ALGEBRAIC GEOMETRY

Alexei Skorobogatov

December 16, 2003

Contents

Basic references

Algebra:

S. Lang. *Algebra.* Addison-Wesley, 1965.

M. Reid. *Undergraduate commutative algebra.* Cambridge University Press, 1995.

B.L. Van der Waerden. *Algebra.* (2 volumes) Springer-Verlag.

Geometry:

M. Reid. *Undergraduate algebraic geometry.* Cambridge University Press, 1988.

I.R. Shafarevich. *Basic algebraic geometry.* (2 volumes) Springer-Verlag. 1994.

Further references

Advanced commutative algebra:

M.F. Atiyah and I.G. Macdonald. *Introduction to commutative algebra.* Addison-Wesley, 1969.

H. Matsumura. *Commutative ring theory.* Cambridge University Press, 1986

O. Zariski and P. Samuel. *Commutative algebra.* (2 volumes) Van Nostrand, 1958.

Advanced algebraic geometry:

R. Hartshorne. *Algebraic geometry.* Springer-Verlag, 1977.

1 Basics of commutative algebra

Let k be a field. (Affine) algebraic geometry studies the solutions of systems of polynomial equations with coefficients in k. Instead of a set of polynomials it is better to consider the ideal of the polynomial ring $k[X_1, \dots, X_n]$ generated by them. The subset of k^n consisting of common zeros of the polynomials of an ideal $I \subset k[X_1, \dots, X_n]$ is called the set of zeros of I. Such subsets of k^n are called *closed algebraic sets*.

Hence our main object of study will be the polynomial ring $k[X_1, \dots, X_n]$, its ideals, their sets of zeros in k^n, and the quotient rings of $k[X_1, \dots, X_n]$. Here is the list of principal facts that we prove in this chapter:

(1) Every ideal of $k[X_1, \dots, X_n]$ is a finitely generated $k[X_1, \dots, X_n]$-module. (Hilbert's basis theorem.)

(2) Every quotient ring of $k[X_1, \dots, X_n]$ is of the following form: it contains a polynomial ring $k[Y_1, \dots, Y_m]$ over which it is a finitely generated module. (Emmy Noether's normalization lemma).

(3) If k is algebraically closed, then all maximal ideals of $k[X_1, \dots, X_n]$ are of the form $(X_1 - a_1, \dots, X_n - a_n)$, $a_i \in k$, that is, consist of polynomials vanishing at a point $(a_1, \dots, a_n) \in k^n$.

(4) Let k be algebraically closed. If a polynomial f vanishes at all the zeros of an ideal of $k[X_1, \dots, X_n]$, then some power f^m belongs to this ideal. (Hilbert's Nullstellensatz.)

Fact (1) says that speaking about ideals and systems of (finitely many) polynomial equations is the same thing. The meaning of (2) will be made clear in the geometric part of the course (an important corollary of (2) is the fact that any algebraic variety is birationally equivalent to a hypersurface). Fact (3) speaks for itself. Finally, (4) implies that certain ideals of $k[X_1, \dots, X_n]$ bijectively correspond to closed algebraic sets.

1.1 Integral closure. Noetherian rings

Most of the time we assume that k is an algebraically closed field. When k is not algebraically closed, $\overline{k}$ denotes a separable closure of k (unique up isomorphism, see [Lang]). Let R be a commutative ring with a 1. We shall always consider ideals $I \subset R$ different from R itself. Then the quotient ring R/I is also a ring with 1. By definition, a ring is an *integral domain* if it has no zero divisors.

If M is an R-module, then $1 \in R$ acts trivially on M. An R-module M is of *finite type* if it is generated by finitely many elements, that is, if there exist

$a_1, \ldots, a_n \in M$ such that any $x \in M$ can be written as $x = r_1 a_1 + \ldots + r_n a_n$ for some $r_i \in R$.

If a module A over a ring R also has a ring structure (compatible with that of R in the sense that the map $R \to A$ given by $r \mapsto r.1_A$ is a ring homomorphism), then A is called an *R-algebra*. An R-algebra A is of *finite type* (or finitely generated) if there exist $a_1, \ldots, a_n \in A$ such that any $x \in A$ can be written as a polynomial in $a_1, \ldots, a_n$ with coefficients in R.

Prime and maximal ideals. An ideal $I \subset R$ is called *prime* if the quotient ring R/I has no zero divisors. An ideal I is *maximal* if it is not contained in another ideal (different from R). Then the ring R/I has no non-zero ideal (otherwise its preimage in R would be an ideal containing I), hence every element $x \in R/I$, $x \neq 0$, is invertible (since the principal ideal (x) must concide with R/I, and thus contain 1), in other words, R/I is a field. Since a field has no non-trivial ideals, the converse is also true, so that *$I \subset R$ is maximal iff R/I is a field.*

Integral closure. We shall consider various finiteness conditions. Suppose we have an extension of *integral domains* $A \subset B$. An element $x \in B$ is called *integral* over A if it satisfies a polynomial equation with coefficients in A and leading coefficient 1.

Proposition 1.1 *The following conditions are equivalent:*

(i) $x \in B$ is integral over A,

(ii) $A[x]$ is an A-module of finite type,

(iii) there exists an A-module M of finite type such that $A \subset M \subset B$ and $xM \subset M$.

The proof of $(i) \Rightarrow (ii)$ and $(ii) \Rightarrow (iii)$ is direct. Suppose we know (iii). Let $m_1, \ldots, m_n$ be a system of generators of M. Then $xm_i = \sum_{i=1}^n b_{ij} m_j$, where $b_{ij} \in A$.

Recall that in any ring R we can do the following "determinant trick". Let S be a matrix with entries in R. Let $adj(M)$ be the matrix with entries in R given by

$$adj(M)_{ij} = (-1)^{i+j} det(M(j,i)),$$

where $M(i,j)$ is M with i-row and j-th column removed. It is an exercise in linear algebra that the product $adj(M) \cdot M$ is the scalar matrix with $det(M)$ on the diagonal.

We play this trick to the polynomial ring $R = A[T]$. For M we take the $n \times n$-matrix $Q(T)$ such that $Q(T)_{ij} = T\delta_{ij} - b_{ij}$. Let $f(T) = det(Q(T)) \in$

$A[T]$ (this is the analogue of the characteristic polynomial of x). We have a matrix identity

$$adj(Q(T)) \cdot Q(T) = diag(f(T)).$$

We consider this as an identity between matrices over the bigger ring $B[T]$. We are free to assign T any value in B. Substitute $T = x \in B$, and apply these matrices to the column vector $(m_1, \ldots, m_n)^t$. Then the left hand side is zero. Hence $f(x)m_i = 0$ for any i. Since the m_i generate M the whole module M, is annihilated by $f(x) \in B$. In particular, $f(x).1 = 0$, that is, $f(x) = 0$. Now note that $f(T)$ has coefficients in A and leading coefficient 1. QED

Remark. This proof does not use the fact that A and B are integral. If we assume this we can remove the condition $A \subset M$ in (iii).

Definitions. Let $A \subset B$ be integral domains, then B is *integral* over A if its every element is integral over A. The set of elements of B which are integral over A is called the *integral closure* of A in B.

Important example. Let K be a number field, that is, a finite extension of $\mathbf{Q}$. One defines the ring of integers $O_K \subset K$ as the integral closure of $\mathbf{Z}$ in K.

Let us prove some basic properties of integral elements.

Proposition 1.2 (a) *The integral closure is a ring.*

(b) *Suppose that B is integral over A, and is of finite type as an A-algebra. Then B is of finite type as an A-module.*

(c) *Suppose that C is integral over B, and B is integral over A, then C is integral over A.*

Proof. (a) Let $x, y \in B$ be integral over A. Consider the A-module generated by all the monomials $x^i y^j$, $i, j \geq 0$. It is of finite type, and xy and $x + y$ act on it.

(b) Suppose that B is generated by b_1, ... , b_n as an A-algebra, then B is generated by monomials $b_1^{i_1} \ldots b_n^{i_n}$ as an A-module. All higher powers of each of the b_i's can be reduced to finitely many of its powers using a monic polynomial whose root is b_i. There remain finitely many monomials which generate B as an A-module.

(c) Let $x \in C$. Consider the A-subalgebra $D \subset C$ generated by x and the coefficients b_i of a monic polynomial with coefficients in B, whose root is x. Then D is an A-module of finite type, as only finitely many monomials generate it (the b_i are integral, and the higher powers of x can be reduced to lower powers) Now use (iii) of the previous proposition. QED

Definition. A ring is *integrally closed* or *normal* if it is integrally closed in its field of fractions.

Examples. $\mathbf{Z}$ and $\mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$ are integrally closed, but $\mathbf{Z}[\sqrt{-3}]$ is not. If k is a field then $k[x]$ and $k[x,y]$ are integrally closed, but $k[x,y]/(y^2-x^2-x^3)$ is not.

Noetherian rings. Another important finiteness property of rings is given in the following definition.

Definition-Proposition. *A ring R satisfying any of the following equivalent properties is called Noetherian:*

(i) any chain of ideals $I_1 \subset I_2 \subset I_3 \subset \dots$ of R stabilizes (that is, there is an integer m such that $I_m = I_{m+1} = I_{m+2} = \dots$),

(ii) any set of ideals of R contains a maximal element,

(iii) any ideal of R is generated by finitely many elements, that is, is an R-module of finite type.

Proof. The equivalence of (i) and (ii) is completely formal.

$(iii) \Rightarrow (i)$: Let $I = \sum I_j$, then I is an ideal which is generated, say, by $x_1, \dots, x_n$ as an R-module. Take m such that I_m contains all the x_i, then the chain stabilizes at I_m.

$(ii) \Rightarrow (iii)$ is based on a trick called "Noetherian induction". Suppose that $I \subset R$ is an ideal which is not of finite type as an R-module. Consider the set of subideals of I which are of finite type as R-modules. This set is not empty: it contains 0. Now it has a maximal element $J \neq I$. Take $x \in I \setminus J$, then the ideal $J + (x) \subset I$ is strictly bigger than J, but is of finite type as an R-module. Contradiction. QED

Examples of Noetherian rings: Fields, principal ideals domains, the ring of integers in a number field.

An easy exercise: Quotients of a Noetherian ring are Noetherian.

Theorem 1.3 (Hilbert's basis theorem) *If R is Noetherian, then so are the polynomial ring $R[T]$ and the formal power series ring $R[[T]]$.*

Sketch of proof. Let $I \subset R[T]$ be an ideal. We associate to it a series of ideals in R:

$$A_0 \subset A_1 \subset A_2 \subset \dots,$$

where A_i is generated but the leading coefficients of polynomials in I of degree i. Since R is Noetherian, this chain of ideals stabilizes, say, at A_r. Then we have a finite collection of polynomials whose leading coefficients generate A_0, ... , A_r. Then the ideal of $R[T]$ generated by these polynomials is I. See Lang's book for the proof of the other statement. QED

1.2 Noether's normalization and Nullstellensatz

The elements $r_1, \ldots, r_n$ of a k-algebra R are *algebraically independent* (over k) if the only polynomial $f(x_1, \ldots, x_n)$ with coefficients in k such that $f(r_1, \ldots, r_n) = 0$, is the zero polynomial.

Theorem 1.4 (E. Noether's normalization lemma.) *Let k be any field, and $I \subset k[T_1, \ldots, T_n]$ be an ideal, $R = k[T_1, \ldots, T_n]/I$. There exist algebraically independent elements $Y_1, \ldots, Y_m \in R$ such that R is integral over $k[Y_1, \ldots, Y_m]$.*

Proof. If $I = 0$ there is nothing to prove. Suppose we have a non-zero polynomial $f \in I$. Let d be a positive integer greater than $deg(f)$. Let us choose new variables in the following tricky way:

$$X_2' = X_2 - (X_1)^d, X_3' = X_3 - (X_1)^{d^2}, X_4' = X_4 - (X_1)^{d^3}, \ldots, X_n' = X_n - (X_1)^{d^{n-1}}.$$

Substituting this into f we rewrite it as a linear combination of powers of X_1 and a polynomial, say, g containing no pure powers of X_1. We observe that the pure powers of X_1 are of the form $i_1 + di_2 + d^2 i_3 + \ldots + d^{n-1} i_n$. Since $d > i_s$ all these integers are different, hence there is no cancellation among the pure powers of X_1. At least one such power enters with a non-zero coefficient. On the other hand, any power of X_1 in g is strictly less than the corresponding pure power. Therefore, we get a polynomial in X_1 with coefficients in $k[X_2', \ldots, X_n']$ and leading coefficient in k. Normalizing this polynomial we conclude that X_1 is integral over $R_1 = k[X_2', \ldots, X_n']/I \cap k[X_2', \ldots, X_n']$. Hence R is integral over R_1. We now play the same game with R_1 instead of R, and obtain a subring R_2 over which R_1 is integral. By Property (c) of integral ring extensions R is also integral over R_2. We continue like that until we get a zero ideal, which means that the variables are algebraically independent. QED

Theorem 1.5 *Let k be an algebraically closed field. All maximal ideals of $k[X_1, \ldots, X_n]$ are of the form $(X_1 - a_1, \ldots, X_n - a_n)$, $a_i \in k$, that is, consist of polynomials vanishing at a point $(a_1, \ldots, a_n) \in k^n$.*

Proof. Any polynomial has a Taylor expansion at the point $(a_1, \ldots, a_n)$. The canonical map

$$k[X_1, \ldots, X_n] \longrightarrow k[X_1, \ldots, X_n]/(X_1 - a_1, \ldots, X_n - a_n)$$

sends f to $f(a_1, \ldots, a_n)$, hence is surjective onto k. It follows that the ideal $(X_1 - a_1, \ldots, X_n - a_n)$ is maximal.

