MMA320
Introduction to Algebraic Geometry

Jan Stevens

Department of Mathematical Sciences
Division of Mathematics
CHALMERS UNIVERSITY OF TECHNOLOGY
UNIVERSITY OF GOTHENBURG

Gothenburg, Sweden 2020

Contents

Introduction

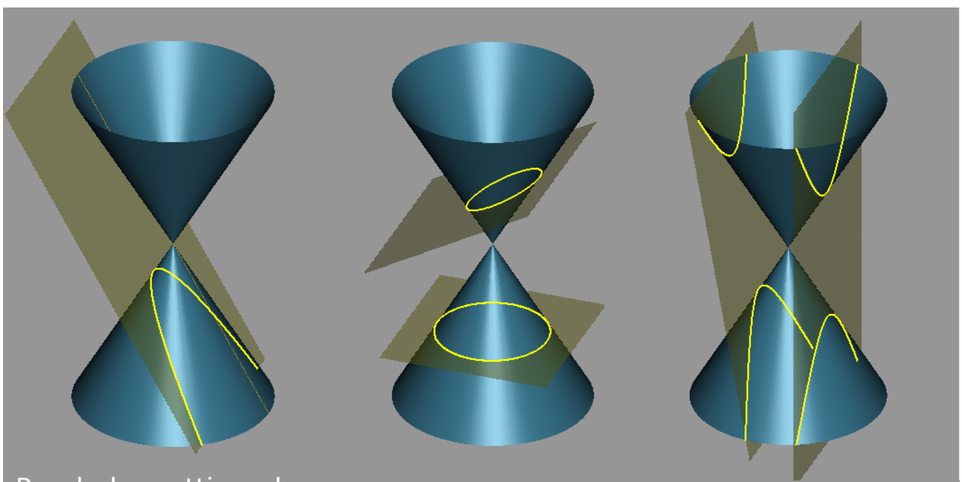
What is algebraic geometry?

Euclidean geometry studies figures composed of lines and planes, culminating in the classification of the Platonic solids. Already in antiquity more complicated curves and surfaces were considered. Since Descartes it is customary to describe them by equations.

We recall the possible (smooth) curves of degree two:

$$\begin{array}{ll} \text{ellipse} & \dfrac{x^2}{a^2} + \dfrac{y^2}{b^2} = 1 \\ \text{parabola} & y = ax^2 \\ \text{hyperbola} & \dfrac{x^2}{a^2} - \dfrac{y^2}{b^2} = 1 \end{array}$$

This list gives a classification up to Euclidean transformations: we have used coordinate transformations to place the figure in a particularly nice position. If we are not interested in metrical properties, we do not consider ellipses with different a, b as distinct, and we allow rescaling of the axes. Then there is only one type of ellipse. These curves are known as conic sections, or shortly conics. The name is explained by the following uniform description: take an ordinary cone $z^2 = x^2 + y^2$ and intersect with planes in 3-space, not passing through the origin.



Parabola- cutting plane parallel to side of cone. Circle and Ellipse Hyperbolas

The picture is from http://en.wikipedia.org, originally uploaded by Duk, released under the GNU Free Documentation License.

If the normal vector of the plane lies inside the cone, we get an ellipse, if it lies outside the cone an hyperbola, and finally a parabola if the plane is parallel to a line on the cone.

Remark. We get singular conics (two intersecting lines or a double line) by taking planes through the origin.

So in a certain sense there is only one type of nonsingular conic. This is made precise in projective geometry. If we have two planes, then projection from the origin sets up a correspondence between the points of both planes, except that some points do not have an image, while other ones are not an image, because lines parallel to a plane do not intersect it. To get rid of these exceptions, we adjoin these points as 'ideal points', which are called points at infinity. In this way each line through the origin in 3-space corresponds to a point in the projective plane. Now two lines always intersect in one point, and there are no parallel lines anymore. The difference between ellipse, parabola and hyperbola only occurs if we go back to an affine (Euclidean) plane by singling out a line as line at infinity.

The conic section might be exemplified by the equation $x^2+y^2=1$. But what about $x^2+y^2=-1$? This equation also defines a curve, if we allow complex solutions. In fact, even if one is interested in problems about real solutions of real equations, a good strategy is to first solve the problem over the complex numbers, and then study the reality of the solution. Most often we will be interested in the complex case.

We are going to study the solution sets of equations (often in projective space). In algebraic geometry this is done with algebraic methods. In contrast to analysis, we do not have the concept of limit and convergence of series. So equations have to be finite sums of terms. We can now give a first answer to the question, what algebraic geometry is:

Algebraic geometry studies the solution sets of systems of polynomial equations.

The algebra needed goes under the name of commutative algebra, which might be described as the study of systems of polynomials.

We allow coefficients in an arbitrary field: we look at systems of polynomials in the polynomial ring

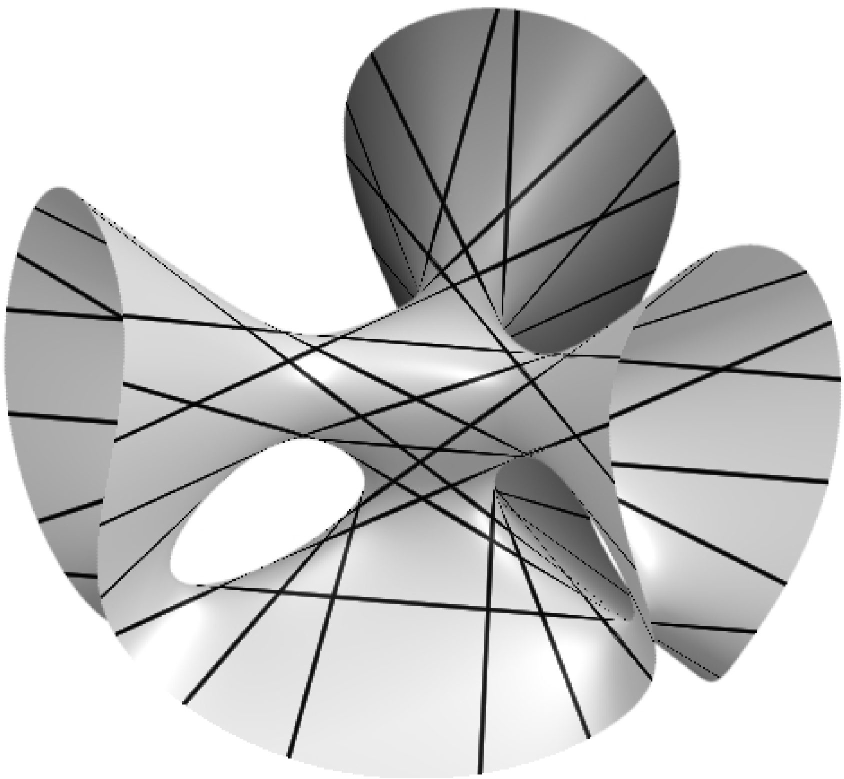
$$k[X_1,\dots,X_n]\ .$$

Special cases are of course $k=\mathbb{C}$, but also $k=\mathbb{Q}$, important for number theory. But k can also be a finite field. This case has applications to coding theory.

It is probably surprising that algebraic geometry is also very much related to theoretical physics. There are theories that the world is not four-dimensional (space-time), but that it has some extra dimensions, on a much smaller scale, making them not directly observable. According to one theory, the world is 10-dimensional, with the six extra real dimensions accounted for by compact complex 3-dimensional algebraic manifolds.

In this course we will develop the general theory of affine and projective varieties (in arbitrary dimensions), but the concrete applications will be to curves and surfaces. The first one concerns cubic curves. It turns out that they are not only points sets, but also have the structure of an abelian group. This makes them relevant for coding theory. The second concrete case is that of cubic surfaces.

In the following picture (by Oliver Labs, for a 3-D model see his website) one can see some straight lines on such a surface. In fact there are always exactly 27 (again allowing complex solutions). To prove this, we first develop some more general theory.



Due to lack of time we do not treat the resolution of curve singularities, mentioned in the course syllabus.

CHAPTER 1

Affine algebraic varieties

In these notes a *ring* will always be a commutative ring with unit.

1.1. Algebraic sets

We want to study solutions of polynomial equations in several variables.

DEFINITION 1.1. Let k be a field. The *affine n-space* over k, denoted by $\mathbb{A}^n(k)$ or simply $\mathbb{A}^n$, if the field k is understood, is the set of n-tuples of elements of k:

$$\mathbb{A}^n(k) = \{(a_1, \dots, a_n) \mid a_i \in k \text{ for } 1 \le i \le n\} .$$

Let $k[X_1, \dots, X_n]$ be the ring of polynomials in n variables with coefficients in k. A point $P = (a_1, \dots, a_n) \in \mathbb{A}^n(k)$ is a *zero* of a polynomial $f \in k[X_1, \dots, X_n]$ if $f(P) = f(a_1, \dots, a_n) = 0$.

DEFINITION 1.2. Given a set S of polynomials in $k[X_1, \dots, X_n]$ the zero set of S is

$$V(S) = \{P \in \mathbb{A}^n(k) \mid f(P) = 0 \text{ for all } f \in S\} \subset \mathbb{A}^n(k) .$$

A subset $X \subset \mathbb{A}^n(k)$ is an *algebraic set* if $X = V(S)$ for some $S \subset k[X_1, \dots, X_n]$.

Note that different subsets of $k[X_1, \dots, X_n]$ can give rise to the same algebraic set. If I is the ideal generated by S, that is

$$I = \{f \in k[X_1, \dots, X_n] \mid f = \textstyle\sum_{i=1}^{l} q_i h_i \text{ with } h_i \in S\} ,$$

then $V(I) = V(S)$. Therefore every algebraic set is of the form $V(I)$ for some ideal I.

PROPOSITION 1.3. *Every algebraic set is the common zero set of a finite number of polynomials.*

NOTATION. We write $V(f_1, \dots, f_n)$ in stead of the more correct $V(\{f_1, \dots, f_n\})$.

The proposition follows from a theorem in commutative algebra, known as Hilbert basis theorem, which we prove below.

PROPOSITION–DEFINITION 1.4. *Let R be a ring. The following conditions are equivalent:*

(1) *every ideal I is finitely generated*

(2) *R satisfies the ascending chain condition (a.c.c): every ascending chain of ideals $I_1 \subset I_2 \subset I_3 \subset \dots$ is eventually stationary, that is, for some m we have $I_m = I_{m+1} = I_{m+2} = \dots$.*

If R satisfies these conditions, it is called Noetherian.

PROOF.
(1) $\Rightarrow$ (2). Given $I_1 \subset I_2 \subset I_3 \subset \dots$, we set $I := \bigcup_i I_i$. Then I is an ideal, generated by finitely many elements $f_1, \dots, f_k$. Each f_j is contained in some $I_{m(j)}$. Set $m = \max\{m(j)\}$. Then $f_j \in I_{m(j)} \subset I_m$ for all j, so $I_m = I$ and therefore $I_m = I_{m+1} = I_{m+2} = \dots$.
(2) $\Rightarrow$ (1). Assume that there is an ideal I that cannot be generated by finitely many elements. We construct inductively a sequence of elements $f_j \in I$ by taking f_1 arbitrary and $f_{j+1} \in I \setminus (f_1, \dots, f_j)$. Then the sequence $(f_1) \subset (f_1, f_2) \subset (f_1, f_2, f_3) \subset \dots$ is not stationary. □

EXAMPLE 1.5. A field k is a Noetherian ring, as the only ideals are (0) and $(1) = k$.

THEOREM 1.6 (Hilbert Basis Theorem). *If R is a Noetherian ring, then $R[X]$ is Noetherian.*

REMARK 1.7. From the example and Hilbert's Basis Theorem it follows by induction that every ideal in $k[X_1, \dots, X_n]$ can be generated by a finite set of elements. In old-fashioned terminology an ideal basis is a finite generating set, so the previous statement can be formulated as: every ideal in $k[X_1, \dots, X_n]$ has a basis. This explains the name of the theorem.

PROOF OF THE THEOREM. Suppose $I \subset R[X]$ is not finitely generated. We define a sequence $f_j \in I$: let f_1 be a polynomial of minimal degree d_1, and pick f_{j+1} of lowest degree d_{j+1} in $I \setminus (f_1, \dots, f_j)$. For all j let c_j be the leading coefficient of f_j (i.e., $f_j = c_j X^{d_j} + c_j' X^{d_j - 1} + \dots$). The chain of ideals $(c_1) \subset (c_1, c_2) \subset \dots$ in the Noetherian ring R is eventually stationary, so there is an m with $c_{m+1} \in (c_1, \dots, c_m)$. Let $c_{m+1} = \sum_{i=1}^m r_i c_i$ for some elements $r_i \in R$. Then the polynomial

$$f_{m+1} - \sum_{i=1}^{m} r_i X^{d_{m+1} - d_i} f_i$$

is not contained in $(f_1, \dots, f_m)$, but has lower degree than f_{m+1}, contradicting the choice of f_{m+1}. Therefore $R[X]$ is Noetherian. □

We note the following properties of algebraic sets.

LEMMA 1.8.
(1) $V(0) = \mathbb{A}^n(k)$, $V(k[X_1, \dots, X_n]) = V(1) = \emptyset$
(2) *if $I \subset J$, then* $V(I) \supset V(J)$
(3) $V(I_1 \cap I_2) = V(I_1) \cup V(I_2)$
(4) $V(\sum_{\lambda \in \Lambda} I_\lambda) = \bigcap_{\lambda \in \Lambda} V(I_\lambda)$

Proof. Only the third property is not obvious. As $I_1 \cap I_2 \subset I_1$, we have $V(I_1) \subset V(I_1 \cap I_2)$. Also $V(I_2) \subset V(I_1 \cap I_2)$, which gives the inclusion '$\subset$'. For the opposite inclusion, suppose that $P \in V(I_1 \cap I_2)$, but $P \notin V(I_1)$. Then there exists an $f \in I_1$ with $f(P) \neq 0$. For all $g \in I_2$ we have $fg \in I_1 \cap I_2$, so $f(p)g(p) = 0$ and therefore $g(P) = 0$. This means that $P \in V(I_2)$. $\square$

The properties (1), (3) and (4) are the defining properties of a topology by means of closed sets.

Definition 1.9. The *Zariski topology* on $\mathbb{A}^n$ is the topology whose closed sets are the algebraic sets.

Remark 1.10. The Zariski topology is not Hausdorff. E.g., a closed subset of $A^1(k)$ consists of finitely many points. An open sets is therefore the complement of finitely many points. If the field k is infinite, two non-empty open sets always have an non-empty (in fact infinite) intersection.

1.2. Hilbert's Nullstellensatz

We associated to an ideal a zero set by the operation $V(-)$. In this section we consider the question to which extent the zero set determines the ideal.

Definition 1.11. Let X be a subset of $A^n(k)$. The ideal of X is

$$I(X) = \{f \in k[X_1, \dots, X_n] \mid f(P) = 0 \text{ for all } P \in X\} .$$

Example 1.12. Let X be the subset of $A^1(\mathbb{R})$, consisting of all points with integer coordinate. Then $I(X) = (0)$.

Proposition 1.13.
1. *$X \subset Y \Rightarrow I(X) \supset I(Y)$,*
2. *$X \subset V(I(X))$ with equality if and only if X is an algebraic set,*
3. *$J \subset I(V(J))$.*

Proof. We prove only the equality statement in (2). If $X = V(J)$, then $J \subset I(X)$ and we get $X \subset V(I(X)) \subset V(J) = X$. Conversely, if $X = V(I(X)$, then X is an algebraic set defined by the ideal $I(X)$. $\square$

What about equality in (3)? There are two ways in which it can go wrong.

Example 1.14. Let $k = \mathbb{R}$, $J = (X^2+1) \subset \mathbb{R}[X]$. Then $V(J) = \emptyset$, but $J \neq I(\emptyset) = \mathbb{R}[X]$. So if the field is not algebraically closed, there might not be enough zeroes.

Example 1.15. Let k be algebraically closed, and f a polynomial in $k[X_1, \dots, X_n]$. Then $f(P) = 0 \Leftrightarrow f^2(P) = 0$, so $V(f) = V(f^2)$, but $(f^2) \neq (f)$.

DEFINITION 1.16. Let I be an ideal in a ring R. The *radical* of I is

$$\operatorname{rad}(I) = \sqrt{I} = \{f \in R \mid f^n \in I \text{ for some } n\} .$$

An ideal I is called *radical*, if $I = \sqrt{I}$.

REMARK 1.17. The radical is again an ideal. Suppose $f, g \in \sqrt{I}$, so $f^m \in I$ and $g^n \in I$. Then $(f+g)^r = \sum \binom{r}{k} f^k g^{r-k} \in I$ if $r \geq n+m-1$.

REMARK 1.18. Obviously $V(I) = V(\sqrt{I})$.

THEOREM 1.19 (Nullstellensatz). *Let k be an algebraically closed field. For every ideal $J \subset k[X_1, \ldots, X_n]$ one has*

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

This theorem follows from the weak form of the Nullstellensatz, with Rabinowitsch' trick.

THEOREM 1.20 (Weak form of the Nullstellensatz). *If $J \neq (1)$ is an ideal in $k[X_1, \ldots, X_n]$, k algebraically closed, then $V(J) \neq \emptyset$.*

PROOF OF THE NULLSTELLENSATZ FROM ITS WEAK FORM. Obviously $\sqrt{J} \subset I(V(J))$. Now let $f \in I(V(J))$, so $f(P) = 0$ for all $P \in V(J)$. Consider the ideal $\bar{J} \subset k[X_1, \ldots, X_n, T]$ generated by $Tf - 1$ and J. Then $\bar{J}$ has no zero in $\mathbb{A}^{n+1}(k)$, as $f(P) = 0$ for all common zeroes P of J. Therefore, by the weak Nullstellensatz, $1 \in \bar{J}$, so we can write

$$1 = \sum_{i=1}^{m} a_i(X_1, \ldots, X_n, T) f_i + b(X_1, \ldots, X_n, T)(Tf - 1) ,$$

where $(f_1, \ldots, f_m)$ are generators of J. Let N be the highest power of T appearing in the a_i and b. Multiplying the above identity by f^N gives a relation of the form

$$f^N = \sum_{i=1}^{m} a_i'(X_1, \ldots, X_n, Tf) f_i + b'(X_1, \ldots, X_n, Tf)(Tf - 1) .$$

Now substitute $T = 1/f$, that is $Tf = 1$. We find that

$$f^N = \sum_{i=1}^{m} a_i'(X_1, \ldots, X_n, 1) f_i ,$$

so $f^N \in J$. $\square$

In the older literature the weak form is shown using elimination theory. Following André Weil's slogan

il faut éliminer l'élimination

most books now follow Artin–Tate and Zariski, and reduce it to an algebraic fact, that a field, which is finitely generated as k-algebra, is algebraic over k. The advent of computer algebra has led to renewed interest for older methods. We now give a proof using elimination. We need to recall some facts about resultants, which we use again in Chapter 3 .

1.3. The resultant

Let k be a field. Then the polynomial ring $k[X]$ in one variable is a unique factorisation domain (UFD). Another example of a UFD is the ring of integers $\mathbb{Z}$. There is a strong analogy between primes and irreducible polynomials. In general, given an integral domain A (this means that A has no zero divisors) one has the concepts of *prime* and *irreducible*: let $p \in A$, $p \neq 0$, p not a unit, then p is *irreducible* if $p = ab$ implies a or b is a unit, and p is *prime* if $p|ab$ implies $p|a$ or $p|b$. Every prime element is irreducible, but the converse is false in general.

EXAMPLE 1.21. Let $A = \mathbb{C}[X, Y, Z]/(Z^2 - XY)$. The class z of Z is irreducible, but not prime, as $z|xy$ but neither $z|x$ nor $z|y$. The ring A is an integral domain, but not a UFD: the element z^2 has two different factorisations: $z^2 = z \cdot z$ and $z^2 = x \cdot y$.

In a UFD every irreducible element is prime. If A is a UFD, also $A[X]$ is a UFD (see the exercises), and by induction we obtain for a field k that $k[X_1, \ldots, X_n]$ is a UFD.

Let A be a unique factorisation domain. We are interested in the question when two polynomials $f(X)$, $g(X) \in A[X]$ have a common factor. Cases of interest are $A = k$, but also $A = k[Y, Z]$. Let:

$$f = a_0X^m + a_1X^{m-1} + \cdots + a_m,$$
$$g = b_0X^n + b_1X^{n-1} + \cdots + b_n,$$

where the case that either $a_0 = 0$ or $b_0 = 0$ (but not both) is allowed.

PROPOSITION 1.22. *The polynomials f and g in $A[X]$ have a non-constant factor h in common, if and only if there exist polynomials u and v of degree less than m, resp. n, not both vanishing, such that $vf + ug = 0$.*

PROOF. We may suppose that $a_0 \neq 0$, so $m = \deg f$. Let $vf = -ug$. All irreducible factors of f have to occur in ug, and not all can occur in u, because $\deg u < \deg f$; therefore f and g have a factor in common. Conversely, given h one finds a v and a u of degree less than n and m, such that $f = -uh$ and $g = vh$, so the equation $vf + ug = 0$ is satisfied. □

Now put:

$$u = u_0X^{m-1} + \cdots + u_{m-1},$$
$$v = v_0X^{n-1} + \cdots + v_{n-1},$$

and consider the coefficients as indeterminates. Comparison of coefficients of powers of X in $vf+ug=0$ gives the system of linear equations for the u_i and v_i:

$$\begin{aligned} a_0v_0 + b_0u_0 &= 0 \\ a_1v_0 + a_0v_1 + b_1u_0 + b_0u_1 &= 0 \\ &\vdots \\ a_mv_{n-1} + b_nu_{m-1} &= 0\,. \end{aligned}$$

This system has a solution if and only if the determinant of the coefficient matrix vanishes: the vanishing of the determinant is a necessary and sufficient condition for the existence of a solution over the quotient field $Q(A)$ of A, and by clearing denominators we get a solution over A. After transposing we get the following determinant $R(f,g)$, which is called the *resultant* of f and g:

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & a_2 & \dots & a_m & & & \\ & a_0 & a_1 & a_2 & \dots & a_m & & \\ & & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & & a_0 & a_1 & a_2 & \dots & a_m \\ b_0 & b_1 & \dots & b_{n-1} & b_n & & & \\ & b_0 & b_1 & \dots & b_{n-1} & b_n & & \\ & & \cdots & \cdots & \cdots & \cdots & & \\ & & & b_0 & b_1 & \dots & b_{n-1} & b_n \end{vmatrix}\,.$$

From Proposition 1.22 follows:

Proposition 1.23. *The polynomials f and g have a non-constant factor h in common, if and only if $R(f,g)=0\in A$.*

Remark 1.24. Writing the resultant as the determinant of the transpose of the coefficient matrix is traditional. A different way to find the matrix is the following. Consider the free module $A[X]_{n+m-1}$ of polynomials of degree at most $m+n-1$ and write polynomials as row vector of coefficients. The existence of a relation $vf+ug=0$ is equivalent to the fact that the polynomials f, Xf, $\dots$, $X^{n-1}f$, g, Xg, $\dots$, $X^{m-1}g$ are linearly dependent row vectors in the $(m+n)$-dimensional vector space $Q(A)[X]_{n+m-1}$. The resultant is the determinant expressing this fact.

Remark 1.25. If A is a polynomial ring, and a_i and b_i are homogeneous polynomials of degree i, then $R(f,g)\in A$ is a polynomial of degree mn.

Remark 1.26. The resultant is in fact a universal polynomial in the a_i and b_j with integral coefficients.

The left-hand side of the last equation $a_mv_{n-1}+b_nu_{m-1}=0$ is the coefficient of the constant term in $vf+ug$. So the first $m+n-1$

equations describe the condition that $vf + ug$ does not involve X. A solution (v, u) for this system of $m + n - 1$ linear equations in $m + n$ variables is given by the maximal minors of the coefficient matrix. Inserting this solution in the last equation computes the determinant $R(f, g)$. This shows:

PROPOSITION 1.27. *For any two polynomials f and g there exist polynomials u and v with* $\deg u < \deg f$ *and* $\deg v < \deg g$*, such that:*

$$vf + ug = R(f, g).$$

1.4. Hilbert's Nullstellensatz (continued)

We will prove the Nullstellensatz by induction on the number of variables. In the induction step the last variable will play a special role, and we have to bring polynomials in suitable form. For an algebraically closed field this is possible by the following lemma.

LEMMA 1.28. *Let $f \in k[X_1, \dots, X_n]$ be a polynomial of degree d over an infinite field k. After a suitable coordinate transformation this polynomial has a term of the form cX_n^d for some non-zero $c \in k$.*

PROOF. Introduce new coordinates by $X_i = Y_i + a_iX_n$ for $i < n$. Let f_d be the highest degree part of f. Then

$$f(Y_1 + a_1X_n, \dots, Y_{n-1} + a_{n-1}X_n, X_n) = f_d(a_1, \dots, a_{n-1}, 1)X_n^d + \cdots ,$$

where the dots stand for terms of lower degree in X_n. As k is infinite, we can find values for the a_i such that $f_d(a_1, \dots, a_{n-1}, 1) \neq 0$. □

THEOREM 1.29 (Weak form of the Nullstellensatz). *If $J \neq (1)$ is an ideal in $k[X_1, \dots, X_n]$, k algebraically closed, then $V(J) \neq \emptyset$.*

PROOF. We use induction on the number of variables. For $n = 1$ each proper ideal in $k[X_1]$ is principal, so the result follows because k is algebraically closed.

Let J be a proper ideal in $k[X_1, \dots, X_n]$. If $J = (0)$, then $V(J) = \mathbb{A}^n(k)$. Otherwise we can, as the algebraically closed field k is infinite, by a suitable coordinate transformation achieve that J contains an element f of degree d, in which the term cX_n^d, $c \neq 0$, occurs. Let

$$J_{n-1} = J \cap k[X_1, \dots, X_{n-1}] .$$

It consists of all polynomials in J, not involving X_n. This is an ideal (possibly the zero ideal) in $k[X_1, \dots, X_{n-1}]$. As $1 \notin J$ and $J_{n-1} \subset J$, we have $1 \notin J_{n-1}$. By the induction hypothesis $V(J_{n-1}) \neq \emptyset$ in $\mathbb{A}^{n-1}(k)$. Let $A = (a_1, \dots, a_{n-1}) \in V(J_{n-1})$ and consider the roots b_i of $f(a_1, \dots, a_{n-1}, X_n)$. By our assumption on the form of f there are finitely many b_i. Suppose that none of the points $P_i = (a_1, \dots, a_{n-1}, b_i)$ is a common zero of J. So for each P_i there exists a polynomial $g_i \in J$ with $g_i(P_i) \neq 0$. Therefore one can find a $g \in J$ with $g(P_i) \neq 0$ for all i. An explicit formula is $g = \sum_i g_i \prod_{j \neq i}(X_n - b_j)$. By construction

$f(a_1, \ldots, a_{n-1}, X_n)$ and $g(a_1, \ldots, a_{n-1}, X_n)$ have no common roots, and therefore their resultant is non-zero. This means that the resultant $R(f, g) \in k[X_1, \ldots, X_{n-1}]$ does not vanish at A. But $R(f, g) = vf + ug \in J_{n-1}$, so $R(f, g)(A) = 0$. This contradiction shows that at least one of the points P_i is a zero of J. □

PROPOSITION 1.30. *A proper ideal $I \subset k[X_1, \ldots, X_n]$, with k algebraically closed, is a maximal ideal if and only if I is of the form $(X_1 - a_1, \ldots, X_n - a_n)$ for some point $P = (a_1, \ldots, a_n)$.*

PROOF. We abbreviate $R = k[X_1, \ldots, X_n]$. A proper ideal I is maximal if and only if R/I is a field.

The ideal $(X_1 - a_1, \ldots, X_n - a_n)$ is maximal, as $R/(X_1 - a_1, \ldots, X_n - a_n) \cong k$ (this direction holds for any field).

Conversely, let I be a maximal ideal and $P = (a_1, \ldots, a_n) \in V(I)$, existing by the weak Nullstellensatz. The ideal $I(P)$ is the kernel of the surjective evaluation map $R \to k$, $f \mapsto f(P)$. As it contains the maximal ideal $(X_1 - a_1, \ldots, X_n - a_n)$, it is in fact equal to it. Now $I \subset I(V(I)) \subset I(P)$, so by maximality $I = I(P) = (X_1 - a_1, \ldots, X_n - a_n)$. □

REMARK 1.31. For general k there are maximal ideals, which look differently, e.g., $(X^2 + 1) \subset \mathbb{R}[X]$. Observe that $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$.

