polynomial $f(X, Y)$ is irreducible in $k[X, Y]$.

Exercise 7.1.2. Let X be an irreducible plane algebraic curve, and let $k(X)$ denote its function field. Show that the transcendence degree $\text{tr deg}_k k(X) = 1$.

The cases of $\deg f = 1$ (*lines*) and $\deg f = 2$ (*conics*, also called *quadrics*) are easier, and first courses on analytic geometry study these in detail. Among the cubic plane curves, those of particular interest are of the form $V(Y^2 - f(X))$, where f is a cubic polynomial. Later on, we shall be able to classify all planar cubics.

Right now it is useful to look at such curves with $f(X) \in k[X]$ a *general* polynomial, and then specialise to some interesting cases of f a cubic polynomial.

Proposition 7.1.3. Let $f(X) \in k[X]$ be a polynomial. Let Z denote the plane curve $V(Y^2 - f(X))$ in $\mathbb{A}^2(k)$. Then:

(i): f is not a square in $k[X]$, (i.e. there does not exist $g(X) \in k[X]$ such that $f(X) = g(X)^2$), if and only if $\langle Y^2 - f(X) \rangle$ is a prime ideal in $k[X, Y]$. In this event, the curve Z is irreducible, and its coordinate ring is $k[Z] = \frac{k[X,Y]}{\langle Y^2 - f(X) \rangle}$, an integral domain.

(ii): Assume f is not a square in $k[X]$, and thus by (i), $B := k[Z] = \frac{k[X,Y]}{\langle Y^2 - f(X) \rangle}$ is a domain. Then B is integrally closed (in its quotient field) iff f is square free (i.e. all the roots of f occur with multiplicity one).

Proof: We note that $A = k[X]$ is a domain, and since the ideal $\mathfrak{a} := \langle Y^2 - f \rangle$ in $A[Y] = k[X, Y]$ is generated by a degree 2 polynomial in Y, the natural map $A \to A[Y] \to A[Y]/\mathfrak{a}$ is an injective map. That is, the natural map:

$$k[X] \to \frac{k[X, Y]}{\mathfrak{a}}$$

is an inclusion.

Let $B := \frac{k[X,Y]}{\mathfrak{a}}$, and let x (resp. y) denote the images of X (resp. Y) in B. Then $y^2 = f(x)$ in B. If $f(X) = g(X)^2$, then we have $(y - g(x))(y + g(x)) = y^2 - g(x)^2 = y^2 - f(x) = 0$. However, $y + g(x)$ and $y - g(x)$ are $\neq 0$, since $Y - g$ and $Y + g$ are degree 1 polynomials in $A[Y]$, and cannot be divisible by $Y^2 - f$, which is of degree 2. Thus B has zero-divisors, and is not a domain. This proves the "if" part of (i)

For the "only if" part, assume that $f(X)$ is not a square in $A = k[X]$. We claim that every element of B can be *uniquely written* as $\alpha(x) + \beta(x)y$. By writing a polynomial $F(X, Y)$ as $\sum_{i=1}^{s} a_i(X)Y^i$, and noting that $y^2 = f(x)$, one sees that $F(x, y) = \alpha(x) + \beta(x)y$ in B. To see uniqueness, note that $\alpha(x) + \beta(x)y = 0$ would imply that:

$$\beta^2 y^2 = \beta^2(x) f(x) = \alpha^2(x)$$

Since the map $k[X] \to B$ mapping X to x is injective, this implies that $\beta^2(X)f(X) = \alpha^2(X)$ in $A = k[X]$. This means that $\frac{\alpha}{\beta}$ is in $k(X)$, and integral over $k[X]$ (satisfying the monic polynomial $T^2 - f$). Since $A = k[X]$ is a UFD, it is integrally closed in $k(X)$, by the Proposition 4.2.8. Thus $\frac{\alpha(X)}{\beta(X)} = g(X) \in k[X]$, and we have $f(X) = g(X)^2$, contradicting the hypothesis on f.

Now if

$$(\alpha(x) + \beta(x)y)(\gamma(x) + \delta(x)y) = (\alpha(x)\gamma(x) + \beta(x)\delta(x)f(x)) + (\alpha(x)\delta(x) + \beta(x)\gamma(x))y = 0$$

then we have $(\alpha(x)\gamma(x) + \beta(x)\delta(x)f(x)) = 0 = (\alpha(x)\delta(x) + \beta(x)\gamma(x))$. Since $k[X] \to B$ is an inclusion, this shows that the above two relations hold with x replaced by X. Multiplying the first of these equations by $\delta(X)$, and the second one by $\gamma(X)$, we find that $\beta(X)(\delta(X)^2 f - \gamma(X)^2) = 0$ in $k[X]$. If the second factor is 0, then we will have (as in the last paragraph) that $f(X)$ a square in $k[X]$, a contradiction. If the first factor $\beta(X) = 0$, then we will have $\alpha(X)\delta(X) = \alpha(X)\gamma(X) = 0$. Which means that either $\alpha(X) = 0$, or both $\gamma(X)$ and $\delta(X) = 0$, in which case we have either $\alpha(x) + \beta(x)y = 0$ or $\gamma(x) + \delta(x)y = 0$, and thus B is an integral domain. This proves (i)

Assume that f is not a square, and hence B is an integral domain. To see (ii), first assume that $f(X)$ has a repeated root, and by translating the X-variable to $X - \alpha$ if necessary, we may assume that 0 is a repeated root. That is, $f(X) = X^2 g(X)$. Then since $y^2 = f(x) = x^2 g(x)$ in B, we have that the rational function $\frac{y}{x} \in Q(B)$ (the quotient field of B) satisfies the monic polynomial $T^2 - g(X)$ over $k[X]$, and hence is integral over $A = k[X]$. Hence it is integral over B. On the other hand, $\frac{y}{x} \in B$ would imply that there is some polynomial $F(X, Y)$ such that $Y - XF(X, Y)$ is divisible by $Y^2 - f(X)$, which is again impossible by looking at the Y-degree. Thus $\frac{y}{x} \notin B$, and B is not integrally closed. This proves the "if" part of (ii).

Now suppose f is square free. It is easy to see that the quotient field of B is the field $Q(B) = k(x)[y]$, where y satisfies the monic polynomial $y^2 - f(x)$. For some $\alpha(x),\ \beta(x) \in k(x)$, let the element $\alpha(x) + \beta(x)y \in Q(B)$, be an element integral over B. Since B is integral over A, it will follow that this element is also integral over $k[x]$. Now there is an automorphism of $Q(B)$ defined by $x \mapsto x,\quad y \mapsto -y$, which leaves $k(x)$, and hence $k[x]$ fixed. Thus a monic relation for $\alpha(x) + \beta(x)y$ over $k[x]$ would also imply the same monic relation for $\alpha(x) - \beta(x)y$ over $k[x]$. So both $\alpha(x) + \beta(x)y$ and $\alpha(x) - \beta(x)y$ are integral over $k[X]$. Since we are assuming $k = \mathbb{C}$ (or more generally, if k has characteristic $\neq 2$), we have $\alpha(x)$ and $\beta(x)y$ are integral over $k[x]$. Since $k[x]$ is integrally closed, $\alpha(x) \in k[x]$. Furthermore, $\beta(x)y$ integral over $k[x]$ implies $\beta^2(x)y^2 = \beta^2(x)f(x)$ is integral over $k[X]$. Write $\beta(x) = p(x)/q(x)$, with $p(X)$ and $q(X)$ relatively prime. Then we have $p^2(x)f(x)/q^2(x)$ is integral over $k[x]$. Again, by Proposition 4.2.8, this implies that $p^2(X)f(X)/q^2(X)$ is in $k[X]$. Thus $q^2(X)$ divides $p^2(X)f(X)$. If $q(X)$ is not a constant polynomial, a linear factor of $q(X)$ does not divide $p(X)$ since p, q are coprime. Thus this factor, and its square will have to divide f, contradicting that f is square free. This proves the "only if" part, and the proposition follows. □.

7.2. **Some Cubic Plane Curves.**

Notation : 7.2.1. From now on, we shall use lower case letters x, y, z etc. for variables in polynomial rings, and also the same lower case letters for their images in coordinate rings. Upper case X, Y, Z etc. will be used for algebraic sets or varieties.

Example 7.2.2 (The Cubic Cusp)**.** This curve has already been discussed in the Example 6.7.2 above. Here we have $f(x) = x^3$, the most degenerate cubic polynomial with one root of multiplicity 3. By (i) of Proposition 7.1.3 above, since $f(x) = x^3$ is not a square in $k[x]$, the ideal $\langle y^2 - x^3 \rangle$ is a prime ideal in $k[x, y]$, and so the plane curve $X := V(y^2 - x^3)$ is irreducible. Also since x^3 is not square free, the coordinate ring $k[X]$ is not integrally closed (in its quotient field $k(X)$). The proof of (ii) of the proposition above shows that $\frac{y}{x} \in k(X)$ is integral over $k[X]$ (since it satisfies the monic equation $t^2 - x = 0$), but $\frac{y}{x} \notin k[X]$. Recall that by the discussion in the Example 6.7.2, the function field $k(X)$ is isomorphic to that of $\mathbb{A}^1(k)$, i.e. $k(t)$, the field of rational functions in one variable, and thus the cubic cusp is a rational curve.

The reader may check that the map $\phi : \mathbb{A}^1(k) \to X$ defined in Example 6.7.2 is a bijection. In fact, it is therefore a homeomorphism from $\mathbb{A}^1(k)$ to X, because the Zariski topologies on each of these is the cofinite topology. However, it is *not* an isomorphism of curves because, as we saw in Example 6.7.2, and there can be no k-algebra isomorphism between X and $\mathbb{A}^1(k)$ because the coordinate ring $k[X]$ is not a UFD, whereas the coordinate ring of $\mathbb{A}^1(k)$ is a polynomial ring in one variable, and hence a UFD.

Example 7.2.3 (The Cubic Node)**.** This is defined as $X = V(y^2 - x^2(x-1))$ inside $\mathbb{A}^2(k)$. In this situation, the polynomial $f(x) = x^2(x-1)$ is slightly less degenerate, it has one root of multiplicity 2. Again this curve is a rational curve. The morphism ϕ, from $\mathbb{A}^1(k)$ to X defined by the homomorphism:

$$\begin{aligned} \phi : k[X] = \frac{k[x,y]}{\langle y^2 - x^2(x-1)\rangle} &\to k[t] \\ x \mapsto 1 + t^2 \quad ; \quad & y \mapsto t(1+t^2) \end{aligned}$$

Again, for the same reason as in the example of the cusp above, is not an isomorphism. Since $k[X]$ is not integrally closed in its quotient field $k(X)$ by (ii) of the Proposition 7.1.3 (the polynomial $f(x) = x^2(x-1)$ is not square-free), it cannot be isomorphic to the coordinate ring of $\mathbb{A}^1(k)$. Specifically, the rational function $\frac{y}{x}$ becomes integral over $k[X]$ in its quotient field, but does not lie in $k[X]$.

The example of f with all three roots distinct will be studied in the next subsection.

7.3. **Smooth points and singular points.** We begin with an algebraic notion.

Definition 7.3.1. Recall from the Definition 4.2.17 that an integral domain which is integrally closed (=integrally closed in its quotient field) is called a *normal* domain (e.g. UFD's are normal domains, by Proposition 4.2.8). An affine algebraic variety whose coordinate ring is normal is called a *normal variety*.

Example 7.3.2. By (ii) of Proposition 7.1.3, the curve $X = V(y^2 - f(x))$ in $\mathbb{A}^2(k)$ is a normal curve iff f is square free in $k[X]$. As we saw above, the cubic cusp and cubic node are *not* normal varieties. Affine spaces $\mathbb{A}^n(k)$, for all n, are normal varieties, since their (polynomial) coordinate-rings are UFD's and hence normal domains.

We shall soon investigate the geometric manifestation of normality for curves. We begin with a definition which may be familiar from several-variable calculus.

Definition 7.3.3. A point (a,b) on a plane curve X (i.e. $X = V(f)$, where $f(x,y) \in k[x,y]$ is a non-constant polynomial) is said to be a *smooth point* or *regular point* if the vector:

$$\mathrm{grad} f(a,b) := \left(\frac{\partial f}{\partial x}(a,b), \frac{\partial f}{\partial y}(a,b)\right) \neq (0,0)$$

A point $(a,b) \in X$ is called a *singular point* if it is not a smooth point. A plane curve is called *smooth* if every point on it is smooth, and a *singular curve* if it is not a smooth curve.

The definition of a smooth point above corresponds to the geometric notion that at a smooth point (a,b) there is a well-defined tangent line, viz., the space of vectors $(v_1, v_2) \in k^2$ which satisfy : $\frac{\partial f}{\partial x}(a,b)v_1 + \frac{\partial f}{\partial y}(a,b)v_2 = 0$ is a line. It is easily checked that in the last two examples of the cubic cusp and node, that the origin $(0,0)$ is the only singular point. The next proposition is another one that relates this geometric concept of smoothness to a purely algebraic one. We prove it at present only for plane curves, but it is true in much greater generality, as we shall see later.

Proposition 7.3.4. If X is a smooth irreducible plane algebraic curve, then its coordinate ring $k[X]$ is a normal domain.

Before proving this proposition, let us prove a couple of lemmas, which are very useful in general.

Lemma 7.3.5. Let A be an integral domain. Then the following are equivalent:

(i): A is a normal domain.

(ii): $A_{\mathfrak{p}}$ is a normal domain for every prime ideal $\mathfrak{p}$ in A

(iii): $A_{\mathfrak{m}}$ is a normal domain for every maximal ideal $\mathfrak{m}$ in A

Proof: We first remark that the quotient field of any localisation $A_{\mathfrak{p}}$ is just the quotient field of A. Let us call it K.

(i)⇒(ii) Let $y = \frac{a}{b}$ be an element of K which is integral over $A_{\mathfrak{p}}$. Then there is a monic relation:

$$y^n + \frac{a_1}{s_1}y^{n-1} + ...\frac{a_n}{s_n} = 0; \quad a_i \in A, \quad s_i \in A \setminus \mathfrak{p}$$

Multiply this equation by $(s_1 s_2 ... s_n)^n$, to get :

$$(s_1 s_2 ... s_n y)^n + b_1(s_1 s_2 ... s_n y)^{n-1} + ...b_n = 0$$

where $b_i := a_i s_1^i .....s_i^{i-1} ...s_n^i \in A$ for $i = 1, 2, ..n$. This is a monic relation for $s_1 s_2 ... s_n y$ over A, which is integrally closed, so $s_1 s_2 ... s_n y = a$ for some $a \in A$. Thus $y = \frac{a}{s_1 s_2 .. s_n} \in A_{\mathfrak{p}}$ since $s_1 s_2 ... s_n \in A \setminus \mathfrak{p}$. Thus $A_{\mathfrak{p}}$ is integrally closed.

(ii)⇒(iii) clearly, since every maximal ideal is prime.

(iii)⇒(i) Let $y \in K$ be integral over A. Since $A \subset A_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$, we have y is integral over $A_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$. By hypothesis (iii) all these localisations are integrally closed in K, so $y \in A_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$, i.e.,

$$y \in \bigcap_{\mathfrak{m} \in \mathrm{Spm} A} A_{\mathfrak{m}}$$

By the Lemma 6.4.19, we have $y \in A$, and A is integrally closed. This proves the proposition. □

Proposition 7.3.6 (Nakayama's Lemma I)**.** Let $\mathfrak{a} \subset A$ be an ideal, and M a finitely generated A-module. Suppose that $\mathfrak{a}M = M$. Then there exists an $a \in \mathfrak{a}$ such that $1 + a \in \operatorname{Ann} M$.

Proof: Let $\{x_i\}_{i=1}^n$ be a set of generators for M. By hypothesis, for each $i = 1, .., n$, there are elements $a_{ij} \in \mathfrak{a}$ such that

$$x_i = \sum_{j=1}^{n} a_{ij} x_j$$

That is, the matrix $[\delta_{ij} - a_{ij}]$ acts as the zero operator on each x_i, and hence all of M. That is,

$$(I_M - \Lambda)x = 0$$

for all $x \in M$, where $\Lambda = [a_{ij}]$. Multiplying by the adjoint of $I_M - \Lambda$, we have by Cramer's rule in any commutative ring that $\det(I - \Lambda)x = 0$ for all $x \in M$. That is, $\det(I_M - \Lambda) \in \operatorname{Ann} M$. Since A has entries in the ideal $\mathfrak{a}$, it follows that $\det(I_M - \Lambda) = 1 + a$ for some $a \in \mathfrak{a}$. The lemma follows. □.

This has some interesting consequences for local rings.

Corollary 7.3.7 (Nakayama's Lemma II)**.** Let A be a local ring, with unique maximal ideal $\mathfrak{m}$. Then:

(i): If M is a finitely generated A-module with $\mathfrak{m}M = M$, then $M = \{0\}$.

(ii): (Krull's Theorem) If A is a *Noetherian* local ring, then we have:

$$\cap_{n=0}^{\infty} \mathfrak{m}^n = \{0\}$$

(iii): If M is a finitely generated module, and there are elements $\{x_i\}_{i=1}^n$ whose images $\overline{x}_i$ generate $M/\mathfrak{m}M$, then $\{x_i\}_{i=1}^n$ generate M.

Proof: By the Proposition 7.3.6 above, there exists a $a \in \mathfrak{m}$ with $(1+a) \in \operatorname{Ann} M$. But since A is a local ring, $1+a$ is a unit in A. Thus $1 \in \operatorname{Ann} M$, and hence $M = \{0\}$. This proves (i).

If A is Noetherian, the ideal $M := \cap_{n=0}^{\infty} \mathfrak{m}^n$ is a finitely generated A-module. Also, by definition, it follows that $\mathfrak{m}M = M$. By (i) above it is the zero ideal, proving (ii).

Let N be the submodule of M generated by $\{x_i\}_{i=1}^n$, and let $\widetilde{M} := M/N$. Since all the $\overline{x}_i$ generate $M/\mathfrak{m}M$, it follows that $N + \mathfrak{m}M = M$. Hence every element $x \in M$ can be written as $ay+n$, where $a \in \mathfrak{m},\ n \in N,\ y \in M$. That is $\widetilde{M} = \mathfrak{m}\widetilde{M}$. By (i) above, $\widetilde{M} = \{0\}$ and $M = N$. This proves (iii) and the corollary. □

Remark 7.3.8. (i) of the Proposition 7.3.7 above is false if one drops the finite generation assumption on M. For example, if we take $A = k[[X]]$ the power series ring, and $M = A_X$ (the localisation $S^{-1}A$ at the multiplicative set $S = \{1, X, X^2, ..., X^n, ..\}$) which is not finitely generated, then clearly we have $XM = M$ for all $r \geq$. Hence $\mathfrak{m}M = M$ for the unique maximal ideal $\mathfrak{m} = \langle X \rangle \subset A$. However $M \neq 0$.

Now we can prove the Proposition 7.3.4.

Proof of the Proposition 7.3.4:
We shall prove that whenever $\mathfrak{m}$ is a smooth point of X, the local ring $A_{\mathfrak{m}}$ for the coordinate ring $A = k[X]$ is a unique factorisation domain, and hence by Propositions 4.2.8 and (iii) of the Lemma 7.3.5 above, we will be done. In fact, we will show below that $A_{\mathfrak{m}}$ is a PID.

By translating the origin if necessary (which is an automorphism of $\mathbb{A}^2(k)$, i.e. of $k[x,y]$), we may assume that the maximal ideal $\mathfrak{m}$ is the origin $(0,0)$. Let $f(x,y)$ be the irreducible polynomial with $X = V(f)$, so that $A = k[X] = k[x,y]/\langle f \rangle$. We also denote the images of the coordinate functions $x, y \in k[x,y]$ in the integral domain A by x, y respectively. By hypothesis, the point $(0,0)$ lies on X, and is a smooth point on it, so that $f(0,0) = 0$ and at least one of the partial derivatives $f_x(0,0) = \frac{\partial f}{\partial x}(0,0), f_y(0,0) = \frac{\partial f}{\partial y}(0,0)$ are non-zero. To be specific, assume that $f_y(0,0) \neq 0$.

In the expression for $f(x,y)$ in the polynomial ring $k[x,y]$, we can separate out the terms not involving y, and the terms involving y. The first part maybe written as $xg(x)$ (since f has no constant term), and the second one as $-yh(x,y)$ where $h(0,0) \neq 0$, by the fact that $f_y(0,0) \neq 0$. Thus in the polynomial ring $k[x,y]$, $f(x,y) = xg(x) - yh(x,y)$.

In the domain A, since $f(x,y) = 0$, we have:

$$h(x,y)y = xg(x)$$

In the local ring $A_{\mathfrak{m}}$, since $h(0,0) \neq 0$, $h(x,y) \notin \mathfrak{m}$ and is therefore a unit. Multiplying by h^{-1} on both sides of the equation above, we have:

$$y = xr(x,y)$$

where $r(x,y) \in A_{\mathfrak{m}}$. Since x, y generate the maximal ideal corresponding to $(0,0)$ in A, it follows that $\mathfrak{m}A_{\mathfrak{m}}$ is generated by x, y. Since $y = xr(x,y)$, it follows that the unique maximal ideal $\mathfrak{m}A_{\mathfrak{m}}$ is a principal ideal, generated by x. To simplify notation, we will write $\mathfrak{m}$ instead of $\mathfrak{m}A_{\mathfrak{m}}$ for the unique maximal ideal in the local ring $A_{\mathfrak{m}}$

Claim: Every non-zero element $a(x,y) \in A_{\mathfrak{m}}$ can be written uniquely as :

$$a(x,y) = x^k v(x,y)$$

where $v(x,y) \in A_{\mathfrak{m}}$ is a unit. The integer $k \geq 0$ is called the *order of zero* of a.

Proof of the Claim: If $a(x,y)$ is a unit, we have $k = 0$ and $a(x,y) = v(x,y)$, and we are done. If not, then the ideal $\langle a(x,y) \rangle \subset A_{\mathfrak{m}}$ is a proper ideal, and since $A_{\mathfrak{m}}$ has a unique maximal ideal $\mathfrak{m}$, it follows that $\langle a(x,y) \rangle \subset \mathfrak{m}$. Since $\cap_{k=0}^{\infty} \mathfrak{m}^k = \{0\}$ by (ii) of the Corollary 7.3.7, and $a(x,y) \neq 0$ by hypothesis, there is a $k \geq 1$ such that

$$a(x,y) \in \mathfrak{m}^k; \quad a(x,y) \notin \mathfrak{m}^{k+1}$$

Since $\mathfrak{m} = \langle x \rangle$, as we saw above, $\mathfrak{m}^k = \langle x^k \rangle$. $a(x,y) \in \mathfrak{m}^k$ implies $a(x,y) = x^k v(x,y)$, for some $v(x,y) \in A_\mathfrak{m}$. Since $a(x,y) \notin \mathfrak{m}^{k+1}$, it follows that $v(x,y) \notin \mathfrak{m}$. Thus $v(x,y)$ is a unit, since $A_\mathfrak{m}$ is a local ring. This proves the claim. □

To get back to the proof of the proposition, i.e.,that $A_\mathfrak{m}$ is a UFD, we note that every element, by the claim above, is uniquely expressible as $x^k u$ where u is a unit. Thus if $\mathfrak{a}$ is *any ideal*, and since $A_\mathfrak{m}$ is Noetherian (because it is the localisation of a Noetherian ring A), we have $\mathfrak{a} = \langle a_1, .., a_r \rangle$. But each $a_j = x^{k_j} v_j$, where v_j is a unit, so $\mathfrak{a} = \langle x^k \rangle$, where $k = \min_j k_j$. That is, $\mathfrak{a}$ is a principal ideal, and $A_\mathfrak{m}$ is a PID, and hence a UFD by Proposition 2.2.12. This completes the proof of the proposition. □

There is also a converse to the above Proposition 7.3.4. We will need the Lemma 5.3.18 about integral extensions.

Proposition 7.3.9. Let $X \subset \mathbb{A}^2(k)$ be an irreducible plane curve, and let $x = (a,b) \in X$ be a point on X, associated with the maximal ideal $\mathfrak{m} \subset k[X]$. Then if the localisation $k[X]_\mathfrak{m} = \mathcal{O}_{X,x}$ is a normal domain, x is a smooth point on X.

Proof: Let $X = V(f)$, where $f(x,y) \in k[x,y]$ is an irreducible polynomial. We denote the coordinate ring $k[X]$ by A. We may assume, by translating coordinates, that $x = (a,b) = (0,0) \in X$, so that $f(0,0) = 0$, and so f has no constant term. To show that $(0,0)$ is a smooth point, by definition, means to show that $f(x,y)$ has a non-vanishing linear term. That is, in the polynomial ring $k[x,y]$, we have

$$f(x,y) = \alpha x + \beta y + (\text{terms of order} \geq 2)$$

where $(\alpha, \beta) \neq (0,0)$. Now $(\alpha, \beta) = (0,0)$ if and only if $\langle f(x,y) \rangle \subset \mathfrak{n}^2$, where $\mathfrak{n} = \langle x, y \rangle \subset k[x,y]$ denotes the maximal ideal in the polynomial ring $k[x,y]$ corresponding to $(0,0)$. Since $A = k[x,y]/\langle f \rangle$, $\langle f \rangle \subset \mathfrak{n}^2$ implies that the $(k[x,y]/\mathfrak{n})$-module (k-vector space) $\mathfrak{n}/\mathfrak{n}^2$ maps isomorphically into the $A/\mathfrak{m}$-module (k-vector space) $\mathfrak{m}/\mathfrak{m}^2$. But this will imply that the k-vector space $\mathfrak{m}/\mathfrak{m}^2$ is two dimensional. Since $\mathfrak{m}A_\mathfrak{m}$, the maximal ideal in the local ring $A_\mathfrak{m} = \mathcal{O}_{X,x}$, is generated by $x := x/1, y := y/1$ as an $A_\mathfrak{m}$ module, it follows that x and y generate $\mathfrak{m}A_\mathfrak{m}/\mathfrak{m}^2 A_\mathfrak{m}$ as an $A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m} = k$ module, so we have

$$\dim_k \frac{\mathfrak{m}A_\mathfrak{m}}{(\mathfrak{m}A_\mathfrak{m})^2} \leq 2$$

On the other hand, we claim that $\mathfrak{m}/\mathfrak{m}^2$ *injects into* $(\mathfrak{m}A_\mathfrak{m}/\mathfrak{m}^2 A_\mathfrak{m})$. For this, it is enough to prove that $\mathfrak{m} \cap (\mathfrak{m}^2 A_\mathfrak{m}) = \mathfrak{m}^2$.

Denote $\mathfrak{a} := \mathfrak{m} \cap (\mathfrak{m}^2 A_\mathfrak{m})$. Then clearly $\mathfrak{m}^2 \subset \mathfrak{a} \subset \mathfrak{m}$. Since $\mathfrak{a} \supset \mathfrak{m}^2$, we have $\mathfrak{a}A_\mathfrak{m} \supset \mathfrak{m}^2 A_\mathfrak{m}$. Also since $\mathfrak{a} \subset \mathfrak{m}^2 A_\mathfrak{m}$, we have $\mathfrak{a}A_\mathfrak{m} \subset \mathfrak{m}^2 A_\mathfrak{m}$. So $\mathfrak{a}A_\mathfrak{m} = \mathfrak{m}^2 A_\mathfrak{m}$. If we let $S = A \setminus \mathfrak{m}$, since localisation preserves exact sequences, we have $S^{-1}(\mathfrak{a}/\mathfrak{m}^2) = S^{-1}\mathfrak{a}/S^{-1}\mathfrak{m}^2 = \mathfrak{a}A_\mathfrak{m}/\mathfrak{m}^2 A_\mathfrak{m} = 0$. In particular $S \cap \mathrm{Ann}(\mathfrak{a}/\mathfrak{m}^2) \neq \phi$. But since $\mathfrak{m}\mathfrak{a} \subset \mathfrak{m}^2$, we have $\mathfrak{m} \subset \mathrm{Ann}(\mathfrak{a}/\mathfrak{m}^2)$. Since $S = A \setminus \mathfrak{m}$ intersects this annihilator, it follows that the $\mathrm{Ann}(\mathfrak{a}/\mathfrak{m}^2)$ is an ideal strictly containing $\mathfrak{m}$ and is therefore all of A. That is, $\mathfrak{a} = \mathfrak{m}^2$. This proves our claim, and hence we have that $\dim_k \frac{\mathfrak{m}A_\mathfrak{m}}{(\mathfrak{m}A_\mathfrak{m})^2} = 2$ if $(0,0)$ is a singular point of X. This k-vector space $\mathfrak{m}A_\mathfrak{m}/(\mathfrak{m}A_\mathfrak{m})^2$, is called the *Zariski cotangent space* to X at x, and what we have shown above is that at a singular point x of a plane irreducible curve, the Zariski cotangent space is 2-dimensional. Thus it is enough to show the

Claim 0: $A_\mathfrak{m}$ integrally closed implies that

$$\dim_k \frac{\mathfrak{m}A_\mathfrak{m}}{(\mathfrak{m}A_\mathfrak{m})^2} = 1$$

We will prove a sequence of further claims, and the above Claim 0 will follow in the end.