Let M a maximal ideal (recall that $M \neq k[X_1, \ldots, X_n]$), then $K = k[X_1, \ldots, X_n]/M$ is a field containing k. By Noetherian normalization K is integral over its subring $A = k[Y_1, \ldots, Y_m]$. But K is a field, and we now show that then A must also be a field, in which case $k[Y_1, \ldots, Y_m] = k$ (no variables at all), and hence K is integral over k. Indeed, let $x \in A$, then it is enough to show that $x^{-1} \in K$ also belongs to A. Since $x^{-1} \in K$ is integral over A it is subject to a polynomial relation $(x^{-1})^n + a_{n-1}(x^{-1})^{n-1} + \ldots + a_1 x^{-1} + a_0 = 0$, for some $a_i \in A$. Multiplying this by x^{n-1} we express x^{-1} as a polynomial in x with coefficients in A, hence $x^{-1} \in A$.

The k-algebra of finite type K is integral over k, hence by Proposition 1.2 (b) K is a k-module (= vector space over k) of finite type (= of finite dimension). Thus the field K is an algebraic extension of k. Since k is algebraically closed, we must have $k = K$. Now let $a_i \in k$ be the image of X_i under the map $k[X_1, \ldots, X_n] \to k = k[X_1, \ldots, X_n]/M$. Then M contains the maximal ideal $(X_1 - a_1, \ldots, X_n - a_n)$, hence coincides with it. QED

Remark. When k is not supposed to be algebraically closed, this proof shows that the quotient by a maximal ideal of $k[X_1, \ldots, X_n]$ is a finite extension of k.

Corollary 1.6 *Let k be an algebraically closed field. If the polynomials of an ideal $I \subset k[X_1, \ldots, X_n]$ have no common zeros in k^n, then $I = k[X_1, \ldots, X_n]$.*

Proof. Assume $I \neq k[X_1, \ldots, X_n]$. Hilbert's basis theorem says that $k[X_1, \ldots, X_n]$ is Noetherian. Then I is contained in a maximal ideal, since the set of ideals that contain I has a maximal element, by (ii) of Definition-Proposition above. Therefore $I \subset (X_1 - a_1, \ldots, X_n - a_n)$, for some $a_i \in k$, since all the maximal ideals are of this form by the previous result. But then all the polynomials of I vanish at the point $(a_1, \ldots, a_n)$, which is a contradiction. QED

Theorem 1.7 (Nullstellensatz.) *Let k be an algebraically closed field. If a polynomial f vanishes at all the zeros of an ideal $I \subset k[X_1, \ldots, X_n]$, then $f^m \in I$ for some positive integer m.*

Proof. We know that I is generated by finitely many polynomials, say, $I = (g_1, \ldots, g_r)$. Let T be a new variable. Consider the ideal $J \subset k[T, X_1, \ldots, X_n]$ generated by $g_1, \ldots, g_r$ and $Tf - 1$. We observe that these polynomials have no common zero. The previous corollary implies that $J = k[T, X_1, \ldots, X_n]$, in particular, J contains 1. Then there exist polynomials $p, p_1, \ldots, p_r$ in variables $T, X_1, \ldots, X_n$ such that

$$1 = p(Tf - 1) + p_1 g_1 + \ldots + p_r g_r.$$

Note that this is an identity in variables $T, X_1, \ldots, X_n$. Thus we can specialize the variables anyway we like. For example, we can set $T = 1/f$. Multiplying both sides by an appropriate power of f we get an identity between polynomials in variables $X_1, \ldots, X_n$, which gives that some power of f belongs to $I = (g_1, \ldots, g_r)$. QED

2 Affine geometry

2.1 Zariski topology

Let k be any field. Let us prove some easy facts about closed algebraic sets. If $X \subset k^n$ we denote by $I(X) \subset k[X_1, \ldots, X_n]$ the ideal consisting of polynomials vanishing at all the points of X. We denote by $Z(J)$ the set of zeros of an ideal $J \subset k[X_1, \ldots, X_n]$. It is a tautology that $X \subset Z(I(X))$ and $J \subset I(Z(J))$. If X is a *closed algebraic set*, then $X = Z(I(X))$ (if $X = Z(J)$, then $I(Z(J)) \supset J$, hence $Z(I(Z(J))) \subset Z(J)$).

Exercise. Show that if $X \subset \mathbf{A}_k^n$ and $Y \subset \mathbf{A}_k^m$ are closed subsets, then $X \times Y \subset \mathbf{A}_k^{n+m}$ is a closed subset.

It is clear that the function $J \mapsto Z(J)$ reverses inclusions; associates the empty set to the whole ring, and the whole affine space k^n to the zero ideal; sends the sum of (any number of) ideals to the intersection of corresponding closed sets; and sends the intersection $I_1 \cap I_2$ to $Z(I_1) \cup Z(I_2)$ (a part of the last property is not completely obvious: if $P \notin Z(I_1) \cup Z(I_2)$, then $f(P) \neq 0$ for some $f \in I_1$ and $g(P) \neq 0$ for some $g \in I_2$, but then $(fg)(P) \neq 0$, whereas $fg \in I_1 \cap I_2$).

Because of these properties we can think of closed algebraic sets as the closed sets for some topology on k^n (any intersections and finite unions are again closed, as are the empty set and the whole space). This topology is called *Zariski topology*. In the case when $k = \mathbf{C}$ or $k = \mathbf{R}$ we can compare it with the usual topology on $\mathbf{C}^n$ where closed sets are the zeros of continuous functions. Any Zariski closed set is also closed for the usual topology but not vice versa. Hence the Zariski topology is weaker. Another feature is that any open subset of k^n is dense (its closure is the whole k^n).

Definition. A closed algebraic subset $X \subset k^n$ is *irreducible* if there is no decomposition $X = X_1 \cup X_2$, where $X_1 \neq X$ and $X_2 \neq X$ are closed algebraic sets.

Proposition 2.1 *A closed algebraic subset $X \subset k^n$ is irreducible iff $I(X)$ is a prime ideal. Any closed set has a unique decomposition into a finite union*

of irreducible subsets $X = \cup_i X_i$ such that $X_i \not\subset X_j$ for $i \neq j$ (these X_i's are called the irreducible components of X).

Proof. Let us prove the first statement. If we have $X = X_1 \cup X_2$, then since $X = Z(I(X))$ for any algebraic set, $I(X)$ is a proper subset of $I(X_i)$. If $f_i \in I(X_i) \setminus I(X)$, then $f_1 f_2 \in I(X)$, hence $I(X)$ is not a prime ideal. Conversely, if $I(X)$ is not prime, we can find two polynomials f_1 and f_2 not in $I(X)$ such that $f_1 f_2 \in I(X)$, and define $I_i = (I(X), f_i)$, $X_i = Z(I_i)$. There exists a point P in X such that $f_1(P) \neq 0$, hence $P \notin X_1$ which implies $X_1 \neq X$. Similarly we have $X_2 \neq X$. Therefore $X = X_1 \cup X_2$ is not irreducible.

Let us prove the second statement. If X is not irreducible, we have some decomposition $X = X_1 \cup X_2$, and then continue for X_1 and X_2. At some point we must stop because the chain of ideals $I(X) \subset I(X_1) \subset \ldots$ stabilizes somewhere (the ring $k[X_1, \ldots, X_n]$ being Noetherian). If $\cup_i X_i = \cup_j Y_j$ are two decompositions into irreducible subsets, then $X_i = \cup_j (X_i \cap Y_j)$, and hence $X_i = X_i \cap Y_j$ for some j (since X_i is irreducible). For the analogous reason we have $Y_j = Y_j \cap X_{i'}$ for some i'. Then $X_i \subset X_{i'}$, hence $i = i'$. It follows that $X_i = Y_j$. Hence the two decompositions differ only in order. QED

Up till now we did not use Hilbert's Nullstellensatz. Let k be an algebraically closed field. Let us call an ideal $I \subset k[X_1, \ldots, X_n]$ *radical* if $f^m \in I$ implies $f \in I$. A corollary of Hilbert's Nullstellensatz is that radical ideals bijectively (via operations I and Z) correspond to closed algebraic sets. The most important class of radical ideals are prime ideals. Again, by Hilbert's Nullstellensatz, these bijectively correspond to irreducible closed algebraic sets. A particular case of prime ideals are maximal ideals, they correspond to points of k^n.

Zero sets of irreducible polynomials of $k[X_1, \ldots, X_n]$ are called irreducible *hypersurfaces*.

2.2 Category of affine varieties

An *affine variety* is a closed irreducible algebraic subset of k^n for some n. The variety k^n will be also denoted $\mathbf{A}^n_k$, and called the affine space of dimension n.

Let $X \subset \mathbf{A}^n_k$ be an affine variety. Let $J = I(X)$ be the corresponding prime ideal. Let us denote $k[X] := k[X_1, \ldots, X_n]/J$. Then $k[X]$ is an integral k-algebra of finite type: $k[X]$ contains no zero divisors. $k[X]$ is called the *coordinate ring* of X. The fraction field of $k[X]$ is denoted by $k(X)$, and is

called the *function field* of X. Its elements are called *rational functions* as opposed to the elements of $k[X]$ which are called *regular functions*.

The function field $k(X)$ is an important object defined by X. Two affine varieties X and Y are called *birationally equivalent* if $k(X) = k(Y)$. A variety X is called *rational* if $k(X)$ is a purely transcendental extension of k, that is, $k(X) = k(T_1, \dots, T_l)$. In other words, X is rational if and only if X is birationally equivalent to the affine space. It is a classical, and often a difficult problem of algebraic geometry to determine whether or not two given varieties are birationally equivalent.

Affine varieties form a category, where a morphism $X \to Y$, $X \subset \mathbf{A}_k^n$, $Y \subset \mathbf{A}_k^m$, is given by a function representable by m polynomials in n variables. The varieties X and Y are called isomorphic if there are morphisms $f : X \to Y$ and $g : Y \to X$ such that fg and gf are identities.

Proposition 2.2 *Let $X \subset \mathbf{A}_k^n$ and $Y \subset \mathbf{A}_k^m$ be affine algebraic varieties.*

(a) *A morphism $f : X \to Y$ defines a homomorphism of k-algebras $f^* : k[Y] \to k[X]$ via the composition of polynomials.*

(b) *Any homomorphism of k-algebras $\phi : k[Y] \to k[X]$ is of the form $\phi = f^*$ for a unique morphism $f : X \to Y$.*

(c) *$f : X \to Y$ is an isomorphism of affine varieties if and only if $f^* : k[Y] \to k[X]$ is an isomorphism of k-algebras.*

Proof. (a) follows from the fact that the composition of polynomials is a polynomial.

(b) Let $x_1, \dots, x_n$ be the coordinates on X, and $t_1, \dots, t_m$ be the coordinates on Y. Let Φ be the composition of the following homomorphisms of k-algebras

$$k[t_1, \dots, t_m] \longrightarrow k[Y] = k[t_1, \dots, t_m]/I(Y) \longrightarrow k[X] = k[x_1, \dots, x_n]/I(X).$$

Let $f_i = \Phi(t_i)$, $i = 1, \dots, m$. The polynomial map $f = (f_1, \dots, f_m)$ maps X to $\mathbf{A}_k^m$. Let $F(t_1, \dots, t_m)$ be a polynomial. Since we consider homomorphisms of k-algebras we have

$$F(f_1, \dots, f_m) = F(\Phi(t_1), \dots, \Phi(t_m)) = \Phi(F(t_1, \dots, t_m)).$$

If $F \in I(Y)$, then $\Phi(F) = 0$. Hence all the polynomials from $I(Y)$ vanish on $f(X)$, that is, $f(X) \subset Z(I(Y)) = Y$.

Finally, $f^* = \phi$ since these homomorphisms take the same values on the generators t_i of the k-algebra $k[Y]$.

(c) follows from (a) and (b). QED

Examples. (1) Hypersurfaces in $\mathbf{A}_k^n$ bijectively correspond to principal ideals in $k[x_1, \ldots, x_n]$ (via the usual operations Z and I).

(2) Square matrices of size n are parametrized by the points of $\mathbf{A}_k^{n^2}$. The multiplication of matrices is a morphism $\mathbf{A}_k^{n^2} \times \mathbf{A}_k^{n^2} \to \mathbf{A}_k^{n^2}$. The determinant is a morphism $\mathbf{A}_k^{n^2} \to \mathbf{A}_k^1$.

The closed subset given by $det(M) = 1$ is the special linear group $SL(n)$. Note that the inverse is an isomorphism $SL(n) \to SL(n)$. The group operations are morphisms – when that is the case then the group is called an *algebraic group*. $SL(n) \subset \mathbf{A}_k^{n^2}$ is a hypersurface of degree n.

(3) The orthogonal group $O(n) \subset \mathbf{A}_k^{n^2}$ given by the conditions $M \cdot M^t = I$ is another example of a closed subset which is an algebraic group. It is defined by n^2 quadratic polynomials.

Exercise. Show that $O(n)$ is not irreducible. (Hint: what are the possible values of $det(M)$?)

Zariski topology on $\mathbf{A}_k^n$ induces a topology on a variety $X \subset \mathbf{A}_k^n$. An open subset $U \subset X$ is an intersection of X with an open set of $\mathbf{A}_k^n$. Such sets are called a *quasi-affine* varieties. An example of a quasi-affine variety is the general linear group $GL(n)$ (square matrices with non-zero determinant). Later we'll see that $GL(n)$ is isomorphic to an affine variety (see the end of this subsection).

Definition. A rational function $f \in k(X)$ is called regular at a point P of X if $f = g/h$, where $g, h \in k[X]$ and $h(P) \neq 0$. A function is regular on an open set $U \subset X$ if it is regular at every point of U.

The ring of regular functions on an open subset $U \subset X$ is denoted by $k[U]$. Since $k[X] \subset k[U] \subset k(X)$ the fraction field of $k[U]$ if $k(X)$.