1.5. Irreducible components

For $R = k[X_1, \ldots, X_n]$ we have now two operations $V(-)$ and $I(-)$,

$$\{\text{ideals of } R\} \quad \overset{V}{\underset{I}{\rightleftarrows}} \quad \{\text{subsets of } \mathbb{A}^n(k)\}$$

which for algebraically closed k induce bijections

$$\begin{array}{ccc} \{\text{radical ideals of } R\} & \Longleftrightarrow & \{\text{algebraic subsets of } \mathbb{A}^n(k)\} \\ \cup & & \cup \\ \{\text{maximal ideals of } R\} & \Longleftrightarrow & \{\text{points of } \mathbb{A}^n(k)\} \end{array}$$

Between radical ideals and maximal ideals lie prime ideals. Recall that a proper ideal I is *prime* if $ab \in I$ implies that $a \in I$ or $b \in I$. We discuss what this concept corresponds to on the side of algebraic sets.

DEFINITION 1.32. An algebraic set X is *irreducible*, if whenever $X = X_1 \cup X_2$ with X_1, X_2 algebraic, then $X = X_1$ or $X = X_2$.

PROPOSITION 1.33. *An algebraic set X is irreducible if and only if its ideal $I(X)$ is prime.*

PROOF.
($\Leftarrow$) Suppose $X = X_1 \cup X_2$ is a non-trivial decomposition. As $X_i \neq X$ there are by Proposition 1.13(2) functions $f_i \in I(X_i) \setminus I(X)$, $i = 1, 2$. As $f_1 f_2 \in I(X)$, the ideal $I(X)$ is not prime.
($\Rightarrow$) Suppose $f_1 f_2 \in I(X)$, but $f_i \notin I(X)$. Then $X_i = V(f_i, I(X))$ is algebraic with $X_i \subsetneq X$, but $X \subset X_1 \cup X_2$. □

REMARK 1.34. We can formulate the concept of irreducibility for any topological space: X is *reducible* if $X = X_1 \cup X_2$ with X_1, X_2 proper closed subsets of X. For other topologies than the Zariski topology this concept is not interesting: a Hausdorff space is always reducible unless it consists of at most one point.

DEFINITION 1.35. A topological space X is *Noetherian* if it satisfies the *descending chain condition*: every descending chain $X \supset X_1 \supset X_2 \supset \dots$ of closed subsets is eventually stationary.

REMARK 1.36. An affine algebraic set is a Noetherian topological space.

PROPOSITION–DEFINITION 1.37. *Every Noetherian topological space has a decomposition*

$$X = X_1 \cup \dots \cup X_r$$

with the X_i irreducible, and satisfying $X_i \not\subset X_j$ for all $i \neq j$. The X_i are called irreducible components of X. The decomposition into irreducible components is unique (up to permutation).

PROOF. Suppose that there exists a space X for which the statement is false. Then $X = X_1 \cup X_1'$ is reducible and at least one of X_1, X_1' is reducible and does not have a decomposition into a finite number of components, say X_1. Then $X_1 = X_2 \cup X_2'$ with say X_2 does not have a decomposition. Continuing this way we find an infinite chain

$$X \supsetneq X_1 \supsetneq X_2 \supsetneq \dots ,$$

contradicting the fact that X is Noetherian.
The condition $X_i \not\subset X_j$ can be satisfied by omitting superfluous terms. Uniqueness is left as an exercise. □

DEFINITION 1.38. An irreducible algebraic subset $V \subset \mathbb{A}^n(k)$ is called an affine k-variety, or *affine variety*.

REMARK 1.39. Some authors do not include irreducibility in the definition, and call our algebraic sets for varieties. The reason for our (traditional) terminology will soon become clearer.

Actually, we shall later on change the definition a bit and introduce (abstract) affine varieties, independent of a given embedding in a particular affine space.

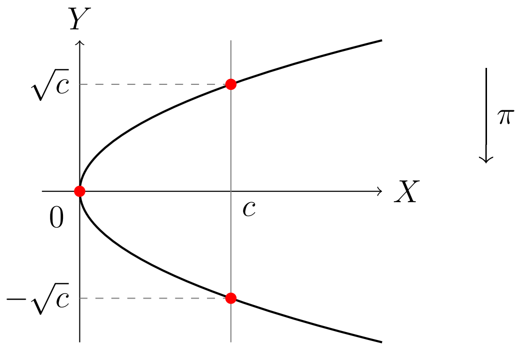
1.6. Affine k-schemes

Now we have extended our correspondence with one more layer:

$$
\begin{array}{ccc}
\{\text{ideals of } R\} & \underset{I}{\overset{V}{\rightleftarrows}} & \{\text{subsets of } \mathbb{A}^n(k)\} \\
\cup & & \cup \\
\{\text{radical ideals of } R\} & \overset{1:1}{\longleftrightarrow} & \{\text{algebraic subsets of } \mathbb{A}^n(k)\} \\
\cup & & \cup \\
\{\text{prime ideals of } R\} & \overset{1:1}{\longleftrightarrow} & \{\text{irreducible subsets of } \mathbb{A}^n(k)\} \\
\cup & & \cup \\
\{\text{maximal ideals of } R\} & \overset{1:1}{\longleftrightarrow} & \{\text{points of } \mathbb{A}^n(k)\}
\end{array}
$$

where the bijections hold for k algebraically closed. We would like to change the top line to obtain a bijection also there, that is, we would like to associate to an arbitrary (non-radical) ideal some kind of space. Such situations occur naturally.

EXAMPLE 1.40. Consider the projection of the parabola $V(X - Y^2) \subset \mathbb{A}^2$ onto the X-axis.



Over the reals there lie two points over each $X > 0$, one over 0 and no points over an $X < 0$. In the complex case for each $c \neq 0$ there are two points over $X = c$, namely $(c, \pm y)$ with y a root of the quadratic equation $y^2 = c$. As usually, to make it true that a quadratic equation always has two roots, we count them with multiplicity. We say therefore that $y^2 = 0$ has a double root. Also geometrically we want to say that over each complex point $X = c$ there lie two points, so we say that over the origin we have a double point. It is on the Y-axis defined by the ideal (Y^2), and in the plane by (X, Y^2).
A somewhat different, but related way to consider the situation is that for $c \neq 0$ we have two points, which come together in the limit $c \to 0$.

DEFINITION 1.41. A *fat point* P is defined by an ideal I, whose radical is a maximal ideal, defining a single point P_{red}. The *multiplicity* of P is $\dim_k k[X_1, \dots, X_n]/I$.

More generally, to an ideal $I \subset k[X_1, \dots, X_n]$ we associate a space X. This will be called an affine *k-scheme*. As a set it is the same as the algebraic set X_{red}, defined by the radical of I, but we give it a different coordinate ring (see Definition 1.55), namely R/I.

1.7. Primary decomposition

For algebraic sets we had a (unique) decomposition into irreducible components. We want to have something similar for k-schemes. We study the problem algebraically, purely in terms of ideals.

DEFINITION 1.42. Let R be a Noetherian ring. An ideal I is *irreducible* if $I = I_1 \cap I_2$ implies $I = I_1$ or $I = I_2$.

LEMMA 1.43. *In a Noetherian ring every ideal is a finite intersection of irreducible ideals.*

EXAMPLE 1.44. A prime ideal is irreducible, but not every irreducible ideal is prime: the ideal $(X, Y^2) \subset k[X, Y]$ is irreducible. The ideal (X^2, XY, Y^2) is not irreducible. Its decomposition as finite intersection of irreducible ideals is not unique. We need another concept, where an ideal as (X^2, XY, Y^2) is not further decomposed.

DEFINITION 1.45. A proper ideal in a ring R is *primary* if $ab \in I$ implies that $a \in I$ or $b^n \in I$ for some n.

PROPOSITION–DEFINITION 1.46. *Let I be a primary ideal. The radical $\sqrt{I}$ of I is the smallest prime ideal containing I. Set $\mathfrak{p} = \sqrt{I}$. The ideal I is called $\mathfrak{p}$-primary.*

PROOF. If $ab \in \sqrt{I}$, then $(ab)^m \in I$ for some m and therefore $a^m \in I$ or $b^{mn} \in I$ for some mn, that is, $a \in \sqrt{I}$ or $b \in \sqrt{I}$, showing that $\sqrt{I}$ is prime. Let $\mathfrak{p} \supset I$ be a prime ideal, and $a \in \sqrt{I}$. Then $a^n \in I \subset \mathfrak{p}$ for some n, so $a \in \mathfrak{p}$, as $\mathfrak{p}$ is prime. Therefore $\sqrt{I} \subset \mathfrak{p}$. □

One can show that in a Noetherian ring every irreducible ideal is primary. It follows that every ideal I has a *primary decomposition*, that is, $I = \bigcap_{i=1}^k I_i$, with I_i primary.

DEFINITION 1.47. A primary decomposition $I = \cap I_i$ is *minimal* if all $\sqrt{I_i}$ are distinct and $I_i \not\supset \bigcap_{j \neq i} I_j$ for all i.

THEOREM 1.48. *Let $I = \cap I_i$ be a minimal primary decomposition. Set $\mathfrak{p}_i = \sqrt{I_i}$. The ideals $\mathfrak{p}_i$ are independent of the particular decomposition.*

A proof can be found in [Atiyah–MacDonald].

DEFINITION 1.49. The prime ideals $\mathfrak{p}_i$ of the theorem are *associated* with I. The minimal elements of the set $\{\mathfrak{p}_i, \dots, \mathfrak{p}_k\}$ are the *isolated* prime ideals associated with I. The other ones are called *embedded* prime ideals.

Let I be an ideal in $k[X_1,\dots,X_n]$, for simplicity k algebraically closed. Then I defines a k-scheme. The radical $\sqrt{I}$ defines the algebraic set X_{red}. The minimal primes $\mathfrak{p}_i$ correspond to the irreducible components of X_{red}, and the embedded primes to subvarieties of these: varieties embedded in irreducible components.

EXAMPLE 1.50. Let $I = (X^2, XY) \subset k[X,Y]$. A primary decomposition is $I = (X) \cap (X^2, XY, Y^2)$. The zero set $V(I)$ is obviously the Y-axis. This is the isolated component, whereas (X,Y) is an embedded component. The primary decomposition is not unique: we can also write $I = (X) \cap (X^2, Y)$.

1.8. The ground field

As we have seen, we need an algebraically closed field (typically $\mathbb{C}$) to assure that equations have solutions. But often the coefficients lie in a subfield (typically $\mathbb{Q}$, in fact we mostly write equations with integral coefficients). One then says that the variety is defined over the subfield. To take this into account, we generalise the definition of the operations $V(-)$ and $I(-)$.

Let $k \subset K$ be a field extension. We consider ideals in $k[X_1,\dots,X_n]$, but look at their zero sets in $\mathbb{A}^n(K)$. So given J one has

$$V(J) = \{P \in \mathbb{A}^n(K) \mid f(P) = 0 \text{ for all } f \in J\}$$

and conversely for a subset $X \subset \mathbb{A}^n(K)$,

$$I(X) = \{f \in k[X_1,\dots,X_n] \mid f(P) = 0 \text{ for all } P \in X\}\ .$$

This sets up a correspondence between ideals in $k[X_1,\dots,X_n]$ and algebraic k-sets in $\mathbb{A}^n(K)$. We have a Zariski k-topology on $\mathbb{A}^n(K)$. If $X = V(J)$, then one says that X is defined over k, and that k is field of definition of X. We regain the previous set-up by taking $k = K$.

It is easy to check that the properties of $V(-)$ and $I(-)$ proved above also hold in the more general situation of a field extension $k \subset K$. Also the Nullstellensatz $I(V(J)) = \sqrt{J}$ remains true with the same proof, starting from the weak form: if $J \neq (1)$ is an ideal in $k[X_1,\dots,X_n]$, then $V(J) \subset \mathbb{A}^n(K)$ is non-empty if K is algebraically closed.

In the sequel we use, unless otherwise stated, a ground field k together with a fixed algebraically closed extension K, and algebraic sets will be subsets of $\mathbb{A}^n(K)$.

1.9. The spectrum of a ring

There is a close relation between algebraic geometry and ring theory. In this section we describe a generalisation of the concept of affine variety that starts from an arbitrary ring. We do not use it in the sequel. See also [Reid, Undergraduate Commutative Algebra] for more discussion. We have to define a space out of a ring, and describe the functions on it.

DEFINITION 1.51. The *spectrum* $\operatorname{Spec}(R)$ of a ring R is the set of all prime ideals $\mathfrak{p}$ of R, $\mathfrak{p} \neq R$. The maximal spectrum is the set of all maximal ideals.

DEFINITION 1.52. The zero set of an ideal $I \subset R$ is

$$V(I) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \supset I\} .$$

The ideal of a subset $X \subset \operatorname{Spec} R$ is

$$I(X) = \bigcap_{\mathfrak{p} \in X} \mathfrak{p} .$$

Elements f of R will be called functions on $\operatorname{Spec} R$ and the value of f in a point $\mathfrak{p}$ is $f \pmod{\mathfrak{p}}$.

EXAMPLE 1.53. Let $R = \mathbb{Z}$ be the ring of integers. The function $5 \in \mathbb{Z}$ takes the value $1 \pmod 2$ in the point (2) and $2 \pmod 3$ in the point (3).

As consequence of the Nullstellensatz we saw that the maximal ideals in $K[X_1, \dots, X_n]$, K algebraically closed, are of the form $(X_1 - a_1, \dots, X_n - a_n)$. So there is a natural one-to-one correspondence between $\mathbb{A}^n(K)$ and the maximal spectrum of $K[X_1, \dots, X_n]$. Things are less simple if K is not algebraically closed. E.g., the maximal ideals in $\mathbb{Q}[X]$ are of the form (f) with f a polynomial, irreducible over $\mathbb{Q}$. In the (maximal) spectrum all maximal ideals in $k[X_1, \dots, X_n]$ define 'points'. So $(X^2+1) \subset \mathbb{R}[X]$ 'is' two complex conjugate points.

1.10. Polynomial maps

Each polynomial $f \in k[X_1, \dots, X_n]$ defines a polynomial function $f\colon \mathbb{A}^n(K) \to K$ by the formula $P \mapsto f(P)$. The polynomial function determines the polynomial: if $f, g \in k[X_1, \dots, X_n]$ and $f(P) = g(P)$ for all $P \in \mathbb{A}^n(K)$, then $f = g$. If we do not require that the extension $k \subset K$ is algebraically closed, we need that K is infinite to get the same conclusion.

DEFINITION 1.54. Let V be an algebraic k-set in $\mathbb{A}^n(K)$. A *polynomial function* $f\colon V \to K$ is the restriction of a polynomial function $F\colon \mathbb{A}^n(K) \to K$ to V, with $F \in k[X_1, \dots, X_n]$.

Two polynomials $F, G \in k[X_1, \dots, X_n]$ define the same function on V if and only if $(F - G)(P) = 0$ for all $P \in V$, that is, if and only if $F - G \in I(V)$.

DEFINITION 1.55. The *coordinate ring* of V is the k-algebra $k[V]$, which is the quotient

$$k[V] = k[X_1, \dots, X_n]/I(V) .$$

The coordinate ring is the smallest ring, containing the coordinate functions, explaining the traditional terminology. It is naturally a k-algebra; recall that an algebra A over a field k (or shortly a *k-algebra*) is a ring, which with its additive group structure is also a vector space over k, while scalar multiplication is compatible with the multiplication in the ring: $(\lambda a)b = a(\lambda b) = \lambda(ab)$ for all $\lambda \in k$ and $a, b \in A$.

Let $X \subset V$ be an affine algebraic set, then $I(V) \subset I(X)$ and $I(X)/I(V)$ is an ideal in $k[V] = k[X_1, \ldots, X_n]/I(V)$. So also on V we have operations $V(-)$ and $I(-)$, and a Zariski topology.

Let now $V \subset \mathbb{A}^n(K)$ and $W \subset \mathbb{A}^m(K)$ be algebraic sets and write $X_1, \ldots, X_n$ for the coordinates on $\mathbb{A}^n(K)$, and $Y_1, \ldots, Y_m$ for those on $\mathbb{A}^m(K)$.

DEFINITION 1.56. A map $f \colon V \to W$ is a *polynomial map* if there are polynomials $F_1, \ldots, F_m \in k[X_1, \ldots, X_n]$, such that

$$f(P) = (F_1(P), \ldots, F_m(P)) \in W \subset \mathbb{A}^m(K)$$

for all $P \in V$.

LEMMA 1.57. *A map $f \colon V \to W$ is a polynomial map if and only if $f_j := Y_j \circ f \in k[V]$ for $j = 1, \ldots, m$.*

PROOF. If f is a polynomial map, then we can write $f_j(P) = F_j(P)$ for some polynomials, determined up to $I(V)$, so f_j is a well-determined element of $k[V]$.

Conversely, if $f_j = Y_j \circ f \in k[V]$, then by definition there exists a polynomial F_j with $F_j(P) = f_j(P)$, so $f(P) = (F_1(P), \ldots, F_m(P))$. $\square$

The composition of polynomial maps is defined in the obvious way.

DEFINITION 1.58. A polynomial map $f \colon V \to W$ is an *isomorphism*, if f is a bijection with polynomial inverse: if there exists a polynomial map $g \colon W \to V$ with $f \circ g = \mathrm{id}_W$ and $g \circ f = \mathrm{id}_V$.

EXAMPLE 1.59. Let $V = \mathbb{A}^1(K)$, $W = V(Y_1^2 - Y_2^3) \subset \mathbb{A}^2(K)$. The polynomial map $f \colon V \to W$, given by $(Y_1, Y_2) = (X^3, X^2)$, is a bijection, but its inverse $X = Y_1/Y_2$ is not a polynomial map.

THEOREM 1.60. *Let $V \subset \mathbb{A}^n(K)$ and $W \subset \mathbb{A}^m(K)$ be algebraic k-sets.*

(1) *A polynomial map $f \colon V \to W$ induces a k-algebra homomorphism $f^* \colon k[W] \to k[V]$, given by $f^*(g) = g \circ f$.*
(2) *Any k-algebra homomorphism $\Phi \colon k[W] \to k[V]$ is of the form $\Phi = f^*$ for a uniquely determined polynomial map $f \colon V \to W$.*

PROOF.
(1) One has $f^*(g_1 + g_2) = (g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f = f^*(g_1) + f^*(g_2)$ and $f^*(g_1 g_2) = (g_1 g_2) \circ f = (g_1 \circ f)(g_2 \circ f) = (f^* g_1)(f^* g_2)$. Furthermore $f^*(a) = a$ for $a \in k$.

(2) Let $y_i = Y_i \bmod I(W)$ be the i-th coordinate function. We have to define $y_i = f_i(x_1, \dots, x_n)$, and we do this by $f_i(x_1, \dots, x_n) = \Phi(y_i)$. Then $f = (f_1, \dots, f_m)$ is a polynomial map $f\colon V \to \mathbb{A}^n(K)$. We have to show that $f(V) \subset W$, or $I(W) \subset I(f(V))$. Let $G \in I(W)$. Then $G \circ f$ is a polynomial in the $f_i = \Phi(y_i)$. As Φ is a homomorphism, $G \circ f = \Phi(G) = \Phi(0) = 0$. So $G \circ f \in I(V)$ and $G \in I(f(V))$. An homomorphism is determined by its values on generators, so $\Phi = f^*$ and this determines f. □

LEMMA 1.61.

(1) *If* $U \xrightarrow{f} V \xrightarrow{g} W$, *then* $(g \circ f)^* = f^* \circ g^*$.
(2) $f\colon V \to W$ *is an isomorphism if and only if* $f^*\colon k[W] \to k[V]$ *is an isomorphism.*

REMARK 1.62. If $I \subset k[X_1, \dots, X_n]$ is an arbitrary ideal, then we also call $k[X_1, \dots, X_n]/I =: k[X]$ the coordinate ring of the associated k-scheme X. In particular, if X is a fat point, then $k[X]$ is a finite-dimensional k-algebra. A polynomial map $f\colon X \to Y$ is as before given by restriction of a polynomial map $\mathbb{A}^n \to \mathbb{A}^m$ and the correspondence between polynomial maps and k-algebra homomorphims works as above.

1.11. Regular and rational functions

DEFINITION 1.63. Let V be an affine algebraic set and $f \in k[V]$. The set

$$D(f) = \{P \in V \mid f(P) \neq 0\}$$

is called a *basic open set.*

DEFINITION 1.64. Let U be an open subset of V. A function $r\colon U \to K$ is *regular* in $P \in U$ if there exist elements $g, h \in k[V]$ such that $P \in D(h) \subset U$ and $r = g/h$ on $D(h)$. We denote the k-algebra of all functions, regular on the whole of U, by $\mathcal{O}(U)$.

REMARK 1.65. The representation $r = g/h$ need not be unique. For example, let r be the restriction of the rational function $\frac{X}{Z}$ to $V(XY - ZT) \subset \mathbb{A}^4(k)$, see the exercises.

THEOREM 1.66. *For a basic open set* $D(f)$ *one has* $\mathcal{O}(D(f)) = k[V][\frac{1}{f}]$, *where* $k[V][\frac{1}{f}]$ *is the ring of polynomials in* $\frac{1}{f}$ *with coefficients in* $k[V]$.

PROOF. Let $r \in \mathcal{O}(D(f))$. Consider the ideal of denominators of r

$$\Delta_r = \{0\} \cup \{h \in k[V] \mid D(h) \subset D(f), \quad r = \frac{g}{h} \text{ on } D(h)\}\,.$$

This is an ideal, as $g/h = gl/hl$, and if $r = g/h = l/m$, then also $r = (g + l)/(h + m)$. For all $P \in D(f)$ we have $r(P) = \frac{g(P)}{h(P)}$ with $h(P) \neq 0$, so $P \notin V(\Delta_r)$, therefore $V(\Delta_r) \subset V(f)$, that is f vanishes on $V(\Delta_r)$ and thus $f^n \in \Delta_r$, by the Nullstellensatz. This implies that $r = g/f^n$ on $D(f^n) = D(f)$. □

COROLLARY 1.67. *$\mathcal{O}(V) = k[V]$.*

LEMMA 1.68. *Let U_1 and U_2 be open sets of V, $r_1 \in \mathcal{O}(U_1)$, $r_2 \in \mathcal{O}(U_2)$. Suppose that $r_1|_U = r_2|_U$ on an open dense subset U with $U \subset U_1 \cap U_2$. Then $r_1|_{U_1\cap U_2} = r_2|_{U_1\cap U_2}$.*

PROOF. Set $A = \{P \in U_1 \cap U_2 \mid r_1|_{U_1\cap U_2}(P) = r_2|_{U_1\cap U_2}(P)\}$. It is a closed subset of $U_1 \cap U_2$: if $P \in U_1 \cap U_2 \setminus A$ and $r_1|_{U_1\cap U_2} - r_2|_{U_1\cap U_2} = f/g$ on $D(g) \subset U_1 \cap U_2$, then $f(P) \neq 0$ and $f/g \neq 0$ on $D(f) \cap D(g)$. As $U \subset A$ and U is dense in V, we have $A = U_1 \cap U_2$. □

COROLLARY 1.69. *Let $U \subset V$ be dense and open and $r \in \mathcal{O}(U)$. Then there are a uniquely determined dense open subset U' with $U \subset U'$ and an $r' \in \mathcal{O}(U')$ with $r'|_U = r$, such that r' cannot be extended to a strictly larger open dense subset.*

DEFINITION 1.70. A regular function r, defined on an open dense subset $U \subset V$, is called a *rational function* on V. The maximal open subset U' to which r can be extended, is called the *domain of definition* $\mathrm{dom}(r)$ of r, and $V \setminus \mathrm{dom}(r)$ its *polar* set.
One adds, subtracts and multiplies rational functions by doing this on the intersection of their domains of definition. This makes the set $R(V)$ of all rational functions on V into a k-algebra.

THEOREM 1.71. *Let $V = \bigcup_{i=1}^k V_i$ be the decomposition of V into irreducible components. The map*

$$R(V) \to R(V_1) \times \cdots \times R(V_k)\ , \qquad r \mapsto (r|_{V_1}, \ldots, r|_{V_k})$$

is an isomorphism of k-algebras.

PROOF. We first show that the map is well-defined. Let $r \in R(V)$. If W is an irreducible component of V, then $\mathrm{dom}(r) \cap W$ is open and dense in W, and the restriction of r is regular on $\mathrm{dom}(r) \cap W$: just represent r locally as f/g with $f, g \in k[V]$, then $r = \bar{f}/\bar{g}$ with $\bar{f}, \bar{g}$ the residue classes of f and g in $k[W] = k[V]/I(W)$.

Now let $(r_1, \ldots, r_k) \in \prod R(V_i)$ and consider for all i the restriction r_i' of r_i to $(V_i \setminus \bigcup_{j\neq i} U_j) \cap U_i = U_i'$. Then U_i' is open and dense in V_i and $U_i' \cap U_j' = \emptyset$ for $i \neq j$. The r_i' define a regular function on the open and dense subset $\cup U_i$ of V and therefore a rational function r on V. Lemma 1.68 implies that the map $(r_1, \ldots, r_k) \mapsto r$ is the inverse of the map in the statement. □

If V is an (irreducible) variety, its ideal is prime, and the ring $k[V]$ does not contain zero divisors. Therefore this ring has a quotient field $k(V)$.

THEOREM 1.72. *Let V be an affine variety. Then $R(V)$ is isomorphic to the quotient field $k(V)$.*

PROOF. Each $f/g \in k(V)$ defines a rational function, as f/g is regular on the open and dense set $D(g)$. Conversely, let r be defined on U. Then the closed set $V \setminus U$ is of the form $V(g_1, \dots, g_k)$, so $U \supset D(g)$ for some polynomial g. By theorem 1.66 the restriction of r to $D(g)$ is of the form f/g^n for some n. □

1.12. The local ring of a point

Let $P \in V$ be a point of an affine algebraic set. Consider the collection $\mathfrak{U}$ of all open subsets of V containing P. On $\bigcup_{U \in \mathfrak{U}} \mathcal{O}(U)$ we define the equivalence relation $r_1 \in \mathcal{O}(U_1) \sim r_2 \in \mathcal{O}(U_2)$ if there exists an $U \subset U_1 \cap U_2 \in \mathfrak{U}$ such that $r_1|_U = r_2|_U$. An equivalence class is called a *germ* of a regular function at P.

DEFINITION 1.73. Let $P \in V$ be a point of an affine algebraic set. Its *local ring* is the ring of germs of regular functions at $P \in V$

REMARK 1.74. If V is irreducible, then

$$\mathcal{O}_{V,P} = \{r \in R(V) \mid r \text{ is regular in } P\} \ .$$

LEMMA 1.75. *The ring $\mathcal{O}_{V,P}$ is a local ring, that is, it has exactly one maximal ideal, which is*

$$\mathfrak{m}_{V,P} = \{r \in \mathcal{O}_{V,P} \mid r(P) = 0\} \ .$$

PROOF. Let $I \subset \mathcal{O}_{V,P}$ be an ideal which contains an f with $f(P) \neq 0$. Then $1/f \in \mathcal{O}_{V,P}$ and $1 = (1/f) \cdot f \in I$. □

We recall the concept of localisation in rings.

DEFINITION 1.76. Let R be a ring. A *multiplicative system* in R is subset $S \subset R^* = R \setminus 0$ with the properties that $1 \in S$ and if $a, b \in S$, then $ab \in S$.

EXAMPLE 1.77. An ideal I is prime if and only if $R \setminus I$ is a multiplicative system. A ring R is an integral domain if and only if the zero ideal is prime, that is if and only if R^* is a multiplicative system.

We now allow elements of S in the denominator. Define the following equivalence relation on $R \times S$:

$$(r_1, s_1) \sim (r_2, s_2) \quad \iff \quad \exists\, s \in S \colon s(r_1 s_2 - r_2 s_1) = 0 \ .$$

An equivalence class is denoted by $\frac{r}{s}$ and the set of equivalence classes by R_S. With the usual addition and multiplication

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \ , \qquad \frac{r_1}{s_1} \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$$

R_S becomes a ring with identity $1 = \frac{1}{1}$ and the map $R \to R_S$, $r \mapsto \frac{r}{1}$ is a ring homomorphism. It is injective if and only if S does not contain zero divisors.

DEFINITION 1.78. The ring R_S is the *localisation* of R with respect to the multiplicative system S.

EXAMPLE 1.79. If R is an integral domain and $S = R^*$, then R_S is the field of fractions $Q(R)$. If R is arbitrary, and S the multiplicative system of non-zero-divisors, then R_S is the *total ring of fractions*, also denoted by $Q(R)$.

For an affine algebraic set V the ring of rational functions $R(V)$ is isomorphic to the total ring of fractions $Q(k[V])$.

EXAMPLE 1.80. For an integral domain and an $f \in R$ let $S_f = \{f^n \mid n \geq 0\}$. We set $R_f := R_{S_f}$. Then $R_f = R[1/f]$.