The field k being algebraically closed, is an infinite field, and by applying a linear change of coordinates, we may assume that (see the Noether Normalisation Lemma 4.2.24)

$$k[x] \subset A$$

is an integral extension (Note that x, y are irreducible in $k[x,y]$, so $\langle f \rangle$ is properly contained in $\mathfrak{n} = \langle x, y \rangle$, so A cannot be k! Also $f(x,y) = 0$ shows that y is algebraic over $k(x)$, so that the transcendence degree of the function field $Q(A)$ over k must be equal to that of $k(x)$ over k, i.e. 1.)

Claim 1: Every non-zero prime ideal in A is a maximal ideal.

Since the polynomial ring $k[x]$ is a PID, every non-zero prime ideal in $k[x]$ is maximal. Let $\mathfrak{q}$ be a non-zero prime ideal in A. Since A is a domain and $k[x] \subset A$ is an integral extension, it follows by Lemma 5.3.18 above that $\mathfrak{p} = \mathfrak{q} \cap k[x]$ is a non-zero prime ideal in $k[x]$. Thus $\mathfrak{p}$ is a maximal ideal in $k[x]$, and $k[x]/\mathfrak{p}$ is a field. Now $A/\mathfrak{q}$ is a domain which is an integral extension of this field, and from 4.2.26 it follows that $A/\mathfrak{q}$ is also a field. Hence $\mathfrak{q}$ is a maximal ideal in A.

Claim 2: The only non-zero prime ideal in the local ring $A_{\mathfrak{m}}$ is its unique maximal ideal $\mathfrak{m}A_{\mathfrak{m}}$.

If $\mathfrak{q}$ is a non-zero prime ideal in $A_{\mathfrak{m}}$, then clearly $\mathfrak{q} \subset \mathfrak{m}A_{\mathfrak{m}}$, because the latter is the only maximal ideal in $A_{\mathfrak{m}}$. Then $\mathfrak{p} = \mathfrak{q} \cap A$ is a prime ideal in A. Since there exists $0 \neq a/s \in \mathfrak{q}$, it follows that $a \neq 0$ is in $\mathfrak{p}$, so that $\mathfrak{p}$ is a non-zero prime ideal. By Claim 1 above, $\mathfrak{p}$ is maximal in A. Also $\mathfrak{q} \subset \mathfrak{m}A_{\mathfrak{m}}$ implies that $\mathfrak{p} \subset A \cap \mathfrak{m}A_{\mathfrak{m}} = \mathfrak{m}$. The maximality of $\mathfrak{p}$ implies $\mathfrak{p} = \mathfrak{m}$. Thus $\mathfrak{q} \supset \mathfrak{p}$ implies $\mathfrak{q} \supset \mathfrak{p}A_{\mathfrak{m}} = \mathfrak{m}A_{\mathfrak{m}}$, and hence the Claim 2 follows.

Claim 3: Let R be a Noetherian integral domain which is a local ring, and a normal domain. Assume every non-zero prime ideal of R is maximal (viz R is a "1-dimensional" ring). Then the unique maximal ideal $\mathfrak{n}$ of R is a principal ideal.

Let $a \in \mathfrak{n}$ be any non-zero element. The radical of the proper non-zero ideal $\langle a \rangle$ is the intersection of all prime ideals in R containing $\langle a \rangle$. But by the hypotheses on R, every non-zero prime ideal in R is maximal, and hence equal to $\mathfrak{n}$. Thus we have:

$$\sqrt{\langle a \rangle} = \mathfrak{n}$$

Since R is Noetherian, $\mathfrak{n} = \langle x_1, .., x_m \rangle$, and by the above we must have $x_i^{m_i} \in \langle a \rangle$, for each generator x_i, for some $m_i \geq 1$. From this it follows that $\mathfrak{n}^r \subset \langle a \rangle$, for all $r \geq m(\max_i m_i)$. By Nakayama it easily follows that $\mathfrak{n}^k$ is *strictly* contained in $\mathfrak{n}^{k+1}$ for each k, so there exists an r such that $\mathfrak{n}^r \subset \langle a \rangle$ but $\mathfrak{n}^{r-1} \not\subset \langle a \rangle$. If $r = 1$, we are done, so assume $r \geq 2$. Choose an element $b \in \mathfrak{n}^{r-1} \setminus \langle a \rangle$, and consider the element $x = a/b \in K := Q(R)$. Since $b \notin \langle a \rangle$, $x^{-1} = b/a \notin R$. Since R is integrally closed in K, we have x^{-1} is not integral over R. If $x^{-1}\mathfrak{n} \subset \mathfrak{n}$, then $\mathfrak{n}$ would be a faithful $R[x^{-1}]$ module which is finitely generated as an R-module, and by the characterisation (iv) of Proposition 4.2.11, we would have x^{-1} integral over R, a contradiction to the last line. Thus $x^{-1}\mathfrak{n} \not\subset \mathfrak{n}$. Since $b \in \mathfrak{n}^{r-1}$, it follows that $b\mathfrak{n} \subset \mathfrak{n}^r \subset \langle a \rangle$, so that $x^{-1}\mathfrak{n} = (b/a)\mathfrak{n} \subset R$. Also $x^{-1}\mathfrak{n}$ is obviously an ideal of R, and since it is not contained in $\mathfrak{n}$, must be all of R. So $x^{-1}\mathfrak{n} = R$, implying that $\mathfrak{n} = Rx = \langle x \rangle$, proving our Claim 3 that $\mathfrak{n}$ is a principal ideal.

By Claim 2, our Claim 3 applies to $R = A_{\mathfrak{m}}$, and hence its unique maximal ideal $\mathfrak{m}A_m$ is generated by a single element. The image of this generator in $\mathfrak{m}A_m/(\mathfrak{m}A_m)^2$ generates it over $A_{\mathfrak{m}}/\mathfrak{m}A_m = k$. That is, the Zariski cotangent space is a 1-dimensional k-vector space, and Claim 0, and hence the proposition follow. □

Corollary 7.3.10. An irreducible plane curve is smooth iff its coordinate ring is a normal domain.

Proof: Immediate from 7.3.4, 7.3.9 and 7.3.5 above. □

Remark 7.3.11. In all dimensions it is true that the coordinate ring of a smooth affine variety is a normal domain, viz., that smooth affine varieties are normal varieties. The converse is not true in dimensions ≥ 2. However, it is true in all dimensions that the "singular set" of a normal affine variety X is of codimension ≥ 2 in X, which is why it is empty if dim $X = 1$, i.e. X is a curve.

Corollary 7.3.12. The coordinate ring of a singular irreducible curve is not a UFD.

Proof: If the coordinate ring were a UFD, it would be integrally closed in its quotient field, by the Proposition 4.2.8, and by 7.3.10 above, X would be smooth. □

The next question which one might naturally ask if the coordinate ring $k[X]$ is itself a UFD for a *smooth* irreducible curve. This is not true. Unlike normality of a domain, which is true iff each localisation is a normal

domain, it is possible for a domain not to be a UFD even if all its localisations are UFD's. This is illustrated in the following example:

Example 7.3.13 (An elliptic curve)**.** Define the plane curve $X = V(y^2 - x(x^2-1)) \subset \mathbb{A}^2(k)$. In this example, it is important for k *not to be of characteristic 2*. It is easily checked that this curve is smooth, and that its coordinate ring $k[X]$ is integrally closed because $x(x^2-1)$ is square free, by (ii) of the Proposition 7.1.3.

We assert that the coordinate ring $k[X]$, is not a UFD. The proof is divided into a series of claims.

Let x, y also denote the images of $x, y \in k[x,y]$ in $k[X] = k[x,y]/\langle y^2 - x(x^2-1)\rangle$, so that $y^2 = x(x^2-1)$ in $k[X]$. Note that $x \mapsto x$ and $y \mapsto -y$ defines an involution (=an automorphism of order 2) of the polynomial ring $k[x,y]$ which preserves the polynomial $f(x,y) := y^2 - x(x^2-1)$. Thus, it descends to an involution:

$$\begin{array}{rccc} \sigma : k[X] & \to & k[X] \\ x & \mapsto & x \\ y & \mapsto & -y \end{array}$$

of the coordinate ring $k[X]$.

Claim 1: $k[x]$ is precisely the subalgebra of $k[X]$ fixed by σ.

It is clear that $k[x]$ is fixed by σ. For the converse, note that since $y^2 = x(x^2-1)$, any element $b(x,y)$ of $k[X]$ can be written uniquely as (see the proof of (i) in Proposition 7.1.3 above). $b(x,y) = a_1(x) + ya_2(x)$. If $\sigma(b) = b$, then:

$$b = \frac{1}{2}(b + \sigma(b)) = \frac{1}{2}(a_1(x) + ya_2(x) + a_1(x) - ya_2(x)) = a_1(x)$$

which proves the claim 1 (dividing by 2 requires characteristic of k is $\neq 2$!)

Claim 2: The subalgebra $k[x]$ of $k[X]$ is a polynomial algebra.

The proof of this is contained in the proof of (i) in Proposition 7.1.3.

We define a map $N : k[X] \to k[x]$, called the *norm* by $N(g) = g\sigma(g)$. Clearly $N(gh) = N(g)N(h)$ for all $g, h \in k[C]$. (We verify that $g\sigma(g)$ is fixed by σ, so that by the fact proved above that the fixed set of σ is $k[x]$, we have $N(g) \in k[x]$ for all $g \in k[X]$). Also $N(1) = 1$.

Claim 3: If $N(g) \in k^*$ for some $g(x,y) \in k[X]$, then $g \in k^*$.

Write, as above, $g(x,y) = a_1(x) + ya_2(x) \in k[X]$. Then we have:

$$N(g) = a_1^2 - y^2a_2^2 = a_1^2 - x(x^2-1)a_2^2$$

If this polynomial in x is a scalar $\lambda \neq 0$ in k, then we would have $x(x^2-1)a_2^2 = -\lambda + a_1^2$. If $a_2(x)$ is not the zero polynomial, in view of claim 2 above, the left hand side, and hence the right hand side would be a polynomial of degree $2k+3$, which is absurd, since the right hand side is a polynomial of even degree. Thus $a_2 = 0$, and $g(x,y) = a_1(x)$, and $a_1(x)^2 = \lambda$, and again by claim 2 above, this forces $a_1(x)$ to be a constant polynomial in k^*.

Claim 4: The units in $k[X]$ are precisely the elements of k^*.

Clearly all elements of $k^* = k \setminus \{0\}$ are units. On the other hand, if $gh = 1$ for some $g, h \in k[C]$, then $N(g)N(h) = 1$. But $N(g)$, $N(h) \in k[x]$, which was a polynomial ring, so both $N(g)$ and $N(h)$ are degree 0 polynomials, i.e. scalars, and also non-zero scalars, since their product is 1. This means, by claim 3 above, that g, h are both elements of k, and also non-zero, since their norms are non-zero.

Claim 5: The elements $x, y \in k[X]$ are irreducible.

First note that, by claims 2 and 4, x and y are not units. First we prove that x is irreducible. Suppose $x = gh$, for $g, h \in k[X]$. We have to show that one of g, h is a unit, viz. an element of k^*. $x = gh$ implies $N(x) = x^2 = N(g)N(h)$. Since $N(g), N(h) \in k[x]$, which is a polynomial ring (and therefore a UFD), by claim 2 above, it follows that one of $N(g), N(h)$ is either a unit, or a unit times x. Say it is $N(g)$. Then in the first case, by claim 3 above, g is itself a unit, and we are done. In the second case we would have, on writing $g = a_1 + ya_2$, that $N(g) = \lambda x$ with $\lambda \neq 0$. This implies that $\lambda x - a_1^2 = -x(x^2-1)a_2^2$ in $k[x]$. Again, the left hand side can either be a polynomial of degree 1 or degree $2k$, whereas the right hand side is a polynomial of degree 0 or degree $2m+3$. This is impossible by claim 2. Thus $N(g)$ cannot be λx ($\lambda \neq 0$) for *any* g in $k[X]$. This proves that x is irreducible.

To see that y is irreducible, apply norms to both sides of $y = gh$ to obtain that $N(g)N(h) = -x(x^2-1)$. If one of $N(g), N(h)$ were of degree 0, we would have that the corresponding g or h is a unit, by claim 4, and we are done. Since $-x(x^2-1)$ is a polynomial of degree 3, we may assume that one of $N(g)$, $N(h)$ is of degree one. Say it is $N(g) = a_1^2 - x(x^2-1)a_2^2$ where, as usual, we have written $g(x,y) = a_1(x) + ya_2(x)$. This means $N(g) = \lambda x$, $\lambda(x-1)$, or $\lambda(x+1)$, for some $\lambda \in k$. If $N(g) = \lambda x$, we have $a_1^2 - x(x^2-1)a_2^2$, a polynomial of degree $2k$ or $2k+3$ equal to λx, a polynomial of degree 1. Thus $\lambda = 0$, $a_2 = 0$, and this implies $a_1 = 0$, a contradiction. If $N(g) = \lambda(x-1)$, or $\lambda(x+1)$, the same reasoning applies. This proves that y is irreducible, and the claim.

Claim 6: $k[X]$ is not a UFD.

Since we have $y^2 = x(x^2-1)$ in $k[X]$, we have x divides y^2. If $k[X]$ were a UFD, x being irreducible in $k[X]$, would therefore be prime, and thus divide y. But y is also irreducible by claim 5, so $y = ax$ where a is a unit, and thus an element in k^*. Taking norms, we would have that $-x(x^2-1) = ax^2$, for $a \neq 0$ in k, a relation that is impossible in the polynomial ring $k[x]$ (claim 2). This proves our claim. □

Exercise 7.3.14. Show that $k[X]$ is the integral closure of $k[x]$ inside the quotient field $k(X)$ of $k[X]$.

Remark 7.3.15. Integrally closed domains of dimension 1 (i.e. in which every non-zero prime ideal is maximal) are called *Dedekind domains*. The Propositions 7.3.4 and 7.3.9 above assert that an irreducible plane curve X is smooth iff its coordinate ring $k[X]$ is a Dedekind domain. Dedekind domains also arise as the rings of integers inside algebraic number fields, e.g. $\mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$ inside $\mathbb{Q}(\sqrt{5})$. There is a unique factorisation available for Dedekind domains, viz. that every non-zero *ideal* factorises uniquely into a product of prime ideals. See Cor.9.4 in Chapter 9 of Atiyah-Macdonald's *Introduction to Commutative Algebra* for a proof. So even though the coordinate ring of, say, the elliptic curve $V(y^2 - x(x^2-1))$ is not a UFD, it is pretty close to being a UFD.

Remark 7.3.16. The study of elliptic curves (over various fields k) is a vast and rich area of number theory, algebraic geometry, complex analysis, representation theory, differential equations and differential geometry. Elliptic curves are a meeting ground for nearly all of mathematics! For example, A. Wiles' proof of Fermat's Conjecture is a statement about elliptic curves. It turns out that the projective closure (we will define this later) of an elliptic curve acquires the structure of an abelian group, with the group operation getting defined in purely geometric terms. (Incidentally, the involution σ constructed above in Example 7.3 corresponds to taking the inverse in this group). The connections between this group structure and the geometry of the elliptic curve leads to far-reaching number-theoretic consequences. For more on this topic, see books on elliptic curves, e.g. the ones by Silverman, or Husemoller.

8. Quasiprojective varieties

8.1. **Motivation.** So far, we have only dealt with closed subsets of affine space. For reasons that will emerge in the sequel, it is important to consider "points at infinity" on the same footing as finite points. The reader may have already encountered this in complex analysis, where the completion of $\mathbb{C}$ by adding a point at infinity gives us the Riemann sphere, thus providing a unified way of looking at rational functions, zeros and poles of meromorphic functions, counting them, etc.

To give another reason, suppose one wants to develop a theory of intersections of algebraic sets. Intuitively, it seems clear that if one intersects an irreducible plane curve $C = V(f) \subset \mathbb{A}^2(k)$ defined by a degree d polynomial $f(X,Y)$ with, say, a line $L = V(aX - Y + c)$, then substituting $Y = aX + c$ into $f(X,Y)$ will lead to a degree d polynomial in X, and this polynomial will have d roots (since k is taken to be algebraically closed) counted with multiplicity. Each such solution for X will lead to a unique value of $Y = aX + c$, so we should expect C to intersect L in d points (counted with multiplicity).

Of course, this expectation is belied even in the case of two lines in $\mathbb{A}^2(k)$. The two parallel lines $V(Y)$ and $V(Y + 1)$ in the plane do not intersect at all. The reason is that they meet at "infinity", and we don't see this point in the affine plane. So the trick is to add one new point at infinity for each direction in the plane, and then it turns out that this "completion" of the affine plane is a very interesting object called the projective plane. (Incidentally, if one completes the affine line, since there is only one direction in the affine line, only one point at infinity is attached to k to get the projective line. If $k = \mathbb{C}$, then we get the Riemann sphere as the corresponding projective line.) Now, in this new completed space, the count of d for the number of intersection points of a curve of degree d and a line turns out to be correct, because the intersection points at infinity get accounted for ! In fact, one gets the beautiful theorem of Bezout which says that two distinct irreducible algebraic curves of degrees m and n in the projective plane intersect in mn points (counted with multiplicity).

A fundamental property of projective space (and closed subsets of projective space) that is at the back of many of the beautiful simplications which result is a geometric property called "completeness", which is akin to the property of compactness in topology. It is precisely this completeness that captures the points at infinity. We shall discuss this in a future section.

For yet another illustration, it is hard to understand all the automorphisms of affine space $\mathbb{A}^n(k)$ for $n \geq 2$, which is impossibly huge. Indeed, the famous Jacobian conjecture (yet unsolved) asserts that a regular (polynomial) map of $\mathbb{A}^n(k)$ (for $n \geq 2$) with everywhere non-vanishing jacobian is an isomorphism. In contrast, the only automorphisms of projective space are linear, so it is a very "rigid" space.

The foregoing discussion hopefully motivates the notion of projective space.

8.2. **Closed Subsets of Projective Space.**

Definition 8.2.1. Let k be a field. We look at the space $\mathbb{A}^{n+1}(k) \setminus \{0\}$, and introduce an equivalence relation on it as follows : $(x_0, x_1, .., x_n) \sim (y_0, y_1, .., y_n)$ if there exists a $\lambda \in k^*$ such that $y_i = \lambda x_i$ for all $i = 0, 1, .., n$. This is clearly equivalent to saying that two points in $\mathbb{A}^{n+1}(k) \setminus \{0\}$ are equivalent if they lie on the same 1-dimensional subspace of $\mathbb{A}^{n+1}(k)$ (same line through the origin or "direction"). The quotient space is called *n-dimensional projective space over k*, and denoted $\mathbb{P}^n(k)$, or simply $\mathbb{P}^n$ if the field is understood. A point p on $\mathbb{P}^n(k)$ is denoted by $p = [x_0 : x_1 : .. : x_n]$ which is the equivalence class of $(x_0, x_1, .., x_n)$. It is therefore understood that the x_i (called *homogeneous coordinates*) in the expression $[x_0 : x_1 : .. : x_n]$ for p are (i) not all zero and (ii) well-defined only upto a common non-zero scalar multiplying them all.

More generally, for V a k-vector space, we will write $\mathbb{P}(V)$ for the projective space of V, i.e. the space of all 1- dimensional subspaces of V.

It is sometimes convenient to think of projective space $\mathbb{P}^n(k)$ *schematically* as an n-simplex. The i-th vertex can be thought of as the point $[0 : 0 : .. : 1 : ..0]$ (with 1 at the i-th spot), the $(n-1)$-faces as the various coordinate hyperplanes ($\{X_i = 0\} \simeq \mathbb{P}^{n-1}(k)$), and so on. Their formal combinatorial relations, e.g. the intersections of hyperplanes, etc. are the same. This formal picture should not be pushed too far ! We will see shortly how a Zariski topology gets defined on $\mathbb{P}^n(k)$.

Let $\pi : \mathbb{A}^{n+1}(k) \setminus \{0\} \to \mathbb{P}^n(k)$ be the quotient map. We would like to define the natural "quotient topology" on $\mathbb{P}^n(k)$.

Let us provisionally define a subset $Z \subset \mathbb{P}^n(k)$ to be a closed subset of $\mathbb{P}^n(k)$ iff $\pi^{-1}(Z)$ is a closed subset of $\mathbb{A}^{n+1}(k) \setminus \{0\}$. That is,

$$\pi^{-1}(Z) = (\mathbb{A}^{n+1}(k) \setminus \{0\}) \cap V(\mathfrak{a})$$

for some ideal $\mathfrak{a} \subset k[X_0, ..., X_n]$. We note that $\pi^{-1}(Z) \cup \{0\}$ is a union of lines through the origin in $\mathbb{A}^{n+1}(k)$, so this will impose a condition on the ideal $\mathfrak{a}$, which we describe next.

For every $f \in \mathfrak{a}$ such that f vanishes at $(a_0, ..., a_n) \in \pi^{-1}(Z) \cup \{0\}$, we must have $f(\lambda a_0, ..., \lambda a_n) = 0$ for all $\lambda \in k^*$, since $(\lambda a_0, ..., \lambda a_n)$ also lies in $\pi^{-1}(Z) \cup \{0\}$. If we write $f = \sum_d f_d$, where f_d is the homogeneous degree d part of f, we must have :

$$\sum_d \lambda^d f_d(a_0, ..., a_n) = 0 \text{ for all } \lambda \in k^*$$

If one considers this as a polynomial in λ, it must be the trivial polynomial (since k is algebraically closed, and therefore infinite). That is, $f_d(a_0, ..., a_n) = 0$ for all d.

Thus the condition on $\mathfrak{a}$ is that it contains the *homogeneous components of all its elements.*

Definition 8.2.2. An ideal $\mathfrak{a} \subset k[X_0, ..., X_n]$ is called a *homogeneous* ideal if it contains the homogeneous components of all its elements.

Exercise 8.2.3. Show that an ideal $\mathfrak{a} \subset k[X_0, .., X_n]$ is homogeneous iff it is generated by *some* finite set of homogeneous generators. Prove that the ideal $\langle Y^2 - X^3 \rangle \subset k[X, Y]$ is not a homogeneous ideal in $k[X, Y]$. Show that the ideal $\langle Y^2 - X^3, 3Y^2 + X^3 \rangle \subset k[X, Y]$ is a homogeneous ideal, and write down a set of homogeneous generators. (It is generally not so trivial to decide the homogeneity of an ideal by looking at some set of generators).

Nevertheless we have the following:

Remark 8.2.4. If $\mathfrak{a} \subset k[X_0, .., X_n]$ is a homogeneous ideal generated by r elements, then it is generated by $\leq r$ homogeneous elements. (Note that for $r = 1$, i.e. a principal homogeneous ideal $\mathfrak{a} = \langle f \rangle$, then f must be homogeneous).

Proof: Let $\mathfrak{a} = \langle f_1, .., f_r \rangle$. Clearly the homogeneity of $\mathfrak{a}$ implies that the set of all the homogeneous components of the f_i, namely the finite set:

$$S = \{g : g \text{ is a homogeneous component of some } f_i\}$$

is also a generating set for the ideal $\mathfrak{a}$. Let $\{g_j\}_{j=1}^m$ be any subset of S which is a *minimal* generating set for $\mathfrak{a}$. We claim that $m \leq r$.

For, assume to the contrary that $m > r$. Since both $\{f_i\}_{i=1}^r$ and $\{g_j\}_{j=1}^m$ generate the ideal $\mathfrak{a}$, let us expand:

$$g_j = \sum_{j=1}^{r} A_{ji} f_i \qquad f_i = \sum_{l=1}^{m} B_{il} g_l$$

where $[A_{ji}]$ is an $(m \times r)$ and $[B_{il}]$ an $(r \times m)$ matrix with entries in $k[X_0, .., X_n]$. Thus we get that the $(m \times m)$ matrix : $C = I_m - AB$ (where I_m is the identity matrix of size m) *annihilates every* g_j. That is, $\sum_l C_{jl} g_l = 0$, for all $1 \leq j \leq m$.

Let d_j denote the degree of the homogeneous polynomial g_j and assume, by relabelling if necessary, that $d_j \leq d_k$ for $j \leq k$. For a fixed j, the degree d_k homogeneous component of the relation $\sum_l C_{jl} g_l = 0$ reads as :

$$\sum_{l : d_l = d_k} C_{jl}^{(0)} g_l + \sum_{l : d_l < dk} C_{jl}^{(d_k - d_l)} g_l = 0$$

where $C_{jl}^{(d)}$ denotes the degree d homogeneous component of C_{jl}. If any of the $C_{jl}^{(0)} \in k$ occurring in the first term above were non-zero, we could divide by it, and thus express the corresponding g_l in terms of $\{g_j\}_{j\neq l}$, contradicting the choice of $\{g_j\}_{j=1}^m$ as a minimal set of ideal generators. Thus, $C_{jl}^{(0)} = 0$ for all j and all l such that $d_l = d_k$. Since k is arbitrary, it follows that that $C_{jl}^{(0)} = 0$ for all j and l.

Thus $C_{jl}(0, 0, .., 0) = 0$, and we have the relation of matrices with entries in k:

$$I_m = A(0, 0, .., 0)B(0, 0, .., 0)$$

where $A(0, 0, .., 0)$ is the matrix $[A_{ji}(0, 0, .., 0)]$ and $B(0, 0, .., 0)$ has a similar meaning. Since $m > r$, the rank of B is $\leq r$, and the rank of AB is less or equal to r, whereas I_m has rank $m > r$, a contradiction. Thus $m \leq r$. □

As before, let $V(\mathfrak{a})$ denote the zero set of the homogeneous ideal $\mathfrak{a}$ in $\mathbb{A}^{n+1}(k)$. Now we can finally define the Zariski topology on $\mathbb{P}^n(k)$.

Definition 8.2.5 (Projective Closed Sets)**.** We define a (Zariski) topology on $\mathbb{P}^n(k)$ by declaring its closed subsets, called *projective closed sets*, to be all sets of the form:

$$V_{\mathbb{P}^n(k)}(\mathfrak{a}) := \pi\left[V(\mathfrak{a}) \cap (\mathbb{A}^{n+1}(k) \setminus \{0\})\right]$$

where $\mathfrak{a}$ is a homogeneous ideal in $k[X_0, .., X_n]$. Note that $V_{\mathbb{P}^n(k)}(\langle 0\rangle) = \mathbb{P}^N(k)$, and $V_{\mathbb{P}^n(k)}(\langle 1\rangle) = \phi$.

Clearly we have :

$$V_{\mathbb{P}^n(k)}(\mathfrak{a}) = \{[a_0 : ... : a_n] : \ f(a_0, .., a_n) = 0 \ \forall \ f \in \mathfrak{a}\}$$

As a matter of notational convenience, we will often drop the subscript $\mathbb{P}^n(k)$, and just write the projective closed set in question as $V(\mathfrak{a})$ whenever it is clear from the context whether we are in $\mathbb{A}^{n+1}(k)$ or $\mathbb{P}^n(k)$.