To a rational function $f \in k(X)$ one associates "the ideal of denominators" $D_f \subset k[X]$ consisting of regular functions h such that $hf \in k[X]$ (it is clearly an ideal!). *The set of all points P where f is regular is $X \setminus Z(D_f)$.* Indeed, we can write $f = g/h$, $g, h \in k[X]$, $h(P) \neq 0$, if and only if $P \notin Z(D_f)$.

An immediate corollary of the Nullstellensatz says that if $I \subset k[X]$ is an ideal, and $f \in k[X]$ vanishes at all the common zeros of I in X, then $f^s \in I$ for some $s > 0$. (Apply Theorem 1.7 to the pre-image of I in $k[x_1, \ldots, x_n]$ under the natural surjective map.) We'll often use the Nullstellensatz in this form.

Lemma 2.3 *Let X be an affine variety. The subset of $k(X)$ consisting of functions regular at all the points of X is $k[X]$. A function is regular on the open subset given by $h \neq 0$, for $h \in k[X]$, if and only if $f \in k[X][h^{-1}]$, in other words, if $f = g/h^s$ for some $g \in k[X]$ and $s > 0$.*

Proof. Let f be such a function. Then $Z(D_f) = \emptyset$. By Corollary 1.6 D_f must be the whole ring, hence contains 1, hence $f \in k[X]$. This proves the first statement. To prove the second statement we note that $Z(D_f)$ is contained in the closed set given by $h = 0$. By Nullstellensatz if h vanishes on $Z(D_f)$, then a power of h is in D_f. QED

One defines *rational maps* using rational functions instead of regular ones. Rational maps are not everywhere defined, that is, are not functions! A rational map is called *dominant* if its image (=the image of the set of points where the map is actually defined, that is, is regular) is dense, that is, not contained in a smaller subvariety. The following proposition is proved along the same lines as Proposition 2.2.

Proposition 2.4 (a) *A dominant rational map $f : X - - > Y$ defines a homomorphism of k-algebras $f^* : k(Y) \to k(X)$.*

(b) *Any homomorphism of k-algebras $\phi : k(Y) \to k(X)$ is of the form $\phi = f^*$ for a unique dominant rational map $f : X - - > Y$.*

We need the condition that f is dominant, as otherwise the composition of rational functions is not always defined. (On substituting the f_i for the coordinates we may have to divide by zero! But this can't happen if the map is dominant, as the f_i then do not satisfy a non-trivial polynomial condition.)

Finally, a morphism of quasi-affine varieties is an everywhere defined rational map. An isomorphism is a morphism that has an inverse. For example, the map $M \mapsto M^{-1}$ is a morphism $GL(n) \to GL(n)$ (and in fact, an isomorphism). On the affine space of square matrices $\mathbf{A}_k^{n^2}$ this is just a rational map.

A rational map which has an inverse (at the same time left and right) is called a *birational* map or a *birational equivalence*. For example, the map $M \mapsto M^{-1}$ is a birational equivalence of $\mathbf{A}_k^{n^2}$ with itself.

Proposition 2.5 *The following conditions are equivalent: a rational map $f : X - - > Y$ is*

(i) birational,

(ii) f is dominant, and $f^* : k(Y) \to k(X)$ is an isomorphism of k-algebras,

(iii) there exist open sets in X and Y such that f defines an isomorphism between them.

Proof. The only implication which is not immediate is $(i) \Rightarrow (iii)$. But this is also easy, see [Reid, UAG], (5.8).

Theorem 2.6 *Any affine variety is birationally equivalent to a hypersurface.*

Proof. By Noether's normalization there exist algebraically independent elements $y_1, \ldots, y_m \in k[X]$ such that $k[X]$ is integral over $k[y_1, \ldots, y_m]$. Then the field extension $k(y_1, \ldots, y_m) \subset k(X)$ is finite. In fact, one can arrange that this extension is separable (this is automatic if the characteristic of k is 0, see [Reid, UAG], (3.16) for the case of finite characteristic). Any separable finite extension can be obtained by adding just one element (primitive element theorem), say, y. Let $F(t)$ be an irreducible polynomial with coefficients in $k(y_1, \ldots, y_m)$ such that $F(y) = 0$. By fiddling with the coefficients can assume that the coefficients of $F(t)$ are in $k[y_1, \ldots, y_m]$, and that F is irreducible as a polynomial in $y_1, \ldots, y_m, t$. Then $k(X)$ is the fraction field of $k[y_1, \ldots, y_m, t]/(F(t))$. Let $V \subset \mathbf{A}_k^{m+1}$ be the hypersuface given by $F = 0$. Then $k(V) = k(X)$. QED

The following lemma allows us to consider only affine open neighbourhoods.

Proposition 2.7 *Every open neighbourhood of a point of an affine variety contains a neighbourhood isomorphic to an affine variety (and not just quasi-affine).*

Proof. It is enough to show how to remove zeros of polynomials. Let $X \subset \mathbf{A}_k^n$ be a closed set given by the polynomial equations $f_1 = \ldots = f_m = 0$ in variables $T_1, \ldots, T_n$, and let g be another polynomial, $g(P) \neq 0$. Let $X_0 \subset X$ be given by $g \neq 0$. Consider the closed subset $X_1 \subset \mathbf{A}_k^{n+1}$ with coordinates $T_0, T_1, \ldots, T_n$ given by $f_1 = \ldots = f_m = T_0 g - 1 = 0$. Then the projection $(T_0, T_1, \ldots, T_n) \mapsto (T_1, \ldots, T_n)$ defines an isomorphism of X_1 with X_0. QED

Exercise. Show that $GL(n)$ is isomorphic to a closed subset of an affine space.

2.3 Examples of rational varieties

Let's do some concrete algebraic geometry.

Let $X \subset \mathbf{A}_k^n$ be a hypersurface given by $f(X_1, \ldots, X_n) = 0$. We shall always assume that no linear change of coordinates $X_1, \ldots, X_n$ reduces f to a polynomial in $n-1$ variables, and that no linear change of coordinates reduces f to a homogeneous polynomial. Then X is called *non-conical*. We shall only consider non-conical hypersurfaces. We call the *degree* of X the degree of f.

In this section we examine some examples of rational hypersurfaces. By definition $X \subset \mathbf{A}_k^n$ is rational if there is a birational map $\mathbf{A}_k^m - - > X$. Such a map is given by rational functions in m variables. The meaning of rationality is that the points of X can be parametrized by rational functions such that this parametrization is an isomorphism on a non-empty open set.

Remark. We observe that a rational variety over any infinite field k has infinitely many k-points. Indeed, it contains an dense open subset isomorphic to a dense open subset of $\mathbf{A}_k^n$, and the latter contains infinitely many k-points (easy exercise).

(1) **Quadrics** (degree 2). If k is not algebraically closed there may be no k-point on X, e.g. $x^2 + y^2 + 1 = 0$ over $k = \mathbf{R}$. Then X is not rational.

The following proposition is a generalization of the classical parametrization of the conic $x^2 + y^2 = 1$ by rational functions $x = (t^2 - 1)/(t^2 + 1)$, $y = 2t/(t^2 + 1)$.

Proposition. *A non-conical quadric with a k-point is rational.*

Proof. The idea is to exploit the classical stereographic projection. We can assume that the k-point is $N = (0, 0, \dots, 0)$ (N stands for the North Pole ...). Then we can write

$$f = Q(x_1, \dots, x_n) + L(x_1, \dots, x_n),$$

where the homogeneous polynomials L and Q have degrees 1 and 2, respectively (there is no constant term). Chose a hyperplane H not passing through N, say the one given by $x_1 = 1$. The coordinates on H are $x_2, \dots, x_n$. Let L be the line passing through N and the point $(1, x_2, \dots, x_n)$. Consider $L \cap X$. The line L is the set $(t, tx_2, \dots, tx_n)$, $t \in \overline{k}$, hence the $\overline{k}$-points of $L \cap X$ correspond to the roots of the following equation in t:

$$t^2 Q(1, x_2, \dots, x_n) + tL(1, x_2, \dots, x_n) = 0.$$

The root $t = 0$ is the point N, but it is the other root $t = -L/Q$ that is interesting to us. Define the rational map $\phi : \mathbf{A}_k^{n-1} - - > X$ by sending $(x_2, \dots, x_n)$ to "the other" (residual) intersection point:

$$\phi(x_2, \dots, x_n) = -\frac{L(1, x_2, \dots, x_n)}{Q(1, x_2, \dots, x_n)}(1, x_2, \dots, x_n).$$

The image is obviously in X. The inverse map sends $(x_1, x_2, \dots, x_n)$ to $(x_2/x_1, \dots, x_n/x_1)$. (Check that this is indeed the inverse to ϕ, both right and left.) QED

(2) **A cubic surface**. Assume that the characteristic of k is not 3, and that k contains a non-trivial cubic root ρ of 1. Consider the hypersurface $X \subset \mathbf{A}^3_k$ given by the equation

$$x_1^3 + x_2^3 + x_3^2 = 1.$$

It contains two skew lines (non-parallel with empty intersection)

$$L_0 = \{(1, x, -x)\}, \quad x \in \overline{k}, \qquad L_1 = \{(y, -\rho y, 1)\}, \quad y \in \overline{k}.$$

Let us write $P_x = (1, x, -x)$, $Q_y = (y, -\rho y, 1)$. Let $L_{x,y}$ be the line passing through P_x and Q_y,

$$L_{x,y} = \{tP_x + (1-t)Q_y\}, \quad t \in \overline{k}.$$

We now contruct a rational map $\phi : \mathbf{A}^2_k - - > X$ by sending (x, y) to the third ("residual") point of intersection of $L_{x,y}$ with X. More precisely, substituting $tP_x + (1-t)Q_y$ into the equation of X we get a cubic polynomial in t with coefficients in $k(x, y)$. It has two obvious roots $t = 0$ (the point Q_y) and $t = 1$ (the point P_x). After checking that its degree is exactly 3 (this is enough to check for a particular choice of x and y, say $x = 1$, $y = 0$) we can write it as $c(x, y)t(t-1)(t-\lambda(x, y))$, where $\lambda(x, y) \in k(x, y)$. Set

$$\phi(x, y) = \lambda(x, y)P_x + (1 - \lambda(x, y))Q_y.$$

By construction this is rational map $\mathbf{A}^2_k - - > X$.

Exercise. Find $\lambda(x, y)$, then check that ϕ is a birational equivalence.

There is a geometric construction of the inverse map. Let R be a point of $X \setminus (L_0 \cup L_1)$. Let Π_i be the plane spanned by R and L_i. Then for R in a non-empty Zariski open subset of X the intersection $\Pi_0 \cap L_1$ is a single point on L_1, call it Q. Similarly, $\Pi_1 \cap L_0$ is a point on L_0, call it P. We have a well-defined rational map

$$f : X \setminus (L_0 \cup L_1) - - - > \mathbf{A}^2_k, \qquad f(R) = (P, Q).$$

Check that f is inverse to ϕ.

(3) **Conic bundles over the affine line.** Let k be algebraically closed. Let

$$F(x_0, x_1, x_2) = \sum_{i_j \geq 0,\ i_0+i_1+i_2 \leq 2} f_{i_0,i_1,i_2}(t) x_0^{i_0} x_1^{i_1} x_2^{i_2}$$

be a rank 3 quadratic form over the field $K = k(t)$. By Tsen's theorem (see Theorem 2.15 below) the conic $C \subset \mathbf{A}^2_K$ given by $F(1, x_1, x_2) = 0$ has a K-point. But we know from (1) that a non-conical quadric with a rational point

is rational. Hence C is rational over K, in other words, $K(C) = K(y) = k(t, y)$ is a purely transcendental extension of K, and hence of k as well.

Multiplying the coefficients of F by a common multiple, we can assume that they are actually in $k[t]$. Hence the equation $F(t; 1, x_1, x_2) = 0$ defines a surface $X \subset \mathbf{A}^3_k$. If we assign to t a value in k we get a plain conic. Thus X is a pencil (1-parameter family) of conics, or a conic bundle. We thus proved that any *conic bundle over the affine line over an algebraically closed field is rational*.

Exercise. Let X be a smooth cubic surface, and $L \subset X$ be a straight line. Planes Π passing through L form a 1-dimensional family. Show that for almost all planes Π the intersection $\Pi \cap X$ is the union of L and a conic. Deduce that X is birationally equivalent to a pencil of conics. Now (3) gives another proof of rationality of X.

2.4 Smooth and singular points

Let $X \subset \mathbf{A}^n_k$ be an affine variety, and suppose that the ideal of X is generated by polynomials $f_1, \dots, f_m$. Let $P = (a_1, \dots, a_n)$ be a point of X. We define the partial derivatives $\partial f_i/\partial T_j$ as partial derivatives of a polynomial (in a purely algebraic way, this works over any field). Then we get some constants $\partial f_i/\partial T_j(P) \in k$. Recall that an affine subspace of $\mathbf{A}^n_k$ is a translation of a vector subspace.

Definition. The affine subspace of k^n given by the system of linear equations in $T_1, \dots, T_n$

$$\sum_{j=1}^{n} \partial f_i/\partial T_j(P)(T_j - a_j) = 0, \quad i = 1, \dots, m,$$

is called the *tangent space* to X at $P = (a_1, \dots, a_n)$, as is denoted by $T_{X,P}$.

Exercise. Let $m = 1$. Show that $T_{X,P}$ is the union of lines passing through P such that the restriction of f to this line is a polynomial in one variable with a multiple root at P.

All we need to know to compute $T_{X,P}$ are partial derivatives of the equations definiting X at P. Thus it makes sense to define $T_{U,P}$, where U is an open subset of X containing P, by the same formula, so that $T_{U,P} = T_{X,P}$.

We have a function from X to non-negative integers given by $dim(T_{X,P})$.