NOTATION. Let $\mathfrak{p}$ be a prime ideal in R and $S_\mathfrak{p} = R \setminus \mathfrak{p}$. We set $R_\mathfrak{p} := R_{S_\mathfrak{p}}$.

The ring $R_\mathfrak{p}$ is a local ring with maximal ideal $\mathfrak{p}R_\mathfrak{p}$.

LEMMA 1.81. *Let $M_P = \{f \in k[V] \mid f(P) = 0\}$ be the maximal ideal defining a point $P \in V$ The local ring $\mathcal{O}_{V,P}$ of a point P is the localisation $k[V]_{M_P}$ of $k[V]$ with respect to $k[V] \setminus M_P$.*

PROOF. The condition that two fractions $f/h \in \mathcal{O}(U_1)$ and $g/l \in \mathcal{O}(U_2)$ represent the same germ is that they agree on the intersection with an open subset of the type $D(w)$ for some $w \in k[V] \setminus M_P$, that is $whl(f/h - g/l) = w(fk - gh) = 0 \in k[V]$. This is the definition of localisation with respect to $k[V] \setminus M_P$. □

1.13. Rational maps

Just as rational functions, which are not functions in a set-theoretic sense, as they are not everywhere defined, we often need maps, which are only defined on dense open subsets.

DEFINITION 1.82. A *rational map* $f \colon V \dashrightarrow W \subset \mathbb{A}^m(K)$ between algebraic k-sets is a map, defined on a dense open subset $U \subset V$, as $f = (f_1, \dots, f_m)$ with $f_i \in \mathcal{O}(U)$ and $f(U) \subset W$.

For the definition of the composition of two rational maps $f \colon V \dashrightarrow W$ and $g \colon W \dashrightarrow X$ one has to be careful. What should be $g(f(P))$ if $f(P)$ lies outside the domain of definition of g? In particular, if the whole image of V lies outside, we are in trouble. If we want to define the composition for all g, we need that the image is dense.

DEFINITION 1.83. A rational map $f \colon V \dashrightarrow W$ is *dominant* if $f(\mathrm{dom}(f))$ is a Zariski dense subset of W.

We now investigate what this means algebraically. As rational maps can be defined on each irreducible component independently, we do this only for varieties.

PROPOSITION 1.84. *A rational map $f\colon V \dashrightarrow W$ between varieties is dominant if and only if the induced map $f^*\colon k[W] \to k(V)$ is injective.*

PROOF. The map f^* is defined, as we always can replace y_i by f_i in a polynomial. Then $g \in \ker f^*$ if and only if $g(f(P)) = 0$ for all $P \in \mathrm{dom}(f)$ if and only if $f(\mathrm{dom}(f)) \subset V(g)$. So f^* is not injective if and only if $f(\mathrm{dom}(f))$ is a proper algebraic subset. $\square$

If f^* is injective, we can also replace the y_i by f_i in denominators, so we get a map $f^*\colon k(W) \to k(V)$ between function fields. Similar to theorem 1.60 we have

THEOREM 1.85.

(1) *A dominant rational map $f\colon V \dashrightarrow W$ between varieties induces a field homomorphism $f^*\colon k(W) \to k(V)$.*
(2) *Any field homomorphism $\Phi\colon k(W) \to k(V)$ is of the form $\Phi = f^*$ for a uniquely determined dominant map $f\colon V \dashrightarrow W$.*

DEFINITION 1.86. A dominant rational map $f\colon V \dashrightarrow W$ between varieties is a *birational isomorphism* if f^* is an isomorphism.

DEFINITION 1.87. A variety V is *rational* if its function field $k(V)$ is isomorphic to $k(X_1, \dots, X_n)$.

EXAMPLE 1.88. An irreducible conic (with a point P defined over k) is k-rational: parametrise using the pencil of lines through P.

1.14. Quasi-affine and affine varieties

DEFINITION 1.89. A *quasi-affine variety* is an open subset of an affine variety.
A morphism f from a quasi-affine variety $U_1 \subset V$ to $U_2 \subset W$ is a rational map $f\colon V \dashrightarrow W$, which is regular at every point $P \in U_1$, such that $f(U_1) \subset U_2$.
An isomorphism is a morphism $f\colon U_1 \to U_2$ with inverse morphism: there exists a morphism $g\colon U_2 \to U_1$ with $g \circ f = \mathrm{id}_{U_1}$ and $f \circ g = \mathrm{id}_{U_2}$.

EXAMPLE 1.90. A basic open set $D(f) \subset V$ is a quasi-affine variety. It is isomorphic to an affine variety, namely $\Gamma_f \subset V \times \mathbb{A}^1$, the graph of $1/f$. If $V = V(I)$ with $I \subset k[X_1, \dots, X_n]$, then Γ_f is defined by the ideal $I + (Tf - 1) \subset k[X_1, \dots, X_n, T]$. The maps $\Gamma_f \to D(f)$, $(x_1, \dots, x_n, t) \mapsto (x_1, \dots, x_n)$, and $D(f) \to \Gamma_f$, $(x_1, \dots, x_n) \mapsto (x_1, \dots, x_n, 1/f(x_1, \dots, x_n))$, are each other's inverse.

We would like to say that $D(f)$ *is* an affine variety. We extend the concept of variety to be independent of a particular embedding in affine space.

DEFINITION 1.91. An (abstract) *affine variety* is a set V together with a finitely generated k-algebra $k[V]$ of functions $f: V \to K$, mapping the k-rational points of V to k, such that for some choice of generators $x_1, \dots, x_n$ the map $V \to \mathbb{A}^n(K)$, $P \mapsto (x_1(P), \dots, x_n(P))$ gives a bijection between V and an affine variety $\mathrm{im}(V) \subset \mathbb{A}^n(K)$.

CHAPTER 2

Projective varieties

2.1. Projective space

Let V be a (finitely-dimensional) vector space over k. We define the projectivisation of V as the space of all lines through the origin (that is, all 1-dimensional linear subspaces).

DEFINITION 2.1. Let V be a k-vector space. Consider on $V \setminus \{0\}$ the equivalence relation

$$v \sim w \Longleftrightarrow \exists\, \lambda \in k^* : v = \lambda w \ .$$

The *projective space* $\mathbb{P}(V)$ associated to V is the quotient

$$\mathbb{P}(V) := (V \setminus \{0\})/ \sim \ .$$

The dimension of $\mathbb{P}(V)$ is $\dim V - 1$.

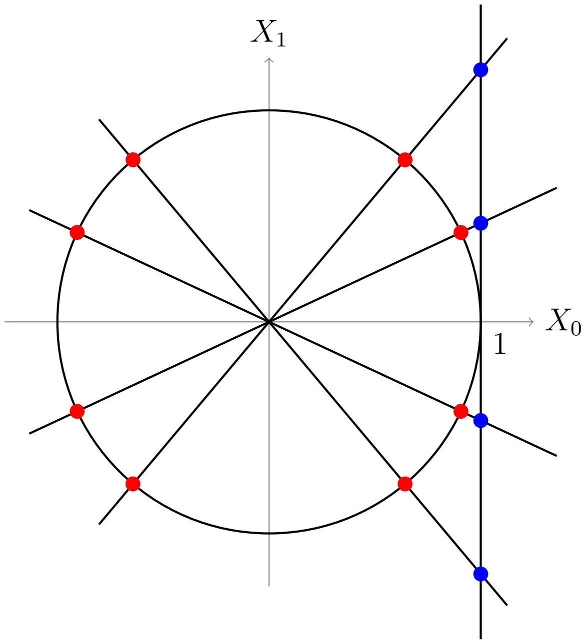
In particular, if $V = k^{n+1}$, we get projective n-space $\mathbb{P}^n(k) = \mathbb{P}(k^{n+1})$. Its elements are called *points*. Two points $(a_0, \dots, a_n) \in k^{n+1}$ and $(\lambda a_0, \dots, \lambda a_n) \in k^{n+1}$, $\lambda \in k^*$, define the same point in $\mathbb{P}^n$, so only the ratios of a_i have a meaning. We write therefore $(a_0 : \dots : a_n)$.

DEFINITION 2.2. If $X_0, \dots, X_n$ are coordinates on k^{n+1}, then their ratios are *homogeneous coordinates* on $\mathbb{P}^n$, denoted by $(X_0 : \dots : X_n)$.

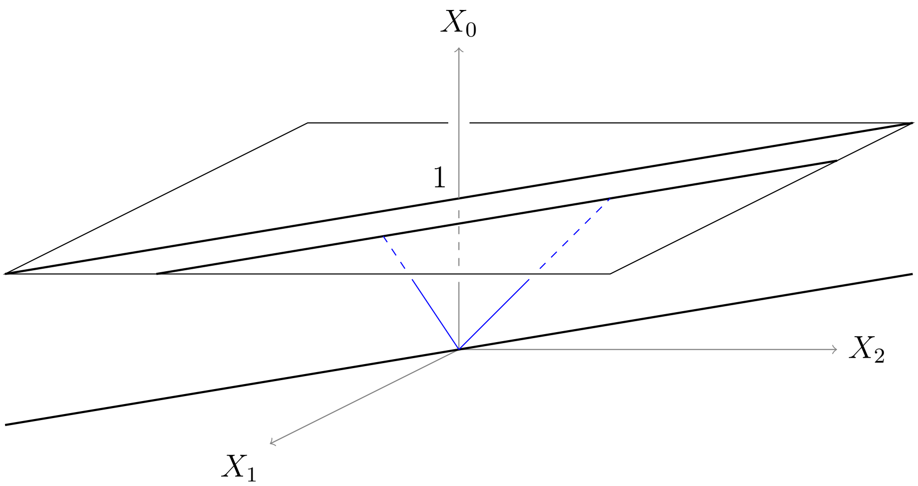
We can embed $\mathbb{A}^n$ in $\mathbb{P}^n$ by $(X_1, \dots, X_n) \mapsto (1 : X_1 : \dots : X_n)$. In fact, for every $0 \le i \le n$ we have a standard way to decompose $\mathbb{P}^n$ into affine space $\mathbb{A}^n_i$ and a hyperplane at infinity $H_i = \{(X_0 : \dots : X_n) \mid X_i = 0\}$; we embed $\mathbb{A}^n$ by $(X_1, \dots, X_n) \mapsto (X_1 : \dots : X_i : 1 : X_{i+1} : \dots : X_n)$. The image $\mathbb{A}^n_i$ is given by $X_i \neq 0$.

EXAMPLE 2.3. Take $n = 1$. Over the reals we have $\mathbb{P}^1(\mathbb{R}) \cong \mathbb{R} \cup \{\infty\}$. Topologically, we get $\mathbb{P}^1(\mathbb{R})$ by identifying opposite points on the circle. So $\mathbb{P}^1(\mathbb{R})$ is homeomorphic to S^1.

In the complex case we have something similar: $\mathbb{P}^1(\mathbb{C}) \cong \mathbb{C} \cup \{\infty\}$, also known as the Riemann sphere. Stereographic projection maps $S^2 \setminus \{\text{north pole}\}$ conformally onto $\mathbb{C}$ and can be extended to $S^2 \to \mathbb{P}^1(\mathbb{C})$.



EXAMPLE 2.4. For $n = 2$ we have that a line through the origin intersects the affine plane $V(X_0 - 1) \subset k^3$ in a point, except when it is parallel to this plane, that is, when it lies in $V(X_0)$. The space of lines in this plane is a $\mathbb{P}^1$, also called the *line at infinity*. So we have a decomposition $\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$. Two lines in $\mathbb{A}^2$ with the same direction are parallel in $\mathbb{A}^2$, but share the same point at infinity (represented by the line through their common direction vector). Therefore two lines in $\mathbb{P}^2$ always intersect.



DEFINITION 2.5. A projective *subspace* of $\mathbb{P}(V)$ is a subset of the form $\mathbb{P}(W)$ for W a linear subspace $W \subset V$.

LEMMA 2.6. *Let* $\mathbb{P}(W_1)$ *and* $\mathbb{P}(W_2)$ *be projective subspaces of* $\mathbb{P}(V)$. *If* $\dim \mathbb{P}(W_1) + \dim \mathbb{P}(W_2) \geq \dim \mathbb{P}(V)$, *then* $\mathbb{P}(W_1) \cap \mathbb{P}(W_2) \neq \emptyset$.

PROOF. We have $\mathbb{P}(W_1) \cap \mathbb{P}(W_2) = \mathbb{P}(W_1 \cap W_2)$ and $\dim W_1 \cap W_2 - 1 \geq \dim W_1 + \dim W_2 - \dim V - 1 = \dim \mathbb{P}(W_1) + \dim \mathbb{P}(W_2) - \dim \mathbb{P}(V) \geq 0$. □

We want to look at zeroes in $\mathbb{P}^n$ of polynomials. The condition that $f \in k[X_0, \dots, X_n]$ has a zero in $(a_0 : \cdots : a_n) \in \mathbb{P}^n$ means that f vanishes on the whole line through $(a_0, \dots, a_n) \in \mathbb{A}^{n+1}$, that is $f(\lambda a_0, \dots, \lambda a_n) = 0$ for all $\lambda \in k^*$.

DEFINITION 2.7. A polynomial $f \in k[X_0, \dots, X_n]$ is *homogeneous* (of degree d) if all monomials in f have the same degree (namely, d).

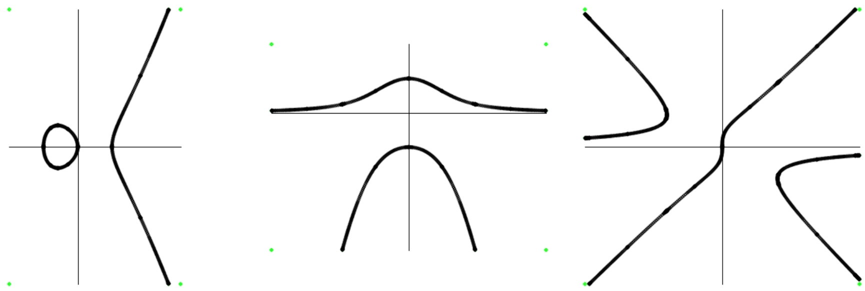
LEMMA 2.8. *We have $f(\lambda X_0, \dots, \lambda X_n) = \lambda^d f(X_0, \dots, X_n)$ for all $\lambda \in k$, if f is homogeneous of degree d. The converse holds if k is infinite. For any field it holds that f is homogeneous of degree d if and only if $f(\lambda X_0, \dots, \lambda X_n) - \lambda^d f(X_0, \dots, X_n)$ as a polynomial in $k[X_0, \dots, X_n, \lambda]$ is the zero polynomial.*

Now write $f = f_0 + \cdots + f_d$ as a sum of homogeneous components. Then $f(\lambda a_0, \dots, \lambda a_n) = f_0(a_0, \dots, a_n) + \cdots + \lambda^d f_d(a_0, \dots, a_n)$ and if $f(\lambda a_0, \dots, \lambda a_n) = 0$ for infinitely many λ, then $f_0(a_0, \dots, a_n) = \cdots = f_d(a_0, \dots, a_n) = 0$. This means that $(a_0 : \cdots : a_n) \in \mathbb{P}^n$ is a zero of homogeneous polynomials.

REMARK 2.9. While the zero set of a homogeneous polynomial in $\mathbb{P}^n$ is thus well defined, the value of a polynomial function in a point makes no sense. In fact the only regular functions on $\mathbb{P}^n$, and more generally on projective varieties, are the constant functions.

Let $\bar{f}(X_0, \dots, X_n)$ be a homogeneous polynomial and consider an affine subspace $\mathbb{A}^n \subset \mathbb{P}^n$, say the one given by $X_0 \neq 0$. Putting $X_0 = 1$ in $\bar{f}$ gives a polynomial $f(X_1, \dots, X_n) = \bar{f}(1, X_1, \dots, X_n)$ in *inhomogeneous coordinates* $(X_1, \dots, X_n)$. Conversely, given $V = V(f) \subset \mathbb{A}^n$ we find an equation $\bar{f}$ for the *projective closure* $\bar{V}$ by homogenising: replace X_i by X_i/X_0 and multiply with X_0^d to clear denominators. So if $f(X_1, \dots, X_n) = f_0(X_1, \dots, X_n) + \cdots + f_d(X_1, \dots, X_n)$, then $\bar{f}(X_0, X_1, \dots, X_n) = X_0^d f_0(X_1, \dots, X_n) + \cdots + f_d(X_1, \dots, X_n)$.

EXAMPLE 2.10. Consider the plane cubic curve $C \colon Y^2 = X^3 - X$. We study how it looks like at infinity. We first homogenise: the curve $\bar{C} \subset \mathbb{P}^2$ is given by $ZY^2 = X^3 - XZ^2$. We look at the two other affine charts, namely $X = 1$ and $Y = 1$. In $X = 1$ we have $ZY^2 = 1 - Z^2$ and $Z = X^3 - XZ^2$ in $Y = 1$. The only point at infinity is the origin of the chart $Y = 1$. It is an inflection point.



$Y^2 = X^3 - X$ $ZY^2 = 1 - Z^2$ $Z = X^3 - XZ^2$

Coordinate transformations of $\mathbb{P}^n$ should come from coordinate transformations in k^{n+1}, which map lines through the origin to lines through the origin. We also want them to be algebraic. The easiest way to achieve this is to take linear transformations in k^{n+1}, given by an invertible $(n+1) \times (n+1)$-matrix. These are in fact the only automorphisms of $\mathbb{P}^n$.

Definition 2.11. The group of projective transformations of $\mathbb{P}^n$ is $PGl(n+1,k) = Gl(n+1,k)/k^*$.

2.2. Algebraic subsets

Definition 2.12. An ideal $I \subset k[X_0, \dots, X_n]$ is *homogeneous* if for all $f \in I$ the components f_j of the homogeneous decomposition $f = f_0 + \dots + f_d$ satisfy $f_j \in I$.

Proposition 2.13. *An ideal is homogeneous if and only if it can be generated by homogeneous elements.*

Proof. The collection of homogeneous components of a set of generators of a homogeneous ideal also generate the ideal.

Conversely, if I is generated by homogeneous elements $f^{(i)}$ of degree d_i, and $f = \sum r^{(i)} f^{(i)}$, we can decompose the $r^{(i)}$ into homogeneous components $r^{(i)}_j$ and the homogeneous component of f of degree k is $\sum r^{(i)}_{k-d_i} f^{(i)} \in I$. $\square$

Now we can define the homogeneous V–I correspondences between homogeneous ideals in $k[X_0, \dots, X_n]$ and subsets of $\mathbb{P}^n(K)$, with $k \subset K$ an algebraically closed extension.

$$V(J) = \{P \in \mathbb{P}^n(K) \mid f(P) = 0 \text{ for all homogeneous } f \in J\} ,$$
$$I(X) = \{f \in k[X_0, \dots, X_n] \mid f(P) = 0 \text{ for all } P \in X\} .$$

Definition 2.14. An *algebraic subset* of $\mathbb{P}^n$ is a set of the form $V(J)$. The *Zariski topology* on $\mathbb{P}^n$ has the algebraic subsets as closed sets.

With the Zariski topology $\mathbb{P}^n$ is a Noetherian topological space. In particular, the concept of irreducibility is defined.

We want to give the projective version of the Nullstellensatz. It follows from the affine case: the zero set of a homogeneous ideal $I \subset k[X_0, \dots, X_n]$ is, considered in $\mathbb{A}^{n+1}$, a cone with vertex at the origin. There is one problem: whereas in $\mathbb{A}^{n+1}$ the empty set is defined by the ideal (1), this is not the only ideal with $V(I) = \emptyset \subset \mathbb{P}^n$.

PROPOSITION 2.15. *Let $I \subset k[X_0, \dots, X_n]$ be a homogeneous ideal. Let $k \subset K$ be an algebraically closed extension. Then*

$$V(I) = \emptyset \subset \mathbb{P}^n(K) \iff (X_0, \dots, X_n) \subset \sqrt{I}\ .$$

PROOF. Let $V_{\text{aff}}(I)$ be the zero set of I in $\mathbb{A}^{n+1}$. Then $V(I) = \emptyset$ if and only if $V_{\text{aff}}(I) \subset \{0\}$, and $V_{\text{aff}}(I) = \{0\}$ if and only if $\sqrt{I} = (X_0, \dots, X_n)$. □

DEFINITION 2.16. A homogeneous ideal $I \subset k[X_0, \dots, X_n]$ with $\sqrt{I} = (X_0, \dots, X_n)$ is called *irrelevant*.

If J is a homogeneous ideal and I is an irrelevant ideal, then $V(J) = V(I \cap J)$. We can get rid of I by taking the radical, but this will not do if we care about multiple structures.

EXAMPLE 2.17. The ideal $J = (X^2)$ defines a 'double line' in $\mathbb{P}^2$. There are many other ideals, which do the same, e.g.,

$$(X^2) \cap (X^3, Y^3, Z^3) = (X^3, X^2Y^3, X^2Z^3)\ .$$

In terms of primary decomposition, the affine cone over the double line (a double plane in 3-space) has now an embedded component at its vertex.

DEFINITION 2.18. The *saturation* of a homogeneous ideal I is

$$I^{\text{sat}} = \{f \in k[X_0, \dots, X_n] \mid \exists s\ \forall g \in (X_0, \dots, X_n)^s \colon gf \in I\}\ .$$

In the sequel we consider mainly saturated homogeneous ideals.

THEOREM 2.19 (projective Nullstellensatz). *Let $k \subset K$ be an algebraically closed extension. For a homogeneous ideal $J \subset k[X_0, \dots, X_n]$ with $\mathbb{P}^n(K) \supset V(J) \neq \emptyset$ we have $I(V(J)) = \sqrt{J}$.*

PROOF. If $V(J) \neq \emptyset$ then $f \in I(V(J)) \Leftrightarrow f \in I(V_{\text{aff}}(J)) \Leftrightarrow f \in \sqrt{J}$. □

If we associate the irrelevant prime ideal $(X_0, \dots, X_n)$ to the empty set, we obtain bijections between homogeneous ideals of $k[X_0, \dots, X_n]$

and k-subsets in $\mathbb{P}^n(K)$:

$$\begin{array}{ccc}
\{\text{proper homog. saturated ideals}\} & \xleftrightarrow{1:1} & \{\text{proj. } k\text{-schemes}\} \\
\cup & & \cup \\
\{\text{proper homog. radical ideals}\} & \xleftrightarrow{1:1} & \{\text{proj. algebraic sets}\} \\
\cup & & \cup \\
\{\text{homog. prime ideals}\} & \xleftrightarrow{1:1} & \{\text{proj. varieties}\} \\
\cup & & \cup \\
\{\text{homog. maximal ideals}\} & \xleftrightarrow{1:1} & \{\text{points}\}
\end{array}$$

Besides taking the affine cone there is another important operation between affine and projective geometry, of taking the projective closure.

DEFINITION 2.20. Let $\mathbb{A}^n \subset \mathbb{P}^n$ be the open subset with $X_0 \neq 0$. The *projective closure* $\bar{V}$ of an affine algebraic set $V \subset \mathbb{A}^n$ is the smallest closed subset containing V.

DEFINITION 2.21. Let $f \in k[X_1, \ldots, X_n]$ with homogeneous decomposition $f_0(X_1, \ldots, X_n) + \cdots + f_d(X_1, \ldots, X_n)$, $f_d \neq 0$. The *homogenisation* of f with respect to the variable X_0 is the homogeneous polynomial $\bar{f}(X_0, X_1, \ldots, X_n) = X_0^d f_0(X_1, \ldots, X_n) + \cdots + f_d(X_1, \ldots, X_n)$.

The *homogenisation* of an ideal $I \subset k[X_1, \ldots, X_n]$ is the ideal in $k[X_0, \ldots, X_n]$, generated by the homogenisations of all elements of I:

$$\bar{I} = (\bar{f} \mid f \in I) \ .$$

PROPOSITION 2.22. *The ideal of the projective closure $\bar{V}$ of an affine algebraic set V with $I(V) = I$ is $\bar{I}$.*

PROOF. Write $g(1, -)$ for the polynomial in $k[X_1, \ldots, X_n]$ obtained by substituting $X_0 = 1$ in $g(X_0, \ldots, X_n)$. If $g \in \bar{I}$, then $g(1, -) \in I$, for if $g = \sum r_i \bar{f}_i$, where $f_i \in I$, then $g(1, -) = \sum r_i(1, -) f_i \in I$. So $g(1, -)$ vanishes on V and therefore its homogenisation (which is g/X_0^a for some $a \geq 0$) vanishes on the closure $\bar{V}$. This shows that $\bar{I} \subset I(\bar{V})$.

Conversely, if $g \in I(\bar{V})$, then $g(1, -)$ vanishes on V, so $g(1, -) \in I$ and its homogenisation is contained in $\bar{I}$, by definition. Therefore $g \in \bar{I}$ □

REMARK 2.23. For a principal ideal $I = (f)$ one has $\bar{I} = (\bar{f})$, but in general $\bar{I}$ is not generated by the homogenisations of the generators of I. As an example, consider the generators $X_1^2 + X_2^3$, $X_1^2 + X_2^3 + X_3$ of the ideal $I = (X_1^2 + X_2^3, X_3)$. Then $\bar{I} = (X_0 X_1^2 + X_2^3, X_3)$, but homogenising only the generators gives the ideal $(X_0 X_1^2 + X_2^3, X_0 X_1^2 + X_2^3 + X_0^2 X_3) = (X_0 X_1^2 + X_2^3, X_0^2 X_3)$. This ideal has an irreducible component, contained in the hyperplane at infinity.

A set of generators $(f_1, \ldots, f_k)$ of I such that $\bar{I} = (\bar{f}_1, \ldots, \bar{f}_k)$, is called a *standard basis*. Buchberger's algorithm finds standard bases. It is implemented in computer algebra systems like SINGULAR and MACAULAY 2.

An ideal $I \subset k[X_1, \dots, X_n]$ is prime if and only if its homogenisation $\bar{I} \subset k[X_0, \dots, X_n]$ is prime (see the exercises).

PROPOSITION 2.24. *The map $V \mapsto \bar{V}$, which associates to an affine algebraic set V its projective closure, is a bijection between the set of non-empty affine algebraic sets in $\mathbb{A}^n$ and the set of projective algebraic sets in $\mathbb{P}^n$ without irreducible components, totally contained in the hyperplane at infinity.*
The set V is irreducible if and only if $\bar{V}$ is irreducible.

2.3. Rational maps

We now define when a function is regular. This goes analogously to the affine case (section 1.11).

DEFINITION 2.25. Let V be a projective algebraic set, with ideal $I(V) \subset k[X_0, \dots, X_n]$. The *homogeneous coordinate ring* of V is the quotient

$$k[V] = k[X_0, \dots, X_n]/I(V) \ .$$

DEFINITION 2.26. Let V be a projective algebraic set and $f \in k[V]$. The set

$$D(f) = \{P \in V \mid f(P) \neq 0\}$$

is a *basic open set*.

DEFINITION 2.27. Let U be an open subset of V. A function $r\colon U \to k$ is *regular* in $P \in U$ if there exist homogeneous elements $g, h \in k[V]$ of the same degree such that $P \in D(h) \subset U$ and $r = g/h$ on $D(h)$. We denote the k-algebra of all functions, regular on the whole of U, by $\mathcal{O}(U)$.

Now lemma 1.68 and corollary 1.69 hold with the same proof.

DEFINITION 2.28. A regular function r, defined on an open dense subset $U \subset V$, is called a *rational function* on V. The maximal open subset U' to which r can be extended, is called the *domain of definition* $\operatorname{dom}(r)$ of r, and $V \setminus \operatorname{dom}(r)$ its polar set.
One adds, subtracts and multiplies rational functions by doing this on the intersection of their domains of definition. This makes the set $R(V)$ of all rational functions on V into a k-algebra.

We can study the ring of rational functions projective varieties by looking at affine pieces. Let $\bar{V}$ be a projective algebraic set. Then there exists a linear function l such that no irreducible component of $\bar{V}$ is contained in $V(l)$: if $l \in I(\bar{V}_i)$ for all l, then $(X_0, \dots, X_n) \subset I(\bar{V}_i)$ so $\bar{V}_i = \emptyset$. So $l \notin I(\bar{V}_i)$ for all l in an open and dense set in the space of linear forms. Take now a linear form in the intersection of these open sets. By a (linear) coordinate transformation we can assume that $l = X_0$.