Exercise 8.2.6. Verify that the closed sets defined as above define a topology on $\mathbb{P}^n(k)$.

Note that the maximal ideal $\langle X_0, .., X_n\rangle \subset k[X_0, ..., X_n]$ defines the origin in $\mathbb{A}^{n+1}(k)$. Hence this homogeneous ideal defines the empty set in $\mathbb{P}^n(k)$. Indeed, for any homogeneous ideal $\mathfrak{a}$ whose radical is the maximal ideal $\langle X_0, .., X_n\rangle$, we have $V_{\mathbb{P}^n(k)}(\mathfrak{a}) = \phi$. More precisely, we have the following:

Lemma 8.2.7. Let I_s be the ideal in $k[X_0, ..., X_n]$ generated by all homogeneous polynomials of degree $\geq s$. Then for a proper homogeneous ideal $\mathfrak{a} \subset k[X_0, ..., X_n]$, $V_{\mathbb{P}^n(k)}(\mathfrak{a}) = \phi$ iff $I_s \subset \mathfrak{a}$ for some $s \geq 1$ ($\Leftrightarrow \ \sqrt{\mathfrak{a}} = \langle X_0, .., X_n\rangle = I_1$.)

Proof: If $I_s \subset \mathfrak{a}$ for some $s \geq 1$, then $X_i^s \in \mathfrak{a}$ for each $i = 0, 1, .., n$. Thus the radical $\sqrt{\mathfrak{a}}$ contains the maximal ideal $\langle X_0, .., X_n\rangle$, and since $\mathfrak{a}$ is a proper ideal, $\sqrt{\mathfrak{a}} \neq \langle 1\rangle$. Thus $V(\mathfrak{a}) = \{0\}$ in $\mathbb{A}^{n+1}(k)$, so that $V(\mathfrak{a}) \cap (\mathbb{A}^{n+1}(k) \setminus \{0\}) = \phi$. Hence its image under π, namely $V_{\mathbb{P}^n(k)}(\mathfrak{a}) = \phi$.

On the other hand, if $\phi = V_{\mathbb{P}^n(k)}(\mathfrak{a}) = \pi(V(\mathfrak{a}) \cap (\mathbb{A}^{n+1}(k) \setminus \{0\})$, then $V(\mathfrak{a}) = \phi$ or 0. The former case is ruled out since $\mathfrak{a}$ is a proper ideal. In the latter case of $V(\mathfrak{a}) = \{0\}$, the radical $\sqrt{\mathfrak{a}} = \langle X_0, .., X_n\rangle$. Hence there exists an $m \geq 0$ such that $X_i^m \in \mathfrak{a}$ for all i. Thus if we choose $s = (n + 1)m$, any monomial of degree $\geq s$ will contain a factor of X_i^m for some i and hence lie in $\mathfrak{a}$, so that $I_s \subset \mathfrak{a}$ for this s. □

Thus, we make the following definition:

Definition 8.2.8. We call a homogeneous ideal $\mathfrak{a}$ *redundant* if its radical is the maximal ideal $\langle X_0, ..., X_n\rangle$. In particular, it it is a proper ideal. Equivalently, $\mathfrak{a}$ is redundant if it is a proper ideal containing the ideal I_s for some $s \geq 1$. For example, the ideal $\langle Y^2 - X^3, 3Y^2 + X^3\rangle \subset k[X, Y]$ of the Exercise 8.2.3 above is redundant, for it clearly contains I_4.

Again, given a subset $S \subset \mathbb{P}^n(k)$, one can consider the ideal of all polynomials that vanish identically on $\pi^{-1}(S)$, i.e. what we denoted $\mathfrak{I}(\pi^{-1}(S))$. This is again a homogeneous ideal, by the reasoning given at the beginning of this subsection.

Notation : 8.2.9. By abuse of language denote this homogeneous ideal as $\mathfrak{I}(S)$.

We have the following proposition:

Proposition 8.2.10 (Homogeneous Nullstellensatz)**.** Let k be an algebraically closed field. If $\mathfrak{a}$ is any non-redundant homogeneous ideal in $k[X_0, .., X_n]$, then $\mathfrak{I}(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$. If $S \subset \mathbb{P}^n(k)$, then $V(\mathfrak{I}(S)) = \overline{S}$, the Zariski closure of S in $\mathbb{P}^n(k)$. There is a 1-1 correspondence between closed subsets of $\mathbb{P}^n(k)$ and homogeneous non-redundant radical ideals of $k[X_0, ..., X_n]$. (We note that the homogeneous ideal $\langle 1 \rangle$ is non-redundant by our definition, and defines the empty set.)

Proof:
If $V_{\mathbb{P}^n(k)}(\mathfrak{a})$ is a closed set in $\mathbb{P}^n(k)$, with $\mathfrak{a}$ a homogeneous non-redundant ideal in $k[X_0, .., X_n]$, the ideal $\mathfrak{I}(V_{\mathbb{P}^n(k)}(\mathfrak{a}))$ is the ideal of polynomials $\mathfrak{I}(\pi^{-1}V_{\mathbb{P}^n(k)}(\mathfrak{a}))$, and assuming $V_{\mathbb{P}^n(k)}(\mathfrak{a}) \neq \phi$, any polynomial f vanishing on $\pi^{-1}(V_{\mathbb{P}^n(k)}(\mathfrak{a}))$ has each of its homogeneous components vanishing on it as well. In particular, all the homogeneous components of f are of degree ≥ 1. But every homogeneous polynomial in $k[X_0, .., X_n]$ of degree ≥ 1 vanishes at the origin in $\mathbb{A}^{n+1}(k)$, so

$$\mathfrak{I}(V_{\mathbb{P}^n(k)}(\mathfrak{a})) = \mathfrak{I}(\pi^{-1}V_{\mathbb{P}^n(k)}(\mathfrak{a})) = \mathfrak{I}(\pi^{-1}V_{\mathbb{P}^n(k)}(\mathfrak{a}) \cup \{0\}) = \mathfrak{I}(V(\mathfrak{a}))$$

But by the affine nullstellensatz Proposition 6.1.1, it follows that the right hand ideal $\mathfrak{I}(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$. This proves the first part of the proposition.

The second assertion is straightforward using the definition of the Zariski topology on $\mathbb{P}^n(k)$, and the corresponding fact for $\mathbb{A}^{n+1}(k)$.

For the last assertion, the only thing to be noted is that the radical of a homogeneous ideal in $k[X_0, ..., X_n]$ is also homogeneous. For, let $f = \Sigma_{d \leq m} f_d$ be a polynomial of degree m lying in $\sqrt{\mathfrak{a}}$, where $\mathfrak{a}$ is homogeneous. Then $f^r \in \mathfrak{a}$ for some r. The highest degree homogeneous term in f^r is clearly f_m^r, so by homogeneity of $\mathfrak{a}$, we have $f_m^r \in \mathfrak{a}$ so that $f_m \in \sqrt{\mathfrak{a}}$. Thus $f - f_m \in \sqrt{\mathfrak{a}}$ and is of lower degree. Induction completes the proof. □

Exercise 8.2.11. Prove that a homogeneous ideal $\mathfrak{a} \subset k[X_0, .., X_n]$ is prime iff for every pair of *homogeneous* polynomials F, G such that $FG \in \mathfrak{a}$, and $F \notin \mathfrak{a}$ then $G \in \mathfrak{a}$.

Example 8.2.12 (Quadrics)**.** Let $A = [a_{ij}]$ be any $n \times n$ symmetric matrix with entries in k, and Q_A be the associated quadratic form, viz. $Q_A(\overline{X}) = \Sigma_{i \leq j} a_{ij} X_i X_j$, where $\overline{X} = (X_1, .., X_n) \in \mathbb{A}^n(k)$. The zero-set $V(\langle Q_A \rangle)$ in $\mathbb{P}^{n-1}(k)$ is called a *quadric*. If A is a singular matrix, it is called a *degenerate* quadric, and otherwise a non-degenerate quadric. For example, a very basic such non-degenerate quadric is the Segre variety $V(X_1X_4 - X_2X_3)$ in $\mathbb{P}^3(k)$ and, as we shall see later, is isomorphic to $\mathbb{P}^1(k) \times \mathbb{P}^1(k)$.

Example 8.2.13 (Determinantal Projective Sets)**.** The affine space $gl(n, k)$ of all $n \times n$ matrices with entries in k has the coordinate ring given by the polynomial ring in n^2 variables, which we denote $k[X_{ij}]_{i,j=1}^n$. If we let $\mathfrak{a}_m$ be the homogeneous ideal of $k[X_{ij}]_{i,j=1}^n$ generated by the determinants of all $m \times m$ minors of the matrix $[X_{ij}]$, the projective closed subset $V(\mathfrak{a}_m) \subset \mathbb{P}(gl(n, k))$ consists of all elements

$$[: X_{ij}] := [X_{11} : X_{12} : ... : X_{nn}] \in \mathbb{P}(gl(n, k))$$

which are of rank $\leq (m - 1)$. Homogenous ideals of the type $\mathfrak{a}_m$ are called *determinantal* ideals. Similar examples of closed projective subsets of $\mathbb{P}(\hom(k^n, k^m))$ defined by

$$\{A \in \hom(k^n, k^m) : \text{rk } A \leq p\}$$

can be constructed, by taking the ideal generated by all $(p \times p)$ minors.

If $k = \mathbb{R}$ or $\mathbb{C}$, one can also put the *classical topology* on $\mathbb{P}^n(k)$ by taking the quotient topology of the classical topology on $\mathbb{A}^{n+1}(k) \setminus \{0\}$. As an exercise, the reader may wish to check that $\mathbb{P}^1(\mathbb{C})$ with the classical topology is homeomorphic to the *Riemann sphere* S^2 via the homeomorphism : $[z_0 : z_1] \longmapsto \frac{z_0}{z_1}$ (the point $[1; 0]$ in $\mathbb{P}^1(\mathbb{C})$ maps to the point ∞ in the Riemann sphere.) The inverse of this map is : $z \longmapsto [z : 1]$, with ∞ going to $[1 : 0]$. Another exercise is to check that $\mathbb{P}^1(\mathbb{R})$ with its classical topology is homeomorphic to the circle S^1.

The following is a straightforward remark, whose proof is analogous to the corresponding statements in the affine case, and left as an exercise.

Remark 8.2.14. Define a projective closed subset of $\mathbb{P}^n(k)$ to be *irreducible* if it is not the union of two proper projective closed subsets. Then

(i): A projective closed set $X \subset \mathbb{P}^n(k)$ is irreducible iff $X = V(\mathfrak{p})$ where $\mathfrak{p}$ is a *non-redundant homogeneous prime ideal* of $k[X_0, ..., X_n]$.

(ii): A projective closed set is a Noetherian space, and finally,

(iii): every projective closed set in $\mathbb{P}^n(k)$ is the irredundant union of finitely many irreducible projective closed sets. As a corollary, we obtain that every non-redundant homogeneous radical ideal in $k[X_0, .., X_n]$ is an irredundant intersection of finitely many homogeneous non-redundant prime ideals.

Exercise 8.2.15. Show that two non-empty projective closed sets $V(\mathfrak{a})$ and $V(\mathfrak{b})$ ($\mathfrak{a}$ and $\mathfrak{b}$ homogeneous non-redundant ideals in $k[X_0, .., X_n]$) are disjoint iff $I_s \subset \mathfrak{a} + \mathfrak{b}$ for some $s \geq 1$, i.e. if $\mathfrak{a} + \mathfrak{b}$ is redundant.

The projective space $\mathbb{P}^n(k)$ has an open covering by $n+1$ open sets $\{U_i\}_{i=0}^n$, each of which (with the induced Zariski topology from $\mathbb{P}^n(k)$) is homeomorphic to the affine space $\mathbb{A}^n(k)$ (with its Zariski topology). Indeed, define :

$$U_i = \{[a_0 :, .., : a_n] \in \mathbb{P}^n(k) : a_i \neq 0\}$$

The mappings $[a_0 :, ..., : a_n] \mapsto (\frac{a_0}{a_i}, .., \widehat{\frac{a_i}{a_i}}, .., \frac{a_n}{a_i})$ from U_i to $\mathbb{A}^n(k)$ (where the hat denotes omission) and $(x_1, ..., x_n) \mapsto [x_1 : .. : 1 : .. : x_n]$ (where 1 is inserted at the i-th place) are clearly inverses of each other. For a homogeneous degree d polynomial $F(X_0, .., X_n)$ in $k[X_0, .., X_n]$, the zero set of F intersected with U_i is the set : $\{[a_0 : .... : a_n] : F(a_0, .., a_n) = 0, \ \ a_i \neq 0\}$, which is the same as the set :

$$\{[a_0 : ..., : 1 :, .. : a_n] : F(a_0, ..., 1, ..a_n) = 0\}$$

by factoring out the common non-zero scalar a_i from all the homogeneous coordinates and a_i^d from the homogeneous polynomial F. If we agree to call the polynomial $F(X_0, ..., 1, ...X_n)$ as ${}_iF^D(X_0, ..., \widehat{X_i}, ., X_n)$ the *i-th dehomogenisation* of F, (in general a non-homogeneous polynomial in $k[X_0, ..., \widehat{X_i}, ., X_n]$) then the closed subset $V_{\mathbb{P}^n(k)}(F) \cap U_i$ of U_i maps precisely to the zero set $V({}_iF^D)$ of the non-homogeneous polynomial ${}_iF^D$ in $\mathbb{A}^n(k)$ under the bijection of U_i with $\mathbb{A}^n(k)$ defined above. It is trivial to check that
${}_i(FG)^D = {}_iF_i^D G^D$, ${}_i(F + G)^D =_i F^D +_i G^D$ for homogeneous polynomials F, G.

Conversely, the zero set of a non-homogeneous polynomial $f(X_0, ..., \widehat{X_i}, ., X_n)$ of degree d in $k[X_0, .., \widehat{X_i}, ., X_n]$ goes to the zero set of the degree d homogeneous polynomial $X_i^d f(\frac{X_0}{X_i}, ..., \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, .. \frac{X_n}{X_i})$. This last polynomial is called the *i-th homogenisation* of f, denoted ${}_if^H$ in $k[X_0, .., X_n]$. Since all closed sets are intersections of closed sets defined by single polynomials, (in both $\mathbb{P}^n(k)$, hence U_i, and in $\mathbb{A}^n(k)$), this shows that the maps defined above are homeomorphisms.

In fact, we make the following:

Definition 8.2.16. Let $X = V(\mathfrak{a})$ be a closed subset of affine n-space $\mathbb{A}^n(k)$ defined by the ideal $\mathfrak{a}$. We define the homogeneous ideal $\mathfrak{a}^H$, called the *0-th homogenisation of* $\mathfrak{a}$ to be the ideal generated by the 0-th homogenisations of all polynomials in $\mathfrak{a}$. We define the *projective closure* or *projectivisation* of X in $\mathbb{P}^n(k)$ to be the projective closed set defined by the homogeneous ideal $\mathfrak{a}^H$ in $k[X_0, ..., X_n]$. It is denoted $\widehat{X}$. Similarly, if $X = V(\mathfrak{b})$ is a projective closed set defined by a non-redundant homogeneous ideal $\mathfrak{b} \subset k[X_0, ..., X_n]$, then the ideal $\mathfrak{b}^D$ of $k[X_1, .., X_n]$, called the *0-th dehomogenisation of* $\mathfrak{b}$, is defined as the ideal generated by the 0-th

dehomogenisations of all the homogeneous elements of $\mathfrak{b}$, (which is just the ideal $\{f(1, X_1, .., X_n) : f \in \mathfrak{b}\}$). $V(\mathfrak{b}^D)$ is called the 0-*th affine piece of* X. Similarly, one can define the *i-th affine piece* of X. It is just the intersection of X with U_i viewed as a closed subset of $\mathbb{A}^n(k)$ after making the above identification of U_i with $\mathbb{A}^n(k)$.

Notation : 8.2.17. For a polynomial $f \in k[X_1, .., X_n]$, f^H will always denote the 0-th homogenisation ${}_0f^H$ of f, for notational convenience. Likewise, for $f \in k[X_0, .., X_n]$, f^D will always mean ${}_0f^D \in k[X_1, .., X_n]$.

Exercise 8.2.18. Check that $(fg)^H = (f^H)(g^H)$. What is $(f+g)^H$? If a homogeneous ideal $\mathfrak{a}$ in $k[X_0, .., X_n]$ is generated by the homogeneous polynomials $\{f_i\}_{i=1}^m$, then show that the 0-th dehomogenisation $\mathfrak{a}^D$ inside $k[X_1, .., X_n]$ is generated by $\{f_i^D\}_{i=1}^m$. Verify that for an ideal $\mathfrak{a} \in k[X_1, .., X_n]$, the 0-th homogenisation is given by:

$$\mathfrak{a}^H = \left\{ \sum_{j=1}^m X_0^{k_j} \, f_j^H \, : \, f_j \in \mathfrak{a} \right\}$$

Remark 8.2.19. If an ideal $\mathfrak{b}$ in $k[X_1, .., X_n]$ is generated by $\{f_i\}_{i=1}^m$, the 0-th homogenisation $\mathfrak{b}^H$ in $k[X_0, .., X_n]$ *may not* be generated by $\{f_i^H\}_{i=1}^m$. For example, the ideal $\mathfrak{a} = \langle X_1, X_2 \rangle$ in $k[X_1, X_2]$ is also generated by the elements $f_1 = X_1^2 + X_2$ and $f_2 = X_1$. The 0-th homogenisation $\mathfrak{a}^H$ is the ideal $\langle X_1, X_2 \rangle \subset k[X_0, X_1, X_2]$. On the other hand $f_1^H = X_1^2 + X_2X_0$ and $f_2^H = X_1$. It is easily checked that $X_2 \in \mathfrak{a}^H$ cannot lie in the ideal generated by f_1^H and f_2^H. Hence, in the expression for $\mathfrak{a}^H$ in the last Exercise 8.2.18, one cannot replace "$f_j \in \mathfrak{a}$" by "f_j in a generating set for $\mathfrak{a}$". This is not surprising, since homogenisation behaves badly with respect to addition, as the last exercise reveals.

Here is a lemma about composing the processes of homogenisation and dehomogenisation.

Lemma 8.2.20.

(i): If $f \in k[X_1, ..\widehat{X}_i, .., X_n]$, then ${}_i({}_if^H)^D = f$. For an ideal $\mathfrak{a} \in k[X_1, .., X_n]$, we have $(\mathfrak{a}^H)^D = \mathfrak{a}$.

(ii): If $F(X_0, ..., X_n)$ is a homogeneous polynomial of degree d, then $(X_i^l)_i({}_iF^D)^H = F$ for some $l \geq 0$. In particular, if F is not divisible by X_i, then ${}_i({}_iF^D)^H = F$.

(iii): If $\mathfrak{p}$ is a homogeneous prime ideal not containing X_0, then $(\mathfrak{p}^D)^H = \mathfrak{p}$ (where the homogenisation and dehomogenisation on the left hand side are with respect to X_0).

Proof:
We just do it for $i = 0$. If $f \in k[X_1, ..., X_n]$ is of degree d, then:

$$f^H(X_0, ..., X_n) = X_0^d f\left(\frac{X_1}{X_0}, ..., \frac{X_n}{X_0}\right)$$

Thus $(f^H)^D(X_1, .., X_n) = f^H(1, X_1, ..., X_n) = f(X_1, ..., X_n)$, hence proving the first statement of (i). For the second statement, note that by the Exercise 8.2.18,

$$\mathfrak{a}^H = \left\{ \sum_{j=1}^m X_0^{k_j} \, f_j^H \, : \, f_j \in \mathfrak{a} \right\}$$

Now, by definition,

$$(\mathfrak{a}^H)^D = \langle \{ (\sum_j X_0^{k_j} \, f_j^H)^D : f_j \in \mathfrak{a} \} \rangle = \langle \{ \sum_j (f_j^H)^D : f_j \in \mathfrak{a} \} \rangle = \langle \{ \sum_j f_j : f_j \in \mathfrak{a} \} \rangle = \mathfrak{a}$$

To see (ii), we note that:

$$(F^D)^H(X_0,....,X_n) = X_0^{d-l}(F^D)\left(\frac{X_1}{X_0},..,\frac{X_n}{X_0}\right) = X_0^{d-l}F\left(1,\frac{X_1}{X_0},..,\frac{X_n}{X_0}\right)$$

if d is the homogeneous degree of F and $d-l \leq d$ is the degree of F^D. Multiplying both sides by X_0^l and using the homogeneity of F yields (ii). Clearly, if F is indivisible by X_0, l has to be 0.

To see (iii), let F be a homogeneous polynomial in $\mathfrak{p}$, a homogeneous prime ideal. Then write $F = X_0^d G(X_0,...,X_n)$ where G is homogeneous and indivisible by X_0. Since $\mathfrak{p}$ is prime and does not contain X_0, it follows (by Exercise 8.2.11) that $G \in \mathfrak{p}$. Thus, by (ii) above, $(G^D)^H = G$ belongs to $(\mathfrak{p}^D)^H$. Thus $F = X_0^d G \in (\mathfrak{p}^D)^H$. This shows $\mathfrak{p} \subset (\mathfrak{p}^D)^H$. On the other hand, if F is a homogeneous element of the form $(G^D)^H$ for some homogeneous $G \in \mathfrak{p}$, then for some $l \geq 0$, $X_0^l F = (X_0^l)(G^D)^H = G$, which is in $\mathfrak{p}$. Since X_0 is not in $\mathfrak{p}$, and $\mathfrak{p}$ is prime, we have $F \in \mathfrak{p}$, proving that all the generators of $(\mathfrak{p}^D)^H$ are in $\mathfrak{p}$, and hence $(\mathfrak{p}^D)^H \subset \mathfrak{p}$. This proves (iii), and the lemma. □

Exercise 8.2.21.

(i): Give examples to show that the hypotheses in (ii) and (iii) of the above Lemma 8.2.20 cannot be dropped.

(ii): Let $\mathfrak{p} \subset k[X_0,..,X_n]$ be a homogeneous non-zero prime ideal with $X_0 \notin \mathfrak{p}$. Then $\mathfrak{p}^D$ is also prime.

Some things need to be checked to ensure that the closing up of affine varieties in projective space by homogenisation of the corresponding ideals is a well-behaved operation. More precisely,

Proposition 8.2.22. The following facts are true of projective closures and affine pieces:

(i): The projective closure of an affine closed set is just its Zariski closure in $\mathbb{P}^n(k)$ considered as a subset of $U_0 \subset \mathbb{P}^n(k)$.

(ii): The homogenisation of a prime ideal is prime, so that the projective closures of irreducible affine closed sets are also irreducible.

(iii): The i-th affine piece of an irreducible closed projective set is an irreducible affine closed set.

Proof:

By the homogeneous nullstellensatz Proposition 8.2.10, we have that the Zariski closure of any subset $S \subset \mathbb{P}^n(k)$ is given by $V_{\mathbb{P}^n(k)}(\mathfrak{I}(S))$, where $\mathfrak{I}(S)$ is the homogeneous ideal of polynomials in $k[X_0,...,X_n]$ vanishing identically on S. Thus for an affine closed set $X = V_{\mathbb{A}^n(k)}(\mathfrak{a})$ defined by the radical ideal $\mathfrak{a} \subset k[X_1,..,X_n]$, the Zariski closure of $X \subset U_0 \subset \mathbb{P}^n(k)$ is exactly $V_{\mathbb{P}^n(k)}(\mathfrak{b})$ where :

$$\mathfrak{b} = \langle F(X_0,.,X_n) \text{ homogeneous}: \ F(1,a_1,.,a_n) = 0 \ \forall \ (a_1,.,a_n) \in V_{\mathbb{A}^n(k)}(\mathfrak{a})\}\rangle$$

This last condition on a homogeneous polynomial F is equivalent to saying that F^D vanishes identically on $V_{\mathbb{A}^n(k)}(\mathfrak{a})$, which by the affine nullstellensatz, implies $F^D \in \mathfrak{a}$, since $\mathfrak{a}$ was assumed to be a radical ideal. This implies $(F^D)^H \in \mathfrak{a}^H$. By (ii) of the previous Lemma 8.2.20, $\mathfrak{b} \subset \mathfrak{a}^H$. Thus $V_{\mathbb{P}^n(k)}(\mathfrak{b}) \supset V_{\mathbb{P}^n(k)}(\mathfrak{a}^H)$. This means $\overline{X} \supset \widehat{X}$. On the other hand, since $\widehat{X}$ is Zariski closed and contains X, we have $\overline{X} \subset \widehat{X}$. This proves (i).

To see (ii), let $\mathfrak{p}$ be a prime ideal in $k[X_1,..,X_n]$. By the Exercise 8.2.11, to establish prime-ness of $\mathfrak{p}^H$, it is enough to show that if F and G are *homogeneous polynomials* with $FG \in \mathfrak{p}^H$, then either $F \in \mathfrak{p}^H$ or $G \in \mathfrak{p}^H$. But $FG \in \mathfrak{p}^H$ implies $(FG)^D \in (\mathfrak{p}^H)^D = \mathfrak{p}$, by (i) of the Lemma 8.2.20 above. Since $\mathfrak{p}$ is prime, one of F^D, or $G^D \in \mathfrak{p}$. Say $F^D \in \mathfrak{p}$. Then $(F^D)^H \in \mathfrak{p}^H$. By (ii) of the Lemma 8.2.20 we have that $F = X_0^l(F^D)^H) \in \mathfrak{p}$.

To see (iii), let $\mathfrak{p}$ be a homogeneous prime ideal in $k[X_0,...,X_n]$, and let $X = V(\mathfrak{p})$ be the corresponding irreducible projective closed set. If $X_0 \in \mathfrak{p}$, we have that $V(\mathfrak{p}) \subset V(X_0)$, so that $X \cap U_0 = \phi$, which is clearly

irreducible. So assume $X_0 \notin \mathfrak{p}$. Then by the part (ii) of the Exercise 8.2.21 the dehomogenised ideal $\mathfrak{p}^D$ is prime. Since this last ideal is the ideal defining the 0-th affine piece of X, (iii) follows. This proves the proposition. □

Remark 8.2.23. Note that it is possible for $X \cap U_i$ to be irreducible for each i, and for X to be reducible. For example,

$$X = V(X_0X_1) = \{[1:0], [0:1]\}$$

is a reducible closed subset of $\mathbb{P}^1(k)$, though its intersections with the affine opens U_0 and U_1 are singletons, and irreducible.

Remark 8.2.24. Except for the redundant maximal ideal $\langle X_0, ..., X_n\rangle$, none of the other maximal ideals in $k[X_0, ..., X_n]$ are homogeneous. The maximal ideals among the homogeneous ideals are the ideals whose affine pieces are either empty, or a single point. The maximal ideal defining the point $[a_0 : a_1 : ..1.. : a_n]$ in $\mathbb{P}^n(k)$ is the ideal :

$$\langle \{X_j - a_jX_i : j = 0, 1, ..n;\ j \neq i\}\rangle$$

It can be written somewhat more symmetrically as the ideal generated by the homogeneous elements $X_ja_k - a_jX_k$ with $k \neq j$ both ranging from 0 to n.

8.3. **Maps and Morphisms between Projective Sets.**

Notation : 8.3.1. In the sequel, we shall often call a homogeneous polynomial of degree m an *m-form*. Note that 0-forms are the elements of k. If $P \in k[X_0, ..., X_n]$ is an m-form and $x = [a_0 : a_1 : .. : a_n]$ is a point in $\mathbb{P}^n(k)$, we write $P(x) = 0$ to mean that $P(a_0, .., a_n) = 0$. This condition clearly depends only on x and not on the representative $[a_0 : a_1 : .. : a_n]$ chosen for x. Similarly $P(x) \neq 0$ is well-defined, and means $P(a_0, .., a_n) \neq 0$.