Lemma 2.8 (Upper semi-continuity) *The subset of X given by the condition $dim(T_{X,P}) \geq s$ is a closed subset of X.*

Proof. The condition $dim(T_{X,P}) \geq s$ is equivalent to the condition that the rank of the matrix $(\partial f_i/\partial T_j(P))$ is at most $n-s$, which is equivalent to the vanishing of the determinants of all its square submatrices of size $n-s+1$. But these determinants are polynomials in $a_1, \ldots, a_n$, which implies our statement. QED

It follows that the subset of X consisting of points where $dim(T_{X,P})$ takes its minimal value is open. It is non-empty, and X is irreducible, hence this subset is dense. The points in this subset are called *smooth* or *non-singular*, and all the other points are called *singular*.

Exercises. When is the curve $X \subset \mathbf{A}_k^2$ given by $x^a + y^b$, where a and b are positive integers, non-singular at $(0,0)$?

Show that any hypersurface defined by a homogeneous polynomial of degree at least 2 is singular at the origin.

Proposition 2.9 *Let $m_P = (T_1 - a_1, \ldots, T_n - a_n) \in k[X]$ be the maximal ideal of a point P in the coordinate ring of X. Then the tangent space $T_{X,P}$ (considered as a vector space with origin at P) is canonically dual to the quotient ring m_P/m_P^2.*

Proof. We first do an exercise in linear algebra. Let V be a vector space, V^* its dual space (that is, the space of linear forms $V \to k$), and S a subspace of V^*. Consider the subspace

$$W = \{v \in V | f(v) = 0, \text{ for any } f \in S\}.$$

Its dual space W^* can be identified with V^*/S (the restrictions of linear functions on V). Since W is canonically isomorphic to $(W^*)^*$ we conclude that W is canonically isomorphic to $(V^*/S)^*$.

After a translation in k^n we can assume without loss of generality that $a_i = 0$, $i = 1, \ldots, n$. Let $V = k^n$. The coordinates T_i form a basis of the dual space V^*. Let $S \subset V^*$ be the subspace of linear terms of functions from $I(X)$, that is, linear combinations of $\sum_{j=1}^n \partial f_i/\partial T_j(P) T_j$. The k-vector space m_P/m_P^2 consists of linear combinations of T_i's modulo linear terms of functions from $I(X)$. This means that $m_P/m_P^2 = V^*/S$. On the other hand, by definition $T_{X,P} \subset V$ is the space of zeros of the functions from S. Now the exercise in linear algebra above gives the required isomorphism. QED

The proposition implies that the tangent space to X at P is an intrinsic invariant of X, in the sense that it only depends on the isomorphism class of X, and not on the particular embedding.

Exercise. Prove that computing m_P/m_P^2 for X and for an open subset $U \subset X$ containing P gives the same thing. (The resulting vector spaces are canonically isomorphic.)

Let $p : \mathbf{A}_k^n \to \mathbf{A}_k^m$ be a collection of polynomials $p_1, \ldots, p_m$ in n variables that defines a morphism $p : X \to Y$. The $m \times n$-matrix of partial derivatives $J = (\partial p_i/\partial x_j)$ is called the Jacobian matrix. Using the chain rule for partial derivatives one easily checks that J defines a linear map $p_* : T_{X,P} \to T_{Y,Q}$, where $Q = p(P)$. The construction of p_* from p is functorial in the sense that if $q : Y \to Z$ is a morphism, then $(qp)_* = q_* p_*$. In particular, if p is an isomorphism, then so is p_*. This is a practical way to check that a given map is not an isomorphism at a given point.

2.5 Dimension. Application: Tsen's theorem

Definition. Let X be an affine variety over a field k. The transcendence degree of $k(X)$ over k is called the *dimension* of X. The dimension of a closed affine set is defined as the maximum of the dimensions of its irreducible components.

For example, $dim(\mathbf{A}_k^n) = n$ since $k(\mathbf{A}_k^n)$ is the purely transcendental field extension $k(x_1, \ldots, x_n)$.

Proposition 2.10 *Let $X \subset \mathbf{A}_k^n$ be a variety, $Y \subset X$ a subvariety, $Y \neq X$. Then $dim(Y) < dim(X)$.*

Proof. Let $tr.deg._k k(Y) = m$, and choose $u_1, \ldots, u_m \in k[X]$ such that their images in $k[Y]$ are algebraically independent. Then $u_1, \ldots, u_m$ are algebraically independent in $k(X)$. In particular, $tr.deg._k k(X) \geq m$. For contradiction assume that $tr.deg._k k(X) = m$. Since $Y \neq X$ the ideal $I(Y) \subset k[X]$ is non-zero. Any $u \in I(Y)$, $u \neq 0$, must be algebraically dependent on $u_1, \ldots, u_m$. Thus there exists a polynomial $F(t, t_1, \ldots, t_m) = \sum_i a_i(t_1, \ldots, t_m)t^i$ such that $F(u, u_1, \ldots, u_m)$ is zero in $k[X]$. We can assume that the a_i are polynomials, and that F is irreducible in all the variables $t, t_1, \ldots, t_m$. In particular, the constant term $a_0(t_1, \ldots, t_m)$ is not the zero polynomial. Since the image of u in $k[Y]$ is zero, the image of $a_0(u_1, \ldots, u_m)$ is zero in $k[Y]$. This gives an algebraic relation between the images of $u_1, \ldots, u_m$, contrary to our choice of $u_1, \ldots, u_m$. This contradiction proves that $tr.deg._k k(X) < m$. QED

Corollary 2.11 *A subvariety $X \subset \mathbf{A}_k^n$ has dimension $n - 1$ if and only if X is a hypersurface. Then $I(X)$ is a principal ideal of the polynomial ring $k[T_1, \ldots, T_n]$.*

Proof. It remains to show that $dim(X) = n - 1$ implies that X is a hypersurface. Since the dimensions are different we have $X \neq \mathbf{A}^n_k$. Let F be a non-zero element in $I(X)$. We write F as a product of irreducible factors $F = F_1 \dots F_m$. Then $X = \cup(X \cap \{F_i = 0\})$. Since X is irreducible we have $X = X \cap \{F_j = 0\}$ for some j, hence $F_i \in I(X)$. Replace F by F_j. Then X is contained in the irreducible hypersurface given by $F = 0$. Since the dimensions are equal, these varieties coincide by Proposition 2.10. QED

Theorem 2.12 *The dimension of the tangent space at a smooth point of X equals $dim(X)$.*

Proof. We know that X is birationally equivalent to a hypersurface $V \subset k^{m+1}$ given by some (non-constant) polynomial $F = 0$. Since $k(X) = k(V)$ we conclude that $dim(X) = dim(V)$.

The dimension of the tangent space to X at any smooth point is the same, and can be computed in any non-empty open subset of X. Wee can arrange that the birational map $X - - > V$ is an isomorphism on this open set. This reduces the whole computation to V.

By Proposition 2.10 $dim(V) \leq m$. On the other hand, the transcendence degree of $k(V)$ is at least m. Indeed, F depends on at least one variable, say x_1. Then the images of $x_2, \dots, x_{m+1}$ in $k[V]$ are algebraically independent (as otherwise we would have a polynomial $G(x_2, \dots, x_{m+1})$ in the principal ideal (F) which is impossible since F depends on x_1 whereas G does not). Therefore, $dim(V) = m$.

On the other hand, the dimension of $T_{V,P}$ for P in a certain dense open subset of V is m: if all the partial derivatives of F vanish everywhere on V, they must belong to the principal ideal (F) by Hilbert's Nullstellensatz. Since they have degrees less than the degree of F, they must be zero polynomials. If the characteristic of k is zero, this implies that F is a constant, which is a contradiction. If the characteristic is p, then F is a p-th power, which contradicts the irreducibility of F. QED

We quote the following result without proof (see Ch. 1 of [Shafarevich] or Ch. 11 of [Atiyah-McDonald]).

Theorem 2.13 *Let k be an algebraically closed field. Let $X \subset \mathbf{A}^n_k$ be a variety, F be a polynomial taking both zero and non-zero values on X. Then $dim(X \cap \{F = 0\}) = n - 1$.*

Corollary 2.14 *Let $F_1, \dots, F_m$, $m \leq n$, be homogeneous polynomials in n variables. Then the closed affine set X given by $F_1 = \dots = F_m = 0$ has dimension at least $n - m$. In particular, X is not empty.*

Proof. Note that the all-zero point is in X. Thus at each successive intersection the dimension drops at most by one. QED

The natural place of this statement is in intersection theory of subvarieties of the projective space. To demonstrate its force we now deduce just one corollary.

Recall that k is algebraically closed. Let

$$F(x_0, x_1, x_2) = \sum_{i_j \geq 0,\ i_0+i_1+i_2 \leq 2} f_{i_0,i_1,i_2}(t) x_0^{i_0} x_1^{i_1} x_2^{i_2}$$

be a homogeneous polynomial of degree 2 with coefficients in $k[t]$.

Theorem 2.15 (Tsen) *There exist non-zero polynomials $p_0(t)$, $p_1(t)$, $p_2(t)$ with coefficients in k such that $x_0 = p_0(t)$, $x_1 = p_1(t)$, $x_2 = p_2(t)$ is a solution of the equation $F(x_0, x_1, x_2) = 0$.*

Proof. Let m be a positive integer. Polynomials of degree m form an $m+1$-dimensional vector space over k. Hence the dimension of the vector space of coefficients of $p_0(t)$, $p_1(t)$, $p_2(t)$ is $3m+3$. We observe that the conditions on these coefficients that must be satisfied in order for $x_0 = p_0(t)$, $x_1 = p_1(t)$, $x_2 = p_2(t)$ to be a solution, are given by homogeneous (quadratic) polynomials. Let us compute the number of these conditions.

Let ℓ be the maximum of the degrees of the $f_{i_0,i_1,i_2}(t)$. Suppose that the degree of $p_j(t)$, $j = 1, 2, 3$, is at most m. Then the degree of $F(p_0(t), p_1(t), p_2(t))$ is at most $\ell + 2m$. This means that the coefficients of the $p_j(t)$ must satisfy $\ell + 2m + 1$ homogeneous polynomial conditions (1 must be added to provide for the zero constant term). For large m we have $3m+3 > \ell+2m+1$, hence the number of variables exceeds the number of equations. By Corollary 2.14 the dimension of the closed affine set of polynomials that are solutions, is positive. We conclude that there exist such non-zero polynomials. QED

A more general approach to dimension. Let R be a ring. The *Krull dimension* of R is defined as the supremum of all integers n such that there exists a chain $I_0 \subset I_1 \subset \ldots \subset I_n$ of distinct prime ideals of R. For example, the Krull dimension of a field is 0. The dimension of $\mathbf{Z}$ and, more generaly, of the ring of integers in a number field is 1. The dimension of $k[T]$ is also 1. The dimension of $k[X, Y]$ is 2, etc.

In fact all given definitions of dimension are equivalent.

Theorem 2.16 *Let X be an affine variety, then the Krull dimension of $k[X]$ equals the transcendence degree of $k(X)$.*

This can be deduced from Theorem 2.13.

3 Projective geometry

3.1 Projective varieties

Below is the list of main notions, and the outline of differences with the affine case.

The projective space $\mathbf{P}_k^n$ is the set of equivalence classes of points of $\mathbf{A}_k^{n+1} \setminus \{(0,\dots,0)\}$, where two points are equivalent if they differ by a common non-zero multiple. The equivalence class of $(x_0, x_1, \dots, x_n)$ is denoted by $(x_0 : x_1 : \dots : x_n)$.

The zeros of homogeneous polynomials (also called forms) are *closed projective sets*. One defines open sets as their complements. This gives rise to Zariski topology on $\mathbf{P}_k^n$. The condition $T_i \neq 0$ defines an open subset of $\mathbf{P}_k^n$ isomorphic to the affine space $\mathbf{A}_k^n$ with coordinates $T_0/T_i, \dots, T_n/T_i$. We get $n+1$ affine spaces which provide an open covering of $\mathbf{P}_k^n$.

Let $f(T_1, \dots, T_n)$ be a polynomial of degree d. It can be written as the sum $f = f_0 + \dots + f_d$, where f_i is a form of degree i. The *homogenization* of f is the form of degree d in $n+1$ variables given by

$$F(T_0, T_1, \dots, T_n) = F = T_0^d f_0 + T_0^{d-1} f_1 + \dots + f_d.$$

If $X \subset \mathbf{A}_k^n$ is a closed affine set, then associating to polynomials in the ideal of X their homogenizations defines the *projective closure* of X.

There are serious reasons for working with projective varieties:

(1) The set of complex-valued points of $\mathbf{P}^n$ is compact in the usual complex topology (e.g. $\mathbf{P}^1$ over $\mathbf{C}$ is just the Riemann sphere),

(2) classifications are simpler (e.g. quadratic forms are classified only by their rank),

(3) intersection theory is simpler (any two curves in the plane, or more generally, any n hypersurfaces in $\mathbf{P}_k^n$ have a common point).

An ideal $J \subset k[T_0, \dots, T_n]$ is called *homogeneous* if whenever $f \in J$ we also have $f_i \in J$, where f_i is the homogeneous part of f of degree i. Homogeneous ideals are generated by homogeneous polynomials.

The *affine cone* of a closed projective set X is the set of points in $\mathbf{A}_k^{n+1}$ given by the same (homogeneous) equations as X. To a closed projective set X one associates the ideal $I(X)$ of all polynomials in $k[T_0, \dots, T_n]$ vanishing on the affine cone of X. The ideal $I(X)$ is clearly homogeneous. To any homogeneous ideal J one associates its set of zeros $Z(J) \subset \mathbf{P}_k^n$. This always gives a non-empty set unless $J = 1$ (empty affine cone) or $J = (T_0, \dots, T_n)$ (the affine cone consists of the zero point). Hence the projective variant

of Nullstellensatz, which immediately follows from the affine Nullstellensatz, reads as follows.