Let U be an open and dense set in V and therefore also in $\bar{V}$. Let $\mathcal{O}_V(U)$ be the ring of affine regular functions on U and $\mathcal{O}_{\bar{V}}(U)$ that of projective rational functions, regular on U. Every $r \in \mathcal{O}_V(U)$ can be considered as element of $\mathcal{O}_{\bar{V}}(U)$: represent $r = F/G$ on U with $F, G \in k[X_1, \dots, X_n]$. Now make F and G homogeneous of the same degree; this makes $r = \bar{f}/\bar{g}$ for some $\bar{f}, \bar{g} \in k[\bar{V}]$. Conversely, dehomogenising by setting $X_0 = 1$ shows that $\mathcal{O}_{\bar{V}}(U) \subset \mathcal{O}_V(U)$. We conclude:

Lemma 2.29. *Let U be an open set in an affine algebraic set V with projective closure $\bar{V}$. Then $\mathcal{O}_V(U) = \mathcal{O}_{\bar{V}}(U)$.*

Theorem 2.30. *Let $\bar{V}$ be the projective closure of a non-empty affine algebraic set V. Then $R(\bar{V}) \cong R(V)$. If $\bar{V}$ is irreducible, then $R(\bar{V})$ is a field.*

Definition 2.31. A *rational map* $f\colon V \dashrightarrow \mathbb{A}^m$ from a projective algebraic set V to affine space is a (partially defined map), given by $P \mapsto (f_1(P), \dots, f_m(P))$ with $f_i \in R(V)$. A rational map $f\colon V \dashrightarrow W \subset \mathbb{A}^m$ is given by a rational map $f\colon V \dashrightarrow \mathbb{A}^m$ with $f(\operatorname{dom} f) \subset W$.

Given a rational map $f\colon V \dashrightarrow \mathbb{A}^m$ we can consider it as a map $f\colon V \dashrightarrow \mathbb{A}^m \subset \mathbb{P}^m$ and clear denominators.

Definition 2.32. A *rational map* $f\colon V \dashrightarrow \mathbb{P}^m$ from a projective algebraic set V to projective space is a (partially defined map), given by $P \mapsto (f_0(P) : \cdots : f_m(P))$ with the $f_i \in k[V]$ homogeneous of the same degree.

There is a bijection between the set of rational maps $f\colon V \dashrightarrow \mathbb{A}^m$ and the set of rational maps $f\colon V \dashrightarrow \mathbb{P}^m$ with the property that $f(V) \not\subset (X_0 = 0)$. We get the following characterisation of regularity.

Proposition–Definition 2.33. *A rational map $f\colon V \dashrightarrow \mathbb{P}^m$ is regular at a point $P \in V$ if there is a representation $f = (f_0 : \cdots : f_m)$ such that there is at least one i with $f_i(P) \neq 0$, that is $P \notin V(f_0, \dots, f_m)$. The open set, where f is regular, is the domain of definition* $\operatorname{dom} f$ *of f.*

Definition 2.34. A rational map $f\colon V \dashrightarrow W \subset \mathbb{P}^m$ is given by a rational map $f\colon V \dashrightarrow \mathbb{P}^m$ with $f(\operatorname{dom} f) \subset W$

Example 2.35 (The rational normal curve of degree n in $\mathbb{P}^n$). Define $f\colon \mathbb{P}^1 \to \mathbb{P}^n$ by $(S : T) \mapsto (S^n : S^{n-1}T : \cdots : T^n)$. This is a regular map. Its image is given by $\binom{n}{2}$ equations, conveniently written as

$$\operatorname{Rank}\begin{pmatrix} X_0 & X_1 & \dots & X_{n-1} \\ X_1 & X_2 & \dots & X_n \end{pmatrix} \leq 1 ,$$

meaning that the 2×2 minors $X_iX_{j+1} - X_{i+1}X_j$ vanish.

DEFINITION 2.36. A rational map $f\colon V \dashrightarrow W$ between (affine or projective) algebraic sets is *birational*, or a *birational equivalence*, if f has a rational inverse $g\colon W \dashrightarrow V$, i.e., $f \circ g = \mathrm{id}_W$ and $g \circ f = \mathrm{id}_V$.

PROPOSITION 2.37. *A map $f\colon V \dashrightarrow W$ between varieties is birational if and only if f is dominant and $f^* : k(W) \to k(V)$ is an isomorphism. This is the case if and only if there exist open sets $V_0 \subset V$ and $W_0 \subset W$ such that $f|_{V_0}\colon V_0 \to W_0$ is an isomorphism.*

PROOF. The only problem is to find V_0 and W_0. As Miles Reid remarks in his book, you should skip this proof if you want to avoid an headache. We have that $f|_{\mathrm{dom}\, f}\colon \mathrm{dom}\, f \to W$ is regular, just as $g|_{\mathrm{dom}\, g}\colon \mathrm{dom}\, g \to V$, where g is the inverse to f. We set

$$V_0 = (f|_{\mathrm{dom}\, f})^{-1}\big((g|_{\mathrm{dom}\, g})^{-1}(\mathrm{dom}\, f)\big)\ ,$$
$$W_0 = (g|_{\mathrm{dom}\, g})^{-1}\big((f|_{\mathrm{dom}\, f})^{-1}(\mathrm{dom}\, g)\big)\ .$$

Note that $V_0 \subset \mathrm{dom}\, f$. So $f|_{\mathrm{dom}\, f}(P) \in (g|_{\mathrm{dom}\, g})^{-1}(\mathrm{dom}\, f)$ for $P \in V_0$. We observe that on $(g|_{\mathrm{dom}\, g})^{-1}(\mathrm{dom}\, f) \subset \mathrm{dom}\, g$ the map $f \circ g$ is a composition of regular maps. As it equals the identity as rational map, we get $f|_{\mathrm{dom}\, f} \circ g|_{\mathrm{dom}\, g}(Q) = Q$ for all $Q \in (g|_{\mathrm{dom}\, g})^{-1}(\mathrm{dom}\, f)$. Therefore $f|_{\mathrm{dom}\, f}(P) = f|_{\mathrm{dom}\, f} \circ g|_{\mathrm{dom}\, g} \circ f|_{\mathrm{dom}\, f}(P)$ and $f|_{V_0}(P) \in W_0$. The map $f|_{V_0}\colon V_0 \to W_0$ is regular with inverse $g|_{W_0}\colon W_0 \to V_0$. □

We have now two types of isomorphism. Birational equivalence gives a coarse classification, which is refined by biregular isomorphy. Classical Italian algebraic geometry was mostly concerned with birational geometry.

Our earlier definition of rational varieties can be formulated as: a variety is rational if it is birational to some $\mathbb{P}^n$.

EXAMPLE 2.38. The map $f\colon \mathbb{P}^1 \to C := V(ZY^2 - X^3) \subset \mathbb{P}^2$, given by $(S : T) \mapsto (ST^2 : T^3 : S^3)$, is birational. The restriction

$$f_0\colon \mathbb{P}^1 \setminus \{(1:0)\} \cong \mathbb{A}^1 \to C \setminus \{(0:0:1)\}$$

is an isomorphism.

EXAMPLE 2.39 (Projection from a point). The map $\pi\colon \mathbb{P}^n \dashrightarrow \mathbb{P}^{n-1}$, $(X_0 : \cdots : X_n) \mapsto (X_0 : \cdots : X_{n-1})$ is a rational map, everywhere defined except at the point $P = (0 : \cdots : 0 : 1)$. Affinely, in the chart $(X_0 = 1)$, this is just parallel projection $\mathbb{A}^n \to \mathbb{A}^{n-1}$.

Let now $n = 3$ and consider the quadric $Q = V(X_0X_3 - X_1X_2)$. Then $P = (0 : 0 : 0 : 1)$ lies on Q and the projection from P restricts to a birational map $Q \dashrightarrow \mathbb{P}^2$ with inverse

$$(X_0, X_1, X_2) \mapsto (X_0^2 : X_0X_1 : X_0X_2 : X_1X_2)\ .$$

The inverse is defined outside the set $V(X_0^2, X_0X_1, X_0X_2, X_1X_2) = V(X_0, X_1X_2)$, that is, outside the points $(0 : 1 : 0)$ and $(0 : 0 : 1)$.

2.4. Products

Contrary to the affine case, where $\mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$, the product of projective spaces is not a projective space: $\mathbb{P}^n \times \mathbb{P}^m \neq \mathbb{P}^{n+m}$. We argue in this section that it is a projective variety.

To define an abstract projective variety we cannot mimic the definition of an abstract affine variety (definition 1.91), as the homogeneous coordinate ring is not preserved by biregular isomorphisms. E.g., the rational normal curve of example 2.35 is isomorphic to $\mathbb{P}^1$, but its coordinate ring is just the subring $k[S^n, S^{n-1}T, \dots, T^n] \subset k[S,T]$.

We need a more general concept of variety. Just as a manifold is a space obtained by glueing together pieces that look like $\mathbb{R}^n$, a variety can be obtained by glueing together affine varieties. Projective varieties are of this type, because they have a covering by standard affine charts. As we already have the variety as global object, we do not have to worry about the glueing.

Returning to $\mathbb{P}^n \times \mathbb{P}^m$, we can easily give a covering by affine pieces. Recall that $\mathbb{A}^n_i \subset \mathbb{P}^n$ is the set $\{X_i \neq 0\}$. Then $\mathbb{A}^n_i \times \mathbb{A}^m_j \cong \mathbb{A}^{n+m}$ is for every i, j a standard affine piece.

Definition 2.40. The *Segre embedding* $s_{n,m} \colon \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^N$, $N = (n+1)(m+1) - 1$, is the map given in *bihomogeneous* coordinates by

$$(X_0, \dots, X_n; Y_0, \dots, Y_m) \mapsto (X_0Y_0 : X_0Y_1 : \dots : X_nY_{m-1} : X_nY_m) \,.$$

With coordinates Z_{ij} on $\mathbb{P}^N$ it is the map $Z_{ij} = X_iY_j$.

The image $\Sigma_{m,n} = s_{n,m}(\mathbb{P}^n \times \mathbb{P}^m)$ is the projective variety given by the determinantal equations

$$\operatorname{Rank} \begin{pmatrix} Z_{00} & \dots & Z_{0m} \\ \vdots & & \vdots \\ Z_{n0} & \dots & Z_{nm} \end{pmatrix} \leq 1 \,.$$

The affine piece $\mathbb{A}^n_i \times \mathbb{A}^m_j \cong \mathbb{A}^{n+m}$ is mapped isomorphically to the affine variety $\Sigma_{n,m} \cap \{Z_{ij} \neq 0\}$.

So once the appropriate definitions are made, we can state that the Segre embedding induces an isomorphism $\mathbb{P}^n \times \mathbb{P}^m \to \Sigma_{m,n}$ and that $\mathbb{P}^n \times \mathbb{P}^m$ *is* an abstract projective variety. As we do not have these definitions at our disposal, we have to content us with defining the product of $\mathbb{P}^n$ and $\mathbb{P}^m$ to be $\Sigma_{m,n}$. The product of a projective subvarieties of $\mathbb{P}^n$ and $\mathbb{P}^m$ is a subvariety of $\Sigma_{m,n}$.

Definition 2.41. A *quasi-projective variety* is an open subset of a projective variety.

This concept includes affine and projective varieties.

2.5. Linear systems

EXAMPLE 2.42. The *Veronese embedding* of $\mathbb{P}^2$ in $\mathbb{P}^5$ is given by

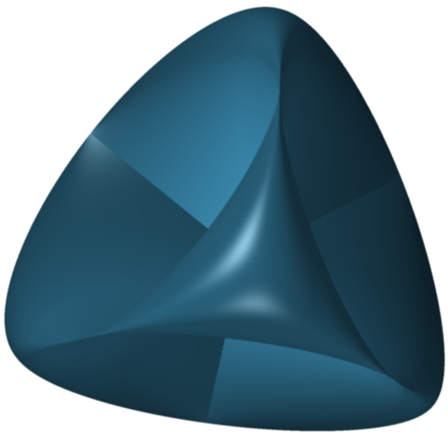
$$(X : Y : Z) \mapsto (X^2 : XY : XZ : Y^2 : YZ : Z^2) .$$

Its image, the Veronese surface V_2, is given by the (2×2)-minors of a symmetric (3×3)-matrix:

$$\operatorname{Rank} \begin{pmatrix} X_0 & X_1 & X_2 \\ X_1 & X_3 & X_4 \\ X_2 & X_4 & X_5 \end{pmatrix} \leq 1 .$$

The inverse map $V_2 \to \mathbb{P}^2$ is given by the rational map $(X_0 : X_1 : X_2 : X_3 : X_4 : X_5) \mapsto (X_0 : X_1 : X_2)$. This map is regular: at the points where the given formula does not work we take the ratio's of another row of the defining matrix.

The hyperplane section $X_2 = X_3$ is the image of the plane curve $V(XZ - Y^2)$. The Veronese map embeds this conic as rational normal curve of degree 4; with $X_2 = X_3$ the minors of the symmetric (3×3)-matrix define the same ideal as the minors of the matrix in example 2.35 in the case $n = 4$.



By projecting from a point outside the surface we obtain a surface in $\mathbb{P}^4$, which again can be projected to a quartic surface in $\mathbb{P}^3$. By imposing extra symmetry we obtain in this way a well known surface, the *Steiner Roman surface*, with parametrisation

$$(X : Y : Z) \mapsto (X^2 + Y^2 + Z^2 : YZ : XZ : XY)$$

and equation

$$X_2^2 X_3^2 + X_1^2 X_3^2 + X_1^2 X_2^2 - X_0 X_1 X_2 X_3 = 0 .$$

In $\mathbb{R}^3$: $X_0 \neq 0$ this is a model of the real projective plane. The map is not an immersion, but has pinch points.

This example can be generalised to all dimensions and degrees; the parametrisation of the rational normal curve of degree n is then a special case of this construction.

A hypersurface of degree d in $\mathbb{P}^n$ is the k-scheme given by a principal homogeneous ideal $I = (f)$ with $\deg f = d$. Let S_d be the vector space of all homogeneous polynomials of degree d in $k[X_0, \dots, X_n]$ (together with the zero polynomial). Two non-zero elements f and λf, $\lambda \in k^*$, determine the same hypersurface in $\mathbb{P}^n$ (possible with multiple components). So the space of all hypersurfaces of degree d is $\mathbb{P}(S_d)$.

Let now $V \subset \mathbb{P}^n$ be a projective variety with homogeneous coordinate ring $k[V]$. The vector space $S_d(V)$ of elements of degree d in $k[V]$ is the image of S_d under the quotient map $k[X_0, \dots, X_n] \to k[V] = k[X_0, \dots, X_n]/I(V)$.

Definition 2.43. A *linear system* on V is $\mathbb{P}(L)$, where $L \subset S_d(V)$ is a linear subspace.

If we take a basis of L and represent it by homogeneous polynomials $f_0, \dots, f_m \subset k[X_0, \dots, X_n]$, then we can write the equations of the hypersurfaces in the linear system (also called *divisors*) as

$$\lambda_0 f_0(X_0, \dots, X_n) + \cdots + \lambda_m f_m(X_0, \dots, X_n) = 0 \; .$$

The formula $Y_i = f_i$ defines a rational map

$$\varphi_L \colon V \dashrightarrow \mathbb{P}^m \; .$$

The hyperplane sections of $\varphi_L(V)$ are precisely the hypersurfaces in $\mathbb{P}(L)$. In particular, the coordinate hyperplanes intersect $\varphi_L(V)$ in the hypersurfaces $\{f_i = 0\}$. We can formulate this without coordinates: the linear system gives a rational map $\varphi_L \colon V \dashrightarrow \mathbb{P}(L^*)$, where L^* is the dual vector space. We have indeed the dual vector space, as the evaluation $\mathrm{ev}_P \colon f \mapsto f(P)$ in a point $P \in V$ is a linear function on L, well defined up to scalar multiplication. The image of a point $P \in V$ is the intersection of all hyperplanes corresponding to the hypersurfaces passing through P. In particular, φ_L is not regular in P if all the hypersurfaces in the linear system pass through P (cf. definition 2.33). Such points are called *base points* of the linear system.

Conversely, given a point $P \in V$, the condition that the hypersurface $V(f)$ passes through P, is that $f(P) = 0$, and this gives one linear condition on the coefficients of f.

Example 2.44. Let $\mathbb{P}(L)$ be the linear system of conics in $\mathbb{P}^2$ through three points, not on a line. The three points are the base points of the system. The whole line connecting two base points is mapped onto the same image point: the only conics through a third point on the line are reducible, consisting of the line itself and a line through the third base point.

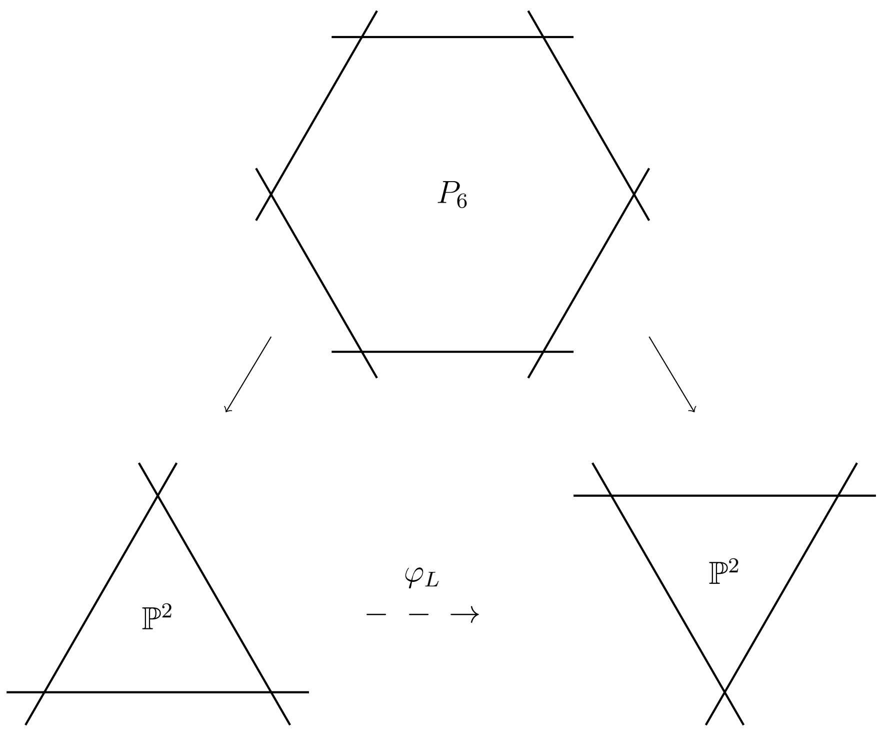
We give a description with coordinates. Take the three points to be $(1:0:0)$, $(0:1:0)$ and $(0:0:1)$. A conic $V(aX^2+bXY+cXZ+dY^2+eYZ+fZ^2)$ passes through these three points if and only if $a=d=f=0$. A basis of L is (YZ, XZ, XY), so φ_L is the map

$$(X:Y:Z) \mapsto (YZ:XZ:XY)\,.$$

This is the standard *Cremona transformation*. It is an involution, as can be seen by rewriting $(YZ:XZ:XY) = (1/X:1/Y:1/Z)$. Using the original formula we find

$$\varphi_L \circ \varphi_L(X:Y:Z) = (X^2YZ:XY^2Z:XYZ^2) = (X:Y:Z)\,.$$

The Cremona transformation is an isomorphism on the complement of the coordinate triangle $V(XYZ)$. It blows down the coordinate lines to points and blows up the points to lines. We can factor the transformation $\varphi_L\colon \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ as $\mathbb{P}^2 \longleftarrow P_6 \longrightarrow \mathbb{P}^2$, with $P_6 \to \mathbb{P}^2$ the blow up of three points. In fact, P_6 is a surface of degree 6 in $\mathbb{P}^6$, called Del Pezzo surface (of degree 6), and the inverse $\mathbb{P}^2 \dashrightarrow P_6$ is the map determined by the linear system of cubics through the three points.

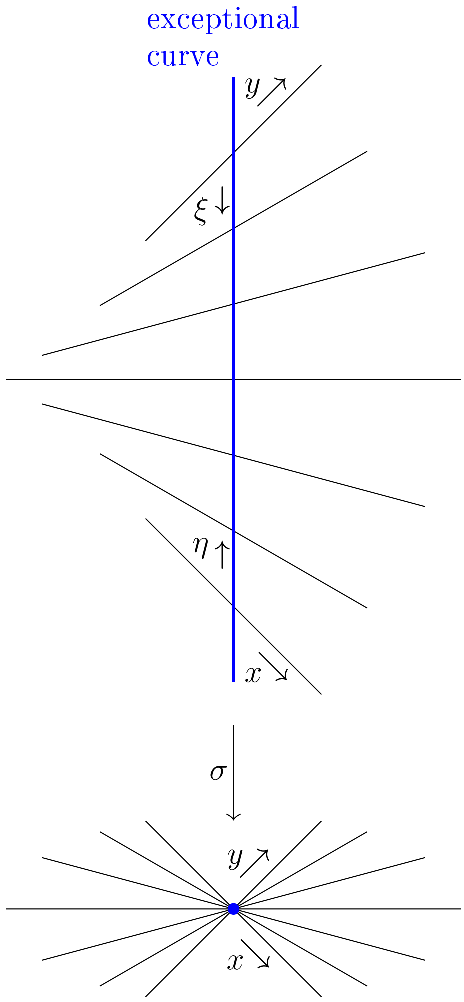


2.6. Blowing up a point

The blow-up of point in $\mathbb{A}^n(k)$ replaces it with the $\mathbb{P}^{n-1}(k)$ of all lines through the point. This works for any field k. Suppose that the point is the origin $0 \in k^n \cong \mathbb{A}^n$. The quotient map $k^n \setminus \{0\} \to \mathbb{P}^{n-1}$ defines a rational map $\pi\colon \mathbb{A}^n \dashrightarrow \mathbb{P}^{n-1}$, which is not defined at the origin. We eliminate the indeterminacy of this map by the following construction. The graph Γ of π is an open subset of the quasi-projective variety $\mathbb{A}^n \times \mathbb{P}^{n-1}$.

Definition 2.45. The *blow up* $\mathrm{Bl}_0\mathbb{A}^n$ of 0 is the closure $\overline{\Gamma}$ of the graph of π. The first projection induces a regular map $\sigma\colon \mathrm{Bl}_0\mathbb{A}^n \to \mathbb{A}^n$. The inverse image of the point 0 is called the *exceptional divisor*.

The projection $\mathbb{A}^n \times \mathbb{P}^{n-1} \to \mathbb{P}^{n-1}$ on the second factor induces a regular map $\widetilde{\pi}\colon \mathrm{Bl}_0\mathbb{A}^n \to \mathbb{P}^{n-1}$, which extends π. As rational maps $\pi = \widetilde{\pi} \circ \sigma^{-1}$.



We give an explicit description in coordinates in the case $n = 2$. Let (X, Y) be coordinates on $\mathbb{A}^2$ and $(\xi : \eta)$ homogeneous coordinates on $\mathbb{P}^1$. Then $\pi(X, Y) = (X : Y)$. If we see $\mathbb{P}^1$ as $k \cup \{\infty\}$, then π is just the rational function X/Y. Where π is defined, we have $(\xi : \eta) = (X : Y)$. The blow up $\mathrm{Bl}_0\mathbb{A}^2$, which is the closure of the graph, is therefore $V(\eta X - \xi Y) \subset \mathbb{A}^2 \times \mathbb{P}^1$.

The variety $\mathrm{Bl}_0\mathbb{A}^2$ can be covered by two affine charts: for $\xi = 1$ we have $Y = \eta X$, so (X, η) are affine coordinates, while for $\eta = 1$ we have

$X = \xi Y$ and (ξ, Y) are affine coordinates. The map $\sigma\colon \mathrm{Bl}_0\mathbb{A}^2 \to \mathbb{A}^2$ is given in these coordinates by $(X,Y) = (X, \eta X) = (\xi Y, Y)$. We compute the transition functions from the one chart to the other to be

$$\eta = \frac{1}{\xi}\ , \qquad X = \xi Y\ .$$

REMARK 2.46. It is impossible to make a real picture, which is correct in all aspects. On the one hand the exceptional curve is a line, on the other hand it is diffeomorphic to a circle. In fact, a neighbourhood of the exceptional curve is a Moebius band.

CHAPTER 3

Projective plane curves

In this chapter we prove Bézout's theorem on the number of intersection points between two plane curves. We also describe the group law on a cubic curve.

DEFINITION 3.1. A *hypersurface* of degree d in $\mathbb{P}^n(K)$ is the k-scheme defined by one equation, so its ideal I is principal: $I = (f)$ with f a homogeneous polynomial of degree d.

Let $f = f_1^{m_1} \dots f_k^{m_k}$ be the factorisation of f. Let $D_i = V(f_i)$ be an irreducible component of $V(f)$. We want $V(f)$ to be non-empty; as explained in section 1.8, we achieve this by considering $V(f)$ in $\mathbb{P}^n(K)$ with the Zariski k-topology, for an algebraically closed field extension K of k. We say that D_i has *multiplicity* m_i.

DEFINITION 3.2. A *divisor* on a projective variety is a linear combination of irreducible components of hypersurfaces, that is, an element of the free Abelian group generated by irreducible components of sets of the type $V(f)$.

For $f = f_1^{m_1} \dots f_k^{m_k}$ we define its divisor (f) as $(f) = \sum m_i D_i$, where $D_i = V(f_i)$. Note that we count with multiplicity.

In particular, if $n = 1$, we consider homogeneous polynomials in two variables (also called *binary forms*). The multiplicity of a point is just the multiplicity of the corresponding root of the inhomogeneous equation of one variable.

For $n = 2$ we call divisors on $\mathbb{P}^2$ with nonnegative coefficients for *curves*. So if we write C, then it is understood that there may be multiple components.

3.1. Bézout's Theorem

The main result about the intersection of plane curves is Bézout's Theorem, which was already formulated by Newton; it occurs explicitly in Bézout's book of 1779.

THEOREM 3.3. *Let C and D be plane curves in $\mathbb{P}^2(k)$ of degree m and n, without common component. Then the number of intersection points of C and D in $\mathbb{P}^2(k)$ is at most mn. If K is an algebraically closed field extension of k, then the number of intersection points in $\mathbb{P}^2(K)$ is equal to mn, counted with multiplicities.*

We will use the resultant to define the multiplicities in such a way, that the theorem becomes trivial. But first we need to know that the number of intersection points is finite. We start with an easy special case of the theorem.

LEMMA 3.4. *Let L be a line and $C = (f)$ a curve of degree d. If L is not a component of C, then the number of intersection points of L and C is at most d.*

PROOF. We parametrise L. If $P = (a_0 : a_1 : a_2)$ and $Q = (b_0 : b_1 : b_2)$ are two points on L, then $\lambda P + \mu Q$ is a rational parametrisation of the line. In coordinates $(X_0 : X_1 : X_2) = \lambda(a_0 : a_1 : a_2) + \mu(b_0 : b_1 : b_2)$. A point on the line lies also on $C = (f)$ if and only $f(\lambda P + \mu Q) = 0$. The homogeneous polynomial $f(\lambda P + \mu Q) \in k[\lambda, \mu]$ has at most d linear factors. □

LEMMA 3.5. *Let $f, g \in k[X, Y, Z]$ be polynomials without common factor. The number of common zeroes is finite.*

PROOF. We consider f and g as polynomials in X, with coefficients in $A = k[Y, Z]$. By proposition 1.23 the resultant $R(f, g)$ is not identically zero, because f and g have no factor in common. Therefore $R(f, g)$ is a homogeneous polynomial in Y and Z, which vanishes only for a finite number of values $(Y : Z)$. A common zero of f and g, which is not $(1 : 0 : 0)$, is of the form $(X_0 : Y_0 : Z_0)$ with $(Y_0 : Z_0)$ one of the finitely many zeroes of $R(f, g)$. It lies on the line though $(1 : 0 : 0)$ and $(0 : Y_0 : Z_0)$. This line is not a component of both $V(f)$ and $V(g)$, so there are only finitely many common zeroes of f and g on it. Therefore the total number of common zeroes is also finite. □

REMARK 3.6. Eliminating X from the equations $F = G = 0$ amounts geometrically to projecting onto the line $X = 0$ (which has homogeneous coordinates $(Y : Z)$) from the point $(1 : 0 : 0)$. This map is not regular at the point $(1 : 0 : 0)$, see example 2.39.

To count the number of common zeroes, that is, intersection points, we want that each line as above only contains one. Therefore we want that the projection point $(1 : 0 : 0)$ does not lie on $C = (f)$ and $D = (g)$ and lies outside all lines connecting two common zeroes of f and g; this is possible by a coordinate transformation, which moves C and D, if k is infinite, so surely if k is algebraically closed.

DEFINITION 3.7. Let the coordinates be chosen as above. Let $P = (X_0 : Y_0 : Z_0)$ be an intersection point of $C = (f)$ and $D = (g)$; by construction it is the only one on the line $V(Z_0 Y - Y_0 Z)$. The *intersection multiplicity* $I_P(C, D)$ of C and D at the point P is the multiplicity of $(Y_0 : Z_0)$ as zero of the resultant $R(f, g)$.