There is a natural grading of the k-algebra $R = k[X_0, .., X_n]$ defined by

$$R_d = \{f \in R : f \text{ is a } d\text{-form}\}$$

Thus $R = \oplus_{d\geq 0}R_d$. Note that R_0 is k, and the redundant maximal ideal $\langle X_0, .., X_n\rangle$ is $\oplus_{d\geq 1}R_d$. Also R_1 generates R as a k-algebra, and for two non-negative integers d, e, we have that

$$R_d.R_e \subset R_{d+e}$$

Clearly an ideal $\mathfrak{a}$ in R is a homogeneous ideal iff $\mathfrak{a} \cap R_d \subset \mathfrak{a}$ for all $d \geq 0$. We denote $\mathfrak{a} \cap R_d$ by $\mathfrak{a}_d$, and so $\mathfrak{a}$ is a homogeneous ideal iff $\mathfrak{a} = \oplus_{d\geq 0}\mathfrak{a}_d$. If $\mathfrak{a}$ is a homogeneous ideal in R, we can form another graded ring, namely $A = R/\mathfrak{a} = \oplus_{d\geq 0}R_d/\mathfrak{a}_d$.

Definition 8.3.2. In the case when $X = V(\mathfrak{p})$ is an irreducible projective closed set, the graded ring:

$$R/\mathfrak{p} = \oplus_{d\geq 0}\, R_d/\mathfrak{p}_d$$

is called the *graded coordinate ring of X*.

This ring is precisely the coordinate ring of the irreducible *affine* closed subset :

$$V_{\mathbb{A}^{n+1}(k)}(\mathfrak{p}) = \pi^{-1}(X) \cup \{0\}$$

of $\mathbb{A}^{n+1}(k)$, where $\pi : \mathbb{A}^{n+1}(k) \setminus \{0\} \to \mathbb{P}^n(k)$ is the quotient map introduced in the beginning.

The unfortunate thing is that, without bringing in line bundles and sections, there is no good elementary interpretation of the graded coordinate ring of an irreducible projective closed set, as there was for a closed irreducible affine set (where the coordinate ring was just the ring of functions on the closed set which were restrictions of polynomials on the ambient affine space). The reason is not hard to see, if f is an m-form in $X_0, ..., X_n$, it will have a well defined value at the point $[a_0 : ... : a_n] \in \mathbb{P}^n(k)$ iff $f(\lambda a_0, ..., \lambda a_n) = f(a_0, ..., a_n)$, for all $\lambda \neq 0$, $\lambda \in k$. But this is only possible if the homogeneous degree of f is zero, (i.e. f is a constant), or $f(a_0, .., a_n) = 0$. Thus, unless f is constant, f does not have a well-defined non-zero value at any point of

$\mathbb{P}^n(k)$. One therefore has to relax the notion of what one means by a "function" on $\mathbb{P}^n(k)$, by allowing it to be undefined at certain points. We recall the analogous situation from complex analysis, where meromorphic functions, for example, were not required to be everywhere defined.

We carry this out next. Denote $R_d/\mathfrak{a}_d$ by A_d, so that $A = \oplus_{d\geq 0} A_d$. If $\mathfrak{a}$ is a proper ideal $\mathfrak{a}_0 = \{0\}$ and so $A_0 = k$. Note that the element 0 is considered to be of degree ∞, since it lies in all the A_d!

Definition 8.3.3. Let $\mathfrak{p}$ be a homogeneous prime ideal in the polynomial ring $R = k[X_0, ..., X_n]$. Consider the graded ring $A = R/\mathfrak{p}$ graded as above. Let S be the multiplicative set defined as $S = (\cup_{d\geq 0} A_d) \setminus \{0\}$. We consider the *homogeneous localisation* of A, namely $S^{-1}A$. Thus we are just inverting all *homogeneous non-zero elements* in A. This can also be made into a graded ring with grading from $\mathbb{Z}$ by defining for $d \in \mathbb{Z}$

$$(S^{-1}A)_d = \left\{ \frac{P(X_0, ..., X_n)}{Q(X_0, ..., X_n)} : \ Q \neq 0, \ P, Q \ \text{ homogeneous}, \ \ \deg P - \deg Q = d \right\}$$

Again, $S^{-1}A = \oplus_{d\in\mathbb{Z}} (S^{-1}A)_d$, and since $\mathfrak{p}$ was assumed to be prime, A is an integral domain and the natural map $A \to S^{-1}A$ is an inclusion which preserves grading. The *ring of rational functions on* the projective closed set $X = V(\mathfrak{p})$ is defined as $(S^{-1}A)_0$, and denoted $k(X)$. It is clearly a k-algebra which is a field, for the inverse of a non-zero element $\frac{P}{Q}$ is $\frac{Q}{P}$.

This field is the closest thing to the field of rational functions on an irreducible closed affine algebraic set defined in Definition 6.5.2. Note that an element $f \in k(X)$ with $f = \frac{P}{Q}$ is a priori undefined on the zero locus of the denominator, so it isn't really a "function" on X. But it is certainly defined on the non-empty Zariski open subset where Q doesn't vanish, which is dense in X, since X is irreducible. Thus every rational function f on an irreducible projective closed set X is defined on a non-empty open (hence dense) subset U of X. For a point $x = [a_0 : a_1 : .. : a_n] \in U$, we can define the value of f at x to be $f(x) = \frac{P(a_0,....,a_n)}{Q(a_0,...,a_n)}$, for since P and Q are homogeneous of the *same degree*, $f(\lambda a_0, .., \lambda a_n) = f(a_0, ..., a_n)$ for $\lambda \neq 0$ in k, as long as $Q(a_0, .., a_n) \neq 0$. Thus it makes sense to define the *value* of f at the point $x = [a_0 : a_1 : .. : a_n]$ of to be $f(a_0, a_1, .., a_n)$ if $Q(a_0, ..., a_n) \neq 0$, for this value is independent of the representative $(a_0, .., a_n)$ chosen for x.

Note that in the above discussion, f *may be* defined at a point x where Q vanishes, because f may have *another representation* with a denominator not vanishing at x (because of quotienting by $\mathfrak{p}$, there are non-trivial relations in A). For instance :

Example 8.3.4. Let $\mathfrak{p} = \langle X_0^2 - X_1X_2 \rangle$ in $k[X_0, X_1, X_2]$, and we denote by x_i the images of the coordinate functions X_i in $A = k[X_0, X_1, X_2]/\mathfrak{p}$, the rational function $f = \frac{x_2}{x_0}$ seems not be defined at the point $x = [0 : 1 : 0] \in X = V(\mathfrak{p}) \subset \mathbb{P}^2(k)$. However, in A, we have the relation $x_0^2 = x_1x_2$, which implies that this rational function is the same as the rational function $\frac{x_0}{x_1}$, which is well-defined (and $= 0$) at the point $x = [0 : 1 : 0]$.

Before we go any further, it helps to have one unified notion which will cover both closed affine algebraic sets and projective closed sets, among other things.

Definition 8.3.5. A *quasiprojective variety* X is an open subset of a projective closed set. An *irreducible quasiprojective variety* is an open subset of an irreducible projective closed set.

Clearly, a projective closed set is a quasiprojective variety. If X is an an affine closed set, it is the open subset $\overline{X} \cap U_0$ of its projective closure $\overline{X}$, and thus a quasiprojective variety. In fact, X is a quasiprojective variety iff it is the difference of two projective closed sets. Note that a non-empty irreducible quasiprojective variety X has to be dense in its projective closure. Indeed, if U is a non-empty open subset of an irreducible (projective or affine) closed set X, then U is Zariski dense in X, otherwise we would have a decomposition $X = \overline{U} \cup (X \setminus U)$ into proper closed subsets.

Example 8.3.6. The complement $\mathbb{A}^n(k) \setminus X$ of any affine algebraic set $X \subset \mathbb{A}^n(k)$ is a quasiprojective variety, because it may be viewed as the difference $\mathbb{P}^n(k) \setminus (\overline{X} \cup V(X_0))$ (where $\overline{X}$ is the projectivisation of $X \subset U_0$) of projective closed sets. Clearly, it is irreducible.

Remark 8.3.7. We recall that the family of (Zariski) closed subsets of $\mathbb{A}^n(k)$ and $\mathbb{P}^n(k)$ are closed under finite unions and arbitrary intersections. Quasiprojectives in $\mathbb{P}^n(k)$ fail on both counts. For example, in $\mathbb{P}^1(k)$, the subsets $A_n = \mathbb{P}^1(k) \setminus \{[1:0], [0:1/n]\}$ are all quasiprojectives. But

$$\cap_{i=1}^n A_n = \mathbb{P}^1(k) \setminus \{[1:0], [0:1], [0:1/2], .., [0:1/n], ...\}$$

and the right hand set cannot be expressed as the difference of two closed subsets of $\mathbb{P}^1(k)$ (verify). Similarly, $A_1 = \mathbb{P}^2(k) \setminus V(X_0X_1) = U_0 \setminus V(X_1) = \mathbb{A}^2(k) \setminus \{X_1\text{-axis}\}$ and $A_2 = [1:0:0]$ are quasiprojectives inside $\mathbb{P}^2(k)$, but their union is not (verify).

Exercise 8.3.8. Show that a quasiprojective variety is irreducible iff it is not the union of two proper closed subsets which are both quasiprojective varieties. Prove that every quasiprojective variety is a Noetherian topological space, and a finite union of irreducible ones. (Just argue with the projective closure, and show that for a quasiprojective variety X, the intersections $Y_i \cap X$ are all non-empty for Y_i an irreducible component of $\overline{X}$, and are precisely the irreducible components of X).

For this reason, we shall work only with irreducible quasiprojective varieties, the generalisations to arbitrary quasiprojective varieties (if any) usually proceeds component by component.

Definition 8.3.9. Let $X \neq \phi$ be an irreducible quasiprojective variety. Define the *field of rational functions* $k(X)$ on X to be $k(\overline{X})$. If $f_i \in k(X)$ for $i = 1, 2, ..m$, we say that the tuple $f = (f_1, ..., f_m)$ is a *rational map* $f : X \to \mathbb{A}^m(k)$. Note that it is *not a map in the usual sense*, for it is only defined on a dense open subset of X.

Definition 8.3.10. A rational function $f \in k(X)$ for X an irreducible quasiprojective variety is said to be *regular at* $x = [a_0 : a_1 :, .., : a_n] \in X$ if there exists a representative of f as $f = \frac{P}{Q}$ where $Q(a_0, .., a_n) \neq 0$, and P and Q are homogeneous of the same degree. Such a representative will be called a *good representative at* x. If f is regular at x, we define the *value of* f *at* x to be $f(x) = \frac{P(x)}{Q(x)}$. This value is well-defined, i.e. the same for all good representatives of f at x. Note that f regular at x implies that f is regular in a Zariski open neighborhood U of x in X (i.e. the complement of $V(Q)$, where $f = \frac{P}{Q}$ is a good representative at x). We say a rational function $f \in k(X)$ is *regular on a subset* $Y \subset X$ if f is regular at each point of Y. Thus a rational function on X which is regular at x is also regular on a neighborhood of x. We denote the k-algebra (check that it is one) of all rational functions on X which are regular at x by $\mathcal{O}_{X,x}$. Finally, the k-algebra of rational functions on X which are regular on some subset $A \subset X$ is denoted $k[A]$.

Proposition 8.3.11. We have the following elementary facts for an irreducible quasiprojective variety $X \subset \mathbb{P}^n(k)$:

(i): There is an evaluation map: $\epsilon_x : \mathcal{O}_{X,x} \to k$ which is a k-algebra homomorphism.

(ii): The kernel $\ker \epsilon_x$ is a maximal ideal, and the unique maximal ideal in $\mathcal{O}_{X,x}$, thus making it a local ring. If $f \in k[X]$, then f has the well-defined value $\epsilon_x(f) = f(x)$ at each point $x \in X$.

(iii): Let X be an irreducible closed projective set in $\mathbb{P}^n(k)$, and assume $X \not\subset V(X_0)$. Consider the 0-th affine piece of X, i.e. the quasiprojective variety $Y = X \cap U_0$, where U_0 is the affine subset $\{X_0 \neq 0\}$ in $\mathbb{P}^n(k)$. The field of rational functions $k(Y)$ defined above in Definition 8.3.9 coincides with the definition of $k(Y)$ in Definition 6.5.2. Further, $k[Y]$ defined above coincides with the coordinate ring of Y as defined in Definition 1.2.3, and $\mathcal{O}_{Y,x} = k[Y]_{\mathfrak{m}_x}$, where $\mathfrak{m}_x$ is the maximal ideal corresponding to the point $x \in Y$.

(iv): $\mathcal{O}_{X,x} = \cup\{k[U] : U \text{ is a neighborhood of } x\}$.

Proof:
(i) is trivial, using a good representative at x.

To see (ii), note ϵ_x takes $k \subset \mathcal{O}_{X,x}$ identically to itself, and is surjective. Its kernel is therefore a maximal ideal in $\mathcal{O}_{X,x}$. To see that it is the unique maximal ideal, note that if $f \notin \ker\epsilon_x$, then $f(x) \neq 0$. If $f = \frac{P}{Q}$ is a good representative for f at $x = [a_0 : a_1 : ..a_n]$, then we have $P(a_0, ..., a_n) \neq 0$, and $\frac{Q}{P}$ is a rational function lying in $\mathcal{O}_{X,x}$, which is an inverse for f, showing that f is invertible in $\mathcal{O}_{X,x}$. Thus $\ker \epsilon_x$ is the unique maximal ideal in $\mathcal{O}_{X,x}$, which is therefore a local ring. The second assertion of (ii) follows from the definition of $k[X]$. This proves (ii).

We now prove (iii). Let $X = V(\mathfrak{p})$ where $\mathfrak{p}$ is a homogeneous prime ideal. Let x_i denote the images of X_i in $A = k[X_0, .., X_n]/\mathfrak{p}$ and note that, since we have assumed X is not contained in the hyperplane $V(X_0)$, the function x_0 is a non-zero element of $A_1 \subset A$. According to the Definition 8.3.9, $k(Y) = k(X)$. If $f = \frac{P(x_0,..,x_n)}{Q(x_0,..,x_n)}$ is an element of $k(X)$, where $P \in A_d$ and $Q \in A_d$ and $Q \neq 0$, then we define the element $\Phi(f) \in Q(k[Y])$ (the quotient field of the affine coordinate ring $k[Y]$ of Y) to be $\frac{p(x_1,..,x_n)}{q(x_1,..,x_n)}$, where $p =_0 P^D$, and $q =_0 Q^D$ are in the coordinate ring $k[Y] = k[X_1, .., X_n]/\mathfrak{p}^D$. We leave it to the reader to check that :

(1): The indeterminacy of the polynomials $P(X_0, .., X_n)$ and $Q(X_0, .., X_n)$ upto homogeneous elements in $\mathfrak{p}_d = \mathfrak{p} \cap R_d$ leads to the indeterminacy of p and q upto elements in $\mathfrak{p}^D$ in $k[X_1, ..., X_n]$, so that $p(x_1, ..., x_n)$ and $q(x_1, .., x_n)$ are well defined in $k[Y]$.

(2): $\Phi(f)$ does not depend on the representative $\frac{P}{Q}$ chosen for f in $k(X)$.

(3): $Q \neq 0$ in A_d implies $q(x_1, .., x_n) \neq 0$ in $k[Y]$. (Just use the Lemma 8.2.20), and finally Φ is a k-algebra homomorphism.

Define the inverse map $\psi : Q(k[Y]) \to k(X)$ by writing an element $f \in Q(k[Y])$ as $\frac{p(x_1,..,x_n)}{q(x_1,..,x_n)}$ where p is an inhomogeneous polynomial of degree d and q is an inhomogeneous polynomial of degree e, and letting

$$\psi(f) = \frac{P(x_0, .., x_n)}{Q(x_0, ..., x_n)}$$

where:

$$P(X_0, ..., X_n) = X_0^{e-d}({}_0p^H(X_0, ..., X_n)) \; ; \; Q(X_0, ..., X_n) = q^H(X_0, ..., X_n) \text{ if } e \geq d$$
$$P(X_0, ..., X_n) = p^H(X_0, ..., X_n) \; ; \; Q(X_0, ..., X_n) = X_0^{d-e}(p^H(X_0, ..., X_n)) \text{ if } e \leq d$$

Again, the reader is urged to use the Lemma 8.2.20 to convince herself that $\psi(f)$ is a well-defined element of $k(X)$ and the inverse to Φ. This proves the first assertion of (iii), viz. that the definitions of $k(Y)$ arising from Definitions 8.3.9 and 6.5.2 agree.

For the remaining assertions of (iii), let $x = [1 : a_1 : .. : a_n] \in Y$. $Q(x) \neq 0$ implies $Q(1, a_1, ..., a_n) \neq 0$, i.e. that $q(a_1, ..a_n) = Q^D(a_1, .., a_n) \neq 0$, so a rational function $f \in k(X)$ being regular at a point $x \in X \cap U_0$ is equivalent to $\Phi(f)$ being regular at the point x of the affine closed set $Y = X \cap U_0$ according to the Definition 6.5.1. Thus $\mathcal{O}_{Y,x}$ is just the subring of functions f representable as $\frac{p}{q} \in Q(k[Y])$ whose denominator q does not vanish at x, viz. the subring $k[Y]_{\mathfrak{m}_x}$.

Finally, by the Remark 6.5.5, all rational functions on the irreducible affine closed set $Y = X \cap U_0$ which are regular at all points of it are precisely the elements of the affine coordinate ring $k[Y]$. This proves the second and third assertions of (iii).

For (iv), note that a rational function that is regular on a neighborhood U of x is regular at x, so that the right hand side is clearly contained in $\mathcal{O}_{X,x}$. On the other hand, if $f \in \mathcal{O}_{X,x}$, then let $\frac{P}{Q}$ be a good representative for f at x, i.e. $Q(x) \neq 0$. Then this representative shows that f is regular all over the neighborhood $U = X \setminus V(Q)$ of x and hence $f \in k[U]$. This proves (iv) and the proposition. □

Exercise 8.3.12. Let $X \subset \mathbb{P}^n(k)$ be an irreducible quasiprojective variety. Show that for $x \in X$, the local ring $\mathcal{O}_{X,x}$ is the same as $\mathcal{O}_{U,x}$ for any neighbourhood U of x.

Remark 8.3.13. We note that in the case of irreducible affine closed sets, we first defined the k-algebra of regular functions, which are restrictions of regular functions on the ambient affine space $\mathbb{A}^n(k)$ (viz. polynomials) and then the rational functions to be the quotient field of this ring. For closed projective sets, one starts first with the rational functions, and then defines regular functions. The reason for this is that the only regular functions on $\mathbb{P}^n(k)$ are constants, as is proved in the following proposition ! (In fact, later we shall see that the only regular functions on an irreducible closed projective set are constants.)

Example 8.3.14. Consider $\mathbb{P}^1(k)$, the projective line. It is covered by:

$$U_0 = \{[1 : z] : z \in k\}; \;\; U_1 = \{[w : 1] : w \in k\}$$

At a point $x \in U_0 \cap U_1$, the affine coordinates z and w of x with respect to U_0 and U_1 respectively are related by $w = \frac{1}{z}$. The rational function $f = \frac{P(X_0,X_1)}{Q(X_0,X_1)}$ with $\deg P = \deg Q$, becomes, according to the proposition above, the rational function $\frac{p(z)}{q(z)}$ on the affine set $U_0 = k$, where $p(z) = P(1, z)$ and $q(z) = Q(1, z)$ are polynomials in one variable, not necessarily of the same degree. It coincides with the rational function $\frac{r(w)}{s(w)}$ obtained by substituting $w = \frac{1}{z}$ in $\frac{p(z)}{q(z)}$ and clearing denominators from numerator and denominator. If $k = \mathbb{C}$, the reader will recognize these as meromorphic functions on $\mathbb{C}$ having at worst a pole, not an essential singularity, at ∞), i.e. rational functions.

Proposition 8.3.15. The ring of regular functions $k[\mathbb{P}^n(k)]$ on projective space is k, the constant functions.

Proof: Let $f \in k(\mathbb{P}^n(k))$ be regular on U_i. Then, by the Proposition 8.3.11 above, we have a polynomial $p_i(X_0, ., \widehat{X}_i, .., X_n)$ such that $f(z_0, ., 1, .., z_n) = p_i(z_0, ., \widehat{z}_i, .., z_n)$ for all $(z_0, ., \widehat{z}_i, .., z_n) \in U_i$. This means that $f(X_0, ..., X_n) = \frac{P_i(X_0,...,X_n)}{X_i^{d_i}}$, where P_i are homogeneous polynomials in $k[X_0, ..., X_n]$ of degree d_i. This means that for each point $[a_0, ..., a_n] \in U_i \cap U_j$, we have the relation :

$$a_i^{d_i} P_j(a_0, ..., a_n) = a_j^{d_j} P_i(a_0, ..., a_n) \quad 0 \leq i, j \leq n$$

Thus the regular functions $X_i^{d_i} P_j(X_0, ..., X_n)$ and $X_j^{d_j} P_i(X_0, ..., X_n)$ on the affine space $\mathbb{A}^{n+1}(k)$ agree on the non-empty open subset $\mathbb{A}^{n+1}(k) \setminus (V(X_i) \cup V(X_j))$. Since this non-empty open set is Zariski dense in $\mathbb{A}^{n+1}(k)$, the relation above holds at all points of $\mathbb{A}^{n+1}(k)$. That is :

$$X_i^{d_i} P_j(X_0, ..., X_n) = X_j^{d_j} P_i(X_0, ..., X_n)$$

in the ring $k[X_0, .., X_n]$. Since X_i are irreducible, and hence prime polynomials in the unique factorisation domain $k[X_0, .., X_n]$ (Proposition 2.2.17), this implies that P_i is divisible by $X_i^{d_i}$ for all $i = 0, 1, ..n$. Since $\deg P_i = d_i$, we have $P_i = c_i X_i^{d_i}$ for $c_i \in k$, and the relation above says that $c_i = c_j$ for all i, j. Thus letting $c = c_i$ we have $f = \frac{P_i}{X_i^{d_i}} = c \in k$, and the proposition follows. □

Definition 8.3.16. Let $X \subset \mathbb{P}^n(k)$ and $Y \subset \mathbb{P}^m(k)$ be quasiprojective varieties. We say that a set map $f : X \to \mathbb{A}^m(k)$ is a *regular map* if each component f_i for $i = 1, 2, ..m$ is a regular function on X, $f_i \in k[X]$ for $i = 1, .., m$, as defined in the Definition 8.3.10 above. (By (ii) of the Proposition 8.3.11, a regular map $f : X \to \mathbb{A}^m(k)$ has a well defined value in $\mathbb{A}^m(k)$ at each $x \in X$). We say that a map $f : X \to Y$ is a regular map if for each $x \in X$, and each affine open $U_i \subset \mathbb{P}^m(k)$ containing $f(x)$, there exists an open neighborhood U of x such that $f(U) \subset U_i$ and $f : U \to U_i \simeq \mathbb{A}^m(k)$ is a regular map, and $f(X) \subset Y$. (Incidentally, an open subset of a quasiprojective variety is also a quasiprojective variety.)

We need to verify that the definition above makes sense, i.e. we have consistency with respect to choice of affine open U_i on the right. This follows because if $f(x) \in U_i \cap U_j$, then both the i-th and j-th homogeneous coordinates of f are non-zero. Let U be an open neighborhood of x such that $f(U) \subset U_i$ and $f : U \to U_i$ a regular map. Let V be a open neighborhood of x such that $f(V) \subset U_j$. Then $f : W \to U_i \cap U_j$ where $W = U \cap V$. If we write $f = [f_0 : ... : 1 : ...f_m]$ on U (with 1 at the i-th slot), the regularity of f implies that the m functions $f_0, .., f_{i-1}, f_{i+1}, ..f_m$ are regular on U. We shrink U so that the good representatives $\frac{P_k}{Q_k}$ for f_k are valid all over U, i.e. *Q_k do not vanish at any point in U for each $k = 0, 1, ..\widehat{i}, ..m$.* In the affine piece $U_i \cap U_j$, this same map can be written as $[\frac{f_0}{f_j} : ... : \frac{1}{f_j} : ..1 : ..\frac{f_m}{f_j}]$ (with 1 in the j-th slot, $\frac{1}{f_j}$ in the i-th slot). Clearly $f_j(y) \neq 0$ for all $y \in W$ since $f(W) \subset U_j$. Thus if we use the affine open U_j on the right, the representation for f on W is $[g_0 :, ... : g_{j-1} : 1 : g_{j+1} : .. : g_m]$, where $g_i = \frac{1}{f_j}$, and $g_k = \frac{f_k}{f_j}$ for $k \neq i$. If we write $f_k = \frac{P_k}{Q_k}$, with P_j nonvanishing all over W, we have $g_i = \frac{Q_j}{P_j}$ and $g_k = \frac{P_k Q_j}{Q_k P_j}$ for $k \neq i$. Clearly these are regular all over W since all the Q_k and P_j are non-vanishing all over W.

There is an easy criterion for a map to be a regular map, without invoking affine pieces on the right. Namely,

Lemma 8.3.17. Let $f : X \to Y$ be a map, with X, Y as in the definition above. Then f is regular iff for each $x \in X$ there exists a neighborhood U of x in X, and homogeneous polynomials (= d-forms) P_i for $i = 0, 1, ..m$, all of the *same degree d*, such that:

(i): f has a representation :

$$f([a_0 : ... : a_n]) = [P_0(a_0, ..., a_n) : .... : P_m(a_0, ..., a_n)]$$

for all $[a_0 : ... : a_n] \in U$

(ii): at least one of the P_i is everywhere non-vanishing on U.

Proof:

For each $x \in X$, we can find a neighbourhood U of x such that $f(U)$ is contained in one affine piece, say $\mathbb{A}^m(k) = U_0 \subset \mathbb{P}^m(k)$ for simplicity. Write $f = (f_1, .., f_m)$ where f_i are regular on U. Write good representatives $f_i = \frac{P_i}{Q_i}$ for f_i at x, so that $Q_i(x) \neq 0$ for all i, and observe that by shrinking U if necessary, one can guarantee that Q_i never vanishes on U for each i. Then the element $[1 : f_1 : ... : f_m] \in U_0$ is the same as the element $[Q_1 Q_2 ..Q_m : P_1 Q_2 ..Q_m : ... : P_m Q_1 Q_2 ..Q_{m-1}]$ by clearing the denominators, and this representative on U satisfies the requirement of the lemma, since the first entry $Q_1 Q_2 ..Q_m$ is everywhere nonvanishing on U. The converse is left as an exercise. □

Remark 8.3.18. We note that the local representation of f from the lemma above is not unique, and two representations $[P_0 : ... : P_m]$ and $[Q_0 : ... : Q_m]$ will satisfy $Q_i P_j = Q_j P_i$ for all $i \neq j$.

In line with the above Lemma 8.3.17, one may also make the following definition:

Definition 8.3.19. If $X \subset \mathbb{P}^n(k)$ is a quasiprojective variety, then a *rational map* $f : X \to \mathbb{P}^m(k)$ is given by an $(m+1)$-tuple of homogeneous polynomials $P_i \neq 0 \in k[X_0, .., X_n]$, *all of the same degree*, and thus defining f by :

$$[X_0 : X_1 : ... : X_n] \mapsto [P_0(X_0, ..., X_n) : ... : P_m(X_0, ..., X_n)]$$

This is actually a set-mapping on the Zariski open subset $X \setminus \cap_{i=0}^m V(P_i)$ where at least one of the P_i is non-zero. Such a rational map will be called *regular at $x = [a_0 : ... : a_n] \in X$* if, as before, $P_i(x) \neq 0$ for some i, so that the point defined by :

$$f(x) = [P_0(a_0, .., a_n) : ... : P_m(a_0, .., a_n)]$$

is well defined, and is the value of f at x. It is easy to check that if one uses the identification of the affine pieces of $\mathbb{P}^m(k)$ with $\mathbb{A}^m(k)$, then this coincides with the definition of rational maps to $\mathbb{A}^m(k)$ given in Definition 8.3.9. We call $f : X \to Y$, where $Y \subset \mathbb{P}^m(k)$ is another quasiprojective variety, a *rational map* if it is a rational map to $\mathbb{P}^m(k)$, and if $f(x) \in Y$ for every $x \in X$ at which f is regular. If X and Y are irreducible, it is easy to check that a rational map $f : X \to Y$ will give rise to a field homomorphism (which is therefore an inclusion) $f^* : k(Y) \to k(X)$, and conversely any such field inclusion will give a rational map $f : X \to Y$. Two irreducible quasiprojective varieties will be called *birationally equivalent* if f^* is an isomorphism of $k(Y)$ with $k(X)$, or

equivalently if there exists a rational map $g : Y \to X$, such $f \circ g(y) = y$ for all $y \in Y$ where g is regular and f is regular at $g(y)$, and $g \circ f\ (x) = x$ for all $x \in X$ where f is regular and g is regular at $f(x)$.