Theorem 3.1 (Projective Nullstellensatz) *If J is a homogeneous ideal, then*

(1) *$Z(J) = \emptyset$ iff the radical of J contains the ideal $(T_0, \ldots, T_n)$ (the maximal ideal of the zero point in $\mathbf{A}_k^{n+1}$),*

(2) *if $Z(J) \neq \emptyset$, then $I(Z(J))$ is the radical of J.*

Projective variety is an irreducible closed projective set. (The definition of irreducible is the same as in the affine case.) Quasi-projective varieties are dense open subsets of projective varieties. Rational functions on a projective variety X are fractions of forms of equal degree $\frac{F}{G}$, where $G \notin I(X)$, modulo natural equivalence: $\frac{F}{G} = \frac{F_1}{G_1}$ if $FG_1 - F_1G \in I(X)$. The rational function $\frac{F}{G}$ is called regular at a point $P \in X$ if $G(P) \neq 0$. The field of rational functions on X is again denoted by $k(X)$, but it is not the field of fractions of the ring of regular functions on X! Indeed, the only regular functions on $\mathbf{P}_k^1$ are constants[1]: $k[\mathbf{P}_k^1] = k$ (easy exercise, in fact every regular function on $\mathbf{A}_k^1 \subset \mathbf{P}_k^1$ is a polynomial, and every non-constant polynomial has a pole at infinity).

A *rational map* $f : X - - > \mathbf{P}_k^n$ is (a not necessarily everywhere defined function) given by $(F_0, \ldots, F_n)$, where $F_i \in k(X)^*$, defined up to an overall multiple from $k(X)^*$. A rational map f is *regular* at $P \in X$ if there exists a representative $(F_0, \ldots, F_n)$, such that all the F_i's are regular at P, and $(F_0(P), \ldots, F_n(P)) \neq (0, \ldots, 0)$. A *morphism* is an everywhere regular rational map.

Examples of projective varieties, rational maps and morphisms

(a) *Rational normal curves.* This is a map $f : \mathbf{P}_k^1 \to C \subset \mathbf{P}^n$ given by

$$f : (X : Y) \mapsto (X^n : X^{n-1}Y : \ldots : XY^{n-1} : Y^n).$$

One checks that f is a morphism, whose image is given by equations $T_0T_2 = T_1^2$, $T_1T_3 = T_2^2$, and so on. The inverse map is given by

$$g : (T_0 : \ldots : T_n) \mapsto (T_0 : T_1) = (T_1 : T_2) = \ldots = (T_{n-1} : T_n)$$

which is everywhere defined (check!). Hence f is an isomorphism of $\mathbf{P}_k^1$ with a closed subvariety $C \subset \mathbf{P}^n$, called the rational normal curve of degree n. For $n = 2$ one recovers the rational parametrization of the conic.

[1]The same is true for any projective variety, see page 20.

(b) *The Veronese embedding of* $\mathbf{P}_k^n$. This is a natural generalization of the previous example, where one considers all monomials of degree d. This defines an isomorphism of $\mathbf{P}_k^n$ with a closed subvariety of $\mathbf{P}_k^N$, where $N = C_n^{n+d}$. For $d = 2$ and $n = 2$ one gets the Veronese surface in $\mathbf{P}_k^5$.

(c) Any quadric in $Q \subset \mathbf{P}_k^3$ is isomorphic to $\mathbf{P}_k^1 \times \mathbf{P}_k^1$. (Think of two families of $\mathbf{P}_k^1$'s on a quadric). The stereographic projection from a point $P \in Q$ defines a birational map $Q - - > \mathbf{P}_k^2$ which is not a morphism (not regular at P). Neither is the inverse map a morphism (two lines of Q passing through P are contracted to points).

(d) *The Segre embedding* $\mathbf{P}_k^n \times \mathbf{P}_k^m \subset \mathbf{P}_k^{nm+n+m}$. This map associates to two vectors their tensor product. The map is well defined everywhere, and is a bijection with the image. The image can be interpreted as the set of non-zero matrices of rank one. In particular, when $n = m = 1$ we get a quadric in $\mathbf{P}_k^3$.

The Segre embedding can be used to define the structure of a projective variety on $\mathbf{P}_k^n \times \mathbf{P}_k^m$. As a consequence we realize the product of two projective varieties as a closed subset of some projective space.

(e) *Elliptic curve.* These are smooth plane cubic curves with a k-point. It can be proved that such a curve is isomorphic to a projective curve $y^2z = x^3 + axz^2 + bz^3$. The map $(x : y : z) \to (x : -y : z)$ is a non-trivial automorphism with exactly four fixed points (there are three obvious fixed points with $y = 0$, $z = 1$, and also $(0 : 1 : 0)$). This shows that the curve is not $\mathbf{P}_k^1$, as any element of $PGL(2)$ that fixes three different point is an identity. This follows from the fact that $\mathrm{Aut}(\mathbf{P}_k^1) = \mathrm{PGL}(2)$, see Proposition 5.4 below.

3.2 Morphisms of projective varieties

Examples show that if $f : X \to Y$ is a morphism of affine varieties, then $f(X) \subset Y$ need not be a closed subset. A standard example is $X \subset \mathbf{A}_k^2$ given by $xy = 1$, mapped to $\mathbf{A}_k^1$ by the morphism $(x, y) \mapsto x$. It is another pleasant feature of projective varieties that the image of a projective variety under a morphism is always closed! We start with a lemma.

Lemma 3.2 *Let X and Y be quasi-projective varieties. The graph Γ_f of any morphism $f : X \to Y$ is closed in $X \times Y$.*

Proof. It is enough to consider the case $Y = \mathbf{P}_k^n$. Consider the morphism $(f, Id) : X \times \mathbf{P}_k^n \to \mathbf{P}_k^n \times \mathbf{P}_k^n$, and let $\Delta \in \mathbf{P}_k^n \times \mathbf{P}_k^n$ be the diagonal (the graph of the identity map). Then $\Gamma_f = (f, Id)^{-1}(\Delta)$. It is clear that the preimage of a closed subset is closed. Thus it is enough to prove that $\Delta \subset \mathbf{P}_k^n \times \mathbf{P}_k^n$ is

closed. But Δ is given by $T_iX_j = T_jX_i$ for all i and j, and hence is closed. QED

Theorem 3.3 *Let X be a projective variety, and Y be a quasi-projective variety. Then the projection to the second factor $p : X \times Y \to Y$ maps closed subsets to closed subsets.*

Corollary 3.4 *Let $f : X \to Y$ be a morphism, where X is a projective variety. Then $f(X)$ is closed in Y.*

Proof. Apply the theorem to $p(\Gamma_f) = f(X)$. QED

Proof of the theorem. We can assume that $X = \mathbf{P}^n_k$. Next, the closedness can be checked locally in a small affine neighbourhood of every point. Thus we can assume that Y is a closed subset of $\mathbf{A}^m_k$. But then Y can be replaced by $\mathbf{A}^m_k$. All in all, we see that the general statement follows from the statement for the projection $\mathbf{P}^n_k \times \mathbf{A}^m_k \to \mathbf{A}^m_k$. Let us prove it.

Let a closed subset in $\mathbf{P}^n_k \times \mathbf{A}^m_k$ be given by equations

$$g_i(T_0, \dots, T_n; Y_1, \dots, Y_m) = 0, \quad i = 1, \dots, s,$$

where the g_i's are homogeneous polynomials in variables $T_0, \dots, T_n$ whose coefficients are polynomials in variables $Y_1, \dots, Y_m$. We must prove that the set U of $y = (y_1, \dots, y_m) \in k^m$ such that the ideal $J_y = (g_i(T_0, \dots, T_n; y_1, \dots, y_m))$ has no zeros in $\mathbf{P}^n_k$, is open. By the projective Nullstellensatz, $Z(J_y) = \emptyset$ iff all T_i's are contained in the radical of J_y, that is, $T_i^{l_i} \in J_y$ for some l_i. Let $l = l_0 + \ldots + l_n$, then in any monomial of degree l at least one variable T_i enters in the power greater or equal to l_i. Hence J_y contains the ideal I_l generated by all monomials of degree l. Let U_l be the set of $y = (y_1, \dots, y_m) \in k^m$ such that $J_y \supset I_l$. Then U is the union of all U_l's, $l = 1, 2, \dots$, hence it is enough to prove that each $U_l \subset \mathbf{A}^m_k$ is open.

If one can represent a monomial as a linear combination of homogeneous polynomials, then the coefficients can be chosen to be homogeneous polynomials. Let d_i be the degree of $g_i(T_0, \dots, T_n; y_1, \dots, y_m)$. Then $y \in U_l$ iff the products of the $g_i(T_0, \dots, T_n; y_1, \dots, y_m)$ with all monomials of degree $l - d_i$ span the vector space of forms of degree l. Equivalently, the corresponding matrix has maximal rank, which is the condition on the non-vanishing of the determinants of its square submatrices of maximal size. This cleary describes an open subset. (Which may well be empty, but it does not matter!) QED

This result hints at the following definition.

Definition. A morphism $f : X \to Y$ of quasi-projective varieties is *proper* if it is a composition of a closed embedding $X \hookrightarrow \mathbf{P}^n_k \times Y$ and the projection $\mathbf{P}^n_k \times Y \to Y$.

It follows from the previous theorem that $f(X) \subset Y$ is closed provided f is proper. It is clear that if f is proper, and $P \in Y$, then $f^{-1}(P)$ is a projective variety.

Proposition 3.5 *Any regular function on a projective variety is constant. Any morphism of a projective variety X to an affine variety sends X to a point.*

Proof. The second statement clearly follows from the first one. A regular function gives rise to a morphism $f : X \to \mathbf{P}^1_k$ whose image does not contain the point at infinity. Hence $f(X) \neq \mathbf{P}^1_k$ is a union of finitely many points. Since X is irreducible, $f(X)$ is just one point. QED

4 Local geometry

4.1 Localization, local rings, DVR

Let R be a ring. A subset $S \subset R$ is called *multiplicative* if it is closed under multiplication and contains 1. The *localization* $S^{-1}R$ of R with respect to S is defined as the set of formal fractions $\frac{a}{b}$, with $a \in R$ and $b \in S$, up to the equivalence relation: $\frac{a}{b} = \frac{a_1}{b_1}$ iff $(ab_1 - a_1 b)s = 0$ for some $s \in S$. When R has no zero divisors, the natural map $a \mapsto \frac{a}{1}$ is an injective homomorphism of rings, so that we can think of R as a subset of $S^{-1}R$. Then $S^{-1}R$ is simply the fractions with "restricted denominators". Note that if $I \subset R$ is an ideal, then $S^{-1}I$ is an ideal in $S^{-1}R$.

Exercise. A localization of a Noetherian ring is Noetherian.

Examples. (1) If $S = R \setminus \{0\}$, then $S^{-1}R$ is just the field of fractions.

(2) Let $P \subset R$ be a prime ideal, then $S = R \setminus P$ is a multiplicative system. Then $S^{-1}R$ is denoted R_P and is called *the localization of R at P*. The ring R_P has a very important property: $S^{-1}P$ is its only maximal ideal (every element not in $S^{-1}P$ is by definition invertible, hence $S^{-1}P$ contains all other ideals). Such rings have a name.

Definition. Rings with just one maximal ideal are called *local rings*.

Examples: (a) rational numbers such that p does not divide the denominator,

(b) p-adic integers $\mathbf{Z}_p$,

(c) rational functions in one variable over a field k such that the denominator does not vanish at 0,

(d) formal power series $k[[T]]$,

(e) rational functions in two variables such that the denominator does not vanish at $(0,0)$.

In all these examples, except the last one, the maximal ideal is principal. Such ring forms the simplest class of local rings.

Definition. A local ring whose maximal ideal is principal is called a *discrete valuation ring* (DVR).

Definition. Any generator of the maximal ideal of a DVR is called a *uniformizer* or a *local parameter*.

Lemma 4.1 *Let R be a Noetherian integral domain, $t \in R \setminus R^*$. Then $\cap_{i=1}^{\infty}(t^i) = 0$.*

Proof. ([Reid, UCA], 8.3) For contradiction let $x \neq 0$ be contained in (t^i), for any $i \geq 1$. We write $x = t^i x_i$, then $(x) \subset (x_1) \subset (x_2) \subset \dots$ is an ascending chain of ideals. Then $(x_{i+1}) = (x_i) = (tx_{i+1})$ for some i. Hence $x_{i+1} = tax_{i+1}$, but this implies $t \in R^*$ since $x_{i+1} \neq 0$ and R is an integral domain. Contradiction. QED

Proposition 4.2 *Let R be a DVR with maximal ideal $m = (\pi)$ and the field of fractions K. Then*

(1) *there exists a discrete valuation on K defined by R, that is, a homomorphism $v : K^* \to \mathbf{Z}$ such that $v(x+y) \geq min\{v(x), v(y)\}$, and $R \setminus \{0\} = \{x \in K^* | v(x) \geq 0\}$, $m \setminus \{0\} = \{x \in K^* | v(x) \geq 1\}$.*

(2) *All non-zero ideals of R are principal ideals $m^i = (\pi^i)$, $i \geq 1$.*

Proof. (1) By the previous lemma every $x \in R$, $x \neq 0$, is in $m^i \setminus m^{i+1}$ for some $i \geq 0$. Then $x = \pi^i u$, where $u \in R$ must be a unit. We also write $y = \pi^j u'$ with $u' \in R^*$. Then $xy = \pi^{i+j} uu'$, hence $v(xy) = v(x) + v(y)$. Suppose that $i \leq j$, then $x + y = \pi^i(u + \pi^{j-i}u')$, hence $v(x+y) \geq v(x) = min\{v(x), v(y)\}$. We now can extend v to K^* by the formula $v(x/y) = v(x) - v(y)$. The remaining properties are clear.

(2) Let s be the infinum of v on the ideal $I \subset R$, then there exists $x \in I$ such that $v(x) = s$. Then $m^s = (x) \subset I$. On the other hand, $v(I \setminus \{0\}) \subset \{s, s+1, \dots\}$, and $m^s \setminus \{0\} = \{x \in K^* | v(x) \geq s\}$, hence $I \subset m^s$. All in all we have $I = m^s$. QED

Observe that (1) implies that $R^* = \{x \in K^* | v(x) = 0\}$.