PROOF OF BÉZOUT'S THEOREM. The first statement follows from the second. To prove the second, we may assume that k itself is algebraically closed. We define the intersection multiplicity as above. The theorem now follows, because the resultant is a homogeneous polynomial in two variables of degree mn. $\square$

REMARK 3.8. A priori our definition of intersection multiplicity depends on the chosen coordinates. But in fact it does not.

A projective coordinate change φ is given by an invertible 3×3 matrix $M = (m_{ij})$. Consider all coordinate changes at once. The resultant $R(f,g)(Y,Z)$ depends now polynomially on the coefficients m_{ij}: it is an element of $k[m_{ij}][Y,Z]$, homogeneous in Y and Z of degree mn. We factorise it in irreducible factors. For each intersection point P of C and D we known that $R(f,g)(Y,Z)$ vanishes on the projection on $X = 0$ of $\varphi(P)$. This locus is given by a polynomial in $k[m_{ij}][Y,Z]$, linear in Y and Z. It is therefore a factor of $R(f,g)(Y,Z)$. Its multiplicity is the common value of the intersection multiplicity $I_{\varphi(P)}(\varphi(C),\varphi(D))$ for an open and dense set of matrices. We denote this by $I_P(C,D)$. We have that $\sum_P I_P(C,D) = mn$. Therefore, if we specialise to a specific coordinate transformation, with the property that $(1:0:0)$ does not lie on $\varphi(C)$ and $\varphi(D)$ and lies outside all lines connecting intersection points, then the intersection multiplicity $I_{\varphi(P)}(\varphi(C),\varphi(D))$ is exactly the multiplicity of the corresponding factor of $R(f,g)(Y,Z)$, which is $I_P(C,D)$, independent of the chosen coordinates.

EXAMPLE 3.9. We compute the intersection of a curve $V(f)$ with a line L not passing through $(1:0:0)$. Let L be given by $l = X - a(Y,Z)$ and let $f = \sum b_i(Y,Z)X^{n-i}$. The resultant is

$$R(l,f) = \begin{vmatrix} 1 & -a & & & & & \\ & 1 & -a & & & & \\ & & & \ddots & & & \\ & & & & 1 & -a & \\ & & & & & 1 & -a \\ b_0 & b_1 & b_2 & \dots & b_{n-2} & b_{n-1} & b_n \end{vmatrix},$$

which we compute to be $\sum b_i a^{n-i}$, the result of replacing every X in the equation of f by $a(Y,Z)$. It is also the polynomial we obtain by restricting f to the line L.

DEFINITION 3.10. The *multiplicity* $m_P(C)$ of a curve C in a point $P \in C$ is the minimal intersection number of C with a line through P (this is the intersection with a general line).

LEMMA 3.11. *The multiplicity $m_P(C)$ of a point $P \in C = (f)$ is the maximal number m such that $f \in M_P^m$, where M_P is the homogeneous maximal ideal in $k[X_0,X_1,X_2]$ of P.*

PROOF. We may assume that $P = (1:0:0)$ and work in affine coordinates ($X_0 = 1$). We write the inhomogeneous equation as sum of non-zero homogeneous components $f(X_1,X_2) = f_m(X_1,X_2) + \cdots +$

$f_d(X_1, X_2)$. Then $f \in M_P^m \setminus M_P^{m+1}$ and m is also the multiplicity of C at the origin. □

DEFINITION 3.12. The homogeneous equation f_m defines a set of lines through P, which is the *tangent cone* to C in P. A point P is a *simple* point, if the multiplicity $m_P(C) = 1$.

DEFINITION 3.13. Two curves C and D intersect *transversally* at P if P is a simple point both on C and D, and if the tangent cones to C and D at P are distinct.

PROPOSITION 3.14. *Two curves C and D intersect transversally at P if and only if $I_P(C, D) = 1$.*

More generally we have

PROPOSITION 3.15. *The intersection multiplicity satisfies*

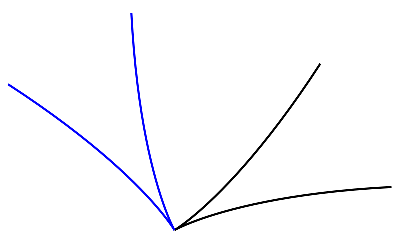
$$I_P(C, D) \geq m_P(C) \cdot m_P(D) ,$$

with equality if and only if the tangent cones to C and D in P have no components in common.

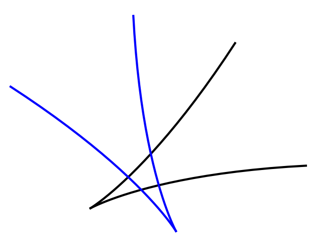
We do not prove this here, as it is more easily seen from other definitions of the intersection multiplicity. A proof using the resultant can be found in [Brieskorn–Knörrer, 6.1 Proposition 3].

In fact, our definition of intersection multiplicity gives a quick proof of Bezout's theorem, but is not very well suited for actual computations. There are several other approaches to the definition, which are easier to use in practice.

What should the intersection multiplicity be? A very classical idea (which can be made rigorous, but not easily) is to move one of the curves until they intersect transversally.



Two curves intersecting only in one point



The shifted curves intersect transversally in four points

The number of points, coming out of the non transverse intersection, is the intersection multiplicity. This agrees with the definition using the resultant: if we compute for the moving curves, we see that a multiple root of the resultant splits in simple roots. In fact, any definition which gives always the same total intersection multiplicity mn and local multiplicity one for transverse intersection, should give the same result.

To motivate the most common definition, which can be found for example in [Fulton], we remark that for transverse intersection the total intersection multiplicity is just the number of points; we can formulate this in a more complicated way as the k-dimension of the ring of rational functions $R(V)$ on the intersection $V = C \cap D$. To describe it, we use affine coordinates. So we suppose that no intersection point lies on the line at infinity. Then $R(V)$ is nothing but the coordinate ring $k[X,Y]/(f,g)$ of $C \cap D = V(f,g)$. So $mn = \dim_k k[X,Y]/(f,g)$. One can show that also for non transverse intersection $\dim_k k[X,Y]/(f,g) = mn$, as long as f and g have no factor in common. The ideal $I = (f,g)$ has primary decomposition $I = I_1 \cap \cdots \cap I_k$. Each component I_i defines a fat point, lying at $P_i = V(I_i)$, with coordinate ring $k[X,Y]/I_i$. By the Chinese remainder theorem $k[X,Y]/I = k[X,Y]/I_1 \times \cdots \times k[X,Y]/I_k$. So Bézout's theorem holds if the intersection multiplicity at P_i is equal to the multiplicity $\dim_k k[X,Y]/I_i$ of the fat point (definition 1.41).

Definition 3.16. Let P be an intersection point of the affine curves $C = (f)$ and $D = (g)$. The *intersection multiplicity* at P is

$$I(P, C \cap D) = \dim_k \mathcal{O}_{\mathbb{A}^2,P}/(f,g) \ .$$

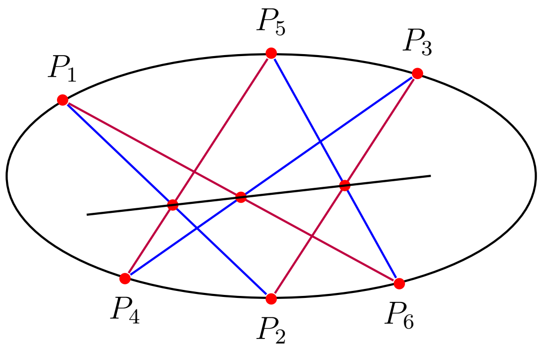
Remark 3.17. This number is indeed the multiplicity of the fat point. Moreover, as it should be, it is the same as our $I_P(C,D)$ defined above. In fact, one can show that the construction with the resultant computes the dimension of the vector space in question, both globally that of $k[X,Y]/(f,g)$ and locally $\mathcal{O}_{\mathbb{A}^2,P}/(f,g)$, see [Eisenbud–Harris, The Geometry of Schemes]. However, this requires more tools from commutative algebra than we now have at our disposal.

We formulate some consequences of Bézout's theorem.

Corollary 3.18. *If C and D meet in mn distinct points, $m = \deg C$, $n = \deg D$, then C and D intersect transversally in all these points.*

Corollary 3.19. *If two curves of degrees m and n have more than mn points in common, then they have a common component.*

Proposition 3.20 (Pascal's theorem). *If a hexagon is inscribed in an irreducible conic, then the opposite sides meet in collinear points.*



Proof. Let the points $P_1, \ldots, P_6$ lie on a conic and let $V(l_{i,i+1})$ be the line joining the points P_i and P_{i+1} (consider the indices modulo 6). The two reducible cubics $V(l_{1,2}l_{3,4}l_{5,6})$ and $V(l_{4,5}l_{6,1}l_{2,3})$ intersect in the 6 points P_i and in the intersection points of opposite sides. Consider the pencil of cubics $C_{(\lambda:\mu)}$: $V(\lambda\, l_{1,2}l_{3,4}l_{5,6} + \mu\, l_{2,3}l_{4,5}l_{6,1})$. Choose a point Q on the conic, distinct from the P_i. There exists a cubic $C_{(\lambda:\mu)}$ passing through Q. As it intersects the conic in seven points, the conic is a component. The other component is a line, which contains the three intersection points. $\square$

3.2. Inflection points

Definition 3.21. Let $f(X_0, X_1, X_2)$ be the equation of a plane curve C, and $P = (a_0 : a_1 : a_2)$ a point on it. The *tangent line* T_P at P is given by the equation

$$(*) \qquad \frac{\partial f}{\partial X_0}(P)X_0 + \frac{\partial f}{\partial X_1}(P)X_1 + \frac{\partial f}{\partial X_2}(P)X_2 = 0\ .$$

If $\left(\frac{\partial f}{\partial X_0}(P), \frac{\partial f}{\partial X_1}(P), \frac{\partial f}{\partial X_2}(P)\right) = 0$, then P is a *multiple point* and the tangent line is not defined. Otherwise it is a simple point.

Remark 3.22. Differentiation of a polynomial can be defined purely algebraically (product rule!), and involves no analysis. The formula (*) is in fact just the familiar one for the tangent space. There are several ways to understand it.

- In affine coordinates (x_1, x_2), write $F(x_1, x_2) = f(1, X_1, X_2)$; in a simple point the tangent cone is a tangent line, given by the linear part of the affine equation. It follows that the tangent line is $\frac{\partial F}{\partial x_1}(P)(x_1 - a_1) + \frac{\partial F}{\partial x_2}(P)(x_2 - a_2) = 0$. By Euler's formula:

$$\sum X_i \frac{\partial f}{\partial X_i} = mf,$$

where m is the degree of f, and the fact that $f(a_0, a_1, a_2) = 0$, we obtain in homogeneous coordinates the expression (*).

- We can view f as equation on $\mathbb{A}^3$, and describe the tangent plane in any point on the line, which projects onto $P \in (k^3 \setminus \{0\})/k^* = \mathbb{P}^2$. As this plane passes through the origin, it is given by (*).
- Finally, the tangent line is the line which intersects f in P with multiplicity at least two. Let $Q = (b_0 : b_1 : b_2)$, and consider the line $P + tQ$. By Taylor's formula:

$$f(P+tQ) = f(P) + t\sum \frac{\partial f}{\partial X_i}(P)\cdot b_i + \text{higher order terms.}$$

  The condition that $t = 0$ is at least a double root, gives that Q satisfies (*).

DEFINITION 3.23. A tangent line L, tangent to $C = (f)$ in the point P, is an *inflectional tangent*, or *flex* for short, and P is an *inflection point*, if the intersection multiplicity of L and C at P is at least 3. The flex is called *ordinary* if $I_P(L, C) = 3$, a higher flex otherwise.

DEFINITION 3.24. The *Hessian* H_f of f is the determinant of the second partial derivatives of f:

$$\det\Big(\frac{\partial^2 f}{\partial X_i \partial X_j}\Big) = 0\ .$$

If H_f is not identically zero, the curve (H_f) is the *Hessian* curve of the curve C, also denoted by H_C.

REMARK 3.25. Euler's formula $(m-1)\frac{\partial f}{\partial X_j} = \sum X_i \frac{\partial^2 f}{\partial X_i \partial X_j}$ shows that the columns of the matrix are dependent if $(m-1)\frac{\partial f}{\partial X_j} = 0$ for all j. So if $p = \operatorname{char} k$ divides $m-1$, the Hessian H_f vanishes identically. Furthermore, if H_f does not vanish identically, then the Hessian curve passes through the multiple points of f.

THEOREM 3.26. *Let $C = (f)$ be a projective curve of degree m without lines as components. Suppose that Hessian H_f does not vanish identically; in particular $p = \operatorname{char} k \nmid (m-1)$, and $p \neq 2$. A simple point $P \in C$ is an inflection point if and only if P lies on the Hessian H_C. More precisely, $I_p(C, T_P) = I_P(C, H_C) + 2$, if $p > m$.*

PROOF. Choose coordinates such that $P = (0 : 0 : 1)$ and the tangent line T_P is the line $X = 0$. Now we can write the equation of the curve in the form $f = Xu(X, Y, Z) + Y^{r+2}g(Y, Z)$ with $u(0, 0, 1) \neq 0$ and $g(0, 1) \neq 0$. For the Hessian we do the same thing, collecting all terms containing X in a first summand. The result is $H_f = Xv(X, Y, Z) + Y^r h(Y, Z)$, where the second summand is computed by putting $X = 0$ in the determinant, defining H_f:

$$\begin{vmatrix} 2u_X & u_Y & u_Z \\ u_Y & (r+2)(r+1)Y^r g + 2(r+2)Y^{r+1}g_Y + Y^{r+2}g_{YY} & (r+2)Y^{r+1}g_Z + Y^{r+2}g_{YZ} \\ u_Z & (r+2)Y^{r+1}g_Z + Y^{r+2}g_{YZ} & Y^{r+2}g_{ZZ} \end{vmatrix}\ .$$

We multiply the first row with Y^r, and divide the second and third columns by Y^r. The new determinant is equal to $h(Y,Z)$. We compute $h(0,1)$ by putting $Y=0$. Note that $r=0$ is allowed. We find

$$h(0,1) = \begin{vmatrix} 2u_X Y^r & u_Y & u_Z \\ u_Y & (r+2)(r+1)g & 0 \\ u_Z & 0 & 0 \end{vmatrix},$$

so $h(0,1) = -(r+2)(r+1)u_Z^2(0,0,1)g(0,1)$. As $(m-1)u = Xu_X + Yu_Y + Zu_Z$, one has $u(0,0,1) \neq 0$ if and only if $u_Z(0,0,1) \neq 0$, as $p \nmid (m-1)$. Therefore, if $r=0$, then $h(0,1) \neq 0$ and $H_f(P) \neq 0$.

To compute the intersection multiplicity of F and H_f at p, we choose suitable coordinates such that p is the only intersection point of f and H_f on $Y=0$. The last column of the determinant defining the resultant has only two nonzero entries, which are $Y^{r+2}g$ and $Y^r h$. By expanding the determinant along this column we compute the resultant to be of the form $Y^{r+2}gq_1 + Y^r hq_2$ with $q_2(0,1)$ up to sign itself the resultant of $u(X,0,Z)$ and $Xv(X,0,Z)$, which is non-zero, as P is the only intersection on $Y=0$. □

Corollary 3.27. *A cubic curve without multiple points over an algebraically closed field k with $\operatorname{char} k > 3$ has exactly nine distinct inflection points.*

3.3. The group law on cubic curves

Consider an irreducible cubic curve $C = (f) \subset \mathbb{P}^2$, which is also irreducible over the algebraic closure of k. Let K be an extension of k, not necessarily algebraically closed; an important case is $K = k$. We shall construct a group law on the set of simple points $C^{\text{reg}} \subset C$, defined over K. Therefore we assume that this set is nonempty. If no confusion arises, we suppress the field from the notation.

We fix a point $E \in C^{\text{reg}}$, which will be the neutral element. We will consider collections of simple points, which we think of as being variable. Then it may be that some points coincide. We can give a precise meaning to this, using fat points, see Definition 1.41. A fat point Z of multiplicity m on a curve C with $Z_{\text{red}} = P$ a simple point of the curve has an particularly simple structure. In affine coordinates (X,Y) with P the origin, and the X-axis as tangent, its ideal is of the form $(Y + f_2 + \dots f_d, Y^m, Y^{m-1}X, \dots, X^m)$. We can solve $Y \equiv g(X) \bmod (X^m)$, so other generators for the ideal are $(Y - g(X), X^m)$. Therefore the coordinate ring of the fat point is isomorphic to $k[X]/(X^m)$. We say that m points coincide at P. A line through two coinciding points $P_1 = P_2 = P$, that is, through a fat point of multiplicity two, is a line, which intersects the curve with multiplicity at least two in P, that is, a tangent line, and a line through three coinciding points $P_1 = P_2 = P_3 = P$ is an inflectional tangent.

Let P and Q be simple points on the irreducible cubic C, defined over K. The line L through P and Q is not a component, and intersects C in three points: the restriction of the equation f to the line $L \cong \mathbb{P}^1$ is a homogeneous polynomial of degree three in two variables, which is divisible by linear forms defining P and Q, so it factorises over K in three linear factors. The point defined by the third linear factor will be called the third intersection point of L and C, and denoted by $P * Q$; it may coincide with P or Q. It is again a simple point: if it is distinct from the simple points P and Q, then L intersects C in the point with multiplicity 1.

LEMMA 3.28. *The map* $\varphi\colon C^{reg} \times C^{reg} \to C^{reg}$, $\varphi(P,Q) = P * Q$, *is a regular map.*

DEFINITION 3.29. The *addition* $P \oplus Q$ on C^{reg} is given by

$$P \oplus Q = (P * Q) * E\ ,$$

so $P \oplus Q$ is the third intersection point on the line through $P * Q$ and E.

THEOREM 3.30. *This operation makes* $(C^{reg}, \oplus)$ *into an abelian group with neutral element* E.

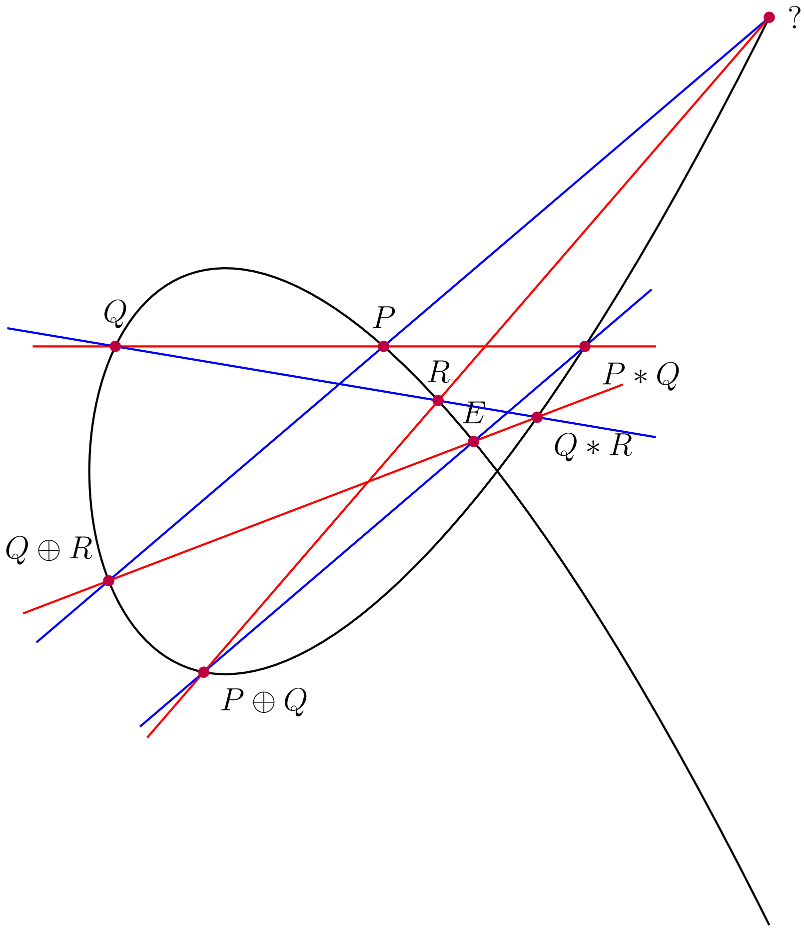
PROOF. Apart from associativity this is easy. Commutativity is obvious. Let us construct $P \oplus E$. Let $P * E$ be the third intersection point on the line L through P and E. Then P is the third intersection point on the line through $P * E$ and E (which is the line L), so $P \oplus E = P$.

For the inverse, let $E * E$ be the third intersection point on the tangent line to C at the point E, then the third point $(E * E) * P$ on the line through P and $E * E$ satisfies $P \oplus ((E * E) * P) = E$, so $-P$ is the point $(E * E) * P$.

For associativity, $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$, it suffices to show that the points $(P \oplus Q) * R$ and $P * (Q \oplus R)$ in the penultimate step of the construction coincide. There are 8 more points involved, which we write in the following 3×3 square.

$$\begin{matrix} P & Q \oplus R & ? \\ P * Q & E & P \oplus Q \\ Q & Q * R & R \end{matrix}$$

The points in each row and each column are collinear. The question mark stands in the first row for the point $P*(Q\oplus R)$, while it represents in the last column the point $(P \oplus Q) * R$, so the points which we want to prove to be equal. All the eight named points in the square lie not only on C, but also on two other cubics, being the product of the lines determined by the rows, respectively the columns, of the square; note that multiple factors may occur. Let $l_1 = 0$ be an equation for the line through P, $Q \oplus R$ and $P * (Q \oplus R)$, $l_2 = 0$ for the line through $P * Q$



and E, and $l_3 = 0$ for the line through Q and R. Consider the pencil of cubics $C_\lambda = (f + \lambda\, l_1 l_2 l_3)$. Each curve $(f + \lambda\, l_1 l_2 l_3)$ passes through the nine points of the square, with ? being $P * (Q \oplus R)$. Choose a fourth point S on the line through P and Q, not on the curve C. Then there is a unique λ_S such that $f(S)+\lambda_S\, l_1(S)l_2(S)l_3(S) = 0$. As the line through P and Q has four points in common (counted with multiplicity) with the curve $C_{\lambda(S)}$, it is a component and the remaining six points of the square lie on a conic. Note that this argument also works if some points coincide. The conic intersects the cubic in six points (counted with multiplicity), which together with the intersection of the cubic with the line through P and Q make up the nine points of the square. As the three points $Q \oplus R$, E and $Q * R$ lie on a straight line, this line is a component of the conic and the three remaining points R, $P \oplus Q$ and $P * (Q \oplus R)$ are collinear. As they also lie on the curve C, the point $P * (Q \oplus R)$ is the third point on the line through R and $P \oplus Q$, so it is equal to $(P \oplus Q) * R$. $\square$

The group law can be simplified by taking an inflection point, if the cubic has one, as neutral element. Then the third point, in which the tangent at E intersects the curve, is E itself. So the inverse $-P$ is the third point on the line EP. Therefore we obtain

$$P \oplus Q \oplus R = E \quad \Longleftrightarrow \quad P,\, Q \text{ and } R \text{ collinear}\ .$$

We can take coordinates with the flex being the line at infinity and the inflection point $(0 : 1 : 0)$. By completing the square ($\operatorname{char} k \neq 2$) we get an equation of the form $Y^2 = X^3 + pX^2 + qX + r$, which if $\operatorname{char} k \neq 3$ can be simplified further to

$$Y^2 = X^3 + aX + b\ .$$

If $P = (X, Y)$, then $-P = (X, -Y)$.

REMARK 3.31. Over the complex numbers a non-singular cubic curve is a Riemann surface of genus 1, so topologically a torus. Let τ be a point in the upper half plane. Then the Riemann surface is $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\,\tau)$. The group structure comes from addition on $\mathbb{C}$. Meromorphic functions on the Riemann surface are doubly periodic functions in the complex plane. In particular, one has the Weierstraß $\wp$ function given by

$$\wp(z) = \frac{1}{z^2} + \sum_{(m,n)\neq(0,0)} \left(\frac{1}{(z-m-n\tau)^2} - \frac{1}{(m+n\tau)^2} \right)\ .$$

It satisfies the equation

$$\left(\wp'(z)\right)^2 = 4\left(\wp(z)\right)^3 - g_2\wp(z) - g_3\ .$$

CHAPTER 4

Dimension

In this chapter we define the dimension of affine and projective varieties. This is done using a general definition for the dimension of commutative rings. It will take some time to prove that the dimension of $\mathbb{P}^n$ (as projective variety) is n.

4.1. Krull dimension

DEFINITION 4.1. Let X be a topological space. If $X = \emptyset$, then its dimension is -1. Otherwise, the *Krull dimension* $\dim X$ of X is the supremum of the lengths n of chains

$$X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n$$

of non-empty irreducible subsets X_i of X.

If $Y \subset X$ is a non-empty closed irreducible subspace, then the *codimension* $\operatorname{codim}_X Y$ of Y in X is the supremum of lengths of chains starting with $X_0 = Y$. The codimension of the empty set is ∞.

LEMMA 4.2.

(1) *If* $\{X_\lambda\}_{\lambda \in \Lambda}$ *is the family of irreducible components of* X*, then* $\dim X = \sup_{\lambda \in \Lambda} \dim X_\lambda$.
(2) *If* $Y \neq \emptyset$*, then* $\dim Y + \operatorname{codim}_X Y \leq \dim X$.
(3) *If* $Y \subset X$ *and* X *is irreducible with* $\dim X < \infty$*, then* $\dim Y < \dim X$ *if and only if* $Y \neq X$.

The definition applies to affine and projective varieties. If $\bar{V}$ is the projective closure of an affine variety V, then $\dim V \leq \dim \bar{V}$; this follows immediately from proposition 2.24. We shall later see that in fact equality holds.

It is not so clear how to compute this dimension, or even to see that it is finite. We translate the problem into one about rings.

Let R be a ring, as always commutative with unit. Similar to the definition above we define the dimension of the ring.

DEFINITION 4.3. The *Krull dimension* $\dim R$ of a ring R is the supremum of the lengths n of chains

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$$

of prime ideals of R.

The *height* $\operatorname{ht}(\mathfrak{p})$ of a prime ideal $\mathfrak{p}$ of R is the supremum of lengths of chains ending with $\mathfrak{p}_n = \mathfrak{p}$.

If I is an ideal, then $\dim I$ is the dimension of the ring R/I.

For an affine k-variety $V \subset \mathbb{A}^n(K)$ we have $\dim V = \dim k[V]$.

EXAMPLE 4.4. $\dim k[X_1, \dots, X_n] \geq n$.
Consider the chain $(0) \subset (X_1) \subset (X_1, X_2) \subset \cdots \subset (X_1, \dots, X_n)$.

EXAMPLE 4.5. $\dim \mathbb{Z} = 1$.

4.2. Integral ring extensions

If $R \subset S$ is a subring of a ring S, we also say that S is a *ring extension* of R.

DEFINITION 4.6. A ring S is *finite* over R, if S is a finitely generated R-module. This means that there is an epimorphism $R^m \to S$ of a free R-module onto S.

A ring S is *of finite type* over R, if S is a finitely generated as R-algebra. This means that there is an epimorphism $R[y_1, \dots, y_m] \to S$.

As an affine k-algebra is a quotient of a polynomial ring, every extension of affine k-algebras is of finite type.

DEFINITION 4.7. Let $R \subset S$ be a ring extension. An element $x \in S$ is *integral* over R, if x satisfies a monic equation

$$x^n + r_1 x^{n-1} + \cdots + r_n = 0\,,$$

where the r_i lie in R.
If I is an ideal in R, and all $r_i \in I$, then x is *integral over I*.
If every $x \in S$ is integral over R, then S is called *integral* over R, or an *integral extension* of R.