Definition 8.3.20. *A* regular map $f : X \to Y$ between irreducible quasiprojective varieties is said to be an *isomorphism* if the inverse $f^{-1} : Y \to X$ exists, and is a regular map. In this case we say X and Y are *isomorphic*. A quasiprojective variety which is isomorphic to an irreducible affine closed set is said to be an *affine variety*. A quasiprojective variety which is isomorphic to an irreducible closed projective set is said to be a *projective variety*.

Example 8.3.21. The quasiprojective variety $U := \mathbb{A}^2(k) \setminus \{(0,0)\}$ is neither an affine variety nor a projective variety. We already saw in Remark 6.6.6 that it is not an affine variety. We also saw noted there that the ring of regular functions $k[U] = k[x, y]$. To see that it is not a projective variety, we need the result that on an irreducible closed projective set, the only regular functions are constants, i.e. elements of k. This fact, which generalises Proposition 8.3.15, will be proved later. Since $k[U] = k[x, y] \neq k$, U cannot be isomorphic to a closed projective set either. Similarly for $\mathbb{A}^n(k) \setminus \{0\}$, and $n \geq 2$.

Exercise 8.3.22. Show that for $n \geq 2$ and any point $x \in \mathbb{P}^n(k)$, the irreducible quasiprojective variety $\mathbb{P}^n(k) \setminus \{x\}$ is neither an affine nor a projective variety. (See the Remark 6.6.6 of §6)

We will see some more examples at the end of this subsection.

Exercise 8.3.23. Show that two irreducible quasiprojective varieties are birationally equivalent iff they contain isomorphic open subsets. (Compare with the Proposition 6.7.3.) Thus, for example, the (projective closures of) the cubic node and the cubic cusp are both birationally equivalent to $\mathbb{P}^1(k)$.

It is convenient to be able to reduce various arguments about rational or regular maps between quasiprojective varieties to the situation of affine closed sets. To this end we have the following propositions:

Proposition 8.3.24 (A basis for the Zariski topology on quasiprojective varieties)**.**

(i): Let $Y \subset \mathbb{P}^n(k)$ be an irreducible projective closed set. For $0 \leq i \leq n$, let Y_i be the affine pieces of Y. Then the family of open sets :

$$\{D(f) = Y_i \setminus V(f) : f \in k[Y_i],\ 0 \leq i \leq n\}$$

constitute a basis for the Zariski topology on Y, and are again called basic open sets of Y. These are again all irreducible affine varieties . Another basis is the collection:

$$\{D_Y(F) = Y \setminus V(F) : F \in k[X_0, .., X_n] \text{ homogeneous}\}$$

(ii): Let Y be an irreducible quasiprojective variety. Then Y has a basis consisting of open sets which are irreducible affine varieties. We will refer to an affine basic open containing a point $x \in Y$ as an *affine neighbourhood of* x.

Proof: The asssertion (i) follows directly from the Proposition 6.4.18, because $Y = \cup_{i=0}^n Y_i$ and the affine pieces Y_i are are open in Y. Since Y is irreducible, any non-empty open subset of Y_i is open in Y, and hence dense in Y, so has closure equal to Y. So all the basic opens of each Y_i are irreducible quasiprojective varieties. By the Exercise 6.6.5, these basic opens are isomorphic to irreducible affine closed sets.

To see (ii), note that Y irreducible and quasiprojective implies it is an open subset of a closed projective set Z, and so any open subset of Y is an open subset of Z, and may be expressed as a union of $D(f_i)$'s. Thus the subfamily of $\{D(f)\}$ where $f \in k[Z_i]$ for some affine piece Z_i of Z, and such that $D(f) \subset Y$ will constitute a basis for Y. Each member of this collection is an affine variety. This proves the proposition. □

Remark 8.3.25. It is natural to enquire whether $D_X(F) = X \setminus V(F)$ for X a projective closed subset in $\mathbb{P}^n(k)$, and $F \neq 0$ a homogeneous polynomial, is an affine variety. If F is linear, i.e. homogeneous of degree 1, then clearly $D_X(F)$ is an affine piece of X, and thus an affine variety (just complete F to a set of coordinates $\{X_i\}$ on $\mathbb{A}^{n+1}(k)$, so that $X_0 = F$). That $D(F)$ is an affine variety in general for $F \neq 0$ any homogeneous polynomial will be seen later after introducing the Veronese embedding.

Lemma 8.3.26. Let X be a topological space, with $X = \cup_{\alpha\in\Lambda} U_\alpha$,where U_α are open subsets of X. Then a subset C of X is closed in X iff $C \cap U_\alpha$ is closed in U_α for each $\alpha \in \Lambda$.

Proof:

Only if is clear. If $C \cap U_\alpha$ is closed in U_α for each α, write $C \cap U_\alpha = Z_\alpha \cap U_\alpha$, where Z_a is closed in X. Let $T_\alpha = X \setminus U_\alpha$, which is also closed in X for each $\alpha \in \Lambda$. Now verify that $C = \cap_{\alpha\in\Lambda}(Z_\alpha \cup T_\alpha)$, which is clearly closed in X. □

Corollary 8.3.27. Let $f : X \to Y$ be a map of topological spaces, and let $\{U_\alpha\}_{\alpha\in\Lambda}$ and $\{V_\beta\}_{\beta\in\Gamma}$ be open coverings of X and Y respectively, such that for each $\alpha \in \Lambda$, there exists a $\beta(\alpha) \in \Gamma$ such that $f(U_\alpha) \subset V_{\beta(\alpha)}$. Then f is continuous iff $f : U_\alpha \to V_{\beta(\alpha)}$ is continuous for each $\alpha \in \Lambda$.

Proof:

Again, only if is clear. If C is closed in Y, $C \cap V_\beta$ is closed in V_β for each $\beta \in \Gamma$. Since we have that $f : U_\alpha \to V_{\beta(\alpha)}$ is continuous, it follows that $f^{-1}(C) \cap U_\alpha$ is closed in U_α for every α. Thus $f^{-1}(C)$ is closed in X by the previous lemma. □

Exercise 8.3.28 (Topology of Quasiprojectives)**.**

(i): Verify that for $X \in \mathbb{P}^n(k)$ a quasiprojective variety, the collection of sets:

$$\{D_X(f) : \ f \text{ is regular on } X\}$$

where

$$D_X(f) := \{x \in X : \ f(x) \neq 0\}$$

constitutes a basis for a topology on X which agrees with the subspace topology on X induced from $\mathbb{P}^n(k)$. (Compare with the Proposition 6.4.18.)

(ii): Show that regular maps between quasiprojective varieties are continuous (with respect to the Zariski topology).

(iii): Show that open (resp. closed) subsets of a quasiprojective variety are also quasiprojective varieties.

We now come to an important characterisation of regular maps between quasiprojective varieties.

Proposition 8.3.29. Let $f : X \to Y$ be a mapping of irreducible quasiprojective varieties, with $X \subset \mathbb{P}^n(k)$ and $Y \subset \mathbb{P}^m(k)$. The following are equivalent:

(i): f is regular.

(ii): f is continuous, and for each $x \in X$, the map $g \longmapsto f^*g := g \circ f$ is a k-algebra homomorphism of $\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$.

Proof:

(i)⇒(ii)

By the Definition 8.3.16 of a regular map, for each $x \in X$, there is an open neighbourhood U of x in X and an affine open set $U_i = D(X_i) \subset \mathbb{P}^m(k)$ such that $f : U \to U_i$ is regular. By Propositions 8.3.24, and 8.3.27, it is enough to show that a regular map $f : U \to U_i$ is continuous for each affine basic open set U in X and $U_i = D(X_i) \subset \mathbb{P}^m(k)$. By (iii) of the Proposition 8.3.24, U and U_i are irreducible affine varieties, so we are reduced to showing that a regular map from an irreducible affine closed set to $\mathbb{A}^m(k)$ is continuous with respect to the Zariski topologies. But this follows from the Proposition 5.1.9, Remark 6.5.5 and the discussion following Proposition 6.1.3, because any such regular mapping is just a morphism as defined there. Thus a regular map is continuous.

Similarly, any k-algebra homomorphism $f^* : A \to B$ between k-algebras of finite type has the property that if $\mathfrak{m}_x$ is a maximal ideal in B, $(f^*)^{-1}(\mathfrak{m}_x)$ is a maximal ideal in A, denoted by $\mathfrak{m}_{f(x)}$, (see Propositions 5.1.7 and 5.1.9). It follows that f^* maps the multiplicative set $A \setminus \mathfrak{m}_{f(x)}$ to the multiplicative set $B \setminus \mathfrak{m}_x$, and the corresponding localisations $A_{\mathfrak{m}_{f(x)}}$ to $B_{\mathfrak{m}_x}$. So the property we desire is true of morphisms between irreducible affine closed sets, and since we have reduced to this case, we are done, by Exercise 8.3.12.

(ii)⟹(i) Again, by continuity, and (iii) of the Proposition 8.3.24 one can reduce the question to $f : X \to Y$ a continuous map of irreducible affine closed sets. We are given that $f^* : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ is a k-algebra homomorphism for each $x \in X$. Since the coordinate ring $k[Y]$ is contained in all the local rings $\mathcal{O}_{Y,f(x)}$, it follows that the image of $k[Y]$ lies in $\cap_{x\in X}\mathcal{O}_{X,x}$. By (v) of the the Proposition 6.5.4, this intersection is precisely $k[X]$. Thus $f^* : k[Y] \to k[X]$ is a k-algebra homomorphism, and each coordinate function $f_i = f^*(x_i)$ (where x_i is the i-th coordinate function on the affine closed set $Y \subset \mathbb{A}^k(m)$) is an element of $k[X]$, and therefore a regular function on X, so that the mapping $f = (f_1, .., f_m)$ is a regular map into Y. This proves the proposition. □

Corollary 8.3.30 (The category of quasiprojective varieties)**.** The composite of regular maps between quasiprojective varieties is a regular map, and that the identity map of a quasiprojective variety is regular, as is clear from (ii) of the foregoing proposition. Thus quasiprojective varieties together with regular maps as morphisms form a category. In the foregoing, we have frequently restricted ourselves to *irreducible* quasiprojective varieties, and one has to make the necessary straightforward modifications to those assertions to obtain the corresponding facts for quasiprojective varieties.

We next go through some examples of quasiprojective varieties and rational maps between them to clarify the foregoing concepts.

Example 8.3.31 (Automorphisms of $\mathbb{P}^1(k)$)**.** First note that all maps $\mathbb{P}^1(k) \to \mathbb{P}^1(k)$ of the form:

$$[z_0 : z_1] \mapsto [az_0 + bz_1 : cz_0 + dz_1]$$

with $ad-bc \neq 0$, are automorphisms of $\mathbb{P}^1(k)$, i.e. regular maps with regular inverses. These are called *projective linear transformations*, and form a group denoted $PGL(2, k)$. In fact the group $PGL(2, k) = GL(2, k)/k^*$, by observing that scaling of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ leads to the same map. We claim that *all* automorphisms of $\mathbb{P}^1(k)$ are of this form. If $\phi : \mathbb{P}^1(k) \to \mathbb{P}^1(k)$ is an automorphism, we may postcompose it with a projective linear transformation to ensure that $\phi([1 : 0]) = [1 : 0]$. So it is enough to show that an automorphism of $\mathbb{P}^1(k)$ fixing the point $[1 : 0]$ is a projective linear transformation.

Now $U_1 = \mathbb{P}^2(k) \setminus \{[1 : 0]\}$ is the affine space $\mathbb{A}^1(k)$, and $\phi : U_1 \to U_1$ is thus an automorphism of $\mathbb{A}^1(k)$. In particular, it is injective, and therefore defined by a degree 1 polynomial $z \mapsto az + b$ (by Example 5.1.10, all morphisms of affine spaces $\mathbb{A}^n(k)$ are given by polynomials). Thus ϕ is the projective linear transformation $[z : 1] \mapsto [az + b : 1]$, or what is the same thing, $[z_0 : z_1] \mapsto [az_0 + bz_1 : z_1]$, a projective linear transformation. Hence our assertion that $\mathrm{Aut}_k(\mathbb{P}^1(k)) = PGL(2, k)$.

This same fact is true for all $\mathbb{P}^n(k)$, i.e. the group of regular automorphisms of $\mathbb{P}^n(k)$ is $PGL(n+1,k) = GL(n+1,k)/k^*$. One needs a little more machinery to prove it, so it is postponed till we get to divisors, intersections etc.

Example 8.3.32 (The Cremona Transformation of $\mathbb{P}^2(k)$)**.** Let us define a rational map of $\mathbb{P}^2(k)$ to itself by the assignment :

$$[X_0 : X_1 : X_2] \mapsto [X_1X_2 : X_0X_2 : X_0X_1]$$

Clearly, this map is regular wherever at least one of the monomials X_1X_2, X_0X_2, X_0X_1 are non-zero, i.e. at all points $[X_0 : X_1 : X_2]$ where at least two of the homogeneous coordinates X_i are non-zero. This set is $\mathbb{P}^2(k) \setminus \{P, Q, R\}$ where $P = [1 : 0 : 0]$, $Q = [0 : 1 : 0]$, $R = [0 : 0 : 1]$. This transformation is called the *Cremona transformation*. It is a birational transformation, whose rational inverse is again the same Cremona transformation, viz. :

$$[X_0 : X_1 : X_2] \longmapsto [X_1X_2 : X_0X_2 : X_0X_1]$$

which is again regular on $\mathbb{P}^2(k) \setminus \{P, Q, R\}$. This map "blows down" the coordinate hyperplanes $V(X_0)$, $V(X_1)$, $V(X_2)$ to the points P, Q, R respectively. Similarly, it "blows up" the points P, Q, R to the coordinate hyperplanes. The tranformation sets up an isomorphism between the basic open sets $D(X_0X_1X_2)$ (the complement of the three coordinate hyperplanes) and itself.

Example 8.3.33 (Projection from a plane in $\mathbb{P}^n(k)$)**.** Let $\pi : \mathbb{A}^{n+1}(k) \setminus \{0\} \to \mathbb{P}^n(k)$ be the natural quotient map. For a k-subspace $V \subset k^{n+1}$, we denote the image $\pi(V \setminus \{0\})$ in $\mathbb{P}^n(k)$ as $\mathbb{P}(V)$, and call it the *projective space on* V. Let $\{L_i\}_{i=0}^m$ be $m+1$ linearly independent linear functionals on k^{n+1}. Let $E := \cap_{i=0}^m \ker L_i$, a k-subspace of k^{n+1} of dimension $n-m$. Define the rational map:

$$\begin{aligned} p : \mathbb{P}^n(k) &\to \mathbb{P}^m(k) \\ [X_0 : X_1 : .. : X_n] &\mapsto [L_0(X_0, .., X_n) : .. : L_m(X_0, .., X_n)] \end{aligned}$$

which is clearly regular on $\mathbb{P}^n(k) \setminus \mathbb{P}(E)$, where $\mathbb{P}(E) \simeq \mathbb{P}^{n-m-1}(k)$. The reason this map is called projection from E (or more precisely, $\mathbb{P}(E)$) is that each point $v = (a_0, .., a_n) \in k^{n+1}$ can be expressed uniquely as a (direct) sum :

$$v = Tp(v) + w$$

where $T : k^{m+1} \to k^{n+1}$ is a k-linear map satisfying $pT(x)) = x$ for all $x \in k^{m+1}$, and $p = (L_0, L_1, .., L_m)$ and $w \in E$. This is just a vector space splitting of the linear map $p = (L_0, .., L_m)$, so that T is an injective mapping of $k^{m+1} = \operatorname{Im} p$ into k^{n+1}. T maps k^{m+1} isomorphically onto the subspace $H := \operatorname{Im} T \subset k^{n+1}$, a vector space complement of E in k^{n+1}. With this above decomposition, the map p just kills the component w. In particular, if $v \notin E$, $p(v) \neq 0$, and hence $Tp(v) \neq 0$, and so $Tp(v)$ determines a line in $\operatorname{im} T = H$, i.e. an element of $\mathbb{P}(H)$. Equivalently, if $v \notin E$, the k-subspace spanned by v and E is a subspace of dimension $n-m+1$, and thus intersects the $m+1$ dimensional subspace H in a 1-dimensional space, viz. the element $p(v) \in \mathbb{P}(H)$.

A particular case, of course, is the projection $[X_0 : .. : X_n] \mapsto [X_0 : ... : X_m]$ of $\mathbb{P}^n(k) \setminus E$ to $\mathbb{P}^m(k)$, from the $(n-m-1)$ dimensional projective space $\mathbb{P}(E)$, where E is the $(n-m)$ dimensional subspace consisting of all points $[0 : 0 : ...0 : X_{m+1} : .. : X_n]$ in $\mathbb{P}^n(k)$.

Example 8.3.34 (The Veronese Embedding)**.** Let R_m be the m-th graded component of $R = k[X_0, .., X_n]$, that is, the k-vector space of all homogeneous polynomials of degree m. Since every homogeneous degree m monomial in $X_0, ..., X_n$ occurs exactly once in the coefficient of t^m in the expression $f(X_0, .., X_n, t) = \Pi_{i=0}^n (1 - tX_i)^{-1}$, it follows that the number of these monomials is precisely the coefficient of t^m in the product $f(1, 1..1, t) = (1-t)^{-n-1}$, which is easily checked to be the binomial coefficient $\binom{n+m}{m}$, which we shall denote by N. Consider the projective space $\mathbb{P}(R_m) \simeq \mathbb{P}^{N-1}(k)$. It is convenient to write a point of this projective space as $x = [: Y_I]_{I \in S}$, where S is defined by :

$$S = \{I = (i_0, .., i_n) : \Sigma_{k=0}^n i_k = m\}$$

We now define a mapping:

$$\begin{aligned} j : \mathbb{P}^n(k) &\rightarrow \mathbb{P}(R_m) \\ [X_0 : ... : X_n] &\mapsto [: X^I]_{I \in S} \end{aligned}$$

where $X^I := X_0^{i_0}....X_n^{i_n}$. This map is clearly regular, since, for example if $X_j \neq 0$, the monomial X^I where $I = (0, 0, .., m, 0, 0)$ with m at the $j+1$-th place and zero elsewhere, will be just X_j^m, which will be non-zero.

For two multi-indices $I, J \in S$, we define $I + J = (i_0 + j_0, .., i_n + j_n)$. Clearly, since $X^I X^J = X^K X^L$ whenever $I + J = K + L$, the image of j lies in the projective closed set $V(\mathfrak{a})$ where $\mathfrak{a}$ is the homogeneous ideal generated by all the quadratic expressions $Y_I Y_J - Y_K Y_L$ with $I + J = K + L$, in the N-variable polynomial ring $k[Y_I]_{I \in S}$.

Claim: The image of j is precisely $V(\mathfrak{a})$.

It is convenient to introduce the following notation. Define the *length* $l(I)$ of a multi-index $I \in S$ to be the number of non-zero entries in I.

We first claim that if a point $[: Y_I]_{I \in S} \in V(\mathfrak{a})$, then there exists a multi-index $I = (0, 0, ..m, ..0)$, of length 1, such that $Y_I \neq 0$. For, if say $Y_{(m,0,0,..0)} = 0$, then using the equation :

$$Y^2_{(m-r,r,..,0)} = Y_{(m-2r,2r,0,0..0)} Y_{(m,0,0..,0)}$$

one sees that $Y_{(m-r,r,0,...,0)} = 0$ for any $r \leq \frac{m}{2}$, since the right hand side is zero by assumption. Interchanging the roles of r and $m - r$, one sees that all $Y_{(i,m-i,0,..,0)} = 0$. By repeating this argument for other multi-indices $I = (0, ..., m, .., 0)$ of length 1, entry, we conclude that $Y_I = 0$ for all multi-indices $I \in S$ with $l(I) \leq 2$. Assume inductively that we have proved that $Y_I = 0$ for all multi-indices with $l(I) \leq r$. Consider for example a multi-index $I = (i_0, i_1, .., i_r, ..0)$ with $r + 1$ non-zero entries. Let us assume, to be specific, that $i_0 \leq i_1$, otherwise we interchange the roles of i_0 and i_1. Again, we have the equation:

$$Y_I^2 = Y_{(2i_0, i_1 - i_0, .., i_r, .., 0)} Y_{(0, i_0 + i_1, i_2, .., i_r, .., 0)}$$

where the extreme right hand term is zero by induction hypothesis, so $Y_I = 0$. One can repeat this argument for any other multi-index with length $r + 1$. Thus we will have that all the homogeneous coordinates are zero, a contradiction. This proves the claim.

Thus for a point $[: Y_I]_{I \in S}$ to lie in $V(\mathfrak{a})$, we must have $Y_I \neq 0$ for at least one of the length 1 multi-indices $I = (0, 0, .., m, .., 0)$. Again, to be specific, say $Y_{(m,0,..,0)} \neq 0$. Define $X_0 = Y_{(m,0,..,0)}$, and $X_i = Y_{(m-1,0,..,1,..,0)}$, where the entry 1 occurs in the $(i + 1)$-th spot in the subscript on the right. We now claim that:

$$j([X_0 : ... : X_n]) = [: Y_I]_{I \in S}$$

Again, we first claim that :

$$\frac{Y_{(m-r,r,0,..,0)}}{Y_{(m,0,...,0)}} = \left(\frac{X_1}{X_0}\right)^r$$

This is true for $r = 1$ by definition, and for other r we inductively apply:

$$Y_{(m-r,r,0,..,0)} Y_{(m-1,1,0,..,0)} = Y_{(m,0,..,0)} Y_{(m-(r+1),r+1,0,..,0)}$$

Similarly for the other multiindices $I = (m-r, 0, .., r, 0, .., 0)$ with r at the $(i+1)$-th spot. Now if $I = (i_0, i_1, .., i_n)$ with $i_0 + i_1 + .. + i_n = m$ is any multi-index, we have the relations:

$$\left(\frac{X_0}{X_0}\right)^{i_0} \left(\frac{X_1}{X_0}\right)^{i_1} ... \left(\frac{X_n}{X_0}\right)^{i_n} = \left(\frac{Y_{(m-i_1,i_1,0,..,0)}}{Y_{(m,0,..,0)}}\right) ... \left(\frac{Y_{(m-i_n,0,..,i_n)}}{Y_{(m,0,..,0)}}\right)$$

Now we we use the relation:

$$Y_{(m-i_1,i_1,..,0)} Y_{(m-i_2,0,i_2,...,0)} = Y_{(m,0,...,0)} Y_{(m-i_1-i_2,i_1,i_2,0,..,0)}$$

to obtain that the right hand side is :

$$\left(\frac{Y_{(m-i_1-i_2,i_1,i_2,..,0)}}{Y_{(m,0,..,0)}}\right) \left(\frac{Y_{(m-i_3,0,..i_3,..0)}}{Y_{(m,0,..,0)}}\right) .... \left(\frac{Y_{(m-i_n,0,..,i_n)}}{Y_{(m,0,..,0)}}\right)$$

and by similar collapsings, and the fact that $i_0 = m - i_1 - ... - i_n$, this reduces to the final equation:

$$\left(\frac{X^I}{X_0^m}\right) = \left(\frac{Y_{(i_0,i_1,..,i_n)}}{Y_{(m,0,..,0)}}\right)$$

for all $I \in S$. This proves the assertion that the image of j is precisely $V(\mathfrak{a})$. In fact, we define the map:

$$\begin{aligned} \psi : V(\mathfrak{a}) &\to \mathbb{P}^n(k) \\ [: b_I]_{I\in S}) &\mapsto [a_0 : a_1 : .. : a_n] \end{aligned}$$

where $a_0 = b_{(m,0,..,0)}$ and $a_i := \frac{b_{(m-1,0,..1,..0)}}{b_{(m,0,...0)}}$ if $b_{(m,0,..,0)} \neq 0$ (resp. the suitable modification of this definition if $b_{(0,0,..m,...0)} \neq 0$). This is clearly well-defined because of the relations of $\mathfrak{a}$, and regular on the affine piece $D(b_{(m,0..,0)}) \cap V(\mathfrak{a})$ (resp. $D(b_{(0,..,m,..0)}) \cap V(\mathfrak{a})$ which is a neighbourhood of the point $x = [: b_I]_{I\in S}$. Since this point x is arbitrary, we have that ψ is a regular inverse to j. Thus the projective space $\mathbb{P}^n(k)$ and $V(\mathfrak{a})$ are isomorphic, and j and ψ are, in particular, homeomorphisms with respect to Zariski topologies.

We now list some applications of the Veronese embedding. The first is the reduction of questions on degree m hypersurfaces in $\mathbb{P}^n(k)$ to questions on hyperplane sections, i.e. degree one hypersurfaces, on the Veronese subvariety $V(\mathfrak{a})$ defined above.

Example 8.3.35 (The space of degree m hypersurfaces in $\mathbb{P}^n(k)$)**.** The closed projective set $V(F) \subset \mathbb{P}^n(k)$, where $F(X_0, X_1, ...X_n)$ is an m-form in $k[X_0, ..., X_n]$, is called a *degree-m hypersurface* in $\mathbb{P}^n(k)$. If we write $F = \sum_{I\in S} a_I X^I$, it is clear that $V(F)$ is uniquely determined as a closed projective set by the point $[: a_I]_{I\in S}$ in $\mathbb{P}^{N-1}(k)$, where $N = \binom{n+m}{m}$. Thus there is a 1-1 correspondence between degree-m hypersurfaces and $\mathbb{P}^{N-1}$. Furthermore, if we let G be the linear functional on k^N defined by $G = \Sigma_{I\in S} a_I Y_I$, then the intersection $V(G) \cap j(\mathbb{P}^n(k))$ is precisely:

$$j(\{[X_0 : X_1 : .. : X_n] : \Sigma_I a_I X^I = 0\}) = j(V(F))$$

which shows that the hypersurface $V(F)$ in $\mathbb{P}^n(k)$ can be recovered as a hyperplane section of the Veronese variety $V(\mathfrak{a}) = j(\mathbb{P}^n(k))$.

As a consequence, we have the following:

Corollary 8.3.36. Basic open subsets of closed projective sets are affine. That is, if X is a closed projective set in $\mathbb{P}^n(k)$, then $D_X(F) = X \setminus V(F)$ is affine. For, by using the Veronese map j, X is isoomorphic to the closed subset $j(X) \subset \mathbb{P}^{N-1}(k)$, and thus $D_X(F)$ is isomorphic to the set $j(X) \setminus V(G)$, (in the notation of the example above), which is a closed subset of the affine space $\mathbb{P}^{N-1}(k) \setminus V(G) \simeq \mathbb{A}^{N-1}(k)$ (see Remark 8.3.25). Thus it is isomorphic to an affine closed set, and so $D_X(F) = X \setminus V(F)$ is an affine variety, for X a closed projective set. This answers the question in Remark 8.3.25.

Remark 8.3.37. If one takes a general *quasiprojective variety* $X \subset \mathbb{P}^n(k)$, and a homogeneous polynomial $F \in k[X_0, ..., X_n]$, then it is *not true* that $D_X(F) = X \setminus V(F)$ is affine. For example, if one takes the quasiprojective variety $X = \mathbb{P}^2(k)\setminus\{[1 : 0 : 0]\}$, and $F = X_0$, then $D_X(F) = U_0 \cap X$, which is just $\mathbb{A}^2(k)\setminus\{(0, 0)\}$, and is not affine by the Example 8.3.21 above.