A DVR, like any other PID, is a UFD (note my excellent style).

Exercise. Prove that any DVR is normal (=integrally closed in its field of fractions).

The local ring of a subvariety. Let $X \subset \mathbf{P}^n_k$ be a variety, and $Y \subset X$ a subvariety. We define the local ring $\mathcal{O}_Y$ of X at Y as the subring of $k(X)$ consisting of the rational functions that are regular on an open set with a non-trivial intersection with Y. It is easy to check the ring axioms. An ideal $m_Y \subset \mathcal{O}_Y$ consisting of functions vanishing on Y is maximal since $\mathcal{O}_Y/m_Y$ is the field $k(Y)$. Any function in $\mathcal{O}_Y \setminus m_Y$ is invertible in $\mathcal{O}_Y$, so that m_Y is the unique maximal ideal. Thus $\mathcal{O}_Y$ is a local ring.

Let $U \subset X$ be an affine open subset of X. Then $\mathcal{O}_Y$ is the localization of $k[U]$ at the prime ideal $I(Y \cap U)$ (i.e. we divide by the functions that do not vanish on Y).

4.2 Regular local rings

Definition 4.3 *A Noetherian local ring R with maximal ideal m and residue field k is regular if the Krull dimension of R is $dim_k(m/m^2)$.*

Key example. It follows from Proposition 2.9, Theorem 2.12 and Theorem 2.16 that if P is a smooth point of X, then $\mathcal{O}_P$ is a regular local ring.

A theorem of Auslander and Buchsbaum says that a regular local ring is a UFD ([Matsumura], 20.3). A very important corollary is

Theorem 4.4 *The local ring of a smooth point of an algebraic variety is a UFD.*

See Appendix A.2 for a sketch of proof of this theorem.

Exercise. Let X be a curve in $\mathbf{P}^2_k$, and $P \in X$ a smooth point. Here is a low level proof that $\mathcal{O}_P$ is a DVR (and hence also a UFD). The question being local we can assume that $X \subset \mathbf{A}^2_k$, $P = (0,0)$. To fix ideas suppose that $T_{X,P}$ is the line $y = 0$. Then X is given by

$$y + \sum_{i+j \geq 2} a_{ij} x^i y^j = 0.$$

The maximal ideal $m_P \subset \mathcal{O}_P$ is $m_P = (x, y)$. All we need to do is to show that it is principal. I claim that $m_P = (x)$. Indeed, on X we have

$$y = -x \frac{\sum_{i+j \geq 2, i \geq 1} a_{ij} x^{i-1} y^j}{1 + \sum_{j \geq 2} a_{0j} y^{j-1}},$$

and the fraction is regular at P, that is, belongs to $\mathcal{O}_P$. Hence $y \in (x)$.

4.3 Geometric consequences of unique factorization in $\mathcal{O}_P$

The following statement is a generalization of Corollary 2.11.

Theorem 4.5 *In a sufficiently small neighbourhood of a smooth point any subvariety of codimension 1 can be given by one equation.*

Proof. Let P be a smooth point of X contained in a subvariety $Y \subset X$ of codimension 1. Replacing X by a neighbourhood of P we can assume that X is affine with coordinate ring $k[X]$. Choose a non-zero element $f \in I(Y) \subset k[X]$. Now $\mathcal{O}_P \subset k(X)$ is a UFD by Theorem 4.4, so that f is a product of prime factors $f = f_1 \dots f_r$, $f_i \in \mathcal{O}_P$. By further shrinking X we can assume that $f_i \in k[X]$, $i = 1, \dots, r$. We have

$$Y = (Y \cap \{f_1 = 0\}) \cup \dots \cup (Y \cap \{f_r = 0\}).$$

Y is irreducible hence $Y = Y \cap \{f_i = 0\}$ for some i. Replacing f by this f_i we can assume without loss of generality that f is a prime element of $\mathcal{O}_P$.

Consider the closed subset $Z = Z(f) \subset X$. By Theorem 2.13 the codimension of Z is 1. Now Proposition 2.10 implies that Y is an irreducible component of Z, so that we can write $Z = Y \cup Y'$, where Y' is the union of irreducible components of Z other than Y. If $P \notin Y'$ we replace X by a small affine neighbourhood of P that does not intersect with Y'. Then $Y = Z(f)$. Let us show that f is an equation of Y, that is, the ideal $I(Y)$ is generated by f. (Recall that we shrinked X a several times by now, so that f does not have to be a global equation of Y in the original X). Indeed, let $g \in I(Y) = I(Z(f))$. By the Nullstellensatz there exists a positive integer m such that g^m is divisible by f in $k[X]$. Then the same thing is also true in $\mathcal{O}_P$. Since $\mathcal{O}_P$ is a UFD we conclude that g is divisible by f.

It remains to exclude the possibility that $P \in Y'$. Choose $h \in I(Y) \setminus I(Y')$, $h' \in I(Y') \setminus I(Y)$, then $hh' \in I(Z)$ whereas $h, h' \notin I(Z)$. By the Nullstellensatz there exists a positive integer n such that $(hh')^n$ is divisible by f in $k[X]$. Then the same thing is also true in $\mathcal{O}_P$. Since $\mathcal{O}_P$ is a UFD we conclude that h or h' is divisible by f, hence vanishes on Z. Contradiction. QED

Corollary 4.6 *Let X be a smooth variety. Then the local ring of a subvariety $Y \subset X$ of codimension 1 is a DVR.*

Proof. The maximal ideal $m_Y \subset \mathcal{O}_Y$ is generated by any local equation of Y in X, which exists by the previous theorem. Hence m_Y is principal which means that $\mathcal{O}_Y$ is a DVR. QED

Recall that a rational map is regular on a non-empty open set. For smooth projective varieties there is a better result:

Corollary 4.7 *A rational map of smooth projective varieties is regular away from a closed subset of codimension at least 2.*

Proof. Without loss of generality we assume that the target space is $\mathbf{P}^n_k$. So let $f : X - - > \mathbf{P}^n_k$ be a rational map. There exist a dense open set $U \subset X$ such that f restricted to U is regular, and U is maximal with this property. Suppose that $Z \subset X$ is a subvariety of codimension 1 contained in $X \setminus U$. Write $f = (f_0, \ldots, f_n)$, where $f_i \in k(X)$. Multiplying all the f_i by a common multiple does not change f. We can choose this common multiple so that all the f_i are in the DVR $\mathcal{O}_Z$ and have no common factor. Then at least one f_i is not divisible by the generator of the maximal ideal of $\mathcal{O}_Z$, hence is non-zero at some point of Z. Therefore, $f = (f_0, \ldots, f_n)$ is regular on an open set which has a non-trivial intersection with Z. This contradicts the fact that U is the largest open set on which f is regular. QED

Corollary 4.8 *Any rational map from a smooth and projective curve to a projective variety is a morphism.*

Corollary 4.9 *A birational map between smooth and projective curves is an isomorphism.*

Hence birationally equivalent smooth projective curves are isomorphic. The same is very far from being true in higher dimensions (there are many examples, e.g. the projection $\mathbf{P}^2_k - - > \mathbf{P}^1_k$ from a point $(0:0:1)$ given by $(x_0 : x_1 : x_2) \mapsto (x_0 : x_1)$, or the stereographic projection of a quadric). The smoothness assumption is also very important. Indeed, let C be the image of the morphism $f : \mathbf{P}^1_k \to \mathbf{P}^2_k$ defined by $(x_0 : x_1) \mapsto (x_0^3 : x_0 x_1^2 : x_1^3)$. Then $f : \mathbf{P}^1_k \to C$ is a birational map, but C is not isomorphic to $\mathbf{P}^1_k$ (C contains a singular point $(1:0:0)$, whereas $\mathbf{P}^1_k$ is smooth).

5 Divisors

5.1 The Picard group

Let X be a smooth variety. Let $\mathrm{Div}(X) = \{\sum_Y n_Y Y\}$ be the free abelian group generated by all subvarieties of codimension 1 $Y \subset X$. The elements of $\mathrm{Div}(X)$ are called *divisors*. Divisors of the form Y, where $Y \subset X$ is a subvariety of codimension 1, are called irreducible. A divisor is called

effective if all the coefficients $n_Y \geq 0$, and at least one coefficient is positive. Then one writes $\sum_Y n_Y Y > 0$. The union of the subvarieties Y such that $n_Y \neq 0$ is called the *support* of $\sum_Y n_Y$.

Corollary 4.6 allows us to define the divisor of a rational function $f \in k(X)^*$ as

$$div(f) = \sum_{codim(Y)=1} val_Y(f).Y,$$

where $val_Y : k(X)^* \to \mathbf{Z}$ is the valuation attached to the irreducible divisor $Y \subset X$. The following lemma shows that this sum is finite.

Lemma 5.1 *Let $f \in k(X)^*$. For almost all subvarieties $Y \subset X$ of codimension 1 we have $val_Y(f) = 0$.*

Proof. Let U be a dense open set where f is regular, and U' be a dense open set where f^{-1} is regular. Then $f \in \mathcal{O}_Y^*$ for any subvariety $Y \subset X$ of codimension 1 that has a non-empty intersection with $U \cap U'$. Hence if $val_Y(f) \neq 0$, then Y is one of the finitely many irreducible components of $X \setminus (U \cap U')$ of codimension 1. QED

The divisors of rational functions are called *principal*.

Proposition 5.2 *Let $f \in k(X)^*$ be such that $div(f) = 0$. Then f is regular on X.*

Proof. Let $P \in X$ be a point where f is not regular. Since $\mathcal{O}_P$ is a UFD we can write $f = u f_1^{i_1} \dots f_n^{i_n}$, where $u \in \mathcal{O}_P^*$, and the f_i are irreducible elements. Since f is not regular at P we must have $i_s < 0$ for some s. But f_s comes from a regular function on some afffine open neighbourhood U of P. Let $Y \subset U$ be given by $f_s = 0$. Its Zariski closure is a subvariety of X of codimension 1 (cf. Theorem 2.13). But then $val_Y(f) = n_s < 0$ contrary to our assumption. QED

Corollary 5.3 *Let X be a smooth and projective variety. Then a rational function is determined by its divisor up to a constant.*

Proof. The ratio of two functions with the same divisor is regular by Proposition 5.2. But Proposition 3.5 says that any regular function on a projective variety is a constant. QED

Definition. The group of classes of divisors modulo principal divisors is called the *Picard group* of the variety X, and is denoted by $\mathrm{Pic}(X)$.

Remark. For a smooth and projective variety X there is an exact sequence of abelian groups

$$1 \to k^* \to k(X)^* \to \mathrm{Div}(X) \to \mathrm{Pic}(X) \to 0.$$

The words 'exact sequence' mean that the kernel of each homomorphism is the image of the previous one.

Remark. Note the analogy with the construction of the class group $\mathrm{Cl}(K)$ of a number field K. In that case we have an exact sequence

$$1 \to O_K^* \to K^* \to \mathrm{Frac}(K) \to \mathrm{Cl}(K) \to 0,$$

where $\mathrm{Frac}(K)$ is the group of fractional ideals of K with respect to multiplication.

The Picard group contains a lot of information about X.

Examples. $\mathrm{Pic}(\mathbf{A}_k^n) = 0$.
$\mathrm{Pic}(\mathbf{P}_k^n) = \mathbf{Z}$ is generated by the class of a hyperplane.
$\mathrm{Pic}(\mathbf{P}_k^{n_1} \times \ldots \times \mathbf{P}_k^{n_m}) = \mathbf{Z}^m$.
$\mathrm{Pic}(\mathbf{P}_k^2 \setminus C) = \mathbf{Z}/d$ where C is a curve of degree d.
The Picard group of a smooth cubic surface is isomorphic to $\mathbf{Z}^7$ (and is generated by 27 lines on it, cf. [Reid, UAG], Ch. 3).

Functoriality of the Picard group. Associating the abelian group $\mathrm{Pic}(X)$ to a smooth variety X is a natural construction in the sense that to any morphism $f : X \to Y$ there corresponds a homomorphism $f^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$. This f^* is functorial: if $g : Y \to Z$ is another morphism, then $(gf)^* = f^*g^*$. We only outline the construction of f^* for smooth and projective curves. See Appendix B.2 for a sketch of a more complicated definition of f^* in the case of varieties of arbitrary dimension.

Consider a surjective morphism $f : X \to Y$ of smooth and projective curves. We know by Corollary 4.6 that the local ring at any point of X or Y is a DVR. This makes it possible to define the *inverse image* homomorphism $f^* : \mathrm{Div}(Y) \to \mathrm{Div}(X)$ as follows. Let $P \in Y$, $Q \in X$ such that $f(Q) = P$. Then we have an injective homomorphism of local rings $f^* : \mathcal{O}_P \to \mathcal{O}_Q$ which allows us to think about $\mathcal{O}_P$ as a subring of $\mathcal{O}_Q$. Let u_P be the local parameter at P, and let val_Q be the valuation defined by the local ring $\mathcal{O}_Q \subset k(Y)$. We define

$$f^*(P) = \sum_{Q \in X, f(Q)=P} val_Q(u_P).Q,$$

and then extend this to $\mathrm{Div}(Y)$ by linearity. It can be checked directly that if $g \in k(Y)^*$ is a rational function, then $div(g \circ f) = f^*(div(g))$. Thus f^*

gives rise to a homomorphism of Picard groups:

$$f^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X).$$

Example. Let X be the conic in $\mathbf{P}^2_k$ given by $x_0x_1 = x_2^2$, $Y = \mathbf{P}^1_k$, and $f : X \to Y$ be given by $(x_0 : x_1 : x_2) \mapsto (x_0 : x_1)$.