LEMMA 4.8. *The following are equivalent:*

(1) *$x \in S$ is integral over R (over I).*
(2) *$R[x]$ is finite over R (and $x \in \operatorname{rad} IR[x]$).*
(3) *$R[x]$ is contained in a subring $S' \subset S$, which is finite over R (and $x \in \operatorname{rad} IS'$).*

PROOF.
(1) $\Rightarrow$ (2) Let $f \in R[X]$ be a monic polynomial $X^n + r_1 X^{n-1} + \cdots + r_n$ such that $f(x) = 0$ is the integral equation for $x \in S$. Division with remainder in $R[X]$ (possible because f is monic) yields that every $g \in R[X]$ can be written as $g = qf + r$ with $\deg r < n = \deg f$. Therefore $1, \dots, X^{n-1}$ generate $R[X]/(f)$ as R-module, and $1, \dots, x^{n-1}$ generate $R[x]$. If all the coefficients of f are in I, then the monic equation implies that $x^n \in IR[x]$, so $x \in \operatorname{rad} IR[x]$.
(2) $\Rightarrow$ (3) Just take $S' = R[x]$.
(3) $\Rightarrow$ (1) Let $m_1, \dots, m_k$ be generators of S' as R-module. Multiplication by x is an endomorphism of S'. We have $xm_i = \sum a_{ij} m_j$, $a_{ij} \in R$, which we can write in matrix form as

$$(xI - A)\underline{m} = 0\ ,$$

where A is the square matrix with entries a_{ij} and $\underline{m}$ is the column vector of the m_i. Multiplying with the matrix of cofactors we obtain $\det(xI - A)m_i = 0$ for all i. As $1 \in S'$ can be written as R-linear combination of the m_i, we get $\det(xI - A) = 0$. This is the desired relation.
If $x \in \operatorname{rad} IS'$, then $x^l \in IS'$ for some l, and consider multiplication by x^l. We can write $x^l m_i = \sum a_{ij} m_j$ with $a_{ij} \in I$. As before, the characteristic polynomial gives the desired relation. □

COROLLARY 4.9. *If S is a finite R-module, then S is integral over R, and $x \in S$ is integral over I if and only if $x \in \operatorname{rad} IS$.*

COROLLARY 4.10. *If $x_1, \dots, x_m \in S$ are integral over R, then $R[x_1, \dots, x_m]$ is finite over R; in particular, an integral extension of finite type is finite.*
If the x_i are integral over I, then $x_i \in \operatorname{rad} IR[x_1, \dots, x_m]$.

PROOF. By induction. The case $m = 1$ is already proved. Write $R[x_1, \dots, x_m] = R[x_1, \dots, x_{m-1}][x_m]$, then $R[x_1, \dots, x_m]$ is, by the case $m = 1$, a finite $R[x_1, \dots, x_{m-1}]$-module as x_m is also integral over $R[x_1, \dots, x_{m-1}]$. Hence $R[x_1, \dots, x_m]$ is finite over R. □

COROLLARY 4.11. *The set of elements of S which are integral over R is a subring of S containing R.*

PROOF. If $x, y \in S$ are integral over R, then $S' = R[x, y]$ is finite over R, so $x \pm y$ and xy are integral over R by part (3) of the proposition. □

DEFINITION 4.12. The set of the above corollary is called the *integral closure* of R in S. If R is its own integral closure, then R is *integrally closed* in S. A ring is integrally closed (without qualification), if it is integrally closed in its total ring of fractions.

An element r of a ring R is *nilpotent* if $r^n = 0$ for some positive integer n.

DEFINITION 4.13. A ring R is *reduced* if it has no nonzero nilpotent elements.

An affine coordinate ring $k[V] = k[X_1, \dots, X_n]/I(V)$ is reduced if and only of the ideal $I(V)$ is radical.

DEFINITION 4.14. The integral closure $\widetilde{R}$ of a reduced ring R in its total ring of fractions is called the *normalisation* of R. The ring R is *normal* if $\widetilde{R} = R$.

EXAMPLE 4.15. Every unique factorisation domain is normal, e.g., $\mathbb{Z}$ and $k[X_1, \dots, X_n]$. Let $Q(R)$ be the quotient field of the UFD R and $x = \frac{r}{s}$ integral over R. The equation $x^n + r_1 x^{n-1} + \cdots + r_n = 0$ implies $r^n + r_1 r^{n-1} s + \cdots + r_n s^n = 0$. Every prime element dividing

s also divides r^n, so by unique factorisation also r. Therefore, after cancelling factors s is a unit, and $x \in R$.

COROLLARY 4.16 (transitivity of integral extensions). *If $R \subset S \subset T$ are ring extensions and if S is integral over R, and T integral over S, then T is integral over R.*

PROOF. Let $x \in T$ satisfy $x^n + s_1 x^{n-1} + \cdots + s_n = 0$. Then $S' = R[s_1, \ldots, s_{n-1}]$ is finite over R, and $S'[x]$ is finite over S', as x is integral over S'. As $S'[x] \subset T$ is finite over R, x is integral over R. $\square$

4.3. Going up and going down

For an integral extension $R \subset S$ there is a close connection between chains of prime ideals in R and in S. In particular, we will see that $\dim R = \dim S$. We need a lemma on the existence of prime ideals.

LEMMA 4.17 (Krull's prime existence lemma). *Let I be an ideal in a ring R and let Σ be a multiplicative system in R with $I \cap \Sigma = \emptyset$. Then there exists a prime ideal $\mathfrak{p}$ of R containing I, and such that $\mathfrak{p} \cap \Sigma = \emptyset$.*

PROOF. The set of ideals J with $I \subset J$ and $J \cap \Sigma = \emptyset$ is partially ordered by inclusion and nonempty since it contains I. If $\{J_\lambda\}_{\lambda \in \Lambda}$ is a totally ordered subset, then also $\bigcup_{\lambda \in \Lambda} J_\lambda$ is an ideal in the set. By Zorn's lemma, there is a maximal element $\mathfrak{p}$. We show that $\mathfrak{p}$ is a prime ideal. First of all, $\mathfrak{p}$ is a proper ideal as $1 \in \Sigma$ is not contained in $\mathfrak{p}$. Let $r_1, r_2 \in R \setminus \mathfrak{p}$ and suppose $r_1 r_2 \in \mathfrak{p}$. As $\mathfrak{p}$ is a maximal element, the ideal $\mathfrak{p} + (r_i)$, $i = 1, 2$, satisfies $\mathfrak{p} + (r_i) \cap \Sigma \neq \emptyset$. We can find $p_i \in \mathfrak{p}$ and $a_i \in R$ such that $p_i + a_i r_i \in \Sigma$. Then $(p_1 + a_1 r_1)(p_2 + a_2 r_2) \in \Sigma \subset R \setminus \mathfrak{p}$, contradicting that $r_1 r_2 \in \mathfrak{p}$. Therefore $\mathfrak{p}$ is prime. $\square$

THEOREM 4.18. *Let S be an integral extension of a ring R. Let $\mathfrak{p}$ be a prime ideal in R.*

(1) *There exists a prime ideal $\mathfrak{q}$ of S with $\mathfrak{q} \cap R = \mathfrak{p}$.*
(2) *Let $\mathfrak{q}_1 \subset \mathfrak{q}_2$ be prime ideals in S. If $\mathfrak{q}_1 \cap R = \mathfrak{q}_2 \cap R = \mathfrak{p}$, then $\mathfrak{q}_1 = \mathfrak{q}_2$.*
(3) *A prime ideal $\mathfrak{q}$ with $\mathfrak{p} = \mathfrak{q} \cap R$ of S is maximal if and only if $\mathfrak{p}$ is maximal.*

DEFINITION 4.19. Let S be an integral extension of a ring R and $\mathfrak{p}$ a prime ideal in R. We say that a prime ideal $\mathfrak{q}$ of S *lies over* $\mathfrak{p}$ if $\mathfrak{q} \cap R = \mathfrak{p}$.

PROOF OF THE THEOREM.
(1) We will show that the ideal $\mathfrak{p}S \subset S$ and the multiplicative system $\Sigma = R \setminus \mathfrak{p} \subset S$ satisfy $\mathfrak{p}S \cap \Sigma = \emptyset$. Krull's prime existence lemma gives an ideal $\mathfrak{q} \subset S$ with $\mathfrak{p}S \subset \mathfrak{q}$ and $\mathfrak{q} \cap R \setminus \mathfrak{p} = \emptyset$. Hence, $\mathfrak{q}$ is a prime ideal of S lying over $\mathfrak{p}$.

If $x \in \mathfrak{p}S$, then x is integral over $\mathfrak{p}$, so there is an equation $x^n + r_1 x^{n-1} + \cdots + r_n = 0$ with the $r_i \in \mathfrak{p}$. If $x \in \mathfrak{p}S \cap \Sigma \subset R$, then $x^n \in \mathfrak{p}$,

so $x \in \mathfrak{p}$, contradicting $x \in \Sigma = R \setminus \mathfrak{p}$. Hence $\mathfrak{p}S \cap \Sigma = \emptyset$.
(2) Note that $S/\mathfrak{q}_1$ is integral over $R/\mathfrak{p}$: just reduce an integral equation for $x \in S$ modulo the ideal $\mathfrak{q}_1$. Both rings $S/\mathfrak{q}_1$ and $R/\mathfrak{p}$ are integral domains. The ideal $\mathfrak{q}_2/\mathfrak{q}_1$ satisfies $(\mathfrak{q}_2/\mathfrak{q}_1) \cap (R/\mathfrak{p}) = (0)$. Suppose $\bar{x} \neq 0 \in \mathfrak{q}_2/\mathfrak{q}_1$. Let $\bar{x}^n + \bar{r}_1\bar{x}^{n-1} + \cdots + \bar{r}_n = 0$ be an integral equation of lowest possible degree. As $\bar{r}_n \in (\mathfrak{q}_2/\mathfrak{q}_1) \cap (R/\mathfrak{p}) = (0)$, we have $\bar{r}_n = 0$. Because $S/\mathfrak{q}_1$ does not contain zero divisors, we can divide by x and obtain an equation of lower degree. This contradiction shows that $\mathfrak{q}_1 = \mathfrak{q}_2$.
(3) If $\mathfrak{p}$ is maximal, then $\mathfrak{q}$ is maximal as well by part (2). For the converse, consider the integral extension $R/\mathfrak{p} \subset S/\mathfrak{q}$. If $S/\mathfrak{q}$ is a field, its only prime ideal is (0). Then, by the first part, (0) is the only prime ideal of $R/\mathfrak{p}$, so $R/\mathfrak{p}$ is a field. □

COROLLARY 4.20. *If S is Noetherian, only finitely many prime ideals of S lie over $\mathfrak{p}$.*

EXAMPLE 4.21. The ring extension $R = \mathbb{Z} \subset S = \mathbb{Z}[\sqrt{-5}]$ is integral, and the ideal $(2) \subset \mathbb{Z}$ is maximal. But the ideal generated by 2 in $\mathbb{Z}[\sqrt{-5}]$ is not prime: $(1+\sqrt{-5})(1-\sqrt{-5}) = 3 \cdot 2$. A prime ideal $\mathfrak{q}$ with $\mathfrak{q} \cap \mathbb{Z} = (2)$ is the ideal $(2, 1+\sqrt{-5})$. This is in fact the only maximal ideal lying over (2).

THEOREM 4.22 (Going up theorem). *Let S be an integral extension of a ring R. Let $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_n$ be a chain of prime ideals of R, and $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m$ $(m < n)$ a chain of prime ideals of S, such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$. Then the chain $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m$ can be extended to a chain $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ lying over $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$.*

PROOF. It suffices (induction!) to consider the case $m = 1$, $n = 2$. As $\overline{S} = S/\mathfrak{q}_1$ is integral over $\overline{R} = R/\mathfrak{p}_1$, there exists a prime ideal $\overline{\mathfrak{q}}_2$ of $\overline{S}$ lying over $\mathfrak{p}_2/\mathfrak{p}_1$. The preimage $\mathfrak{q}_2$ of $\overline{\mathfrak{q}}_2$ in S has the required properties. □

COROLLARY 4.23. $\dim S = \dim R$.

DEFINITION 4.24. A polynomial map $f\colon V \to W$ of affine algebraic sets with dense image is *finite* if $f^* : k[W] \to k[V]$ is an integral (and hence finite) ring extension.

Note that f has dense image if and only if f^* is injective. Then we can consider $k[W]$ as subring of $k[V]$.

COROLLARY 4.25. *Let $f\colon V \to W$ be a finite morphism of affine algebraic sets. The image of every algebraic subset of V is an algebraic subset of W. That is, f is a closed map.*

Let $W_1 \supset W_2 \supset \cdots \supset W_n$ be a chain of subvarieties of W, and $V_1 \supset \cdots \supset V_m$ $(m < n)$ a chain of subvarieties of V, such that $f(V_i) = W_i$. Then the chain $V_1 \supset \cdots \supset V_m$ can be extended to a chain $V_1 \supset \cdots \supset V_n$ over $W_1 \supset \cdots \supset W_n$.

Proof. Let $I(W_1) \subset \cdots \subset I(W_m)$ be the chain of ideals of the W_i. By going up there is a chain of prime ideals $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ lying over it. Then $V_i = V(\mathfrak{q}_i)$ is a subvariety of V with $f(V_i) \subset W_i$. Equality follows from the first statement, which we now show.

We may assume that $V_1 = V(\mathfrak{q}_1)$ is an irreducible subset of V. Then $f(V_1) \subset W_1 = V(\mathfrak{p}_1)$, where $\mathfrak{p}_1 = \mathfrak{q}_1 \cap k[W]$. Let $Q \in W_1$ be a point. Then, by what we just said, there is a subvariety $P \in V_1$ with $f(P) = Q$ (in fact a point, as it is defined by a maximal ideal). $\square$

Example 4.26. Let $V = V(Y^2 - X) \subset \mathbb{A}^2$ and $W = \mathbb{A}^1$. The projection $f\colon V \to W$, $(X, Y) \mapsto X$ is finite. Indeed, $f^*\colon k[X] \to k[X,Y]/(Y^2 - X)$ is injective and $k[X,Y]/(Y^2 - X)$, which is as $k[X]$-module generated by 1 and the class of Y, is as ring generated by the one element Y, which satisfies the monic equation $Y^2 - X = 0$.

Example 4.27. The algebraic set $V(Y^2X - Y)$ is the union of a hyperbola and the X-axis. Projection on the X-axis is a surjective polynomial map with finite fibres. But is is not a finite map.

There is also a 'going down' theorem. This needs the stronger hypothesis that R is a normal domain. We first prepare a lemma.

Lemma 4.28. *Let R be a normal domain with quotient field $K = Q(R)$, and $\mathfrak{p}$ a prime ideal of R. Let L/K be a field extension. If $x \in L$ is integral over $\mathfrak{p}$, then x is algebraic over K, and all coefficients of the minimal polynomial $m = X^n + \cdots + a_n$ of x over K lie in $\mathfrak{p}$.*

Proof. Clearly x is algebraic over K. Let $x = x_1, \ldots, x_n$ be the roots of m in the algebraic closure $\overline{K}$ of K. There is an automorphism of $\overline{K}$ fixing K, which maps x to x_i. So if $f(x) = 0$ is an integral equation for x with coefficients in $\mathfrak{p}$, then also $f(x_i) = 0$ for each i, that is the x_i are integral over $\mathfrak{p}$. Since the coefficients of m are symmetric functions in the x_i, they lie in $\operatorname{rad}\mathfrak{p}\widetilde{R}$ by Corollary 4.9, where $\widetilde{R}$ is the normalisation of R. Since $R = \widetilde{R}$ and $\mathfrak{p}$ is prime, they actually lie in $\mathfrak{p}$. $\square$

Theorem 4.29 (Going down theorem). *Let $R \subset S$ be an integral extension of integral domains. Assume that R is normal. Let $\mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \cdots \supset \mathfrak{p}_n$ be a chain of prime ideals of R, and $\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_m$ ($m < n$) a chain of prime ideals of S, such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$. Then the chain $\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_m$ can be extended to a chain $\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_n$ lying over $\mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n$.*

Proof. We may assume $m = 1$, $n = 2$. We consider three multiplicative systems in S: $\Sigma_1 := S \setminus \mathfrak{q}_1$, $\Sigma_2 := R \setminus \mathfrak{p}_2$ and $\Sigma := \Sigma_1 \cdot \Sigma_2 = \{s_1 s_2 \mid s_1 \in \Sigma_1, s_2 \in \Sigma_2\}$. Then $\Sigma_i \subset \Sigma$. If $\mathfrak{p}_2 S \cap \Sigma = \emptyset$, then Krull's prime existence lemma 4.17 gives a prime ideal $\mathfrak{q}_2$ in S with $\mathfrak{p}_2 S \subset \mathfrak{q}_2$ and $\mathfrak{q}_2 \cap \Sigma = \emptyset$. As $\mathfrak{q}_2 \cap \Sigma_1 = \emptyset$, $\mathfrak{q}_2 \subset \mathfrak{q}_1$; from $\mathfrak{q}_2 \cap \Sigma_2 = \emptyset$ follows that $\mathfrak{q}_2$ lies over $\mathfrak{p}_2$.

Suppose therefore that $x \in \mathfrak{p}_2 S \cap \Sigma$. Then x is is integral over $\mathfrak{p}_2$, so by the lemma above the minimal polynomial $m = X^n + \cdots + a_n$ of $x \in L = Q(S)$ over $K = Q(R)$ has coefficients in $\mathfrak{p}_2$. As $x \in \Sigma$, we may write $x = s_1 s_2$ with $s_1 \in \Sigma_1$ and $s_2 \in \Sigma_2$. Then $X^n + \cdots + a_n/s_2^n$ is the minimal polynomial of s_1 over K (the degree cannot be lower, because any relation of this type implies one of the same degree for x). Its coefficients a_i/s_2^i are contained in R, as s_1 is integral over R, by the same lemma. Put $a_i = b_i s_2^i$. As $s_2 \notin \mathfrak{p}_2$ and $a_i \in \mathfrak{p}_2$, we have that $b_i \in \mathfrak{p}_2$ and s_1 is integral over $\mathfrak{p}_2$, and therefore $s_1 \in \operatorname{rad} \mathfrak{p}_2 S \subset \mathfrak{q}_1$. This contradicts $s_1 \in \Sigma_1$. So $\mathfrak{p}_2 S \cap \Sigma = \emptyset$. □

COROLLARY 4.30. *For every prime ideal $\mathfrak{q}$ of S the height $h(\mathfrak{q})$ is equal to $h(\mathfrak{q} \cap R)$.*

EXAMPLE 4.31. Consider the integral extension

$$R = k[s, y, z]/(z^2 - y^2(y + 1)) \subset k[s, t] = S$$

where $y = t^2 - 1$ and $z = t(t^2 - 1)$. Geometrically, the map $\mathbb{A}^2 \longrightarrow \mathbb{A}^3$ corresponding to the ring extension parametrises the surface $V(z^2 - y^2(y + 1))$. The ring R is not normal. We give an example that going down does not hold in this situation. The ideal $\mathfrak{q}_2 = (s - t)$ of the diagonal in $\mathbb{A}^2$ is the only prime ideal lying over the prime ideal $\mathfrak{p}_2 = \mathfrak{q}_2 \cap R = (s^2 - 1 - y, s(s^2 - 1) - z)$. Above the prime ideal $\mathfrak{p}_1 = (s-1, y, z)$ of the point $(1, 0, 0)$ on the double line lie two maximal ideals of S, namely $(s - 1, t + 1)$ and $(s - 1, t - 1)$, as $\mathfrak{p}_1 S = (s - 1, t^2 - 1) = (s - 1, t + 1) \cap (s - 1, t - 1)$. Then $\mathfrak{p}_1 \supset \mathfrak{p}_2$ is a chain of prime ideals of R and $\mathfrak{q}_1 = (s - 1, t + 1)$ is a prime ideal of S with $\mathfrak{q}_1 \cap R = \mathfrak{p}_1$. The chain $\mathfrak{q}_1$ cannot be extended to a chain lying over $\mathfrak{p}_1 \supset \mathfrak{p}_2$, as only $\mathfrak{q}_2$ lies over $\mathfrak{p}_2$, but $\mathfrak{q}_1$ does not contain $\mathfrak{q}_2$. Geometrically, the point $(1, -1)$ does not lie on the diagonal.

4.4. Noether normalisation

We return to the proof of weak Nullstellensatz 1.29. In it we projected the zero set of an ideal J to a space of one dimension lower. In general the image of an algebraic set is not closed, but using a suitable coordinate transformation (lemma 1.28) we ensured that it is so. This procedure can be repeated until the ideal $J \cap k[X_1, \ldots, X_d]$ is the zero ideal. Then we have found a finite projection onto $\mathbb{A}^d$. So $V(J)$ has the same dimension as $\mathbb{A}^d$. Algebraically this means that we are in the situation of the following definition.

DEFINITION 4.32. A *Noether normalisation* of an affine algebra $A = k[X_1, \ldots, X_n]/J$ is a finite ring extension $k[Y_1, \ldots, Y_d] \subset A$ such that the $Y_i \in A$ are algebraically independent over k (meaning that the natural map from the polynomial ring $k[T_1, \ldots, T_d]$ to $k[Y_1, \ldots, Y_d]$ is an isomorphism).

REMARK 4.33. Noether normalisation should not be confused with the normalisation of definition 4.14.

To show that $\mathbb{A}^d$ has dimension d, we need a refinement of Noether normalisation.

THEOREM 4.34 (Noether normalisation). *Let A be an affine algebra over an infinite field k and $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_r$ a chain of proper ideals of A. Then there exist algebraically independent elements $Y_1, \dots, Y_d \in A$ such that*

(1) *$k[Y_1, \dots, Y_d] \subset A$ is a finite extension,*
(2) *for $i = 1, \dots, r$ there is an $h(i)$ such that $\mathfrak{p}_i \cap k[Y_1, \dots, Y_d] = (Y_1, \dots, Y_{h(i)})$.*

The geometric interpretation of the theorem is as follows. If $V \subset \mathbb{A}^n$ is an algebraic set and a chain $W_1 \supset \cdots \supset W_r$ of subsets, then there is a surjective map $V \to \mathbb{A}^d$ with finite fibres, mapping $W_1 \supset \cdots \supset W_r$ onto a chain of linear subspaces of A^d.

PROOF.
Step 1. We have $A = k[X_1, \dots, X_n]/\mathfrak{q}_0$ for some ideal $\mathfrak{q}_0$. Let $\varphi\colon B = k[X_1, \dots, X_n] \to A$ be the projection. Set $\mathfrak{q}_i = \varphi^{-1}(\mathfrak{p}_i)$. Suppose that the theorem holds for B and the chain $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_r$: there exist $Y'_1, \dots, Y'_e \in B$ such that $k[Y'_1, \dots, Y'_e] \subset B$ is a finite extension and there exist $h'(i)$ with $\mathfrak{q}_i \cap B = (Y'_1, \dots, Y'_{h'(i)})$. Now (1) and (2) hold for A with $Y_i = \varphi(Y'_{i+h'(0)})$ and $h(i) = h'(i) - h'(0)$. So we may assume that $A = k[X_1, \dots, X_n]$ is a polynomial ring. The proof will be by induction on r and shows that $d = n$ in this case.
Step 2. Let $r = 1$ and suppose that $\mathfrak{p}_1 = (f) \neq (0)$ is a principal ideal in $A = k[X_1, \dots, X_n]$. Then $\deg f \geq 1$, as (f) is a proper ideal. We take coordinates Y_i as in the proof of Lemma 1.28, except that we consider X_1 as special variable. By dividing by a constant we achieve that $f \in k[Y_2, \dots, Y_n][X_1]$ is monic in X_1: $f = X_1^m + \cdots + f_0(Y_2, \dots, Y_n)$. We put $Y_1 = f$. Then $A = k[Y_1, \dots, Y_n][X_1]$ and X_1 is integral over $k[Y_1, \dots, Y_n]$, as $f - Y_1 = X_1^m + \cdots + f_0 - Y_1 = 0$. So A is finite over $k[Y_1, \dots, Y_n]$ by Lemma 4.8. The elements $Y_1, \dots, Y_n$ are algebraically independent, for otherwise $k(Y_1, \dots, Y_n)$ and therefore also $k(X_1, \dots, X_n)$ would have transcendence degree less than n over k.

To show that $\mathfrak{p}_1 \cap k[Y_1, \dots, Y_n] = (Y_1)$ we write an element $g = af$ of the intersection as $g = aY_1$ where $a = g/Y_1 \in A \cap k(Y_1, \dots, Y_n)$. As the polynomial ring $k[Y_1, \dots, Y_n]$ is normal (Example 4.15), $A \cap k(Y_1, \dots, Y_n) = k[Y_1, \dots, Y_n]$, so $a \in k[Y_1, \dots, Y_n]$ and $\mathfrak{p}_1 \cap k[Y_1, \dots, Y_n] = (Y_1)$.
Step 3. The case $r = 1$ and $\mathfrak{p}_1 \neq (0)$ an arbitrary ideal will be proved by induction on n. If $n = 1$, every ideal is principal, and we are done by Step 2.

For the induction step, let $f \in \mathfrak{p}_1$ be a non-zero element and construct $k[T_1, \ldots, T_n]$ with $T_1 = f$ as in Step 2. The induction hypothesis is that there exist algebraically independent $Y_2, \ldots, Y_n \in k[T_2, \ldots, T_n]$ such that $k[T_2, \ldots, T_n]$ is finite over $k[Y_2, \ldots, Y_n]$ and $\mathfrak{p}_1 \cap k[Y_2, \ldots, Y_n] = (Y_2, \ldots, Y_{h(1)})$ for some $h(1) \leq n$. Set $Y_1 = T_1$. As $k[Y_1, T_2 \ldots, T_n]$ is finite over $P = k[Y_1, Y_2, \ldots, Y_n]$, the same holds for A by Corollary 4.16, and (1) holds. Then $Y_1, \ldots, Y_n$ are algebraically independent over k. Furthermore, as $\mathfrak{p}_1 \cap k[Y_2, \ldots, Y_{h(1)}] = (Y_2, \ldots, Y_{h(1)})$ and $Y_1 = f \in \mathfrak{p}_1$, we find $\mathfrak{p}_1 \cap P \supset (Y_1, \ldots, Y_{h(1)})$. Conversely, if $g = \sum g_i(Y_2, \ldots, Y_n) Y_1^i \in \mathfrak{p}_1 \cap P$, then $g_0 \in \mathfrak{p}_1$, as $Y_1 \in \mathfrak{p}_1$. Hence $g_0 \in \mathfrak{p}_1 \cap k[Y_2, \ldots, Y_n] = (Y_2, \ldots, Y_{h(1)})$ and $g \in (Y_1, \ldots, Y_{h(1)})$. Therefore (2) holds.

Step 4. Suppose now that the theorem holds for $r-1$. Let $T_1, \ldots, T_n$ algebraically independent elements satisfying (1) and (2) for the chain $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_{r-1}$. Put $h = h(r-1)$. Applying Step 3 to the ideal $\mathfrak{p}_r \cap k[T_{h+1}, \ldots, T_n] \subset k[T_{h+1}, \ldots, T_n]$ gives $Y_{h+1}, \ldots, Y_n$ and

$$\mathfrak{p}_r \cap k[Y_{h+1}, \ldots, Y_n] = (Y_{h+1}, \ldots, Y_{h(r)})$$

for some $h(r) \leq n$. Put $Y_i = T_i$ for $1 \leq i \leq h$. By assumption A is a finite extension of $k[T_1, \ldots, T_n]$, and $k[T_1, \ldots, T_n]$ is by construction a finite extension of $P = k[Y_1, \ldots, Y_n]$, so by Corollary 4.16 A is a finite extension of P.

Consider a fixed i with $1 \leq i \leq r$. Then $(Y_1, \ldots, Y_{h(i)}) \subset \mathfrak{p}_i$. Write an element $g \in \mathfrak{p}_i \cap P$ as polynomial in $Y_1, \ldots, Y_{h(i)}$ with coefficients in $k[Y_{h(i)+1}, \ldots, Y_n]$. The constant term g_0 of g lies in $\mathfrak{p}_i \cap k[Y_{h(i)+1}, \ldots, Y_n]$. If $i < r$, then $\mathfrak{p}_i \cap k[Y_{h(i)+1}, \ldots, Y_n] \subset \mathfrak{p}_i \cap k[T_{h(i)+1}, \ldots, T_n] = (0)$. For $i = r$ by construction $\mathfrak{p}_r \cap k[Y_{h+1}, \ldots, Y_n] = (Y_{h+1}, \ldots, Y_{h(r)})$ so also in this case $\mathfrak{p}_r \cap k[Y_{h(r)+1}, \ldots, Y_n] = (0)$. Therefore $g_0 = 0$ and $g \in (Y_1, \ldots, Y_{h(i)})$. Thus $\mathfrak{p}_i \cap P = (Y_1, \ldots, Y_{h(i)})$, and (2) holds. □

4.5. Dimension of affine and projective varieties

Finally we can prove that the polynomial ring $k[X_1, \ldots, X_n]$ has Krull dimension n.

THEOREM 4.35. *Let $k[Y_1, \ldots, Y_d] \subset A$ be a Noether normalisation of an affine algebra A. Then* $\dim A = d$.

PROOF. We have already seen that $\dim A = \dim k[Y_1, \ldots, Y_d] \geq d$ (Corollary 4.23 and Example 4.4). Let $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ be a chain of prime ideals in $k[Y_1, \ldots, Y_d]$. We have to show that $r \leq d$. By Theorem 4.34 there exists a Noether normalisation $k[T_1, \ldots, T_d] \subset k[Y_1, \ldots, Y_d]$ with $\mathfrak{p}_i \cap k[T_1, \ldots, T_d] = (T_1, \ldots, T_{h(i)})$ for $1 \leq i \leq r$. Then $r \leq h(r) \leq d$. □

DEFINITION 4.36. A chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ of prime ideals in a ring R is *maximal* if it cannot be extended to a longer chain by inserting a prime ideal.