Exercise 8.3.38 (Structure sheaf of a quasiprojective)**.** Let $X \subset \mathbb{P}^n(k)$ be an irreducible quasiprojective variety. Define a sheaf $\mathcal{O}_X$ by declaring:

$$\mathcal{O}_X(U) := \{f \in k(X) : \ f \ \text{ is regular on } \ U\} = \cap_{x\in U} \mathcal{O}_{X,x}$$

Verify that this defines a sheaf on X, and makes X into a locally ringed space. In contrast with the case of an irreducible affine closed set, if X is an irreducible projective closed set, we shall see later that $\mathcal{O}_X(X)$, the *global sections of the sheaf* $\mathcal{O}_X$ or what is the same thing, the k-algebra of functions regular on all of X, consists only of constants.

8.4. **Products of Quasiprojective Varieties.** For the affine spaces $\mathbb{A}^n(k)$, $\mathbb{A}^m(k)$, their product $\mathbb{A}^{n+m}(k)$ is another affine space, with its topology and structure as an affine variety, so nothing needs to be done in this situation. Note that the coordinate ring of the product, namely $k[X_1,..,X_n,Y_1,..,Y_m]$ is just the tensor product (as k-algebras) $k[X_1,..,X_n]\otimes_k k[Y_1,..,Y_m]$ of the coordinate rings of $\mathbb{A}^n(k)$ and $\mathbb{A}^m(k)$ respectively.

For projective spaces, the product is no longer a projective space, but can be given the structure of a closed projective set. More precisely,

Definition 8.4.1 (Segre Embedding)**.** Denote a point on $\mathbb{P}^{(n+1)(m+1)-1}(k)$ by $[:W_{ij}]$ where $i=0,1,..n$ and $j=0,1,...m$. It is convenient to think of this point as the line defined by the $(n+1)\times(m+1)$ matrix $[W_{ij}]$. Define a map:

$$\begin{aligned} j:\mathbb{P}^n(k)\times\mathbb{P}^m(k) &\to \mathbb{P}^{(n+1)(m+1)-1}(k)\\ ([X_0:...:X_n],[Y_0:...:Y_m]) &\mapsto [:X_iY_j]\end{aligned}$$

Since some $X_k\neq 0$ and some $Y_l\neq 0$, the homogeneous coordinate X_kY_l on the right will be non-zero, so this map is certainly regular. We need to find its image. Consider the homogeneous ideal defined by:

$$\mathfrak{a}=\langle W_{ij}W_{kl}-W_{il}W_{kj}: 0\leq i,k\leq n;\ 0\leq j,l\leq m\rangle$$

It is clear that the image of j is contained in $V(\mathfrak{a})$. On the other hand, it is easy to define a map $\psi: V(\mathfrak{a})\to\mathbb{P}^n(k)\times\mathbb{P}^m(k)$ which is an inverse for j. If, for example, $p=[:w_{ij}]$ is a point on $V(\mathfrak{a})$ with, say, the entry $w_{rs}\neq 0$, then we may define:

$$\psi([:w_{ij}])=([w_{0s}:..:w_{rs}:...w_{ns}],[w_{r0}:...:w_{rs}:...:w_{rm}])$$

(picking out the row and column of the matrix $[w_{ij}]$ that contain w_{rs}). This makes sense regardless of choice of the non-zero entry w_{rs} because of the relations in the ideal $\mathfrak{a}$, which say that if $[:w_{ij}]\in V(\mathfrak{a})$, all the 2×2 minors of the matrix $[w_{ij}]$ are zero, so it is of rank 1, and hence all rows are multiples of one row, and likewise all columns.

It is easy to show that if $X=V(\mathfrak{a})\subset\mathbb{A}^n(k)$ and $Y=V(\mathfrak{b})\subset\mathbb{A}^m(k)$ are affine closed sets defined by the radical ideals $\mathfrak{a}$ and $\mathfrak{b}$ respectively, then $X\times Y$ is an affine closed subset of $\mathbb{A}^{n+m}(k)$. In fact, if $\mathfrak{c}$ is the radical of the ideal in $k[X_1,..,X_n,Y_1,..,Y_m]$ generated by $\mathfrak{a}$ and $\mathfrak{b}$ (regarded as subsets of $k[X_1,..,X_n,Y_1,..,Y_m]$ via the obvious inclusions), then it is easily checked that $X\times Y=V(\mathfrak{c})$. Note that with this structure of an affine closed set, the projection $p_1: X\times Y\to X$ is a surjective and corresponds to the ring homomorphism:

$$p_1^*: k[X]=k[X_1,..,X_n]/\mathfrak{a}\to k[X_1,..,X_n,Y_1,..,Y_m]/\mathfrak{c}=k[X\times Y]$$

and is therefore regular. Likewise, for the other projection $p_2: X\times Y\to Y$.

Exercise 8.4.2. Check that for affine closed sets X and Y, the coordinate ring $k[X\times Y]$ is the k-algebra tensor product $k[X]\otimes_k k[Y]$.

We again emphasise that the (Zariski) topology on $X\times Y$ is *not* the product of the Zariski topologies on X and Y. However, if U is open in X and V is open in Y, then the product $U\times V=p_1^{-1}(U)\cap p_2^{-1}(V)$ is open in $X\times Y$, since the maps p_i are regular, and hence continuous with respect to the respective Zariski topologies, in view of Proposition 8.3.29. Thus the Zariski topology on $X\times Y$ is *finer* than the product topology.

Next we define the product of two projective closed sets. Let $X=V(\mathfrak{a})$ and $Y=V(\mathfrak{b})$ be closed projective sets defined by the homogeneous non-redundant radical ideals $\mathfrak{a}$ in $k[X_0,..,X_n]$ and $\mathfrak{b}$ in $k[Y_0,...,Y_m]$. A point:

$$(x,y)=([a_0:..:a_n],[b_0:...:b_m])$$

of $\mathbb{P}^n(k)\times\mathbb{P}^m(k)$ lies in $X\times Y$ iff $F(a_0,...,a_n)=0$ for each homogeneous $F\in\mathfrak{a}$ and $G(b_0,...,b_m)=0$ for each homogeneous $G\in\mathfrak{b}$. This is equivalent to the statement that $(x,y)\in X\times Y$ iff $F(a_0b_j,...,a_nb_j)=0$ and $G(a_ib_0,..,a_ib_m)=0$ for each i,j and all $F\in\mathfrak{a}$, and $G\in\mathfrak{b}$. From this it follows that $X\times Y=V(\mathfrak{c})$ where $\mathfrak{c}$ is the homogeneous ideal in $k[W_{ij}]_{0\leq i\leq n,0\leq j\leq m}$ generated by the homogeneous polynomials $F(W_{0j},..,W_{nj})$ for $F\in\mathfrak{a}$, $G(W_{i0},...,W_{im})$ for $G\in\mathfrak{b}$, and the polynomials $W_{ij}W_{kl}-W_{il}W_{kj}$ for $0\leq i,k\leq n$; $0\leq j,l\leq m$. This makes the product of two projective closed sets, more generally two projective varieties, a projective variety. Thus we have the following proposition:

Proposition 8.4.3. If $X \subset \mathbb{P}^n(k)$ and $Y \subset \mathbb{P}^m(k)$ are quasiprojective varieties, then their product $X \times Y$, contained in $\mathbb{P}^{nm+n+m}(k)$, is also a quasiprojective variety.

Proof:
Clearly, $X = X_1 \setminus X_2$ where X_i are closed subsets of $\mathbb{P}^n(k)$, and $Y = Y_1 \setminus Y_2$, where Y_i are closed subsets of $\mathbb{P}^m(k)$. Thus, $X_i \times Y_j$ are closed subsets of $\mathbb{P}^{nm+n+m}(k)$, and since $X \times Y = (X_1 \times Y_1) \setminus [(X_2 \times Y_1) \cup (X_2 \times Y_1)]$, it is a difference of two closed projective subsets of $\mathbb{P}^{nm+n+m}(k)$, and hence a quasiprojective variety. □

Lemma 8.4.4. The closed subsets of various products are as follows:

(i): closed subsets of $\mathbb{A}^n(k) \times \mathbb{A}^m(k)$ are common zero sets of polynomials in $n+m$ variables.

(ii): closed subsets of $\mathbb{A}^n(k) \times \mathbb{P}^m(k)$ are common zero sets of polynomials in $n+m+1$ variables $X_1.., X_m$, $Y_0, ..., Y_m$ which are homogeneous in the last $m+1$ variables Y_i.

(iii): closed subsets of $\mathbb{P}^n(k) \times \mathbb{P}^m(k)$ are common zeros of polynomials in $n+m+2$ variables which are *bihomogeneous*, i.e. separately homogeneous in the variables X_i and Y_j (which is stronger than homogeneity in all the variables together).

Proof:
(i) is obvious, since $\mathbb{A}^n(k) \times \mathbb{A}^m(k) = \mathbb{A}^{n+m}(k)$.

For (ii), just note that a subset C of $\mathbb{A}^n(k) \times \mathbb{P}^m(k)$ is closed iff its intersection with each of the affine pieces $\mathbb{A}^n(k) \times U_i$ where $U_i = D(Y_i) \subset \mathbb{P}^m(k)$ is closed. That is, $C \cap (\mathbb{A}^n(k) \times U_i)$ is precisely the common zero set of some polynomials $F_j(X_1, .., X_n, \frac{Y_0}{Y_i}, .., \widehat{\frac{Y_i}{Y_i}}, .. \frac{Y_m}{Y_i})$. But this implies that $(x_1, .., x_n, y_0, ..., y_m) \in C$ iff it is a zero of the i-th partial homogenisation in the last $m+1$ variables, which we may write as $\widetilde{F}_j(X_1, .., X_m, Y_0, .., Y_m)$ for each j. And conversely, if C is the common zero set of such polynomials, its intersection with $\mathbb{A}^n(k) \times U_i$ is a closed subset thereof, for each $i = 0, 1, .., m$. This proves (ii). The proof of (iii) is similar, and left as an exercise. □

Proposition 8.4.5. Let $f : X \to Y$ be a regular map of quasiprojective varieties. Then the *graph of* f, defined as :

$$\Gamma_f = \{(x, y) \in X \times Y : y = f(x)\}$$

is a closed subset of $X \times Y$.

Proof: We first claim that the diagonal in Y, defined as :

$$\Delta_Y = \{(y, y) \in Y \times Y\}$$

is closed in $Y \times Y$. For $Y = V(\mathfrak{a}) \subset \mathbb{P}^n(k)$ a closed projective set defined by the homogeneous ideal $\mathfrak{a}$, this is clear, since by (iii) of Lemma 8.4.4 above, Y is the common zero set of the bihomogenous polynomials: $F(X_0, ..., X_n)$ for $F \in \mathfrak{a}$ and the bihomogeneous polynomials $X_iY_j - Y_iX_j$ for $i,\ j = 0, 1, .., n$. For an arbitrary quasiprojective variety $Y = Y_1 \setminus Y_2$, we note that $\Delta_Y = \Delta_{Y_1} \cap (Y \times Y)$, which is a closed subset of the open subset $Y \times Y$ of $Y_1 \times Y_1$.

Now if $f : X \to Y$ is a regular map, it is easy to check that the map:

$$f \times id_Y : X \times Y \to Y \times Y$$

is also a regular map, and hence continuous. $\Gamma_f = (f \times id_Y)^{-1}(\Delta_Y)$ is therefore closed in $X \times Y$. □

8.5. **Main Theorem of Elimination Theory.** We now come to an important proposition about regular maps from projective varieties, and has to do with eliminating variables. Suppose one has some *homogeneous* polynomials $\{F_i(X_0,..,X_n)\}_{i=0}^m$, and one subjects the point $[a_0 : a_1 : .. : a_n] \in \mathbb{P}^n(k)$ to lie in some closed projective set $X \in \mathbb{P}^n(k)$. That is $[a_0 : .. : a_n]$ are subjected to some "constraints", i.e. required to be zeros of some *homogeneous* polynomials $\{g_k(X_0,..,X_n)\}_{k=1}^r$. Then one wants to know if the image points $[F_0(a_0,..,a_n) : ... : F_m(a_0,..,a_n)]$ are all the solutions to some polynomials $\{h_j(Y_0,..,Y_m)\}_{j=1}^s$. This amounts to solving the equations:

$$Y_i - F_i(X_0,..,X_n) = 0, \quad (0 \leq i \leq m)$$
$$g_k(X_0,..,X_n) = 0, \quad (1 \leq k \leq r)$$

in the form:

$$h_j(Y_0,..,Y_m) = 0, \quad (0 \leq j \leq s)$$

That is, we want to eliminate $(X_0,..,X_n)$ from the equations above, and express the general solution as relations among the Y_i's. The next proposition answers this in the affirmative.

Proposition 8.5.1 (Main Theorem of Elimination Theory)**.** Let $f : X \to Y$ be a regular map, with X a projective variety, and Y a quasiprojective variety. Then the image of f is a closed subset of Y.

Proof:

Let us say $X \subset \mathbb{P}^n(k)$ and $Y \subset \mathbb{P}^m(k)$. Since the inclusion $i : Y \to \mathbb{P}^m(k)$ is a regular (hence continuous) map, it is enough to prove it for $Y = \mathbb{P}^m(k)$. Also, note that the image of f, for $f : X \to \mathbb{P}^m(k)$, is the image of the graph Γ_f of f under the second projection:

$$p_2 : X \times \mathbb{P}^m(k) \to \mathbb{P}^m(k).$$

So, in view of the Proposition 8.4.5 above, it is enough to show that for X a closed projective set, the above projection p_2 is a closed map. Thus it is enough to show that if C is closed in $X \times \mathbb{P}^m(k)$, then $p_2(C) \cap U_i$ is closed in U_i, (where U_i is the i-th affine piece of $\mathbb{P}^m(k)$), by the Lemma 8.3.26. Since the pieces $C \cap (X \times U_i)$ are closed in $X \times U_i$, and the images of these pieces are precisely $p_2(C) \cap U_i$, we may as well just verify that the second projection:

$$p_2 : X \times \mathbb{A}^m(k) \to \mathbb{A}^m(k)$$

is a closed map, for X a closed projective set. Since the inclusion $i : X \subset \mathbb{P}^n(k)$ is a closed embedding (i.e., it is homoeomorphism onto its image, and its image is closed), it is easy to check that the inclusion $X \times \mathbb{A}^m(k) \subset \mathbb{P}^n(k) \times \mathbb{A}^m(k)$ is a closed embedding. Thus it is enough to check that the second projection:

$$p_2 : \mathbb{P}^n(k) \times \mathbb{A}^m(k) \to \mathbb{A}^m(k)$$

is a closed map. Let $C \subset \mathbb{P}^n(k) \times \mathbb{A}^m(k)$ be a closed set, defined as the common zero set of some polynomials $\{F_i(X_0,..,X_n,Y_1,..,Y_m)\}_{i=1}^r$, which are homogeneous in the X_j variables, in accordance with (ii) of Lemma 8.4.4. For each $y = (y_1,..,y_m) \in \mathbb{A}^m(k)$, let $\mathfrak{a}_y$ denote the homogeneous ideal in $k[X_0,..,X_n]$ generated by the homogeneous polynomials $F_i(X_0,.,X_n,y_1,.,y_m)$, $1 \leq i \leq r$. For convenience, denote these polynomials by $F_i(X_0,.,X_n;y)$. For each $s \geq 0$, define the set:

$$D_s = \{y = (y_1,..,y_m) \in \mathbb{A}^m(k) : \mathfrak{a}_y \not\supset I_s\}$$

Note that since $I_s \supseteq I_t$ for $t \geq s$, we have $D_t \subset D_s$ for $t \geq s$. Now, $y \in p_2(C)$ iff the zero set $V(\mathfrak{a}_y)$ is non-empty, which is true iff $\mathfrak{a}_y$ does not contain I_s for any $s \geq 0$, by the Lemma 8.2.7. Thus $p_2(C) = \cap_s D_s$. We claim that the sets D_s are closed, for s sufficiently large. This will imply that $p_2(C)$ is closed. Choose s to be greater than or equal to maximum of $\{d_j\}_{j=1}^r$ where d_j is the homogeneous X-degree d_j of F_j. It is enough to show that for such an s, the set D_s^c of all $y \in \mathbb{A}^m(k)$ such that $\mathfrak{a}_y \supseteq I_s$ is open. Enumerate all the monomials

$$\{X^I : I = (i_0,..,i_n) \text{ with } \Sigma i_j = s\}$$

as the index set Λ. Then, if $\mathfrak{a}_y \supseteq I_s$, we have relations:

$$X^I = \Sigma_{j=1}^r a_{Ij}(X_0,..,X_n;y)F_j(X_0,..,X_n;y)$$

for some elements $a_{Ij}(X_0,...,X_n;y)$ which are polynomials in the X-variables (though not necessarily in the y-variables), and which we can assume to be homogeneous of degree $s - d_j$ in the X-variables, for each $I \in \Lambda$.

Expand $F_j(X_0,..,X_n;y) = \Sigma_{|J|=d_j} F_{j,J}(y)X^J$, where $F_{j,J}$ (y) are *polynomials* in y, and expand $a_{Ij}(X_0,..,X_n;y) = \Sigma_{|K|=s-d_j} a_{Ij}^K(y)X^K$, where $a_{Ij}^K(y)$ are some k-valued functions of y. Plugging these into the above equation, we get:

$$X^I = \Sigma_{L\in\Lambda}(\Sigma_{j,|K|=s-d_j,L\geq K}\ a_{Ij}^K(y)F_{j,L-K}(y))X^L$$

where $L \geq K$ means that each entry L_k of L is greater than the entry K_k of K. This implies that:

$$\Sigma_{j,|K|=s-d_j} a_{Ij}^K(y)F_{j,L-K}(y) = \delta_{I,L} \text{ for all } I, L \in \Lambda$$

This means that the matrix A defined by $A_{jK,L}(y) := F_{j,L-K}(y)$ for $L \geq K$, and $= 0$ otherwise, with rows indexed by $\Gamma = \{jK : |K| = s - d_j\}$ and columns indexed by $L \in \Lambda$ has a left-inverse, and so is of of full rank $=N$, say. Conversely, if this matrix has a left-inverse for some y, then by reversing all the steps above we get X^I, for $I \in \Lambda$, as combinations of the $F_j(X_0,..,X_n;y)$, so that $\mathfrak{a}_y \supseteq I_s$. Thus $\mathfrak{a}_y \supseteq I_s$ iff at least one principal $N \times N$ minor of this matrix $A_{jK,L}(y)$ is non-singular. Let us denote the principal $N \times N$ minors of $A_{jK,L}(y)$ by $M_\beta(y)$, with β in some finite set S. Thus $D_s^c = \cup_{\beta\in S}\{y : \det(M_\beta(y)) \neq 0\}$. However, $\det(M_\beta(y))$ is a polynomial in the non-zero entries $F_{j,L-K}(y)$ of $A_{jK,L}(y)$. Since $F_{j,L-K}(y)$ are polynomials in y, $\det(M_\beta(y))$ is a polynomial in $y = (y_1,..,y_m)$ for all $\beta \in S$. This proves that D_s^c is open for all $s \geq \max_{j=1}^r d_j$, and the proposition. □

Remark 8.5.2. Of course, the second projection $p_2 : \mathbb{A}^n(k) \times \mathbb{A}^m(k) \to \mathbb{A}^m(k)$ is not a closed map. For example, for the map $p_2 : \mathbb{A}^1(k) \times \mathbb{A}^1(k) \to \mathbb{A}^1(k)$, the image of the closed hyperbola $V(X_1X_2 - 1)$, in $\mathbb{A}^2(k)$, is the subset $\mathbb{A}^1(k) \setminus \{0\}$, which is not closed in $\mathbb{A}^1(k)$. (Where does the above proof break down) ?

In particular, if we consider the problem of eliminating (X_1, X_2) from the equations:

$$Y = X_2$$
$$X_1X_2 - 1 = 0$$

by writing one or more polynomial relations for Y, we find that it cannot be done. We just get the rather silly result $Y \neq 0$. The homogeneity of all the polynomials being considered (i.e. the fact that we are the setting of closed projective sets as opposed to affine closed sets) is crucial to the truth of the main theorem of elimination theory.

We now have a generalisation of the Proposition 8.3.15. Namely,

Corollary 8.5.3. Let X be an irreducible projective variety, and Y an affine variety, and let $f : X \to Y$ be a regular map. Then f is a constant.

Proof: It is enough to take $X \subset \mathbb{P}^n(k)$ an irreducible closed projective set, and $Y \subset \mathbb{A}^m(k)$ an affine closed set. Since the coordinate functions $\{y_i\}_{i=1}^m$ are regular functions on Y, it is enough to prove that the components of f, namely the regular functions $f_i = y_i \circ f$, are constant. We will prove every regular map $g : X \to k$ is constant. i.e. $k[X] = k$ for an irreducible closed projective set (and hence irreducible projective variety) X.

Consider the composite $j \circ g : X \to \mathbb{P}^1(k)$ where j is the inclusion $\mathbb{A}^1(k) \subset \mathbb{P}^1(k)$ as the affine piece $U_0 = D(X_0)$. Clearly, $j \circ g$ is a regular map from X to $\mathbb{P}^1(k)$, and its image is contained in U_0, so cannot be all of $\mathbb{P}^1(k)$. By the previous proposition, it is therefore a proper closed subset of $\mathbb{P}^1(k)$. But the only proper closed subsets of $\mathbb{P}^1(k)$ are finite sets. Since the point at infinity $[0 : 1]$ is not in the image of g, we have $\operatorname{Im} g = \{a_1, ..., a_r\}$ for some $a_i \in \mathbb{A}^1(k) = U_1$. This means $X = \cup_{i=1}^r g^{-1}(a_i)$. Since $g^{-1}(a_i)$ are closed subsets of X, which is irreducible, we have $r = 1$, and $\operatorname{Im} g = \{a_1\}$, so that g is a constant map. □

The above corollary is an analogue of the Liouville theorem in complex analysis, which says that a holomorphic map on a connected compact complex manifold is a constant.

Corollary 8.5.4. Let $X \subset \mathbb{P}^n(k)$ be a quasiprojective variety. If X is a projective variety, then X is a closed subset of $\mathbb{P}^n(k)$.

Proof: Since X is a projective variety, there is a closed projective set $Y \subset \mathbb{P}^m(k)$ with regular a map $f : X \to Y$ having a regular inverse $g : Y \to X$. The composite $j \circ g$, where $j : X \subset \mathbb{P}^n(k)$ is the inclusion, is a regular map from the closed projective set to $\mathbb{P}^n(k)$, so by the foregoing proposition its image, namely X, must be closed. □

Contrast the above corollary with the affine situation, where the affine variety $\mathbb{A}^1(k) \setminus \{0\} = D(X)$ is not a closed subset of $\mathbb{A}^1(k)$.

Corollary 8.5.5. Let X be a projective variety, and Y any quasiprojective variety. Then the second projection $p_Y : X \times Y \to Y$ is a closed map.

Proof: In the beginning of the proof of Proposition 8.5.1, we showed that the second projection is closed for the case $Y = \mathbb{P}^m(k)$, which reduced to proving it for $Y = \mathbb{A}^m(k)$. For $Y \subset \mathbb{A}^m(k)$ an affine closed set, a closed subset C of $X \times Y$, by the Proposition 8.4.4, will actually be a closed subset of $X \times \mathbb{A}^m(k)$, so applying the earlier case we are done. This implies the result for Y any affine variety. Now, for Y a general quasiprojective variety, use an affine open covering, and the Proposition 8.3.26. □

Corollary 8.5.6. In the space $P^{N-1}(k)$ of all degree m hypersurfaces in $\mathbb{P}^n(k)$ described in Example 8.3.35, the reducible ones form a proper closed subset.

Proof: Let N_k denote the binomial coefficient $\binom{n+k}{k}$. Consider the map :

$$\phi_k : \mathbb{P}^{N_k-1}(k) \times \mathbb{P}^{N_{m-k}-1}(k) \to \mathbb{P}^{N_m-1}(k)$$

which maps the pair $([:\ a_J]_{|J|=k}, [:\ b_K]_{|K|=m-k})$ to $([:\ c_L]_{|L|=m})$ where $c_L = \Sigma_{J+K=L}\ a_J b_K$. This map is clearly well defined and regular. The hypersurface $V(F)$ is reducible iff the homogeneous degree m polynomial $F = \Sigma_{|L|=m} c_L X^L$ is a product of a degree k homogeneous polynomial $H = \Sigma_{|J|=k} a_J X^J$ and a degree $m-k$ homogeneous polynomial $G = \Sigma_{|K|=m-k} b_K X^K$. In other words, the point $[:\ c_L]_{|L|=m}$ representing the hypersurface $V(F)$ in $\mathbb{P}^{N_m-1}(k)$ is in the image of ϕ_k for some $k = 1, 2, ..., m-1$. But, by the Proposition 8.5.1 above, these images are all closed, and so is their union $\cup_{k=1}^{m-1}(\operatorname{Im}\phi_k)$. Since there exist irreducible hypersurfaces, the subset is proper. This proves the result. □

We close this subsection with some additional exercises.

Exercise 8.5.7. We saw in Proposition 8.5.1 that the image of a regular map from closed projective set into a projective space is a closed projective set. On the other hand, if we allow the domain to be just a quasiprojective, the image need neither be an affine nor a projective variety, indeed need not even be a quasiprojective! For example, consider the regular map:

$$\begin{aligned} f : \mathbb{A}^2(k) &\to \mathbb{P}^2(k) \\ (a, b) &\mapsto [a : ab : 1] \end{aligned}$$

Compute the image of f and show that it is not a quasiprojective in $\mathbb{P}^2(k)$.

Exercise 8.5.8. Let $X = V(X_0^2 + X_1^2 + X_2^2) \subset \mathbb{P}^2(k)$, and consider the rational map:

$$\begin{aligned} f : X &\to \mathbb{P}^1(k) \\ [a_0 : a_1 : a_2] &\mapsto [a_0^2 + a_1^2 : a_1 a_2] \end{aligned}$$

Find the largest open subset U of X on which f is regular, and compute $f(U)$.

Exercise 8.5.9. Determine the parameter space of all conics (=degree 2 hypersurfaces) in $\mathbb{P}^2(k)$ that pass through 2 distinct given points $p_1, p_2 \in \mathbb{P}^2(k)$.

9. Plane Projective Curves and Bezout's Theorem

9.1. **Plane projective Curves.**

Definition 9.1.1. We call a closed projective set $C \subset \mathbb{P}^2(k)$ a *plane projective curve* if $C = V(F)$ for F a non-zero homogeneous polynomial in $k[X_0, X_1, X_2]$ which is square free (i.e. F is a product of *distinct* irreducible factors, so that $\langle F \rangle$ is a radical homogeneous ideal of $k[X_0, X_1, X_2]$). For example, the projectivisations of all the plane affine curves discussed earlier will be plane projective curves. A plane projective curve is said to be *smooth* if all its affine pieces are smooth.

Exercise 9.1.2. Verify that a plane projective curve $V(F)$ is smooth iff the only zero of

$$\operatorname{grad} F = \left(\frac{\partial F}{\partial X_0}, \frac{\partial F}{\partial X_1}, \frac{\partial F}{\partial X_2} \right)$$

in k^3 is the point $(0, 0, 0)$. Show that a smooth plane projective curve is irreducible.

Proposition 9.1.3. Let C be a smooth irreducible plane projective curve. Then any rational map $f : C \to \mathbb{P}^n(k)$ is regular.