Let $P = (1 : 0) \in Y$. We compute $f^*(P)$. It is clear that $f^{-1}(P) = Q = (1 : 0 : 0)$. We first check that x_2/x_0 is a local parameter at Q. Indeed, in the affine plane given by $x_0 \neq 0$ where the coordinates are $t_1 = x_1/x_0$ and $t_2 = x_2/x_0$, the equation of X is $t_1 = t_2^2$. Hence the maximal ideal of Q is $(t_1, t_2) = (t_2)$. Next, t_1 is a local parameter at P. In $k(X)$ we have $t_1 = t_2^2$, thus $val_Q(u_P) = 2$, and finally $f^*(P) = 2Q$.

Now we want to compute $f^*(R)$, where $R = (1 : 1) \in Y$. It is clear that $f^{-1}(R) = \{Q_+, Q_-\}$, where $Q_\pm = (1 : 1 : \pm 1)$. Obviously $t_1 - 1$ is a local parameter at R. Let us find a local parameter at Q_+. The maximal ideal at this point is $(t_1 - 1, t_2 - 1)$. But in $k(X)$ we have $t_1 - 1 = (t_2 - 1)(t_2 + 1)$ so that $(t_1 - 1, t_2 - 1) = (t_2 - 1) = (t_1 - 1)$ since $t_2 - 1$ is regular and invertible at Q_+. A similar computation shows that $t_1 - 1$ is also a local parameter at Q_-. Thus $val_{Q_\pm}(u_P) = 1$, hence $f^*(P) = Q_+ + Q_-$.

5.2 Automorphisms of $\mathbf{P}^n_k$ and of $\mathbf{A}^n_k$

As an application of the fact that $\mathrm{Pic}(\mathbf{P}^n_k)$ is isomorphic to $\mathbf{Z}$ we prove the following useful statement.

Proposition 5.4 *Any automorphism of $\mathbf{P}^n_k$ is given by a linear transformation of the corresponding $n+1$-dimensional vector space, so that* $\mathrm{Aut}\,\mathbf{P}^1_k = \mathrm{PGL}(n+1)$.

Proof. The group of non-degenerate matrices $\mathrm{GL}(n+1)$ acts on k^{n+1}. Lines through the origin are mapped to lines through the origin, hence $\mathrm{GL}(n+1)$ also acts on $\mathbf{P}^n_k$. The only matrices that act trivially on the lines through the origin are scalar matrices. Hence $\mathrm{PGL}(n+1) = \mathrm{GL}(n+1)/k^*$ acts faithfully on $\mathbf{P}^n_k$ (the only element acting trivially is the identity). We must show that any automorphism of $\mathbf{P}^n_k$ is of such a form.

We first consider $\mathbf{P}^1_k$. Any rational map $\mathbf{P}^1_k - - > \mathbf{P}^1_k$ is given by a bijective rational function $t \mapsto f(t)$. Then $f(t) = (at + b)/(ct + d)$ for some $a, b, c, d \in k$. (It is easy to check that other rational functions are never bijective.) This morphism clearly comes from the linear transformation with matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Since $\mathrm{Pic}(\mathbf{P}^n_k) = \mathbf{Z}$ the induced morphism f^* sends a generator to a generator. Let $H \subset \mathbf{P}^n_k$ be the projective subspace of codimension 1, also called a hyperplane. We denote by $[H]$ its class in $\mathrm{Pic}(\mathbf{P}^1_k)$. The classes $[H]$ and $-[H]$ are the only classes that generate $\mathrm{Pic}(\mathbf{P}^n_k)$. But the hyperplane class $[H] \in \mathrm{Pic}(\mathbf{P}^n_k) = \mathbf{Z}$ contains effective divisors, whereas $-[H]$ does not. Hence $f^*([H]) = [H]$. Therefore the inverse image of a hyperplane is a hyperplane. Now any rational map $\mathbf{P}^n_k - - > \mathbf{P}^n_k$ is given by a collection of n rational functions $f_1, \ldots, f_n$ in the affine coordinates $t_1, \ldots, t_n$. The condition $f^*(H) = H$ says that $\sum a_i f_i = a$ defines a hyperplane for any $a, a_1, \ldots, a_n \in k$, where not all of the a_i are equal to 0. Write each f_i as a fraction in lowest terms F_i/G_i. Then, for $a, a_1, \ldots, a_n$ general enough, we get a hyperplane only if all the G_i are of degree 1 and proportional, and the F_i are of degree 1 (the details of this argument are left to the reader). This is precisely what we needed to prove. QED

Exercise. Compute $\mathrm{Aut}(\mathbf{A}^1_k)$ by proving that every automorphism of $\mathbf{A}^1_k$ extends uniquely to an automorphism of $\mathbf{P}^1_k$ which fixes the point at infinity.

Remark. In contrast, $\mathrm{Aut}(\mathbf{A}^n_k)$ for $n \geq 2$ is *very* big. Note that $(x, y) \mapsto (x, y + g(x))$, where $g(x)$ is any polynomial, is an automorphism of $\mathbf{A}^2_k$. There are also automorphisms of $\mathbf{A}^2_k$ defined by the elements of PGL(2) that preserve the line at infinity. It can be proved that these automorphisms generate the whole group. See [Shafarevich] for more details.

The Jacobian Conjecture. Let $F(x, y)$, $G(x, y)$ be polynomials in x and y. When is the map $f : \mathbf{A}^2_k \to \mathbf{A}^2_k$ given by $(x, y) \mapsto (F(x, y), G(x, y))$ an automorphism of the affine plane?

Consider the Jacobian matrix

$$J(f) = \begin{pmatrix} \frac{\partial F}{\partial x} & \frac{\partial F}{\partial y} \\ \frac{\partial G}{\partial x} & \frac{\partial G}{\partial y} \end{pmatrix}$$

If $g : \mathbf{A}^2_k \to \mathbf{A}^2_k$ is another polynomial map, then one checks by using the chain rule for partial differentiation that $J(fg) = J(f)J(g)$. If f is an automorphism, then we can find g such that fg is the identity map, so that $J(f)J(g)$ is the identity matrix. This implies that $det(J(f)) \cdot det(J(g)) = 1$. This says that the polynomial $det(J(f))$ is invertible in the polynomial algebra $k[x, y]$, and so must be a constant. The famous Jacobian Conjecture asserts that if $det(J(f)) \in k$, then $f \in \mathrm{Aut}(\mathbf{A}^2_k)$. Many cases of polynomials of small degree are known, but the general case of this hard conjecture remains open.

5.3 The degree of the divisor of a rational function on a projective curve

From this point on all our varieties are smooth and projective curves. For curves one defines the degree of the divisor $\sum n_P P$ as the integer $\sum n_P$. It is clear that this produces a surjective homomorphism $deg : \mathrm{Div}(X) \to \mathbf{Z}$ which sends any point to 1.

Lemma 5.5 *Let $f : X \to Y$ be a surjective morphism of curves. Then $k(X)$ is a finite extension of $k(Y)$.*

The proof is omitted. The number $[k(X) : k(Y)] = dim_{k(Y)}k(X)$ is called the *degree* of f, and is denoted by $deg(f)$. A sketch of proof of the following theorem can be found in Appendix B.1.

Theorem 5.6 *Let $f : X \to Y$ be a surjective morphism of smooth and projective curves. Then the degree of the divisor $f^*(P)$ equals $deg(f)$, for any $P \in Y$.*

In the notation of the example in the end of Subsection 5.1 we have $deg(f^*(P)) = deg(2Q) = 2$, $deg(f^*(R)) = deg(Q_+ + Q_-) = 2$. This agrees with the fact that the degree of the map f in that example is 2: indeed, $k(X) = k(\sqrt{t_1})$ is a quadratic extension of $k(Y) = k(t_1)$.

Corollary 5.7 *The degree of the divisor of a non-zero rational function on a smooth projective curve is zero.*

Proof. If f is constant there is nothing to prove. By Corollary 4.8 any rational non-constant function $f \in k(X)^*$ gives rise to a dominant morphism $f : X \to \mathbf{P}^1_k$. Since X is projective, $f(X)$ is closed, hence $f(X) = \mathbf{P}^1_k$. A comparison of definitions shows that the divisor $div(f)$ equals $f^*(0) - f^*(\infty)$. By Theorem 5.6 $deg(f^*(0))$ and $deg(f^*(\infty))$ both equal to $deg(f)$, hence $deg(div(f)) = 0$. QED

Due to Corollary 5.7 deg descends to a surjective homomorphism $deg : \mathrm{Pic}(X) \to \mathbf{Z}$. Define $\mathrm{Pic}^0(X)$ as the kernel of deg.

Proposition 5.8 *Let X be a smooth and projective curve.*
(i) The divisor $P - Q$ is principal for some $P \neq Q$ if and only if $X = \mathbf{P}^1_k$.
(ii) $\mathrm{Pic}^0(X) = 0$ if and only if $X = \mathbf{P}^1_k$.

Proof. We already know that $\mathrm{Pic}(\mathbf{P}^1_k) = \mathbf{Z}$ is generated by the class of a point. Hence *deg* is an isomorphism in this case, so that $\mathrm{Pic}^0(\mathbf{P}^1_k) = 0$.

To prove (i) let $P \neq Q$ be points on X such that $P - Q = div(f)$. As in the proof of Corollary 5.7 f defines a morphism $f : X \to \mathbf{P}^1_k$. If we write $div(f) = f^*(0) - f^*(\infty)$, then the divisors $f^*(\infty)$ and $f^*(0)$ are effective and disjoint. This implies that $f^*(0) = P$. By Theorem 5.6 the degree of the morphism f is 1, hence f is birational, hence is an isomorphism (Corollary 4.9).

The degree of $P - Q$ is 0. Thus (ii) follows from (i). QED

Among the plane curves this proposition applies to lines and conics.

5.4 Bezout theorem for curves

Let $X \subset \mathbf{P}^n_k$ be a smooth curve, and let F be a homogeneous form in $n+1$ variables not vanishing identically on X. Cover X by open subsets $U_i = X \cap \{G_i \neq 0\}$, where $deg(G_i) = deg(F)$. Then F/G_i is a regular function on U_i. We define the divisor of F by the formula

$$div(F) = \sum_{P \in X} val_P(F/G_i).P,$$

where in the term corresponding to P we take any G_i such that $P \in U_i$, or equivalently, $G_i(P) \neq 0$. The definition does not depend on what U_i we choose for a given point P, because G_i/G_j is an invertible rational function on $U_i \cap U_j$, so that for $P \in U_i \cap U_j$ we have $val_P(F/G_i) = val_P(F/G_j)$. Similarly, one shows that another family of G_i's produces the same divisor $div(F)$.

Definition. The *intersection index* $(X.F)$ is the degree of $div(F)$.

Since the function F/G_i is regular on U_i we see from the definition that $div(F) \geq 0$, therefore $(X.F) \geq 0$. The intersection index counts the number of intersection points of X with the hypersurface $F = 0$ with 'correct multiplicities'.

Definition. The degree of X in $\mathbf{P}^n_k$, denoted by $deg(X)$, is the intersection index of X with the hyperplane.

Of course, we need to show that this definition makes sense, that is, it does not matter which hyperplane we take.

Theorem 5.9 (Bezout) *The intersection index $(X.F)$ depends only on X and the degree of F. We have $(X.F) = deg(X)deg(F)$.*

Proof. If F' is another form of the same degree, then $div(F) - div(F')$ is clearly the divisor of the rational function F/F'. Thus $(X.F) = (X.F')$ since by Corollary 5.7 $deg(div(F/F')) = 0$. This shows that the intersection index depends only on $deg(F)$ and not F itself. To compute $(X.F)$ we can now replace F by any other form of the same degree, for example by $H^{deg(F)}$, where H is linear. This proves the second statement. QED

Exercise. Let $X \subset \mathbf{P}^2_k$ be a plane curve, $P \in X$ be a smooth point, and $L \subset \mathbf{P}^2_k$ be a line passing through P. Let $div(L)$ be the divisor on X given by a linear form defining L.

1. Show that the multiplicity of P in $div(L)$ is 1 if and only if L is not the tangent line to X at P. Solution: This question is local. Assume that $P = (0,0) \in X \subset \mathbf{A}^2_k$, then X is given by $0 = ax + by +$ terms of higher degree in x and y. Since P is smooth, a and b are not both 0. To fix ideas assume that $b \neq 0$. Then x is a local parameter at P. Indeed, the maximal ideal of $\mathcal{O}_P$ is (x, y), but modulo the equation of X we can write y as the product of x and a rational function that is regular at P. Hence $m_P = (x)$. If $L = \mu x + \nu y$, then $L = (\mu - \frac{a}{b}\nu)x +$terms of degree at least 2 in x. Therefore, if L' is a linear form such that $L'(P) \neq 0$, then $val_P(L/L') = 1$ if and only if $b\mu - a\nu \neq 0$, that is, when the vectors (a, b) and (μ, ν) are not proportional. On the other hand, $T_{X,P}$ is given by $ax + by = 0$.

2. The set of lines in $\mathbf{P}^2_k$ has a natural structure of the projective variety $\mathbf{P}^2_k$. Show that the map $P \mapsto T_{X,P}$ defines a rational map $f : X - - > \mathbf{P}^2_k$ (called the Gauss map). Conclude that $dim(f(X)) = 1$.

3. By comparing the dimensions we see that $\mathbf{P}^2_k \setminus f(X) \neq \emptyset$. Thus there are infinitely many lines L such that $div(L)$ is the sum of distinct points taken with multiplicity 1. (Recall that k is algebraically closed hence infinite.)

Therefore, $deg(X)$ *equals the maximal number of points in the intersection* $X \cap L$. This is also true for the curves in $\mathbf{P}^n_k$, where we need to replace lines by hyperplanes. See [Shafarevich] for details. For plane curves, however, we can also say that $deg(X)$ equals the degree of the form by which X is defined. Since a curve in $\mathbf{P}^n_k$ is defined by two or more forms, this property has no higher dimensional analogue. (Warning: two forms may not be enough to define a curve in $\mathbf{P}^3_k$! An example is provided by the rational normal cubic curve, that is, the image of $\mathbf{P}^1_k$ under the map $(x : y) \mapsto (x^3 : x^2y : xy^2 : y^3)$.)