THEOREM 4.37. *Let A be an affine algebra, which is an integral domain. Then all maximal chains of prime ideals have the same length $d = \dim A$.*

PROOF. Let $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_r$ be a maximal chain of prime ideals. Then, as A is a domain, $\mathfrak{q}_0 = (0)$ and $\mathfrak{q}_r$ is a maximal ideal. By Theorem 4.34 there is a Noether normalisation $P = k[Y_1, \dots, Y_d]$, $\mathfrak{p}_i = \mathfrak{q}_i \cap k[Y_1, \dots, Y_d] = (Y_1, \dots, Y_{h(i)})$. Then $h(0) = 0$ and as $\mathfrak{p}_r$ is a maximal ideal by Theorem 4.18, $h(r) = d$. Suppose that there is an i such that $h(i)+1 < h(i+1)$. Then one could insert the prime ideal $(Y_1, \dots, Y_{h(i)+1})$ between $\mathfrak{p}_i$ and $\mathfrak{p}_{i+1}$. Now $P/\mathfrak{p}_i = k[Y_{h(i)+1}, \dots, Y_d]$ is a polynomial ring and therefore normal, and the extension $P/\mathfrak{p}_i \subset A/\mathfrak{q}_i$ is integral because $P \subset A$ is integral. By 'going down' (Theorem 4.29) one can then insert a prime ideal between (0) and $\mathfrak{q}_{i+1}/\mathfrak{q}_i$, so between $\mathfrak{q}_i$ and $\mathfrak{q}_{i+1}$, contradicting the maximality of the chain. Therefore $h(i + 1) = h(i) + 1$ and the chain has length d. □

COROLLARY 4.38. *Let $\mathfrak{p}$ be a prime ideal in an affine algebra A, which is an integral domain. Then $\dim A = \operatorname{ht}(\mathfrak{p}) + \dim(A/\mathfrak{p})$.*

PROOF. Start from a chain ending with $\mathfrak{p}$ of length $\operatorname{ht}(\mathfrak{p})$ and extend it to maximal chain. The maximal chain has length $\dim A$ and the part starting from $\mathfrak{p}$ gives a maximal chain in $A/\mathfrak{p}$. □

THEOREM 4.39. *Let $V \subset \mathbb{A}^n$ be an algebraic set and $\bar{V} \subset \mathbb{P}^n$ its projective closure. Then $\dim V = \dim \bar{V}$.*

PROOF. It suffices to consider the case that V is irreducible. Let

$$\emptyset \neq W_0 \subsetneq \cdots \subsetneq W_d = \bar{V}$$

be a maximal chain in $\bar{V}$, starting from a point W_0. Let V' be an affine open subset of $\bar{V}$ containing the point W_0. The chain of irreducible subsets $W_i \cap V'$ shows that $\dim V' = \dim \bar{V}$.

On the other hand, a maximal chain in $V \cap V'$ gives by taking the closure rise to maximal chains in V and in V'. As all maximal chains in V have the same length and the same holds for V' we get $\dim V = \dim V' = \dim \bar{V}$. □

REMARK 4.40. If V is an affine variety with Noether normalisation $k[Y_1, \dots, Y_d] \subset k[V]$, then $\dim V = d$ is also the transcendence degree of the function field $k(V)$ over k. This is the classical definition of the dimension of affine and projective varieties.

CHAPTER 5

Tangent space and nonsingularity

In this chapter we define what it means that a variety is smooth. In the case $k = \mathbb{C}$ one gets, as it should be, that $V \subset \mathbb{A}^N$ is smooth at P if and only if V is a complex submanifold of $\mathbb{A}^N$ in an Euclidean neighborhood of P.

There are two notions of tangent space. Firstly, we can consider the tangent space as linear subspace of the ambient affine or projective space; the projective one will be the projective closure of the affine tangent space, defined on a affine open set of projective space. The other notion is intrinsic, defined without explicit reference to an embedding. It is no restriction to treat this only in the affine case. After all, the tangent space should be the best local approximation.

5.1. Embedded tangent space

We start with the hypersurface case, where we generalise the definition used for curves in 3.21.

Definition 5.1. Let $V = (f) \subset \mathbb{P}^n$ be a projective hypersurface. The *tangent space* $T_P V$ to V at $P \in V$ is the linear subvariety

$$V\left(\frac{\partial f}{\partial X_0}(P)X_0 + \frac{\partial f}{\partial X_1}(P)X_1 + \dots + \frac{\partial f}{\partial X_n}(P)X_n\right) .$$

The point P is a *nonsingular point* if $T_P V$ is a hyperplane, that is, if $df(P) = (\frac{\partial f}{\partial X_0}(P), \dots, \frac{\partial f}{\partial X_n}(P)) \neq 0$.

The *tangent space* to an affine hypersurface $V = (f) \subset \mathbb{A}^n$ in the point $P = (a_1, \dots, a_n)$ is the linear subvariety

$$V\big(\frac{\partial f}{\partial x_1}(P)(X_1 - a_1) + \dots + \frac{\partial f}{\partial x_n}(P)(X_n - a_n)\big) .$$

Proposition 5.2. *Let $f \in k[X_1, \dots, X_n]$, k algebraically closed, a polynomial without multiple factors. The set of nonsingular points of $V = (f)$ is an open dense subset of V.*

Proof. We have to show that the set of singular points is a proper closed subset of each irreducible component. The singular set Σ is $V(f, \frac{\partial f}{\partial x_i})$, so closed. Suppose that an irreducible component $V(f_j)$ of V is contained in Σ. This means that all partial derivatives $\frac{\partial f}{\partial x_i}$ vanish on $V(f_j)$. By the product rule this is the case if and only if all $\frac{\partial f_j}{\partial x_i}$ vanish on $V(f_j)$. So we may as well assume that f is irreducible.

We then have that $\frac{\partial f}{\partial x_i} \subset (f)$, and therefore $\frac{\partial f}{\partial x_i} = 0$, as its degree is lower than that of f. If $\operatorname{char} k = 0$, this implies that f is constant, contradicting our assumption that V is a hypersurface. If $\operatorname{char} k = p > 0$, we conclude that f is a polynomial in $X_1^p, \dots, X_n^p$. Then $f = g^p$, where the coefficients of g are pth roots of those of f. This contradicts the fact that (f) is a radical ideal. □

EXAMPLE 5.3. Let $f = g^2$ for an irreducible polynomial g. Then every point in $V(f) = V(g)$ is singular.

We now look at arbitrary algebraic sets.

DEFINITION 5.4. Let V be an affine or projective algebraic set. The *tangent space* T_pV to V in the point $P \in V$ is the linear subvariety

$$T_PV = \bigcap_{f \in I(V)} T_pV(f) \,.$$

To describe the tangent space it suffices to use generators of the ideal. In the projective case, if $(f_1, \dots, f_k)$ generate the homogeneous ideal of V, then $T_PV = V(\sum_j \frac{\partial f_1}{\partial X_j}(P)X_j, \dots, \sum_j \frac{\partial f_k}{\partial X_j}(P)X_j)$, and analogously in the affine case.

This last formulation works for any ideal. E.g., for the fat point with coordinate ring $k[X,Y]/(X,Y^2)$ the tangent space at the origin is $V(X)$, whereas for the fat point with ring $k[X,Y]/(X^2,XY,Y^2)$ it is $\mathbb{A}^2$.

LEMMA 5.5. *Let $(f_1, \dots, f_k)$ generate the ideal of V. Then*

$$\dim T_PV = n - \operatorname{Rank}\left(\frac{\partial f_i}{\partial X_j}\right)(P) \,,$$

where $(\frac{\partial f_i}{\partial X_j})$ is the Jacobian matrix.

The function $V \to \mathbb{N}$, $P \mapsto \dim T_PV$, is upper semicontinous in the Zariski topology on V. That is, for any integer r the subset $\{P \in V \mid \dim T_PV \geq r\}$ is Zariski closed.

PROOF. This is just linear algebra. The Jacobian matrix has rank at most $n-r$ if and only if all the $(n-r+1) \times (n-r+1)$ minors vanish. □

EXAMPLE 5.6. Let $V = V(XZ, YZ) \subset \mathbb{A}^3$. Its zero set consists of a line L (the Z-axis) and a plane Π (the X,Y-plane) through the origin O. Then $\dim T_PV = 1$ for $P \in L \setminus \{O\}$, $\dim T_PV = 2$ for $P \in \Pi \setminus \{O\}$ and $\dim T_OV = 3$.

DEFINITION 5.7. Let $P \in V \subset \mathbb{A}^n$ be point of an algebraic set. The *local dimension* of V at P, written $\dim_P V$, is $\dim \mathcal{O}_{V,P}$.

The dimension $\dim_P V$ is the maximum dimension of an irreducible component of V containing P.

REMARK 5.8. We always have $\dim T_P V \geq \dim_P V$. In contrast to the hypersurface case, however, the result for arbitrary algebraic sets does not follow directly from the definitions.

We sketch several approaches to it.

The first one reduces it to the case of hypersurfaces. One needs the intrinsic description of the tangent space below, and shows that the minimal dimension is a birational invariant. Every variety is birational to a hypersurface. This follows from Noether normalisation together with the Theorem of the Primitive Element: let $K \subset L$ be a finite separable field extension of an infinite field, then there exists an $x \in L$ such that $L = K(x)$.

In the complex case the fact that the Jacobian matrix has rank $n-d$, say that the first $(n-d)\times(n-d)$ minor does not vanish, implies that in an Euclidean neighbourhood of P the zero set of $f_1, \dots, f_{n-d}$ is a submanifold of dimension d. But the implicit function theorem does not hold with Zariski open sets, because they are much too large. It does hold using formal power series. One has to show that $\dim \mathcal{O}_{V,P} = \dim k[[X_1 - a_1, \dots, X_n - a_n]]/I(V)$.

The best proof requires more commutative algebra. One needs again the intrinsic characterisation of the tangent space, as $(\mathfrak{m}/\mathfrak{m}^2)^*$, where $\mathfrak{m}$ is the maximal ideal of the local ring $\mathcal{O}_{V,P}$. Then it is a general fact about local Noetherian rings, that $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 \geq \dim R$. We will prove it below for the local rings of affine algebraic sets.

DEFINITION 5.9. An algebraic set V in $\mathbb{A}^n$ or $\mathbb{P}^n$ is *smooth* (or *nonsingular*) at $P \in V$ if $\dim T_P V = \dim_P V$. Then P is a *smooth* (or *nonsingular*) *point* of V. Otherwise, V is *singular* at P, and P is a *singular point* or a *singularity* of V.

The set Σ_V of singular points of V is called the *singular locus* of V. If Σ_V is empty, that is, if V is smooth at each of its points, then V is called *smooth*.

5.2. Zariski tangent space

Usually elements of the affine tangent space are called tangent vectors; indeed, $T_P V$ is not only an affine linear subspace, but it has a distinguished point, P, which can serve as origin of a vector space. A point $Q \in T_P V$ is then the endpoint of the vector $\overrightarrow{PQ}$. There are therefore two coordinates involved, those of $P = (a_1, \dots, a_n) \in \mathbb{A}^n$ and $Q = (a_1 + b_1, \dots, a_n + b_n) \in \mathbb{A}^n$ (so that the b_i are the coordinates of Q when P is the orgin). A convenient way to write the coordinates of a tangent vector is as $(a_1 + b_1\varepsilon, \dots, a_n + b_n\varepsilon)$, where ε is as in analysis a very small number, algebraically expressed by $\varepsilon^2 = 0$. Recall that the inclusion $\{P\} \to V$ corresponds to a k-algebra homomorphism $\mathrm{ev}_p \colon k[V] \to k$, given by $\mathrm{ev}_P(f) = f(a_1, \dots, a_n)$. This can be seen as a map from an abstract point $\mathbb{P}$ to V, where by changing the map (by changing the a_i) we vary the point $P \in V$. Now consider the fat point $\mathbb{T}$ with coordinate ring $k[\varepsilon] = k[t]/(t^2)$, sometimes called the ring of dual numbers. Then in the same sense a tangent vector is a map from $\mathbb{T}$ to V, given by evaluation $\mathrm{ev}_{\overrightarrow{PQ}}$. By Taylors formula and $\varepsilon^2 = 0$ we have

$$\begin{aligned}\mathrm{ev}_{\overrightarrow{PQ}}(f) &= f(a_1 + b_1\varepsilon, \dots, a_n + b_n\varepsilon) \\ &= f(a_1, \dots, a_n) + \varepsilon \sum b_i \tfrac{\partial f}{\partial X_i}(a_1, \dots, a_n)\ .\end{aligned}$$

EXAMPLE 5.10. Let $Gl(n, k)$ be the affine algebraic variety of invertible $n \times n$ matrices. We determine the tangent space at I, the identity matrix. Let $A \in M(n, n; k)$ be any $n \times n$ matrix. Then we have $\det(I + \varepsilon A) = 1 + \varepsilon \operatorname{Tr} A$, which is a unit in $k[\varepsilon]$. So $T_I Gl(n, k) = M(n, n; k)$. For $Sl(n, k)$, the matrices with determinant one, we find that $T_I Sl(n, k) = \{A \in M(n, n; k) \mid \operatorname{Tr} A = 0\}$.

Another way to distinguish the coordinates b_i is to write a tangent vector as differential operator. A tangent vector is then $X = \sum b_i \frac{\partial}{\partial X_i}$. The condition that $X \in T_P V$ is that $X(f)(P) = 0$ for all $f \in I(V)$. We can use this description to give an intrinsic characterisation of the tangent space.

THEOREM 5.11. *Let $P \in V$ be a point on an affine algebraic set, with maximal ideal $M_P \subset k[V]$; let $\mathfrak{m}_p$ be the maximal ideal in $\mathcal{O}_{V,P}$. The $k[V]$-module M_P/M_P^2 is naturally a k-vector space, as is the $\mathcal{O}_{V,P}$-module $\mathfrak{m}_P/\mathfrak{m}_P^2$. There are natural isomorphisms of vector spaces*

$$T_P V \cong (M_P/M_P^2)^* \cong (\mathfrak{m}_P/\mathfrak{m}_P^2)^*\ ,$$

where the $*$ denotes the dual vector space.

PROOF. We first note that $\mathfrak{m}_P/\mathfrak{m}_P^2$ is a module over $\mathcal{O}_{V,P}/\mathfrak{m}_P = k$, so a k-vector space.

A tangent vector $X = \sum b_i \frac{\partial}{\partial X_i}$ gives a linear function on M_P, which is well-defined modulo $I(V)$, as $X(f) = 0$ for all $f \in I(V)$. Conversely, if a linear function l is given, we define $b_i = l(X_i)$.

The inclusion $M_P \subset \mathfrak{m}_P$ induces an injection $M_P/M_P^2 \to \mathfrak{m}_P/\mathfrak{m}_P^2$. We show that it is surjective. Let f/g be a representative of a function germ in $\mathfrak{m}_P$. Let $c = g(P)$. Then $f/c - f/g = f(1/c - 1/g) \in \mathfrak{m}_P^2$, so the classs of f/g in $\mathfrak{m}_P/\mathfrak{m}_P^2$ is the image of the class of $f/c \in M_P/M_P^2$.

Note that a tangent vector $X = \sum b_i \frac{\partial}{\partial X_i}$ acts on $\mathfrak{m}_P$ by the quotient rule. $\square$

DEFINITION 5.12. We call $(\mathfrak{m}_P/\mathfrak{m}_P^2)^*$ the *Zariski tangent space* to V at P.

DEFINITION 5.13. Let $f\colon V \to W$ be a regular map between affine algebraic sets, and let $f^*\colon k[W] \to k[V]$ be the corresponding map of coordinate rings. Suppose $f(P) = Q$. Then the dual of the induced map $f^*\colon \mathfrak{m}_Q/\mathfrak{m}_Q^2 \to \mathfrak{m}_P/\mathfrak{m}_P^2$ is the *differential* $d_Pf\colon T_PV \to T_QW$ of f at P.

5.3. The dimension of the tangent space

In this section we show that the dimension of the Zariski tangent space is at least that of the algebraic set. This is a consequence of the following geometric version of Krull's Hauptidealsatz.

PROPOSITION 5.14. *Let V be an affine (or projective) variety of dimension d, and $f \in k[V]$ be a (homogeneous) element of the (homogeneous) coordinate ring of V. If $f \neq 0$ then all irreducible components of $V(f)$ have dimension $d-1$.*

We quote the general algebraic version.

THEOREM 5.15 (Krull's Hauptidealsatz). *Let R be a Noetherian ring and $(a) \neq R$ a principal ideal. For all minimal primes $(a) \subset \mathfrak{p}$ the height of $\mathfrak{p}$ is at most 1, and equal to 1 if a is not a zero-divisor.*

Before proving Proposition 5.14 we give an example, which shows that codimension can behave unexpectedly in general rings.

EXAMPLE 5.16 (taken from Ravi Vakil's notes *Foundations Of Algebraic Geometry*, see http://math216.wordpress.com). Let A be the local ring of the affine line at the origin, so $A = k[x]_{(x)}$. We consider the ring $R = A[t]$. One has $\dim R = 2$: the chain $(0) \subset (t) \subset (x,t)$ shows that the dimension is at least 2. The principal ideal $I = (xt-1)$ is prime: it is a maximal ideal, as $R/I \cong k[x]_{(x)}[\frac{1}{x}] \cong k(x)$ is a field. By Krull's Hauptidealsatz this ideal has height 1 and $(0) \subset (xt-1)$ is a maximal chain. Thus we have a dimension 0, codimension 1 prime in a two-dimensional ring.

Such behaviour cannot happen for affine varieties.

PROOF OF PROPOSITION 5.14. It suffices to prove the affine case. Suppose first that $W = V(f) \subset V$ is irreducible. Let $\mathfrak{p} = \sqrt{(f)}$ be the corresponding prime ideal. We choose a Noether normalisation $k[Y_1,\dots,Y_d] \subset k[V]$ with $\mathfrak{p} \cap k[Y_1,\dots,Y_d] = (Y_1,\dots,Y_h)$. We claim that $\mathfrak{p} \cap k[Y_1,\dots,Y_d]$ is again a principal ideal and therefore $h=1$. It then follows that the dimension of W is $d-1$.

Let $L = K(V)$ be the quotient field of $k[V]$ and $K = k(Y_1,\dots,Y_d)$ that of $k[Y_1,\dots,Y_d]$. Then L/K is a finite algebraic extension. Let $f_0 = N_{L/K}(f)$ be the norm of f. Let $X^n + \cdots + a_n$ be the minimal polynomial of f over K. Then f_0 is a power a_n^m of a_n and all coefficients a_i lie in $k[Y_1,\dots,Y_d]$ by Lemma 4.28, so in particular $f_0 \in k[Y_1,\dots,Y_d]$, and as

$$0 = a_n^{m-1}(f^n + \cdots + a_n) = f(a_n^{m-1}f^{n-1} + \cdots + a_n^{m-1}a_{n-1}) + f_0$$

also $f_0 \in \mathfrak{p}$. If now $g \in \mathfrak{p} \cap k[Y_1, \dots, Y_d]$ then $g \in \sqrt{(f)}$ so $g^r = fh$ and by taking norms

$$g^{r[L:K]} = N_{L/K}(g^r) = N_{L/K}(f)N_{L/K}(h) \in (f_0)$$

as $N_{L/K}(h) \in k[Y_1, \dots, Y_d]$ by Lemma 4.28. Therefore $\mathfrak{p} \cap k[Y_1, \dots, Y_d] = \sqrt{(f_0)}$. In $k[Y_1, \dots, Y_d]$ the primary decomposition of a principal ideal is just the product of decomposition of the generator into irreducible elements. Therefore f_0 is a unit times f_{00}^l for some integer l and some irreducible f_{00} and we find that $\mathfrak{p} \cap k[Y_1, \dots, Y_d] = (f_{00}) = (Y_1)$.

If W is reducible, we decompose $W = W_1 \cup \dots \cup W_m$. Let $g \in k[X_1, \dots, X_n]$ a polynomial that vanishes on $W_2, \dots, W_m$, but not on W_1 and consider $V_g = V \cap D(g)$. This is an affine variety of dimension d, and $V_g \cap V(f)$ has only one component, of dimension $d-1$, by the first part of the proof. Its closure in V has also dimension $d-1$. □

COROLLARY 5.17. *Let V be an affine (or projective) variety. Let $f_1, \dots, f_m \in k[V]$ be (homogeneous) elements of the (homogeneous) coordinate ring of V, with non empty zero set $W = V(f_1, \dots, f_m) \subset V$. Then $\dim Z \geq \dim V - m$ for every irreducible component Z of W.*

THEOREM 5.18. *Let $f\colon V \to W$ be a regular surjective map of varieties, $n = \dim V$, $m = \dim W$. Then $\dim F \geq n - m$ for any point $Q \in W$ and every irreducible component F of the fibre $f^{-1}(Q)$.*

PROOF. Let $P \in f^{-1}(Q)$. By taking affine neighbourhoods of P and Q we may suppose that V and W are affine. Let $\pi\colon W \to \mathbb{A}^m$ be a finite map (Noether normalisation!). Then the fibre of $\pi \circ f$ over $\pi(Q)$ (with reduced structure) is the disjoint union of the fibres of f over the points of $\pi^{-1}(\pi(Q))$. It suffices to prove the statement for $\pi \circ f\colon V \to \mathbb{A}^m$, that is, we may assume that $W = \mathbb{A}^m$. Then $I(Q) = (Y_i - b_i)$, and the fibre is given by the m equations $f_i = b_i$. Therefore each irreducible component has dimension at least $n-m$. □

To prove the statement about the dimension of the Zariski tangent space we need an important argument, valid for local rings.

THEOREM 5.19 (Nakayama's Lemma). *Let R be a local ring with maximal ideal $\mathfrak{m}$, let M be a finitely generated R-module, and let $N \subset M$ be a submodule. Then $N + \mathfrak{m}M = M$ if and only if $N = M$.*

PROOF. Replacing M by M/N, we may assume N = 0. We have to show that $\mathfrak{m}M = M$ implies $M = 0$. Let $m_1, \dots, m_r$ be generators of M. If $\mathfrak{m}M = M$ we may write $m_i = \sum a_{ij}m_j$ for each i with the $a_{ij} \in \mathfrak{m}$, or in matrix notation,

$$(I - A)\underline{m} = 0 \,,$$

where A is the square matrix with entries a_{ij} and $\underline{m}$ is the column vector of the m_i. Therefore $\det(I - A)m_i = 0$. As $\det(I - A) \equiv 1 \bmod \mathfrak{m}$, it is a unit and $m_i = 0$ for all i. Thus $M = 0$. □

COROLLARY 5.20. *Elements $m_1, \dots, m_r$ generate M as R-module if and only their residue classes $m_i + \mathfrak{m}M$ generate $M/\mathfrak{m}M$ as $R/\mathfrak{m}$-vector space. In particular, any minimal set of generators for M corresponds to an $R/\mathfrak{m}$-basis for $M/\mathfrak{m}M$, and any two such sets have the same number of elements.*

PROOF. Take $N = (m_1, \dots, m_r) \subset M$. $\square$

THEOREM 5.21. *Let $P \in V$ be a point of an affine algebraic set. Then* $\dim T_P V \geq \dim_P V$.

PROOF. Let M_P be the maximal ideal of P in $k[V]$, and $\mathfrak{m}_P$ the maximal ideal in $\mathcal{O}_{V,P}$. Then $\dim T_P V = \dim_k \mathfrak{m}_P/\mathfrak{m}_P^2$. Say that this dimension is m. Choose elements $f_1, \dots, f_m \in k[V]$, which project onto a basis of $M_P/M_P^2 \cong \mathfrak{m}_P/\mathfrak{m}_P^2$. By Nakayama's lemma $(f_1, \dots, f_m) = \mathfrak{m}_P$. Therefore $\{P\}$ is an irreducible component of $V(f_1, \dots, f_m) \subset V$, of dimension 0. Let V_1 be an irreducible component of V passing through P, with $\dim V_1 = \dim_P V$. Then $\{P\}$ is also an irreducible component of $V(f_1, \dots, f_m) \subset V_1$, of dimension $0 \geq \dim V_i - m$. Therefore $m \geq \dim_P V$. $\square$

5.4. The main theorem of elimination theory

THEOREM 5.22. *The image of a projective algebraic set V under a regular map $f\colon V \to W$ is a closed subset of W in the Zariski topology.*

DEFINITION 5.23. A map $f\colon V \to W$ is *closed* if for every closed subset $Z \subset V$ its image $f(Z)$ is a closed subset of W.

PROOF OF THE THEOREM.
Step 1: reduction to a projection. We factor the map f via its graph: we write $f\colon V \xrightarrow{\Gamma} V \times W \xrightarrow{\pi} W$, where $\Gamma(P) = (P, f(P))$ and π is the projection on the second factor. To show that the graph $\Gamma(V)$ is a closed subset of $V \times W$ we observe that it is the inverse image of the diagonal $\Delta(W) \subset W \times W$ under the map (f, id_W), which is a closed subvariety, as it is cut out by the equations $x_i = y_i$, if the x_i are coordinates on the first factor of $W \times W$, and y_i the corresponding coordinates on the second factor. It remains to show that $\pi\colon V \times W \to W$ is a closed map.
Step 2: reduction to the case $V = \mathbb{P}^n$, $W = \mathbb{A}^m$. If Z is a closed subset of $V \times W$ and $V \subset \mathbb{P}^n$, then Z is also closed in $\mathbb{P}^n \times W$, and $\pi(Z)$ is also the image under the projection $\mathbb{P}^n \times W \to W$, so we may assume that $V = \mathbb{P}^n$.

As the condition that a subset is closed can be checked in affine open sets, we may assume that W is affine. Being closed in W then follows from being closed in $\mathbb{A}^m$, so we may assume that $W = \mathbb{A}^m$.
Step 3: the projection $\mathbb{P}^n \times \mathbb{A}^m \to \mathbb{A}^m$ is closed. We have defined the product $\mathbb{P}^n \times \mathbb{P}^m$ as variety as the image under the Segre embedding

2.40. A closed subset of $\mathbb{P}^n \times \mathbb{P}^m$ is given by homogeneous polynomials in the Z_{ij}, but by substituting $Z_{ij} = X_i Y_j$ we can also work with polynomials *bihomogeneous* in the X_i and Y_j. For $\mathbb{P}^n \times \mathbb{A}^m$ we make the Y_j coordinates inhomogeneous, but the polynomials are still homogeneous in the X_i. So let Z be given by polynomials $f_1, \dots, f_k \in k[X_0, \dots, X_n, Y_1, \dots, Y_m]$, of degree d_i in the X_i.

Consider a fixed point $Q = (b_1, \dots, b_m) \in \mathbb{A}^m$. Then $Q \in \pi(Z)$ if and only if the ideal I_Q, generated by the polynomials

$$f_{i,Q} = f_i(X_0, \dots, X_n, b_1, \dots, b_m) ,$$

has a zero in $\mathbb{P}^n$. By Proposition 2.15 $V(I_Q) = \emptyset$ if and only if $(X_0, \dots, X_n)^s \subset I_Q$ for some s. This condition means that every homogeneous polynomial of degree s can be written as $\sum g_i f_{i,Q}$. So $Q \in \pi(Z)$ if $(X_0, \dots, X_n)^s \not\subset I_Q$ for all s.

Consider the set

$$W_s = \{Q \in \mathbb{A}^m \mid (X_0, \dots, X_n)^s \not\subset I_Q\} .$$

Then the image $\pi(Z)$ is the intersection of all the sets W_s. It suffices therefore to show that W_s is closed for any s. For the purpose of this proof let $S_d \subset k[Y_1, \dots, Y_m][X_0, \dots, X_n]$ be the $k[Y_1, \dots, Y_m]$-module of all polynomials, homogeneous of degree d in the X_i. A generating set are the monomials of degree d in the X_i. Now consider the homomorphism of $k[Y_1, \dots, Y_m]$-modules

$$S_{s-d_1} \oplus \cdots \oplus S_{s-d_k} \to S_s, \quad (g_1, \dots, g_k) \mapsto \sum g_i f_i .$$

It is given by a matrix with entries in $k[Y_1, \dots, Y_m]$. Then W_s is the set of points where this map has rank less than $\binom{n+s}{s}$ and it is defined by the minors of size $\binom{n+s}{s}$ of the matrix. Therefore W_s is closed. $\square$

CHAPTER 6

Lines on hypersurfaces

In this chapter k is an algebraically closed field of characteristic not equal to 2, unless otherwise stated.

6.1. A dimension count

We consider the following problem. Let V be a hypersurface of degree d in $\mathbb{P}^n$. When does V contain a linear subspace of dimension k, and if so, how many? In particular, does V contain lines ($k = 1$)?