Proof: By definition, for $[x_0 : x_1 : x_2] \in C$, we have the representation:

$$f([x_0 : x_1 : x_2]) = [P_0(x_0, x_1, x_2) : .... : P_n(x_0, x_1, x_2)]$$

where P_i are all homogeneous polynomials of the same degree. Let us consider a point $p \in C \cap U_0$, say $p = [1 : a : b]$, and show that f is regular at p. Let $p_i(X, Y)$ be the 0-th dehomogenisations of P_i, i.e. $p_i(X, Y) = P_i(1, X, Y)$. Since the affine piece $C \cap U_0$ is smooth, we have that the polynomial functions $p_i(X, Y)$ are elements of the affine coordinate ring $A = k[C \cap U_0]$, and are certainly regular at p. By 7.3.4, there is a function $t \in A_{\mathfrak{m}_p}$ (in fact $t = x$ or y, from the proof given there) such that $p_i(x, y) = t^{d_i} u_i$ where $u_i(p) \neq 0$, $u_i \in A_{\mathfrak{m}_p}$ and x, y are the images of X, Y respectively in A. Writing $u_i = \frac{r_i(x,y)}{s_i(x,y)}$, where $r_i, s_i \in A$, we have :

$$f(x, y) := f([1 : x : y]) = [t^{d_0} r_0 s_1 s_2 .. s_n : t^{d_1} s_0 r_1 s_2 .. s_n : ... : t^{d_n} s_0 s_1 .. s_{n-1} r_n]$$

where $r_i(a, b) \neq 0$ for all i and $s_i(a, b) \neq 0$ for all i. If $d_j = \min\{d_i\}$, one can divide out by t^{d_j} throughout, and obtain:

$$f([X_0 : X_1 : X_2]) = [t^{d_0 - d_j} Q_0 : t^{d_1 - d_j} Q_1 : ... : Q_j : ... : t^{d_n - d_j} Q_n]$$

where $Q_i(X_0, X_1, X_2) := X_0^{m_i} (s_0 s_1 .. r_i .. s_n)^H$ (the superscript denoting 0-th homogenisation) and m_i is defined by:

$$m_i + \deg(s_0 s_1 .. r_i .. s_n) = m$$

where $m = \max_i\{\deg(s_0 s_1 .. r_i .. s_n)\}$. Since:

$$Q_j(p) = Q_j([1 : a : b]) = s_0(a, b) s_1(a, b) .. r_j(a, b) .. s_n(a, b) \neq 0$$

we have a representation for f at p which shows that it is regular at p. This proves the proposition. □

Corollary 9.1.4. Let $\phi : C_1 \to C_2$ be a birational equivalence between two *smooth* irreducible plane projective curves $C_i \subset \mathbb{P}^2(k)$. Then ϕ is an isomorphism.

Proof: By definition, we have a rational map $\phi : C_1 \to \mathbb{P}^2(k)$, and by the Proposition 9.1.3 above, this map is regular at all points of C_1. Similarly, $\phi^{-1} : C_2 \to \mathbb{P}^2(k)$ is regular. Since ϕ is an isomorphism of an open (and thus dense) subset U of C_1 with an open dense subset V of C_2, and ϕ being regular on C_1 makes it continuous, it follows that $\phi(C_1) = \phi(\overline{U}) \subset \overline{\phi(U)} = \overline{V} = C_2$. Similarly, $\phi^{-1}(C_2) \subset C_1$, and thus ϕ and ϕ^{-1} are regular inverses of each other and C_1 and C_2 are isomorphic curves. □

Corollary 9.1.5. The projectivised elliptic curve $X = V(y^2 z - x(x^2 - z^2)) \subset \mathbb{P}^2(k)$ is not a rational curve, i.e., is not birationally equivalent to $\mathbb{P}^1(k)$. In particular it is not birationally equivalent to the projectivised cubic cusp $V(y^2 z - x^3)$ or the cubic node $V(y^2 z - x^2(x - z))$.

Proof: By the Corollary 9.1.4 above, if X were birationally equivalent to $\mathbb{P}^1(k)$, it would be isomorphic to it, since X is easily checked to be a smooth curve. In that case, the affine piece $X_0 = V(y^2 - x(x^2-1)) = X \setminus \{[0:1:0]\}$ of X would be isomorphic to $\mathbb{P}^1(k) \setminus \{p\} = \mathbb{A}^1(k)$ (where the point $p := \phi([0:1:0])$). We saw in the Example 7.3 that the coordinate ring of X_0 is not a UFD, whereas that of $\mathbb{A}^1(k)$ is $k[x]$, which is a UFD. Thus X_0 cannot be isomorphic to $\mathbb{A}^1(k)$, and X cannot be birationally equivalent with $\mathbb{P}^1(k)$.

Since the projectivised cubic cusp and projectivised cubic node are birationally equivalent to $\mathbb{P}^1(k)$, it follows that X cannot be birationally equivalent to either of these curves. □

9.2. **The resultant of two polynomials.**

Lemma 9.2.1 (The Resultant)**.** Let $p(z) = \sum_{i=0}^{n} a_i z^i$ and $q(z) = \sum_{i=0}^{m} b_i z^i$ be two polynomials of degrees n and m respectively, in $k[z]$ where k is algebraically closed as always. Then p and q have a common root if and only if the $(m+n) \times (m+n)$ *resultant* defined as:

$$R(p,q) := \det \begin{bmatrix} a_0 & a_1 & .. & a_n & 0 & 0 & .. & 0 \\ 0 & a_0 & a_1 & .. & a_n & 0 & .. & 0 \\ 0 & 0 & a_0 & a_1 & .. & a_n & .. & 0 \\ .. & .. & .. & .. & .. & .. & .. & .. \\ 0 & 0 & 0 & .. & a_0 & a_1 & .. & a_n \\ b_0 & b_1 & .. & .. & b_{m-1} & b_m & .. & 0 \\ 0 & b_0 & b_1 & .. & b_{m-2} & b_{m-1} & b_m & 0 \\ 0 & 0 & b_0 & b_1 & .. & b_m & .. & 0 \\ .. & .. & .. & .. & .. & .. & .. & .. \\ 0 & 0 & 0 & .. & b_0 & b_1 & .. & b_m \end{bmatrix}$$

(with the first m rows of a's and the last n-rows of b's) is 0.

Proof: Let λ be a common root of p and q. Then, factorising out $(z-\lambda)$, we have two polynomials p_1 (resp. q_1) of degrees $(n-1)$ (resp. $(m-1)$) satisfying:

$$p(z) = (z-\lambda)p_1(z); \quad q(z) = (z-\lambda)q_1(z)$$

so that $p_1(z)q(z) = q_1(z)p(z)$, upon eliminating $(z-\lambda)$. Conversely, if there exist p_1, q_1 of degrees $(n-1)$ and $(m-1)$ respectively, satisfying $p_1(z)q(z) = q_1(z)p(z)$, then we may cancel out common linear factors of p_1 and q_1 and assume they are coprime of degrees $\leq (n-1)$ and $\leq m-1$ respectively. Thus we have have:

$$\begin{aligned} \frac{p(z)}{p_1(z)} &= \frac{q(z)}{q_1(z)} \\ &= \text{a polynomial of degree } \geq 1 = \text{(say) } (az+b)r(z) \end{aligned}$$

and since $a \neq 0$, we get $p(z) = (az+b)r(z)p_1(z)$ and $q(z) = (az+b)r(z)q_1(z)$ have the common root $\lambda = -b/a$.

Now let us write $p_1(z) = \sum_{i=0}^{n-1} c_i z^i$ and $q_1(z) = \sum_{i=0}^{m-1} d_i z^i$. We substitute this into the relation $p_1(z)q(z) = p(z)q_1(z)$, and equate coefficients to obtain:

$$\begin{aligned} c_0 b_0 = a_0 d_0 &\Rightarrow a_0(-d_0) + b_0 c_0 = 0 \\ c_0 b_1 + c_1 b_0 = a_0 d_1 + a_1 d_0 &\Rightarrow a_0(-d_1) + a_1(-d_0) + b_0 c_1 + b_1 c_0 = 0 \\ .... \quad .. \quad .... & \end{aligned}$$

and so on. These $(m+n)$ equations can be written in matrix form as:

$$[-d_0,...,-d_{m-1},c_0,..,c_{n-1}]\begin{bmatrix} a_0 & a_1 & .. & a_n & 0 & 0 & .. & 0 \\ 0 & a_0 & a_1 & .. & a_n & 0 & .. & 0 \\ 0 & 0 & a_0 & a_1 & .. & a_n & .. & 0 \\ .. & .. & .. & .. & .. & .. & .. & .. \\ 0 & 0 & 0 & .. & a_0 & a_1 & .. & a_n \\ b_0 & b_1 & .. & .. & b_{m-1} & b_m & .. & 0 \\ 0 & b_0 & b_1 & .. & b_{m-2} & b_{m-1} & b_m & 0 \\ 0 & 0 & b_0 & b_1 & .. & b_m & .. & 0 \\ .. & .. & .. & .. & .. & .. & .. & .. \\ 0 & 0 & 0 & .. & b_0 & b_1 & .. & b_m \end{bmatrix} = 0$$

Clearly, this system of linear equations has a non-zero solution for the vector $(-d_0,...,-d_{m-1},c_0,..,c_{n-1})$ iff the matrix on the right, viz. is singular. This happens iff its determinant $R(p,q)=0$. The lemma follows. □

Corollary 9.2.2. Let $p(z)=\sum_{i=0}^{n} a_i z^i$ be a polynomial of degree n, with $a_n \neq 0$. Then $p(z)$ has a repeated root iff a polynomial $\Delta(p)$, which is a polynomial in the a_i vanishes. $\Delta(p)$ is called the *discriminant of p.*

Proof: It is easy to see that $p(z)$ has a repeated root iff $p(z)$ and its derivative $p'(z)=\sum_i i a_i z^{i-1}$ have a common root. Thus p has a repeated root iff the resultant $R(p,p')=0$. This is clearly a polynomial in the a_i's. As an exercise, the reader may wish to compute the discriminants of quadratic and cubic polynomials. □

Corollary 9.2.3. Suppose $f=\sum_{i=0}^{n} a_i z^i$ and $g=\sum_{i=0}^{m} b_i z^i$ are two polymomials in $k[x,y,z]$ such that $a_i=a_i(x,y)$ is a homogeneous polynomial in x,y of degree $(n-i)$, and $b_i=b_i(x,y)$ is homogeneous of degree $(m-i)$. Then if $R(f,g)\not\equiv 0$, it is a homogenous polynomial $R(x,y)$ in x,y of degree nm.

Proof: The homogeneity hypotheses of a_i and b_i imply that $a_i(tx,ty)=t^{n-i}a_i(x,y)$ and $b_i(tx,ty)=t^{m-i}b_i(x,y)$. The determinant expression for $R(tx,ty)$, is therefore:

$$\det\begin{bmatrix} t^n a_0(x,y) & t^{n-1}a_1(x,y) & .. & a_n(x,y) & 0 & 0 & .. & 0 \\ 0 & t^n a_0(x,y) & t^{n-1}a_1(x,y) & .. & a_n & 0 & .. & 0 \\ 0 & 0 & t^n a_0(x,y) & t^{n-1}a_1(x,y) & .. & a_n(x,y) & .. & 0 \\ .. & .. & .. & .. & .. & .. & .. & .. \\ 0 & 0 & 0 & .. & t^n a_0(x,y) & t^{n-1}a_1(x,y) & .. & a_n(x,y) \\ t^m b_0(x,y) & t^{m-1}b_1(x,y) & .. & .. & tb_{m-1} & b_m & .. & 0 \\ 0 & t^m b_0(x,y) & t^{m-1}b_1(x,y) & .. & t^2 b_{m-2}(x,y) & tb_{m-1} & b_m & 0 \\ 0 & 0 & t^m b_0(x,y) & t^{m-1}b_1(x,y) & .. & b_m(x,y) & .. & 0 \\ .. & .. & .. & .. & .. & .. & .. & .. \\ 0 & 0 & 0 & .. & t^m b_0(x,y) & t^{m-1}b_1(x,y) & .. & b_m(x,y) \end{bmatrix}$$

If we multiply the first row by t^{-n}, the second by t^{-n-1},..,the m-th now by t^{-n-m+1}, the $(m+1)$-st row again by t^{-m}, the $(m+2)$-nd by t^{-m-1} ..., the $(m+n)$-th row by t^{-m-n+1}, then we will have a common factor of t^{-1} from the second column, of t^{-2} from the third, and a factor of t^{-m-n+1} from the last column. Thus we have:

$$t^{-[(n+(n+1)+...+(n+m-1)+(m+(m+1)+...+(m+n-1)]}R(tx,ty)=t^{-1-2+...-(m+n-1)}R(x,y)$$

That is

$$t^{-\frac{1}{2}[m(2n+m-1)+n(2m+n-1)]}R(tx,ty)=t^{-\frac{1}{2}[(m+n)(m+n-1)]}R(x,y)$$

which implies that $t^{-mn}R(tx,ty)=R(x,y)$, i.e. that $R(tx,ty)=t^{mn}R(x,y)$. Thus R is homogenous of degree mn in (x,y), and the corollary follows. □

Now we can prove Bezout's Theorem.

Theorem 9.2.4 (Bezout's Theorem)**.** Let C and D be two projective plane curves, and assume that C and D have no irreducible components in common. Then if C has degree n (i.e. $C = V(F)$ where $F(X_0, X_1, X_2)$ is an n-form), D is of degree m, the set $C \cap D$ is a finite set of cardinality nm, provided each point of intersection is counted with its multiplicity (to be explained in the proof).

Proof: First note that if $C = V(f)$ and $D = V(g)$ are distinct irreducible *affine* plane curves in $\mathbb{A}^2(k)$, then $f(x, y)$ and $g(x, y)$ are not scalar multiples of each other. Write $f(x, y) = \sum_{i=0}^{n} a_i(x)y^i$ with $a_n(x) \neq 0$, and $g(x, y) = \sum_{i=0}^{m} b_i(x)y^i$ with $b_m(x) \neq 0$. If $(\lambda, \mu) \in C \cap D$, it follows that the 1-variable polynomials $f(\lambda, y)$ and $g(\lambda, y)$ have the common root μ. Thus, from the Lemma9.2.1 it follows that the resultant $R(f(\lambda, -), g(\lambda, -)) = 0$. If we consider the polynomial in x defined by $G(x) := R(f(x, -), g(x, -))$, this polynomial G is not identically zero since $C \neq D$, and hence has only finitely many roots. For each of these finitely many roots λ_i, there are only finitely many common roots of $f(\lambda_i, -)$ and $g(\lambda_i, -)$. Thus $C \cap D$ is a finite set.

Now if C and D are any two affine plane curves with no irreducible components in common, then the cardinality of $C \cap D$ is bounded by the sum of the cardinalities of $C_i \cap D_j$, where C_i and D_j are the irreducible components of C and D respectively. And for each i, j, since $C_i \neq D_j$, we have that $C_i \cap D_j$ is a finite set, by the last paragraph, so $C \cap D$ is also finite.

Finally, if C and D are two plane projective curves, with no common irreducible components, then by applying the above affine case to the affine plane curves $U_i \cap C$ and $U_i \cap D$, we find that $C \cap D$ is a finite set. Define $S := C \cap D$.

By a *line* in $\mathbb{P}^2(k)$, we mean a linear subspace of the kind $V(F)$, where $F \neq 0$ is a 1-form. Since both C and D have finitely many irreducible components, we may choose a line L such that L is not an irreducible component of either C or D.

Given any pair p, q of distinct points in $\mathbb{P}^2(k)$, there is a unique line containing both p and q. Consider the lines L_{pq} joining $p, q \in S$ for $p \neq q$, and note that these are finitely many lines. We can choose a point P such that P does not lie on L, does not lie on C, does not lie on D, and also does not lie in L_{pq} for each pair of points $p, q \in S$ with $p \neq q$. We can define a coordinate system (X_0, X_1, X_2) (by a linear change of coordinates if necessary) so that $P = [1 : 0 : 0]$, and $L = V(X_0)$.

Now let us write:

$$\begin{aligned} F(X_0, X_1, X_2) &= a_0(X_1, X_2) + a_1(X_1, X_2)X_0 + ... + a_n(X_1, X_2)X_0^n \\ G(X_0, X_1, X_2) &= b_0(X_1, X_2) + b_1(X_1, X_2)X_0 + ... + b_m(X_1, X_2)X_0^m \end{aligned}$$

where $a_i(X_1, X_2)$ is homogeneous of degree $(n-i)$ and $b_i(X_1, X_2)$ is homogeneous of degree $(m-i)$. Thus we are in the setting of the Corollary 9.2.3. Note that if the scalar $a_n = 0$, then since $a_i(0, 0) = 0$ for $0 \leq i \leq (n-1)$, we would have $P = [1 : 0 : 0]$ in C, contrary to the choice of P. Hence $a_n \neq 0$. Similarly $b_m \neq 0$, so F and G are polynomials of degree n and m in the first variable X_0. Again, if $a_0 \equiv 0$, we would have $L = V(X_0)$ becoming an irreducible component of C, which contradicts the choice of L. So $a_0 \not\equiv 0$. Similarly $b_0 \not\equiv 0$.

Now consider the resultant $R(X_1, X_2) = R(F(-, X_1, X_2), G(-, X_1, X_2)$. If this were identically zero, then for every choice of $(a, b) \neq (0, 0)$, we would have that there exists a common root $\lambda(a, b)$ of $F(-, a, b)$ and $G(-, a, b)$. This gives infinitely many points $[\lambda(a, b) : a : b] \in C \cap D$, contradicting that $C \cap D$ is a finite set.

Thus, by the Corollary 9.2.3, $R(X_1, X_2)$ is a non-zero homogeneous polynomial of degree nm, and for each $[c : a : b] \in C \cap D = S$, we first observe that $(a, b) \neq (0, 0)$, since $[c : 0 : 0] = [1 : 0 : 0] = P \notin C \cap D$. Thus for each $[c : a : b] \in S$, we have $[a : b] \in \mathbb{P}^1(k)$ is a point on $V(R)$, by the Lemma9.2.1. Thus we have defined a map $\tau : S \to V(R)$ which takes $[c : a : b] \in S$ to $[a : b] \in V(R)$.

This map τ is surjective, for if the point $[a : b] \in \mathbb{P}^1(k)$ is a point on $V(R)$, then $F(-, a, b)$ and $G(-, a, b)$ have a common root c, and $[c : a : b] \in S$, again by Lemma 9.2.1. Then $\tau([c : a : b]) = [a : b]$.

Finally, τ is injective. For if there are two distinct points $p = [c_1 : a : b]$ and $q = [c_2 : a : b]$ which lie in $S = C \cap D$, we have that $p \neq q$, and the line L_{pq} is the line $V(aX_2 - bX_1)$. Since the point $P = [1 : 0 : 0]$

clearly satisfies the equation $aX_2 - bX_1 = 0$, we have that $P \in L_{pq}$, contrary to choice of P. Thus the map $\tau : S \to V(R)$ defined by $[c : a : b] \mapsto [a : b]$ is a bijection of sets.

Now since $R(X_1, X_2)$ is a non-zero homogeneous polynomial of degree nm, $V(R) \subset \mathbb{P}^1(k)$ has exactly nm points, where each point is counted with its multiplicity. Associate to the point $p = [c : a : b] \in S$ the multiplicity of $[a : b]$ as a root of R. Then, by the last para, the cardinality of S, counting each point with this multiplicity, is exactly nm. Hence the proposition. □

Remark 9.2.5. We note that the proof above associated to each point in $S = C \cap D$ the multiplicity of a certain corresponding point in $V(R)$ after a choice of good coordinate system was made. It is not clear that these multiplicities are independent of the choice of coordinate system. There are both algebraic and topological ways of defining these multiplicities which establish their independence of the choice of coordinate system. For details, the reader may look up the proof of the general Bezout Theorem given in the chapter on intersection theory in Shafarevich's *Basic Algebraic Geometry*. We will return to this point soon.

Corollary 9.2.6. Every projective plane curve C intersects every other projective plane curve D. If C is a line in the projective plane, then either C is an irreducible component of D, or intersects it in at most m points.

Proof: If C and D are two projective plane curves of degrees n and m respectively, then if they have a common irreducible component, they cetainly intersect. If they don't have a common irreducible component, by the Bezout theorem above, the cardinality of their intersection counted with multiplicity, is nm, and hence non-zero. If C is line, it is a projective plane curve $V(F)$ where F is a degree 1 polynomial, so of degree 1, and hence C is irreducible. Hence it is either an irreducible component of D, or meets it in at most m points. □

Example 9.2.7. If $L_i = V(a_iX_0 + b_iX_1 + c_iX_2)$ with $(a_i, b_i, c_i) \neq (0, 0, 0)$ and $i = 1, 2$ are two distinct lines in $\mathbb{P}^2(k)$, they intersect in the unique point

$$[b_1c_2 - b_2c_1 : a_2c_1 - a_1c_2 : a_1b_2 - a_2b_1]$$

Note that all three of the homogeneous coordinates above cannot be zero since we have assumed L_1 and L_2 to be distinct lines.

9.3. **Multiplicity of a point on a plane curve.** We now define an important geometric notion for a point on a plane curve. It is enough to look at plane affine curves to define this notion, and then carry it over to projective plane curves by looking at affine pieces.

Let $f(x, y)$ be a polynomial in $k[x, y]$, of degree m. Assume that $f(0, 0) = 0$, and let $P = (0, 0)$ be the origin of $\mathbb{A}^2(k)$. Thus the curve $V(f)$ passes through P. Let us write f as:

$$f(x, y) = f_1(x, y) + f_2(x, y) + ... + f_m(x, y)$$

where f_i is a homogeneous polynomial of degree i. Note $f_0 = 0$ since $f(0, 0) = 0$.

Now let $L := L_{(a,b)} = \{(ta, tb) : t \in k\}$ be any line passing through the origin in $\mathbb{A}^2(k)$, where $(a, b) \neq (0, 0)$. We substitute $x = ta$ and $y = tb$ in $f(x, y) = 0$ to get the equation:

$$f(ta, tb) = tf_1(a, b) + t^2f_2(a, b) + ... + t^mf_m(a, b)$$

We define:

Definition 9.3.1. The *order of contact* of the line $L_{(a,b)}$ with the curve $C := V(f)$ at the origin P is defined to be the highest power of t dividing $f(ta, tb)$. It is clearly equal to d, where d is the smallest j for which $f_j(a, b) \neq 0$. We will denote it as $o_P(L, C)$. If a line L does not pass through P, we set $o_P(L, C) = 0$. Note that by definition, $0 \leq o_P(L, C) \leq m$ for any line $L = V(ax + by + c)$ in $\mathbb{A}^2(k)$.

Finally, we define the *multiplicity of* P on C to be:

$$m_P(C) = \inf\{o_P(L, C) : \ L \text{ is a line passing through } \ P\}$$

Again, by definition $1 \leq m_P(C) \leq m$. If P is a point with $m_P(C) = 1$, we say P is a *simple point* on C, if it is 2, a *double point* and in the extreme case it is m, an *m-ple point.*

What we are doing in defining the multiplicity is viewing the line L through P as affine 1-space $\mathbb{A}^1(k)$, and regarding the restriction of the polynomial $f(x, y)$ to L as a regular function on L, and taking the order of the zero of this regular function at $P \in L$.

Remark 9.3.2.

(i): If $P = (c, d)$ is not the origin, but some other point on C, we can again define the order of contact of a line through P with C, and the multiplicity of P on C, by a translation of coordinates. That is, substitute $x = c + ta$, $y = d + tb$ in the equation $f(x, y) = (0, 0)$, and again look at the highest power of t which factors out of the resulting polynomial of degree m in t, etc.

(ii): If C is a plane projective curve in $\mathbb{P}^2(k)$, and P is a point on C, we again define for a line L in $\mathbb{P}^2(k)$ through P the order of contact $o_P(L, C)$ by taking an affine piece $C_i := C \cap U_i$ of C in which P lies, and similarly $L_i := L \cap U_i$ (where $U_i = \{[X_0 : X_1 : X_2] \in \mathbb{P}^2(k) : \ X_i \neq 0\}$), and setting $o_P(L, C) = o_P(L_i, C_i)$. Similarly, define $m_P(C) = m_P(C_i)$. Again it is easy to check that these definitions do not depend on which affine piece containing P we choose.

Example 9.3.3. For example let us consider the three affine cubics we encountered in §7. For $P = (0, 0)$ on $C = V(y^2 - x^3)$, we note that every line $L = L_{(a,b)} = \{(ta, tb) : t \in k\}$ with $b \neq 0$ has $o_P(L, C) = 2$. When $b = 0$, the line is the x-axis $V(y)$, and for this line $o_P(L, C) = 3$. Thus $m_P(C) = 2$. All other points $P \neq (0, 0)$ on C have $m_P(C) = 1$. For the node $V(y^2 - x^2(1 + x))$, and $P = (0, 0)$, the $f(ta, tb) = t^2(b^2 - a^2 - a^3t)$. Thus if $b \neq \pm a$, we have $o_P(L_{(a,b)}, C) = 2$. On the other hand, for $L = L_{(a,\pm a)}$, $a \neq 0$, we have $o_P(L, C) = 3$. Again $m_P(C) = 2$, and for all $P \neq (0, 0)$, we have $m_P(C) = 1$. Finally for the elliptic curve $V(y^2 - x(x^2 - 1))$, we leave it to the reader to see that $m_P(C) = 1$ for all $P \in C$. At each of these points $P \in C$, there is exactly one line (the tangent line at P) whose order of contact with C at P is ≥ 2, and all other lines through P have order of contact 1 at P.

Proposition 9.3.4. Let $P \in C$, where C is an affine or projective plane curve. Then $m_P(C) = 1$ (i.e. P is a simple point on C) iff P is a smooth point on C. In this case there is a unique line L through P whose order of contact at P is ≥ 2, and this line is the tangent to C at P. If P is a simple point and the order of contact of the tangent line at P to C is ≥ 3, we call P a point a *point of inflexion* on C.

Proof: We will just do the affine case, since the projective case follows from the affine case by the definitions. As before, we may assume $P = (0, 0) \in C = V(f)$, and write:

$$f = tf_1(a, b) + t^2 f_2(a, b) + ... + t^m f_m(a, b)$$

If $m_P(C) = 1$, there is a line $L_{(a,b)} = \{(ta, tb) : t \in k\}$ which has order of contact 1 with C at $(0, 0)$. That is $f_1(a, b) \neq 0$. But in the linear term $f_1(x, y) = \alpha x + \beta y$ of f, we have $\alpha = \frac{\partial f}{\partial x}(0, 0)$ and $\beta = \frac{\partial f}{\partial y}(0, 0)$. Thus

$$f_1(a, b) = \alpha a + \beta b = \frac{\partial f}{\partial x}(0, 0)\, a + \frac{\partial f}{\partial y}(0, 0)\, b \neq 0$$

implies that $(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y})(0, 0) \neq (0, 0)$, and $P = (0, 0)$ is a smooth point on C. Further, if for some line $L = L_{(a,b)}$ we have $o_P(L, C) \geq 2$, it will follow that for this (a, b) we have $f_1(a, b) = \frac{\partial f}{\partial x}(0, 0)\, a + \frac{\partial f}{\partial y}(0, 0)\, b = 0$, which

implies that $L_{(a,b)}$ is the tangent line to C at $(0,0)$ from elementary calculus. It is unique because it is defined by the equation $\frac{\partial f}{\partial x}(0,0)\,x + \frac{\partial f}{\partial y}(0,0)\,y = 0$.

Conversely, if $m_P(C) \geq 2$, then for every line $L_{(a,b)}$ through $P = (0,0)$, we have order of contact $o_P(L_{(a,b)}, C)$ greater than or equal to 2, so that $f_1(a,b) = a\frac{\partial f}{\partial x}(0,0) + b\frac{\partial f}{\partial y}(0,0) = 0$ for all $(a,b) \neq (0,0)$, which clearly implies that $(\text{grad}\, f)(0,0) = (\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y})(0,0) = (0,0)$ and hence $P = (0,0)$ is a singular point on C. This proves the proposition. □

Corollary 9.3.5. If C is smooth affine plane curve, then all of its irreducible components are pairwise disjoint. If C is a smooth projective plane curve, then it is irreducible.

Proof: Let $C = V(f)$ be an affine plane curve, and let $P \in C_1 \cap C_2$, where $C_1 = V(g)$ and $C_2 = V(h)$ are two intersecting irreducible components of C. Then we have f is divisible by gh (by the UFD property of $k[x,y]$), and for any line L through P, we will have $o_P(L,C) \geq o_P(L,C_1) + o_P(L,C_2)$. From this it follows that $m_P(C) \geq m_P(C_1) + m_P(C_2)$. Since $P \in C_1$ and $P \in C_2$, we have $m_P(C_i) \geq 1$ for $i = 1,2$, so that $m_P(C) \geq 2$. By the previous Proposition 9.3.4 P is a singular point on C.

If C is a projective plane curve with any pair of distinct irreducible components C_1 and C_2, by the Corollary 9.2.6, they must intersect nontrivially. Take P in this intersection, an affine open U_i containing P, and apply the above affine case to the i-th affine pieces of C_1 and C_2 to conclude that C must be singular at P. □

Proposition 9.3.6. Let L be any line in $\mathbb{P}^2(k)$, and $C = V(F)$ be a projective plane curve, where deg $F = m$. Then, if L is not an irreducible component of C, we know by Bezout that $C \cap L = \{P_1, .., P_s\}$. In this event, $\sum_{i=1}^{s} o_{P_i}(L,C) = m$. Also we have $\sum_{i=1}^{s} m_{P_i}(C) \leq m$.

Proof: That the intersection $C \cap L$ is a finite set follows from Bezout's theorem 9.2.4, since we are assuming that L is not an irreducible component of C. By a linear change of coordinates assume that this line is $L = V(X_0)$. Thus X_0 does not divide F. Then it is obvious that the resultant of $F = \sum_{i=0}^{m} a_i(X_1, X_2)X_0^i$ and $G = X_0$ is the determinant of the $(m+1) \times (m+1)$ matrix:

$$\begin{bmatrix} a_0 & a_1 & .. & a_m & 0 \\ 0 & 1 & 0 & 0.. & 0 \\ 0 & 0 & .. & 0 & 0 \\ .. & .. & .. & .. & .. \\ 0 & 0 & 0 & .. & 1 \end{bmatrix}$$

since $b_0 = 0$ and $b_1 = 1$ in the notation of Corollary 9.2.3. But this determinant is precisely $a_0(X_1, X_2)$, which is the homogeneous degree m polynomial $F(0, X_1, X_2)$.

In the proof of the Bezout theorem, we had seen that $\sum_{i=0}^{s} \nu(P_i) = m$, where $\nu(P_i)$ is the multiplicity of the root (a_i, b_i) in the resultant above, for each $P_i = [0 : a_i : b_i]$. But since the resultant is $F(0, X_1, X_2)$, we have that $\nu(P_i) = o_{P_i}(L,C)$, where $L = V(X_0)$. This proves that $\sum_i o_{P_i}(L,C) = m$. The inequality of the last statement follows from the fact that $o_{P_i}(L,C) \leq m_{P_i}(C)$ for each i by definition. The proposition follows. □

Remark 9.3.7. As one would expect, the first (equality) part of the proposition above is *false* for affine plane curves. For example, if we look at $C = V(y^2 - x^3)$, and consider its intersection with the line $L = V(x)$ which is the $y - axis$, we have L meeting C only at $P = (0,0)$, and also putting $(x,y) = (0,t)$ a general point on L into $f(x,y) = y^2 - x^3$ gives t^2, so that the sum on the left side is $o_P(L,C) = 2$. On the other hand $m = 3$.

If we projectivise this curve to $C = V(Y^2Z - X^3)$, we find that the projectivisation of the line $x = 0$ is the line $X = 0$ in $\mathbb{P}^2(k)$. Another point $Q = [0 : 1 : 0]$ in the hyperplane at infinity $V(Z)$ occurs in $C \cap L$. At this point, one checks that the order of contact is 1, and now we have $o_P(L,C) + o_Q(L,C) = 2 + 1 = 3$. All part of the magic of projective space!

Finally, we note that the second inequality of the Proposition 9.3.6 can be a strict one, even in projective space. For if L is a line tangent to C at say P_1, and P_1 is a smooth point on C, we will have $o_{P_1}(L, C) \geq 2$ which is strictly greater than $m_{P_1}(C) = 1$, since P_1 is a smooth point.

Corollary 9.3.8. Let $C = V(F)$ be a plane projective curve of degree m (viz. $\deg F = m$). Then the number of singular points on C is finite. If $m = 1$, C has no singular points. If $m = 2$, C can have at most one singular point, and in that case C is a pair of intersecting straight lines and their point of intersection is the only singularity. If $m = 3$, and C is irreducible, then again C can have at most one singular point.

Proof: Let $C = \cup_{i=1}^{r} C_i$ be the irredundant decomposition of C into its irreducible components. From the Proposition 9.3.4, a point $P \in C$ is singular iff $m_P(C) \geq 2$. If P is a point of C_i which is not on any other $C_j \neq C_i$, then $m_P(C) = m_P(C_i)$, so that P is a singular point of C_i. On the other hand, if $P \in C_i \cap C_j$ for $i \neq j$, we have seen in the Corollary 9.3.5 that P is a singular point. Thus we have that the set $\Sigma(C)$ of C is the union of the singular points $\Sigma(C_i)$ and the union of $C_i \cap C_j$ for $i \neq j$. The second set is finite by Bezout's Theorem. So we are reduced to showing that for an irreducible plane projective curve C, its singular set $\Sigma(C)$ is finite. So if $C = V(F)$, with F irreducible, we consider the polynomials $G_i := \frac{\partial F}{\partial X_i}$ for $i = 0, 1, 2$. All of them cannot be identically 0, because that would mean $F \equiv 0$. So say $G_0 \not\equiv 0$, and is homogeneous of degree $m - 1$. Since F is irreducible, $V(G_0)$ and $C = V(F)$ have no common irreducible components. By Bezout $C \cap V(G_0)$ is a finite set. Since the set of singular points of C is the set $C \cap V(G_0) \cap V(G_1) \cap V(G_2) \subset C \cap V(G_0)$, we have that this set is finite. This proves the first part of the proposition.

Clearly if $m = 1$, every point P of C has multiplicity $1 \leq m_P(C) \leq m = 1$, and thus by Proposition 9.3.4, every point on it is smooth.

If $m = 2$, then there are two cases. In the first, when C is reducible, i.e. the degree 2 polynomial F defining $C = V(F)$ is reducible, we have that F must be a product of two distinct degree 1 polynomials. Thus $C = L_1 \cup L_2$ is the union of two distinct lines, these lines must intersect exactly at one point, by Example 9.2.7, so that C is a pair of straight lines intersecting at a point.

If $m = 2$, and C is irreducible, we claim that C must be smooth. For let $P \in C$ is any point of C. Let Q be another point of C, with $P \neq Q$. Clearly there is a line L passing through P and Q, and since C is irreducible, L is not an irreducible component of C. We know by Bezout that the set $L \cap C$ can have cardinality at most 2, so that $L \cap C = \{P, Q\}$. By the second part of the Proposition 9.3.6 that $m_P(C) + m_Q(C) \leq 2$. However, since both $m_P(C)$ and $m_Q(C)$ are ≥ 1 by definition, they are both exactly one. By Proposition 9.3.4, P is a simple point. Since P is arbitrary, C is smooth. In fact, a little linear algebra and changes of coordinates shows that we can express $F(X_0, X_1, X_2) = \sum_{i=0}^{2} X_i^2$ (we are assuming k algebraically closed, and $\operatorname{char} k = 0$ here).

In the case $m = 3$, and C irreducible, let there be two singular points P and Q in C, if possible. Then the line L joining P and Q is not an irreducible component of C, since C is irreducible. By the second inequality of 9.3.6, it follows that $m_P(C) + m_Q(C) \leq 3$. If P and Q are both singular points, then by 9.3.4, we have both $m_P(C)$ and $m_Q(C) \geq 2$, which is a contradiction. The proposition follows. □

9.4. **Points of Inflexion.** From now on, for the rest of this section, we will assume that k is algebraically closed and of characteristic zero. Our aim is to completely classify plane projective curves of degree ≤ 3. We first need a criterion to determine when a point on a smooth curve is a point of inflexion.

Proposition 9.4.1. Let $C = V(F) \in \mathbb{P}^2(k)$ be a plane projective curve, with $F(X, Y, Z) \in k[X, Y, Z]$ a homogeneous polynomial of degree $m \geq 1$. Let $P \in C$ be a smooth point of C. Then P is a point of inflexion iff the determinant of the hessian matrix at P defined by:

$$H_P(F) := \det \begin{bmatrix} F_{XX}(P) & F_{XY}(P) & F_{XZ}(P) \\ F_{YX}(P) & F_{YY}(P) & F_{YZ}(P) \\ F_{ZX}(P) & F_{ZY}(P) & F_{ZZ}(P) \end{bmatrix}$$

is zero. (Here $F_{XX}(P)$ denotes $\frac{\partial^2 F}{\partial X^2}(P)$ etc.).

Proof: We recall from the Proposition 9.3.4 that P is a point of inflexion if it is a smooth (=simple $\Leftrightarrow$ $m_P(C) = 1$) point, and if the tangent line L at P has order of contact $o_P(L, C) \geq 3$.

It is an easy exercise to check that if we make a linear change of coordinates $(X, Y, Z) \mapsto A(X, Y, Z) =: (X_1, Y_1, Z_1)$ where $A \in GL(3, k)$ is a nonsingular (3×3) matrix, then the old coordinate partials are related to the new ones by

$$\frac{\partial}{\partial X} = A_{11}\frac{\partial}{\partial X_1} + A_{21}\frac{\partial}{\partial Y_1} + A_{31}\frac{\partial}{\partial Z_1}$$

and so on, so that the old hessian determinant is related to the new one by $H_P(F) = (\det A)^2 H_{P_1}(F_1)$, where $F_1(X_1, Y_1, Z_1) = F(X, Y, Z)$. Since A is nonsingular, $H_P(F) = 0$ iff $H_{P_1}(F_1) = 0$, where $P_1 = A.P$. Thus we may linearly change coordinates and assume that the point $P = [0 : 0 : 1]$, and the tangent line is $L = V(Y)$. We may also ensure that Z is so chosen that $V(Z)$ is not an irreducible component of C.

The affine piece of the curve $C_2 := C \cap U_2$ is defined by the dehomogenisation $f(x, y)$ of $F(X, Y, Z)$ by setting $Z = 1$. That is $f(x, y) = F(X, Y, 1)$. The point $P = [0 : 0 : 1] \in C \cap U_2$ is a smooth point of C, so the point $Q = (0, 0) \in V(f)$ is a smooth point of $C_2 = V(f)$, by definition. The affine piece $L_2 = L \cap U_2$ of the line L is the line $L \cap U_2 = V(y)$, the x-axis. Now, by the fact that L_2 is tangent to $C_2 = V(f)$ at $(0, 0)$, we have that:

$$f(x, y) = \alpha y + f_2(x, y) + ... + f_m(x, y)$$

where $\alpha \in k$ and $\alpha \neq 0$ by the fact that $(0, 0)$ is a smooth point, and f_d is homogeneous of degree d in x, y. Thus we have, on homogenisation, and the fact that $V(Z)$ is not an irreducible component of C, that

$$F(X, Y, Z) = \alpha Z^{m-1}Y + Z^{m-2}f_2(X, Y) + ... + f_m(X, Y)$$

and that $f_m(X, Y) \not\equiv 0$. Now one can calculate:

$$\begin{aligned}
F_{XX}(0,0,1) &= f_{2,XX}(0,0) + ...f_{m,XX}(0,0) = f_{xx}(0,0) \\
F_{XY}(0,0,1) &= F_{YX}(0,0,1) = f_{2,XY}(0,0) + .. + f_{m,XY}(0,0) = f_{xy}(0,0) \\
F_{YY}(0,0,1) &= f_{2,YY}(0,0) + ... + f_{m,YY}(0,0) = f_{yy}(0,0) \\
F_{XZ}(0,0,1) &= F_{ZX}(0,0,1) = (m-2)f_{2,X}(0,0) + (m-3)f_{3,X}(0,0) + .. + f_{m-1,X}(0,0) = 0 \\
F_{YZ}(0,0,1) &= (m-1)\alpha + (m-2)f_{2,Y}(0,0) + .. + f_{m-1,Y}(0,0) = (m-1)\alpha \\
F_{ZZ}(0,0,1) &= \alpha(m-1)(m-2).0 + (m-2)(m-3)f_2(0,0) + ... + f_{m-2}(0,0) = 0
\end{aligned}$$

(Note that for any homogeneous polynomial g of degree ≥ 1, we have $g(0, 0) = 0$, which is why $f_r(0, 0) = f_{r,X}(0, 0) = f_{r,Y}(0, 0) = 0$ for all $r \geq 2$.) Now the hessian matrix at $P = [0 : 0 : 1]$ is:

$$\begin{bmatrix} f_{xx}(0,0) & f_{xy}(0,0) & 0 \\ f_{yx}(0,0) & f_{yy}(0,0) & (m-1)\alpha \\ 0 & (m-1)\alpha & 0 \end{bmatrix}$$

whose determinant $H_P(F) = -(m-1)^2\alpha^2 f_{xx}$. Since $\alpha \neq 0$, $H_P(F) = 0$ iff $f_{xx}(0, 0) = 0$.

From the equation $f(x, y) = \alpha y + f_2(x, y) + ..f_m(x, y)$, we note on substituting the parametric point $(t, 0)$ on the tangent L_2 that $f(t, 0) = t^2 f_{2,xx}(0, 0) + t^3 g(t)$, so that L_2 has order of contact $o_Q(L_2, C_2) \geq 3$ at $Q = (0, 0)$ if and only if $f_{2,xx}(0, 0) = f_{xx}(0, 0) = 0$. Thus P is a point of inflexion of C iff $H_P(F) = 0$ and the proposition is proved. □

Corollary 9.4.2. The proof of the Proposition 9.4.1 above also yields the following criterion for $(0, 0)$ to be a smooth inflexion point of the *affine curve* $C = V(f)$ to have the x-axis $V(y)$ as a tangent at P with order of contact ≥ 3, i.e. that $f(0, 0) = f_x(0, 0) = f_{xx}(0, 0) = 0$ but $f_y(0, 0) \neq 0$. This condition may be familiar from single variable calculus.

Corollary 9.4.3. Let $C \subset \mathbb{P}^2(k)$ be a projective plane curve. If C is of degree 1, i.e. a line, every point on it is a point of inflexion. If C is of degree 2 (i.e. a *conic*), then it has no point of inflexion iff it is irreducible. If it is reducible (i.e. a union of two lines), then every smooth point is a point of inflexion. If C is of degree 3, then there exists at least one point of inflexion.

Proof: If $C = V(F)$ is a degree 1 curve, i.e. a line, F is a degree 1 homogeneous polynomial, so $H_P(F) \equiv 0$.

If C is a conic, denote the determinant $H_P(F)$ by A. If write $(X, Y, Z) \in k^3$, as a column vector P, we have $F(X, Y, Z) = P^t AP$, in matrix notation. Also we get a bilinear form $B(P, Q) = P^t AQ$ on k^3. By elementary linear algebra, A is singular iff the map $P \mapsto B(P, -)$ is non- invertible, i.e. has a kernel. So if $H_P(F) = 0$, we have A is singular, and hence there is a $0 \neq P \in k^3$ such that $B(P, -)$ is the zero map. Since the derivative $(F_X(P), F_Y(P), F_Z(P)) = B(P, -) = P^t A$ (as a row vector), we have that P is a singular point on C. In the Proposition 9.3.8 above, we have seen that this implies that C is reducible, i.e. is a pair of intersecting straight lines. In that case, every smooth point is a point on *exactly* one of these two lines, and is a point of inflexion by the last para. Thus if C is irreducible, A is a non- singular matrix, and $H_P(F) = \det A$ is not zero and there are no inflexion points.

For a cubic polynomial $F(X, Y, Z)$, the polynomials F_{XX}, F_{XY} etc. are all degree 1 homogeneous polynomials, so the hessian determinant $H_P(F)$ is a cubic polynomial in $P = (X, Y, Z)$. If this polynomial is identically zero (as can happen if for example $F(X, Y, Z) = X^3 + Y^3$), then certainly every smooth point on C is a point of inflexion. If it is not identically zero, the curve $D := V(H_P(F))$ is a curve of degree 3 in $\mathbb{P}^2(k)$. By the Bezout theorem, the intersection $C \cap V(H_P(F)) \subset \mathbb{P}^2(k)$ is non-empty, and we are done. (Note that in this last case, there are at most nine points of inflexion). □

Exercise 9.4.4. Let $C \subset \mathbb{P}^2(k)$ be a plane projective curve of degree m. Assuming that the set of inflexion points in C is finite, show that this set has cardinality at most $3m(m-2)$.

9.5. **Classification of plane projective curves of degree ≤ 3.** A degree 1 curve in $\mathbb{P}^2(k)$ is a line. All lines in $\mathbb{P}^2(k)$ are isomorphic, via a linear coordinate change (i.e. an automorphism of $\mathbb{P}^2(k)$) to $V(X_0)$.

For a degree two curve there are two possibilities. Either it is reducible, and equal to a pair of lines (not necessarily distinct), or it is irreducible and smooth (by the Corollary 9.3.8). In this case, $C = V(F)$ where F is a non-degenerate quadratic form. The reader may show (using the fact that k is of characteristic zero and algebraically closed) that a linear change of coordinates brings F to the normal form $F(X_0, X_1, X_2) = \sum_{i=0}^{2} X_i^2$. Thus every smooth plane quadric is equivalent to $V(X_0^2 + X_1^2 + X_2^2)$.

The classification of cubics falls into three cases. We disregard the first case when it is reducible, because it has irreducible components of the kind considered above, i.e. lines and quadrics. The second case is that of singular irreducible cubics, and the third of smooth irreducible cubics. The second case is easier to handle, and is the content of the next proposition.

Proposition 9.5.1 (Singular cubics)**.** Let C be an irreducible singular cubic curve in $\mathbb{P}^2(k)$. Then, after a linear coordinate change in $\mathbb{P}^2(k)$, we have that $C = V(Y^2Z - X^3)$ (cusp) or $C = V(Y^2Z - X^2(X - Z))$ (node).

Proof: From the Proposition 9.3.8, we see that if the irreducible cubic C is singular, it has exactly one singular point. Let us linearly change coordinates so that this singular point is $P = [0 : 0 : 1]$. Since P is a singular point of C, we have by the Proposition 9.3.4 that $m_P(C) \geq 2$. Now, write the U_2 affine piece of C, viz $C_2 = C \cap U_2 = V(f)$ by setting $Z = 1$ in $F(X, Y, Z)$ to get:

$$f(x, y) := F(X, Y, 1) = f_2(x, y) + f_3(x, y)$$

($P \in C_2$ implies $f(0, 0) = 0$, and P a singular point of C_2 implies $f_1(x, y) = f_x(0, 0)x + f_y(0, 0)y \equiv 0$). Since C is irreducible, and $P \in C$, it follows that $(0, 0) \in C_2$, and so $C_2 \neq \phi$, and is also irreducible. In particular $f_2(x, y) \not\equiv 0$ (otherwise $f = f_3(x, y)$ and $V(f)$ is the union of 3 lines meeting at $(0, 0)$ and thus reducible). Hence $f_2(x, y) = (\alpha x + \beta y)(\gamma x + \delta y)$ with $(\alpha, \beta) \neq (0, 0)$ and $(\gamma, \delta) \neq (0, 0)$. Two cases arise:

Case 1: $[\alpha : \beta] = [\gamma : \delta]$. In this case we have $f_2 = \lambda(\alpha x + \beta y)^2$, $\lambda \neq 0$, and there is *exactly one line* $L = V(\alpha x + \beta y)$ through the origin whose order of contact $o_P(L, C_2) = 3$. In this event let us make a linear change of coordinates (x, y) (which corresponds to a linear change of the homogeneous coordinates X, Y, Z in $\mathbb{P}^2(k)$ such that $Z \mapsto Z$) so that $L = V(y)$. Then:

$$f(x, y) = \lambda y^2 + f_3(x, y)$$

We may rescale y so that we have $f(x, y) = y^2 + f_3(x, y)$. If the coefficient of x^3 in $f_3(x, y)$ were zero, $L = V(y)$ would become an irreducible component of C_2, contradicting the irreducibility of C_2, so this coefficient is non-zero. Rescaling x and leaving y as it is we may assume that this coefficient is 1. Thus

$$f(x, y) = y^2 + (x^3 + ax^2y + bxy^2 + cy^3)$$

which on homogenising, reads:

$$F(X, Y, Z) = Y^2Z + (X^3 + aX^2Y + bXY^2 + cY^3)$$

By a linear change $X \mapsto X + \lambda Y$, $Y \mapsto Y$ and $Z \mapsto Z$, we can get rid of the X^2Y term. Thus we have:

$$F(X, Y, Z) = Y^2Z + (X^3 + bXY^2 + cY^3)$$

where b and c are not the old b and c. This last equation maybe rewritten as:

$$F(X, Y, Z) = Y^2(Z + bX + cY) + X^3$$

Now set $Z_1 = -(Z + bX + cY)$, to obtain $F(X, Y, Z_1) = X^3 - Y^2Z_1$. This is precisely the projective cusp.

Case 2: $[\alpha : \beta] \neq [\gamma : \delta]$. In this case we make a linear change of coordinates so that $\alpha x + \beta y \mapsto x$ and $\gamma x + \delta y \mapsto y$. In this case then:

$$f(x, y) = xy + f_3(x, y)$$

Again since f is irreducible, the coefficients of x^3 and y^3 in f_3 are both non-zero. We can rescale x and y so that f_2 becomes λxy, $\lambda \neq 0$ and $f_3(x, y) = x^3 + ax^2y + bxy^2 + y^3$. On homogenising we have:

$$\begin{aligned} F(X, Y, Z) &= \lambda XYZ + (X^3 + aX^2Y + bXY^2 + Y^3) \\ &= \lambda XYZ + (X + Y)^3 + (a - 3)X^2Y + (b - 3)XY^2 \\ &= XY(\lambda Z + (a - 3)X + (b - 3)Y) + (X + Y)^3 \\ &= XYZ_1 + (X + Y)^3 \end{aligned}$$

Now note $XY = \frac{1}{4}\left[(X + Y)^2 - (X - Y)^2\right]$, so changing to $(X + Y) \mapsto X$, $X - Y \mapsto Y$, and $4Z_1 \mapsto -Z$, we have $F(X, Y, Z) = X^3 - (X^2 - Y^2)Z = -(Y^2Z - X^2(X - Z))$, and thus $C = V(Y^2Z - X^2(X - Z))$ which is precisely the projective cubic node. This proves the proposition. □

It remains to tackle the third case, that of the smooth cubics. This is done next.

Proposition 9.5.2. Let $C = V(F) \subset \mathbb{P}^2(k)$ be a smooth cubic. Then after a linear change of coordinates, we have $C = V(ZY^2 - X(X - Z)(X - \mu Z))$ for some $\mu \neq 0, 1$.

Proof: Note that a smooth cubic is irreducible, by the Corollary 9.3.5. By the last part of Corollary 9.4.3, there exists a point of inflexion P on C. By a linear change of coordinates let us assume that (i) $P = [0 : 1 : 0]$ and (ii) the tangent line L at P which has order of contact $o_P(L, C) \geq 3$ is the line $V(Z)$. If we consider the affine chart $U_1 = D(Y) = \{[X : Y : Z] : Y \neq 0\}$, we again have that $P = (0, 0)$ is an inflexion point for the non-empty irreducible affine piece $C_1 = C \cap U_1 = V(f)$ which is defined by the dehomogenisation $f(x, z) = F(X, 1, Z)$. Since $(0, 0) \in C_1$, we have $f(0, 0) = 0$, and since the line $z = 0$ is tangent to C_1 at $(0, 0)$, we have $f_x(0, 0) = 0$. Since $(0, 0)$ is a point of inflexion, the Corollary 9.4.2 we have $f_{xx}(0, 0) = 0$. Thus we have:

$$f(x, z) = \gamma z + (2\alpha zx + 2\beta z^2) + f_3(x, z)$$

where $\gamma \neq 0$. Since C_2 is irreducible, the coefficient of x^3 in the degree 3 homogeneous polynomial f_3 is non-zero. By scaling z and x, we may assume that $\gamma = 1$ and the coefficient of x^3 in f_3 is also 1. We homogenise with respect to Y and get:

$$\begin{aligned} F(X,Y,Z) &= ZY^2 + Y(2\alpha ZX + 2\beta Z^2) + f_3(X,Z) \\ &= Z(Y^2 + 2\alpha XY + 2\beta ZY) + f_3(X,Z) \\ &= Z\left[(Y + \alpha X + \beta Z)^2 - (\alpha X + \beta Z)^2\right] + f_3(X,Z) \\ &= Z(Y + \alpha X + \beta Z)^2 + g_3(X,Z) \end{aligned}$$

where $g_3(X,Z) := f_3(X,Z) - Z(\alpha X + \beta Z)^2$ is another homogeneous polynomial in X, Z of degree 3. Note that the coefficient of x^3 in g_3 is the same as its coefficient in f_3, which is 1. Now change coordinates linearly by $X \mapsto X$, $(Y + \alpha X + \beta Z) \mapsto Y$ and $Z \mapsto Z$. Then our F looks like

$$F(X,Y,Z) = ZY^2 + g_3(X,Z)$$

where $g_3(X,Z) = X^3 + aX^2Z + bXZ^2 + cZ^3$. Clearly, we may write $g_3(X,Z) = (X - \lambda_1 Z)(X - \lambda_2 Z)(X - \lambda_3 Z)$. Changing linearly $X - \lambda_1 Z$ to X, and keeping Z and Y unchanged, we have

$$F(X,Y,Z) = ZY^2 - X(X - \lambda Z)(X - \mu Z)$$

Now if both λ and μ are zero, we have C is a cusp, which is a contradiction since our C is smooth. If one of λ or μ is zero, we have C is a node, which is also a contradiction for the same reason. Thus both λ and μ are non-zero. Scaling Z, we may assume $\lambda = 1$. This will alter the term ZY^2 to $\lambda^{-1}ZY^2$, but rescaling Y will again restore it to ZY^2. Thus we now have:

$$F(X,Y,Z) = ZY^2 - X(X - Z)(X - \mu Z)$$

where $\mu \neq 0$ and $\mu \neq 1$, for both of these situations would give us a node, which is singular. This proves the proposition. □

Remark 9.5.3. The issue addressed in the foregoing subsection is the purely algebraic problem:

Let $F(X_0, X_1, X_2)$ be a homogeneous polynomial of degree ≤ 3. Making only non-singular linear changes of coordinates (X_0, X_1, X_2), bring F to standard form, and classify the standard forms thus possible.

As pointed out at the outset of this subsection, the question yields to pure algebraic methods for deg $F \leq 2$. If one wanted to tackle the case of cubics, i.e. say F is irreducible of degree 3, by purely algebraic means, the task would be completely hopeless. However, the Propositions 9.5.2 and 9.5.1 show that the full power of geometry, viz. the use of Bezout, the notion of orders of contact, smoothness, multiplicity, singular and inflexion points, can make the problem soluble, and indeed one just gets the three irreducible cubics we have been discussing all along.

In the case of singular irreducible cubics, there is a unique normal form, viz. node or cusp. In the smooth case of the elliptic curve $V(Y^2Z - X(X - Z)(X - \mu Z))$ (in Proposition 9.5.2), the reader may wonder how much freedom the parameter μ has. It turns out that two of these with parameters μ and λ are equivalent by a linear coordinate change in $\mathbb{P}^2(k)$ iff $\lambda = \mu$, $\frac{1}{\mu}$, $\frac{\mu}{1-\mu}$, $\frac{1}{1-\mu}$, $\frac{1-\mu}{\mu}$ or $1 - \mu$. The reader is urged to empirically demonstrate that at least these values lead to equivalent elliptic curves. The fact that these are the only ones possible is a slightly deeper fact.