Given a line $L \subset \mathbb{P}^n$, say

$$(X_0 : X_1 : X_2 : \cdots : X_n) = (S : T : 0 : \cdots : 0)\ ,$$

it is easy to write down a hypersurface of degree d containing L: just take $f = X_2 g_2 + \cdots + X_n g_n$ with $g_i \in k[X_0, \ldots, X_n]$ of degree $d - 1$. We can choose (f) to be non-singular. The condition that (f) is non-singular at the line L is that $V(\frac{\partial f}{\partial X_i}) \cap V(X_2, \ldots, X_n) = \emptyset$. We compute the $\frac{\partial f}{\partial X_i}$ and put in $X_2 = \cdots = X_n = 0$ and find $(\frac{\partial f}{\partial X_0}, \ldots, \frac{\partial f}{\partial X_n}) = (0, 0, g_2, \ldots, g_n)$ so the g_i should not have a common zero on the line.

The general hypersurface of degree d will not contain lines. Then the question becomes for which degree does the general hypersurface of that degree contain lines, and how many.

Let $V = (f)$ with $f \in k[X_0, \ldots, X_n]$ of degree d. We write down the condition that a given line lies on V. Let P and Q be two points of L. Then L can be given in parametric form as

$$\lambda P + \mu Q = (\lambda p_0 + \mu q_0 : \cdots : \lambda p_n + \mu q_n)\ ,$$

and L lies on V if and only if the polynomial $f(\lambda P + \mu Q)$ in $(\lambda : \mu)$ is the zero polynomial. We develop

$$f(\lambda P + \mu Q) =$$
$$\lambda^d f_0(P, Q) + \lambda^{d-1}\mu f_1(P, Q) + \cdots + \lambda\mu^{d-1} f_{d-1}(P, Q) + \mu^d f_d(P, Q),$$

where $f_0(P, Q) = f(P)$ and $f_d(P, Q) = f(Q)$. Basically by Taylor's theorem we can write $f_1(P, Q) = \sum q_i \frac{\partial f}{\partial X_i}(P)$. Denote by Δ_Q the differential operator $\Delta_Q = \sum q_i \frac{\partial}{\partial X_i}$. With this notation $f_1(P, Q) = \Delta_Q f(P)$ and we find that $f_2(P, Q) = \frac{1}{2}\Delta_Q^2 f(P)$, if $\operatorname{char} k \neq 2$.

So we get, for a fixed f, $d+1$ equations in the p_i, q_i. We will discuss below how we can make the p_i, q_i into coordinates on the space of all lines in $\mathbb{P}^n$. It turns out that this is a projective variety of dimension $2(n-1)$. So we expect lines as long as $d+1 \leq 2(n-1)$.

Let us look at $n = 3$.

$d = 1$: A plane contains a two-dimensional family of lines.
$d = 2$: Any nondegenerate quadric has two rulings, that is, two 1-dimensional families of lines.
$d = 3$: We will show that a smooth cubic surface contains exactly 27 lines.
$d \geq 4$: In general no lines.

In the case $n = 4$ we expect a finite number of lines on a quintic threefold. Indeed, the general quintic contains 2875 lines, but there also exist smooth quintic threefolds containing 1-parameter families of lines. On a general quintic the number of rational curves of given degree d is finite. A formula for this number was first conjectured by the physicists Candela, de la Ossa, Green and Parker. This was starting point for an enormous activity, which goes under the name of mirror symmetry.

6.2. Grassmann variety

The construction in this section works for any field, notably $k = \mathbb{R}$. We show that the space of $r-1$-dimensional subspaces of $\mathbb{P}^{n-1}$ is a smooth projective variety, the Grassmannian G^n_r. The indexing is explained by the fact that it is also the space of r-dimensional linear subspaces of the n-dimensional vector space k^n.

An r-dimensional linear subspace L is determined by r linearly independent vectors $v_0, \dots, v_{r-1}$. We write these vectors as row vectors, and put them in an $r \times n$ matrix M_L. If we take a different basis, we get a matrix of the form $M'_L = AM_L$, where A is the $r \times r$ base change matrix. All the minors are therefore multiplied by the same factor $\det A$, and the ratios of the minors give a well-defined point in $\mathbb{P}^N$, where $N = \binom{n}{r} - 1$.

Definition 6.1. The *Plücker coordinates* of L are the $r \times r$ minors of the matrix M_L formed by the vectors in a basis of L.

Proposition 6.2. *The Grassmann variety G^n_r of all r-dimensional linear subspaces of k^n is a smooth projective variety of dimension $r(n-r)$.*

Proof. We describe an affine open set. Let M_L be a matrix representing the linear subspace L. Suppose $p_{i_0,\dots,i_{r-1}} \neq 0$, where $p_{i_0,\dots,i_{r-1}}$ is the minor formed with columns $i_0, \dots, i_{r-1}$. For ease of notation we suppose that these columns are the first r columns. Let then A be the $r \times r$ matrix, formed by the first r columns. The condition $p_{0,\dots,r-1} \neq 0$ means that A is invertible, so $A^{-1}M_L$ is another matrix representing the same subspace. We conclude that every L in this affine chart can be represented by a matrix of the form $(I\ N)$, where I is the $r \times r$ identity matrix and N is an $r \times (n-r)$ matrix. Moreover, this representation is unique. So the open set $p_{0,\dots,r-1} \neq 0$ is the space of $r \times (n-r)$ matrices, which is isomorphic to $\mathbb{A}^{r(n-r)}$. The Grassmann variety is the projective closure of this affine open set. The explicit description shows that it is smooth. □

REMARK 6.3. We can also describe the above in a coordinate free way. Let V be a finite dimensional k-vector space, and $L \subset V$ a linear subspace of dimension r. There is an induced map $\Lambda^r L \to \Lambda^r V$ of exterior powers. As $\dim \Lambda^r L = 1$, we obtain the Grassmann variety $G_r(V)$ as variety in $\mathbb{P}(\Lambda^r V)$.

Let L be a fixed subspace. Then almost all other subspaces can be described as graph of a linear map $L \to V/L$ (with as matrix the matrix N from above).

REMARK 6.4. To describe the ideal defining G_r^n we can start from the affine chart $p_{0,\dots,r-1} \neq 0$. Note that each entry n_{ij} of the matrix N is up to sign a Plücker coordinate: take the minor formed from columns $0, \dots, i-i, i+1, \dots, r-1, r-1+j$. All Plücker coordinates are given by the minors of N of arbitrary size, and they can be expressed in terms of the entries n_{ij}. We can give quadratic equations: just compute a minor by (generalised) Laplace expansion. Then make these equations homogeneous with the coordinate $p_{0,\dots,r-1}$. Now consider the ideal generated by all equations of this form, where now $p_{0,\dots,r-1}$ has no longer a preferred role.

EXAMPLE 6.5. Look at G_2^4. Then there is only one relation. It can be found as explained in the previous remark, by writing $p_{2,3} = n_{02}n_{13} - n_{12}n_{03}$. There is also a direct derivation, using the description of the previous section. So let L be the line through two points $P = (p_0 : p_1 : p_2 : p_3)$ and $Q = (q_0 : q_1 : q_2 : q_3)$, write the matrix M_L. The determinant of two copies of this matrix is obviously zero; it can be computed by Laplace expansion. We find

$$\begin{vmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \\ p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{vmatrix} = 2(p_{0,1}p_{2,3} - p_{0,2}p_{1,3} + p_{0,3}p_{1,2}) = 0 \,.$$

6.3. Incidence correspondence

Now consider hypersurfaces of degree d in $\mathbb{P}^n$; they are parametrised by $\mathbb{P}(S_d)$ in the notation of p. 35. We define a space parametrising pairs consisting of a linear subspace of $\mathbb{P}^n$ and a hypersurface containing the subspace.

DEFINITION 6.6. The *incidence correspondence* $I(r,d;n)$ of linear subspaces of dimension r and hypersurfaces of degree d in $\mathbb{P}^n$ is

$$I(r,d;n) = \{(L,f) \in G_{r+1}^{n+1} \times \mathbb{P}(S_d) \mid f_{|L} = 0\} \,.$$

PROPOSITION 6.7. *The incidence correspondence is a smooth closed irreducible subset of* $G^{n+1}_{r+1} \times \mathbb{P}(S_d)$ *of codimension* $\binom{r+d}{d}$.

PROOF. It is difficult to find which linear subspaces lie on a given hypersurface, but it is easy to find the hypersurfaces through a given linear subspace. Suppose $L = V(X_{r+1}, \dots, X_n)$, then $f(P) = 0$ for all $P \in L$ if and only if $f \in (X_{r+1}, \dots, X_n)$ if and only if f contains no monomials involving only $X_0, \dots, X_r$. This gives as many linearly independent conditions as there are monomials of degree d in these variables, namely $\binom{r+d}{d}$.

Now consider an affine chart of G^{n+1}_{r+1}. The condition that f vanishes on the subspace $X_i = \sum_{j=0}^{r} n_{ij}X_j$, $i = r+1, \dots, n$, is that upon substituting $X_i = \sum_{j=0}^{r} n_{ij}X_j$ the resulting polynomial in the $X_0, \dots, X_r$ is the zero polynomial. This gives equations, which are linear in the coefficients of f and polynomial in the n_{ij}. By the Jacobian criterion they define a smooth subset of the stated codimension. □

COROLLARY 6.8. *If* $(n-r)(r+1) < \binom{r+d}{d}$, *then the general hypersurface of degree* d *in* $\mathbb{P}^n$ *does not contain an* r*-dimensional linear subspace.*

PROOF. Observe that the hypersurfaces containing a linear subspace are exactly those, which lie in the image of the projection of the incidence correspondence $I(r, d; n)$ on $\mathbb{P}(S_d)$. If $\binom{r+d}{d} > (n-r)(r+1)$, then the dimension of $I(r, d; n)$ is less than the dimension of $\mathbb{P}(S_d)$. □

The argument in the above proof is a precise version of our earlier dimension count. One might expect that each hypersurface contains a linear subspace if $(n-r)(r+1) \geq \binom{r+d}{d}$. This is not true: if $d = r = 2$, $n = 4$, both numbers are 6 but a three-dimensional nondegenerate quadric does not contain two-dimensional subspaces. On the other hand, the projective cone over a quadric surface contains one-dimensional families of two-dimensional subspaces. The space S_2 of quadrics in $\mathbb{P}^4$ has dimension $\binom{6}{2} - 1 = 14$, just as the incidence corespondence $I(2, 2; 4)$, and the subspace Σ of singular quadrics is a hypersurface of dimension 13. The fibres of the map $I(2, 2; 4) \to \Sigma$ have dimension at least 1, in accordance with Theorem 5.18.

LEMMA 6.9. *If* $(n-r)(r+1) = \binom{r+d}{d}$ *then the image* $I(r, d; n)$ *in* $\mathbb{P}(S_d)$ *is either the whole of* $\mathbb{P}(S_d)$, *or it is a proper subvariety and every fibre of the projection map has dimension at least one.*

PROOF. The image of $I(r, d; n)$ is closed by the main theorem of elimination theory 5.22. If it is not the whole of $\mathbb{P}(S_d)$, then the dimension of the image is less than the dimension of $I(r, d; n)$ and every fibre has dimension at least one by the theorem 5.18 on the dimension of fibres. □

THEOREM 6.10. *Every cubic surface in* $\mathbb{P}^3$ *contains a line.*

PROOF. We are in the case $d = 3$, $n = 3$ and $r = 1$, so $(n-r)(r+1) = \binom{r+d}{d} = 4$ and $\dim I(1,3;3) = \dim \mathbb{P}(S_3) = \binom{3+3}{3} - 1 = 19$.

We claim that the singular surface $V(XYZ + T^3)$ contains only finitely many lines, in fact exactly 3 lines (counted without multiplicity). So the fibre above the point $\{F\} \in \mathbb{P}(S_3)$ has dimension zero. Therefore the first alternative of the previous lemma occurs, that the image of $I(1,3;3)$ is the whole of $\mathbb{P}(S_3)$. This means that every cubic surface contains a line.

To prove the claim we first observe that the surface contains the three lines $X = T = 0$, $Y = T = 0$ and $Z = T = 0$. Other lines do not exist: such a line would intersect the plane $T = 0$ in a point on one of the three lines. Without loss of generality we may assume that this line passes through the points $(1 : a : 0 : 0)$ and $(0 : b : c : 1)$. It is given parametrically by

$$(X : Y : Z : T) = (1 : a + \lambda b : \lambda c : \lambda) \ .$$

We insert these values in the equation f and find

$$\lambda c(a + \lambda b) + \lambda^3 = 0$$

as the condition that the line lies on the surface. As this should hold for all λ such an additional line does not exist. □

6.4. The 27 lines on a cubic surface

Let S be an irreducible cubic surface. By theorem 6.10 it contains at least one line. Our first goal is to find more lines. This can be done by studying the 1-dimensional linear system (also called *pencil*) of planes through the line l. Each plane Π through l intersects the surface S in a reducible cubic plane curve, consisting of l and a conic, which we refer to as the *residual* conic. In general this conic will be irreducible, but for some planes it will be reducible, consisting of two lines.

DEFINITION 6.11. A *tritangent plane* of a cubic surface is a plane intersecting the surface in three lines (counted with multiplicity).

Note that on a smooth surface three lines through a point always lie in a plane, namely the tangent plane through that point.

LEMMA 6.12. *For a non-singular cubic surface S the three lines in a tritangent plane are distinct.*

PROOF. We choose coordinates $(X : Y : Z : T)$ such that the tritangent plane is $(T = 0)$. Suppose it contains a multiple line. Then the equation of S can be written as $Tg + l_1^2 l_2$ with l_1 and l_2 linear forms. By the product rule all partial derivatives vanish in $V(T, g, l_1)$, contradicting the fact that S is smooth. □

We search for tritangent planes in the pencil of planes through l by determining the condition that the residual conic degenerates. A conic is given by a quadratic form. It is degenerate if and only if its discriminant, that is, the determinant of the matrix of the associated bilinear form vanishes.

Given l, choose coordinates such $l = V(Z, T)$. Then $V(\mu Z - \lambda T)$ is the pencil of planes through the line l, with $(\lambda : \mu)$ homogeneous coordinates. We expand the equation f of S as

$$f = AX^2 + 2BXY + CY^2 + 2DX + 2EY + F\ ,$$

where $A, \ldots, F$ are homogeneous polynomials in Z and T of degree $1, 1, 1, 2, 2, 3$ respectively. In matrix fom

$$f = \begin{pmatrix} X & Y & 1 \end{pmatrix} \begin{pmatrix} A & B & D \\ B & C & E \\ D & E & F \end{pmatrix} \begin{pmatrix} X \\ Y \\ 1 \end{pmatrix}\ .$$

Let $\Delta(Z, T)$ be the determinant

$$\Delta(Z, T) = \begin{vmatrix} A & B & D \\ B & C & E \\ D & E & F \end{vmatrix}\ .$$

This is a polynomial of degree 5 in Z and T (if it is not the zero polynomial).

LEMMA 6.13. *The plane* $\Pi = V(\mu Z - \lambda T)$ *is a tritangent plane if and only if* $\Delta(\lambda, \mu) = 0$.

PROOF. We fix λ and ν and take homogeneous coordinates $(X : Y : W)$ on Π. We put $(X : Y : Z : T) = (X : Y : \lambda W : \mu W)$. Then $\Delta(\lambda, \mu)$ is the discriminant of the residual conic. □

PROPOSITION 6.14. *Let* S *be a smooth cubic surface. Five distinct tritangent planes pass through each line.*

PROOF. We show that $\Delta(Z, T)$ has only simple zeroes. Suppose $\Delta(1 : 0) = 0$. As S is smooth, the lines in the tritangent plane $(Z = 0)$ are distinct. We may suppose that one of them is $(X = 0)$. We write $f = Zg + TXl$, with $l = aX + 2bY + 2dT$ a linear form. We expand g in the same way as we did before for f, and write $g = A_1X^2 + 2B_1XY + C_1Y^2 + 2D_1X + 2E_1Y + F_1$, where the degrees of $A_1, \ldots, F_1$ are $0, 0, 0, 1, 1, 2$ respectively. Then $\Delta(Z, T)$ is the determinant of the matrix

$$Z \begin{pmatrix} A_1 & B_1 & D_1 \\ B_1 & C_1 & E_1 \\ D_1 & E_1 & F_1 \end{pmatrix} + T \begin{pmatrix} a & b & dT \\ b & 0 & 0 \\ dT & 0 & 0 \end{pmatrix}\ .$$

We compute (with Sarrus' rule) that $\Delta(Z, T)$ is, modulo terms with Z^2, given by

$$(2bdE_{1,T} - b^2F_{1,T^2} - d^2C_1)T^4Z\ ,$$

where $E_{1,T}$ is the coefficient of T in E_1 and F_{1,T^2} that of T^2 in F_1. The coefficient $2bdE_{1,T} - b^2F_{1,T^2} - d^2C_1$ is also the value $-g(0,d,0,-b)$. The point $(0:d:0:-b)$ is the point $Q = V(Z,X,l)$. We compute the partial derivatives in this point . By nonsingularity not all vanish. All partial derivatives of TXl vanish in Q, and the only nonvanishing derivative is $\frac{\partial f}{\partial Z}(Q) = g(Q)$. Therefore $d^2C_1 - 2bdE_{1,T} + b^2F_{1,T^2} = g(0,d,0,-b) \neq 0$ and Z is a factor of multiplicity 1 of $\Delta(Z,T)$. □

THEOREM 6.15. *A nonsingular cubic surface contains exactly 27 lines.*

PROOF. The smooth surface has a tritangent plane Π, containing three lines l_1, l_2 and l_3. Let l be a line on the surface, not in Π. Then l intersects Π in a point of one of the lines l_i, say l_1, this cannot be an intersection point with another line, say l_2, as the three lines l, l_1 and l_2 do not lie in a plane. So l lies in one of the tritangent planes through l_1.

There are four tritangent planes, besides Π, through each of the l_i, each containing two lines besides l_i, so there are 24 lines on the cubic besides the three lines in Π; that is to say, twenty seven in all. □

We investigate the configuration formed by the 27 lines. It may be the case that the three lines in a tritangent plane go through one point. Such a point of the surface is called *Eckhardt point*. But the abstract configuration (meaning that one only considers the lines and the pairwise intersections) is independent of the surface. So if one makes a graph, whose vertices correspond to the lines, and where two vertices are joined by an edge if and only if the lines intersect, then the graph of three distinct lines in the plane is always the same (a triangle), whether the lines pass through one point or not.

Let l and m be two disjoint lines on S (also called *skew* lines). They exist, take lines in different tritangent planes through a given line. Let Π_i, $i = 1, \dots, 5$, be the tritangent planes through l, containing the lines l, l_i and l'_i. Then m intersects Π_i in a point of l_i or l'_i. Choose the labeling such that m intersects l_i. Then the plane through m and l_i contains a third line l''_i, intersecting l_i and therefore not intersecting l and l_i. The line l''_i lies in a different tritangent plane through m as l_j for $j \neq i$. As l''_i intersects one of the lines l, l_i and l'_i, it intersects l'_j for $j \neq i$.

We say that a line n is a *transversal* of another line in $\mathbb{P}^3$, if n intersects this line.

LEMMA 6.16. *If l_1, ..., l_4 are four disjoint lines in $\mathbb{P}^3$, then either all four lie on a smooth quadric surface Q, and there are infinitely many common transversals, or they do not lie on any quadric, and they have one or two common transversals. The first possibility cannot occur if the four lines lie on a smooth cubic surface.*

PROOF. If a quadric contains three disjoint lines, it has to be smooth: it cannot have a plane as component and neither can it be a cone. Now through three lines always passes a quadric: the linear system of quadrics through nine points, three on each line, is not empty. A smooth quadric is isomorphic to the Segre embedding of $\mathbb{P}^1 \times \mathbb{P}^1$ and therefore contains two *rulings*, systems of lines.

Take a (smooth) quadric Q through l_1, l_2 and l_3. They lie in one ruling. Any transversal in $\mathbb{P}^3$ of the lines lies on Q, as it intersects Q in three points, and lies therefore in the other ruling. Now l_4 can lie on Q, as a line in the same ruling as l_1, l_2 and l_3, or it does not lie on Q. Then it intersects Q in two points, unless it is a tangent line. The common transversals are the lines in the other ruling through the intersection point(s).

If the four lines lie on a cubic surface S, all transversals lie on S, as they intersect the surface in at least four points. So if $l_4 \subset Q$, then Q is a component of S. □

PROPOSITION 6.17. *A line n on S, not one of the 17 lines l, l_i, l_i', l_i'' or m, meets exactly three of the five lines $l_1, \ldots, l_5$. Conversely, for each three element subset $\{i,j,k\} \subset \{1,2,3,4,5\}$ there is a unique line l_{ijk} (distinct from l) intersecting l_i, l_j and l_k.*

PROOF. The line n cannot meet four of the l_i, as these four lines have l and m as common transversals. If it meets at most two, it meets at least three of the l_i', say it meets l_3', l_4' and l_5'. It also meets two of the four lines l_1, l_1', l_2, l_2'. Say it meets l_1 or l_2'. This is a contradiction, as l and l_1'' are common transversals of l_1, l_2', l_3', l_4' and l_5'.

There can only be one such line l_{ijk}. Every possibility has to occur as there are 27 lines in total. We can also find in this way the number 27, by looking, say, at the lines l_{ij5}: all six possibilities have to occur, as l_5 intersects 10 lines, of which only l, l_5', l_5'' and m belong to the 17 lines. □

We summarise the incidence relations.

$$\begin{array}{lll} l & \text{meets} & l_i, l_i' \\ m & \text{meets} & l_i, l_i'' \\ l_i & \text{meets} & l, m, l_i', l_i'', l_{ijk} \\ l_i' & \text{meets} & l, l_i, l_j'', l_{jkn} \\ l_i'' & \text{meets} & m, l_i, l_j', l_{jkn} \\ l_{ijk} & \text{meets} & l_i, l_{inp}, l_n', l_n'' \end{array}$$

Here the indices run through all possibilities, where i, j, k, n, p stand for distinct elements of $\{1,2,3,4,5\}$.

The 27 lines on a cubic surface are the intersection of the cubic with a hypersurface of degree 9. This surface was found by Clebsch in 1861, by eliminating Q from the equations f_1, f_2, f_3 and the condition that Q lies in a plane (the notation is that of the begin of this chapter). He used the so-called symbolic method. A modern treatment seems not to be available. We describe his result. Let $S = (f)$, let H be the Hessian of f, which is the determinant of the Hesse matrix $M_H = \left(\frac{\partial^2 f}{\partial X_i \partial X_j}\right)$. Let A be the adjugate (or classical adjoint) matrix of M_H, that is the matrix of cofactors; as M_H is symmetric, there is no need to transpose. Define

$$\Theta = \sum_{i,j=0}^{3} \frac{\partial H}{\partial X_i} A_{ij} \frac{\partial H}{\partial X_j}$$

and

$$T = \sum_{i,j=0}^{3} A_{ij} \frac{\partial^2 H}{\partial X_i \partial X_j} \ .$$

Then the hypersurface of degree 9 is given by

$$F = \Theta - 4HT = 0 \ .$$

6.5. Rational cubic surfaces

THEOREM 6.18. *An irreducible cubic surface is either a cone over a plane cubic curve or is rational.*

PROOF. If S is singular with a point of multiplicity 3, then S is a cone. If there is a point of multiplicity 2, then projection from this point shows that the surface is rational.

Suppose now that S is smooth. Then S contains two skew lines l and m. We define a rational map from $l \times m \cong \mathbb{P}^1 \times \mathbb{P}^1$ to S, by $\sigma(P, Q) = R$, where R is the third point of intersection of the line $\overline{PQ}$ through $P \in l$ and $Q \in m$. It is possible that R coincides with P or Q. The map is not defined when the line $\overline{PQ}$ lies entirely on S. This happens for five lines. The inverse of this map is the regular map defined in the following way. If $R \in S$, then there is a unique transversal n to l and m, passing through R. We define $\pi(R) = (l \cap n, m \cap n)$. One can find n if R does not lie on l or m, by taking say the plane Π through R and l, and intersecting it with m. Then n is the line through R and $\Pi \cap m$. This construction does not involve S, but breaks down if $R \in l$ or $R \in m$. Note that Π intersects S in l and a residual conic, on which R lies. This description makes also sense if $R \in l$: require that R lies on the residual conic in Π. This implies that n intersects S in the point R with multiplicity 2, so it is a tangent line, and Π is the tangent plane to S at the point R. The maps π and σ are obviously inverse to each other. $\square$

REMARK 6.19. The map π constructed in the above proof, maps to an abstract, non-embedded copy of $\mathbb{P}^1 \times \mathbb{P}^1$. We can map to a plane Π' in $\mathbb{P}^3$ by sending R to the intersection point of n with Π'. This is called *skew projection*. This map is not defined if the line lies in the plane. This happens for the line connecting $\Pi' \cap l$ and $\Pi' \cap m$, that is, for one point of the surface S. The hyperplane sections of S are mapped to plane curves of degree 4 with two double points. We can get an everywhere defined map by choosing the plane Π' through one of the five transversals of l and m on S. Then the map π contracts exactly 6 lines to points. The inverse is the map of the linear system of cubics through these six points.

REMARK 6.20. A plane cubic curve is rational if and only if it is singular. In higher dimension, it was proved by Clemens and Griffiths in 1971 that a smooth cubic threefold is not rational. Some cubic fourfolds are rational, but it is conjectured that the general one is not. There is weaker notion: an algebraic variety V is *unirational* if its function field $k(V)$ is isomorphic to a subfield of $k(X_1, \dots, X_n)$ for some n. Every smooth cubic hypersurface is unirational.

Further reading

The question of good texts was discussed at `http://mathoverflow.net/questions/2446`.

Algebraic geometry books at introductory level are

- William Fulton, *ALGEBRAIC CURVES, An Introduction to Algebraic Geometry*, available from the Author's homepage
  `www.math.lsa.umich.edu/~wfulton/`
  This is a classic text, still useful.
- Miles Reid, *Undergraduate Algebraic Geometry*, Cambridge Univ. Press, 1988. See also this TeX edition.
  Written in typical Miles Reid style. Nice choice of topics.
- Klaus Hulek, *Elementary Algebraic Geometry*. American Mathematical Society, 2003.
  An adaptation of Miles' book for use in Germany.
- Andreas Gathmann, *Algebraic Geometry*, Notes for classes taught at the University of Kaiserslautern
  There are currently three versions of the notes. A nice text.
- Brieskorn–Knörrer, *Ebene algebraische Kurven* Birkhäuser, 1981
  An english translation exists. It treats the singularities of plane curves, both from an algebro-geometric and a topological point of view. On the way much elementary algebraic geometry is covered.
- J.S. Milne, Algebraic Geometry
  online notes
- David A. Cox, John B. Little and Don O'Shea, *Ideals, Varieties, and Algorithms* Springer, 4rd Ed. 2015
  From the book's webpage:
  This book is an introduction to computational algebraic geometry and commutative algebra at the undergraduate level. It discusses systems of polynomial equations ("ideals"), their solutions ("varieties"), and how these objects can be manipulated ("algorithms").

The basics of algebraic geometry needs a lot of commutative algebra. One of the earliest textbooks, Zariski-Samuel, started out as preparation for algebraic geometry, and grew to two volumes.

Books on elementary level:

- Miles Reid, *Undergraduate Commutative Algebra.* LMS Student Texts 29, Cambridge Univ. Press 1995.
- Ernst Kunz, *Eine Einführung in die kommutative Algebra und algebraische Geometrie.* Vieweg 1978.
  An english translation exists. Although it has algebraic geometry in the title, the book contains mainly commutative algebra.
- Atiyah–MacDonald, *Introduction to commutative algebra*, Addison-Wesley 1969
  Another classic. Still used as textbook.
- Allen Altman and Steven Kleiman, A Term of Commutative Algebra
  Based on years of teaching Atiyah-MacDonald.
- Greuel–Pfister, *A Singular Introduction to Commutative Algebra*, 2nd ed. 2008, 690 p.

Books on algebraic geometry for further study:

- Robin Hartshorne, *Algebraic geometry*, Springer 1977
  This is the standard reference on algebraic geometry.
- Griffiths–Harris, *Principles of Algebraic Geometry*, Wiley 1978
  Studies mainly varieties over the complex numbers. The standard reference for transcendental methods.
- Eisenbud and Harris, *The Geometry of Schemes*, Springer 2000
- Ravi Vakil, *The Rising Sea, Foundations Of Algebraic Geometry*
  see `http://math216.wordpress.com`
  Very readable notes from a course at Stanford.
- Semple and Roth, *Introduction to Algebraic Geometry*, Oxford 1949
  An old-fashioned textbook, but with a wealth of examples.
- David Eisenbud, *Commutative Algebra, with a View Toward Algebraic Geometry*, Springer 1995

Index