Exercise. Let $X \subset \mathbf{P}^2_k$ be a plane curve, $P \in X$ be a smooth point. Let $L \subset \mathbf{P}^2_k$ be the tangent line to X at P. Show that the multiplicity of P in $div(L)$ is 2 if and only if the Hessian matrix of X at P is non-degenerate. The

Hessian matrix of the curve given by $f(x_0, x_1, x_2) = 0$ is defined as follows:

$$H(f) = \begin{pmatrix} \frac{\partial^2 f}{\partial x_0^2} & \frac{\partial^2 f}{\partial x_0 \partial x_1} & \frac{\partial^2 f}{\partial x_0 \partial x_2} \\ \frac{\partial^2 f}{\partial x_1 \partial x_0} & \frac{\partial^2 f}{\partial x_1^2} & \frac{\partial^2 f}{\partial x_1 \partial x_2} \\ \frac{\partial^2 f}{\partial x_2 \partial x_0} & \frac{\partial^2 f}{\partial x_2 \partial x_1} & \frac{\partial^2 f}{\partial x_2^2} \end{pmatrix}$$

Solution ($\mathrm{char}(k) \neq 2$): The question is local. Assume that $P = (0,0) \in X \subset \mathbf{A}_k^2$ and that L is given by $y = 0$. Then X is given by $0 = y + ax^2 + bxy + cy^2 +$ terms of higher degree in x and y. As in the previous example one shows that x is a local parameter at P. A direct computation shows that the Hessian of f at P is non-degenerate if and only if $a \neq 0$. On the other hand, y can be written as the product of the polynomial in one variable $ax^2 +$terms of higher degree in x, and a rational function that is regular at P.)

We define $deg(X)$, where X is a reducible curve, as the sum of the degrees of components. We then extend the Bezout theorem to reducible curves X, and get the same formula $(X.F) = deg(X)deg(F)$. Note that $(X.F)$ is only defined when F does not vanish identically on some component of X.

In the case of plane curves the Bezout theorem says that the number of common points of two (possibly reducible) curves without common components is the product of their degrees, provided we count points with correct multiplicities. As an illustration of this we now prove Pascal's mysterious theorem.

Theorem 5.10 (Pascal) *Let $C \subset \mathbf{P}_k^2$ be a conic. For any six distinct points of C consider the hexagon with vertices in these points. Then the common points of the three pairs of opposite lines of the hexagon are collinear.*

Proof. (Plücker) Let the sides of the hexagon be $l_1, m_2, l_3, m_1, l_2, m_3$ in this order. We denote their equations by the same letters. Then $Q_x = l_1 l_2 l_3 + x m_1 m_2 m_3$ is a cubic form that depends on the parameter $x \in k$. We observe that for any x this cubic passes through the six vertices of the hexagon. Let $P \in C$ be a point different from these six points. Then $l_i(P) \neq 0$, $m_i(P) \neq 0$ for $i = 1, 2, 3$, as no line contains more than two points of a conic. Thus we can find $x \in k$ such that $Q_x(P) = 0$. Write $Q = Q_x$. Either C is a component of Q, or it isn't. In the second case by the Bezout theorem $C \cap Q$ consists of at most six points, but there are visibly seven points in this intersection. Hence the cubic form defining Q is a product of the quadratic form defining C and some linear form L. Let $A_i = l_i \cap m_i$, $i = 1, 2, 3$. Since a line intersects a conic in at most two points, we have $A_i \notin C$. On the other hand, $A_i \in Q$, hence these points must be in L. QED

Let $X \subset \mathbf{P}^2_k$ be a smooth curve of degree d given by $f = 0$. A point $P \in X$ is a called a *flex* if the tangent line $T_{X,P}$ intersects X in P with multiplicity at least 3. We have seen that P is a flex of X if and only P belongs to the closed set given by $det(H(f)) = 0$, called the Hessian H_X of X. It can be shown that if $d \geq 3$, then the Hessian H_X is a curve of degree $3(n-2)$. By applying the Bezout theorem we see that every curve of degree at least 3 has a flex, and at most $3n(n-2)$ of them. (Check that X is not a component of H_X.)

We now study smooth plane cubics $X \subset \mathbf{P}^2_k$ in some more detail.

Exercise. ($\mathrm{char}(k) \neq 2, 3$) Choose a flex P on smooth plane cubic X. Suppose that $P = (0 : 1 : 0)$, and $T_{X,P}$ has the equation $z = 0$. Show that X is then given by the affine equation $y^2 + axy = f(x)$, where $f(x)$ is a polynomial in x of degree 3. Now show how to reduce to the equation $y^2z = x^3 + axz^2 + bz^3$.

Let us consider $\mathrm{Pic}^0(X)$ where X is a smooth plane cubic. In the following proposition we do not assume that k is algebraically closed.

Proposition 5.11 *Let X be a smooth cubic curve in $\mathbf{P}^2_k$ with a k-point P_0. Then the map $P \mapsto P - P_0$ is a bijection from the set of k-points $X(k)$ to* $\mathrm{Pic}^0(X)$.

Proof. By virtue of example (e) in Subsection 3.1 X is not isomorphic to $\mathbf{P}^1_k$. (Note that the previous exercise shows how to reduce the equation of X to $y^2z = x^3 + axz^2 + bz^3$, at least when k is algebraically closed.) By Proposition 5.8 (i) the divisor $P - P_0$ is never equivalent to 0 for $P \neq P_0$. This proves injectivity. To prove surjectivity use secants and tangents to decrease the number of points in the support of the divisor. QED

For any smooth and projective curve X it can be proved that $\mathrm{Pic}^0(X)$ is isomorphic to the group of k-points on the so called Jacobian variety of X.

Further exercises: Directly prove the associativity of the group law on a cubic curve.

5.5 Riemann–Roch theorem

Definition. Let X be a smooth projective curve, $D \in \mathrm{Div}(X)$. The space of functions associated with D is the subset $L(D) \subset k(X)$ consisting of 0 and rational functions f such that $div(f) + D \geq 0$ (that is, is 0 or an effective divisor).

Note that any function $f \in L(D)$ is regular away from the support of D.

Proposition 5.12 *Let D be a divisor on a smooth and projective curve X.*

(i) Let $g \in k(X)^*$. Then the map $f \mapsto f/g$ identifies $L(D)$ with $L(D + div(g))$.

(ii) $L(D) = 0$ if $deg(D) < 0$.

(iii) $L(0) = k$.

(iv) $L(D)$ is a vector space of dimension at most $deg(D) + 1$.

Proof. (i) is obvious.

(ii) follows from Corollary 5.7 and the trivial observation that an effective divisor has positive degree.

(iii) reflects the fact that $div(f) = 0$ implies that f is a constant function.

(iv) Let $D = \sum_P n_P P$. Then $f \in L(D)$ if and only if $val_P(f) \geq -n_P$. The ultrametric inequality (Proposition 4.2) shows that $L(D)$ is closed under addition; and $L(D)$ is obviously closed under multiplication by constants.

Now we prove $dim(L(D)) \leq deg(D) + 1$ for all D of non-negative degree by induction on $deg(D)$. Because of (i) we can assume that D is effective or zero. In the last case we conclude by (ii). Now D is effective, hence of positive degree. Suppose that the inequality is proved for all divisors of degree at most $deg(D) - 1$. We can write $D = n_Q Q + \sum_{P \neq Q} n_P P$ where $n_Q > 0$ and $n_P \geq 0$. Then $D' = D - Q \geq 0$, and $L(D') \subset L(D)$. It suffices to show that the codimension of $L(D')$ in $L(D)$ is 0 or 1. Choose a local parameter u_Q at Q. Then it is immediate from the definition of $L(D)$ that $f u_Q^{n_Q}$ is regular at Q. Consider the linear form on $L(D)$ given by the value of $f u_Q^{n_Q}$ at Q. The set of zeros of this form is precisely $L(D')$, hence the codimension of this subspace is at most 1. Now we use the inductive assumption to finish the proof. QED

Let $\ell(D) = dim(L(D))$.

Exercise. If the curve is $\mathbf{P}^1_k$, then $\ell(D) = deg(D) + 1$ if $deg(D) \geq 0$, and $\ell(D) = 0$ otherwise. To show this it is enough to assume that $D = n(\infty)$. In this case $L(D)$ is the space of polynomials of degree at most n in x, where x is the coordinate on $\mathbf{A}^1_k = \mathbf{P}^1_k \setminus \infty$.

Exercise. If the curve X is not isomorphic to $\mathbf{P}^1_k$, then $\ell(D) \leq deg(D)$. Hint: combine the proof of (iv) above with Proposition 5.8 (i).

The Riemann–Roch theorem is the following formula:

$$\ell(D) - \ell(K - D) = deg(D) - g + 1.$$

Here K is the canonical class, defined as the class of the divisor of any differential form on X, and g is the genus of X, defined as $g = \ell(K)$. By letting $D = K$ we see that $deg(K) = 2g - 2$. If $deg(D) > 2g - 2$, then the

degree of $K - D$ is negative implying that $\ell(K - D) = 0$, so that in this case we have $\ell(D) = deg(D) - g + 1$. In general, we only have Riemann's inequality $\ell(D) \geq deg(D) - g + 1$.

The main reason to introduce $L(D)$ is that this is a nice way to build morphisms $f : X \to \mathbf{P}^n_k$, where $n = \ell(D) - 1$. Indeed, let D be an effective divisor on X, and let $1, f_1, \ldots, f_n$ be a basis of $L(D)$. Consider the rational map f which sends $P \in X$ to the point $(1 : f_1(P) : \ldots : f_n(P))$. It is actually a morphism, as is any rational map from a smooth and projective curve to a projective space.

Exercise. Let H be a hyperplane in $\mathbf{P}^n_k$. Show that $deg(f^*(H)) = deg(D)$. In particular, if f is injective, then $f(X)$ is a curve of degree $deg(D)$.

It can be shown that if $deg(D) > 2g$, then f is an embedding, that is, f defines an isomorphism of X with its image $f(X)$.

5.6 From algebraic curves to error correcting codes

In this subsection k is a finite field. Recall that if p is the characteristic of k, then k has p^s elements for some $s > 0$. (Indeed, k contains $\mathbf{F}_p$, and is a vector space over it.)

The vector space k^n is turned into a metric space with the Hamming distance between two vectors v and v' defined as the number of coordinates where v and v' differ:

$$|v, v'| = \#\{i = 1, \ldots, n | v_i - v'_i \neq 0\}.$$

Let $D(v, r)$ be the disc of radius r with centre in $v \in k^n$. A subset $C \subset k^n$ is a code correcting at least r errors if the discs $D(v, r)$ with centres in $v \in C$ are disjoint. Then one can correct up to r errors occuring in the elements of C, called the *code words*. The number

$$dist(C) = min_{v,v' \in C, v \neq v'} |v, v'|$$

is called the *minimum distance* of C. It is easy to see that C corrects r errors if $2r + 1 \leq dist(C)$.

A *linear* code is a vector subspace $C \subset k^n$. For a linear code $dist(C)$ is simply the minimal number of non-zero coordinates of a code word.

The main problem of the theory of linear error-correcting codes is to construct codes with both $dist(C)$ and $dim(C)$ as large as possible. (Another, more practical task is to construct efficient coding and decoding algorithms, but we don't discuss this here.) There are combinatorial bounds that say that

$dist(C)$ and $dim(C)$ can't both be too big. The contribution of algebraic geometry is an explicit construction of linear codes from algebraic curves. These codes turn out to be very good (better than those provided by the randomly chosen vector subspaces) when n tends to infinity, and p^s is not too small.

Let X be a smooth and projective curve over k, and let $\{P_1, \ldots, P_n\}$ be k-rational points of X. Choose a divisor D on X of degree at most n. Assume for simplicity that the points P_i are not in the support of D. Then we can evaluate any function $f \in L(D)$ at the points $P_1, \ldots, P_n$ since f is regular at these points. The collection of values $\{f(P_1), \ldots, f(P_n)\}$ is an element of k^n. This gives a linear map

$$ev : L(D) \to k^n.$$

Let $C = ev(L(D))$.

Theorem 5.13 *We have $dim(C) \geq deg(D) - g + 1$ and $dist(C) \geq n - deg(D)$.*

Proof. We have

$$dim(C) = dim(L(D)) - dim(L(D - \sum_{i=1}^{n} P_i)) = \ell(D) - \ell(D - \sum_{i=1}^{n} P_i).$$

Since $deg(D) < n$ the second term is 0, and so the Riemann-Roch theorem gives the first inequality. By Corollary 5.7 the degree of $div(f)$ is 0. Hence the degree of the divisor of zeros of f outside the support of D is at most $deg(D)$. In particular, a non-zero code word has at least $n - deg(D)$ non-zero coordinates. Thus we obtain the second inequality. QED

Exercise. Work out C in the case when $X = \mathbf{P}^1_k$, $P_1, \ldots, P_n$, $n = p^s$, are the k-points in $\mathbf{A}^1_k \subset \mathbf{P}^1_k$, and $D = d\infty$, $0 < d < n$. In this way we get Reed–Solomon codes (much used in practice).

A More algebra

A.1 Krull's intersection theorem

The proof of the following general property of Noetherian rings uses primary decomposition of ideals ([Lang], VI.5, [Reid, UCA], 7).

Lemma A.1 (Krull's intersection theorem) *Let R be a Noetherian integral domain with an ideal m. Then $\cap_{i=1}^{\infty} m^i = 0$.*

Proof. Let $M = \cap_{i=1}^{\infty} m^i$. This is an ideal in R, and hence has a finite basis, say, $\mu_1, \dots, \mu_n$. It is clear that $m.M \subset M$. We claim that we also have $M \subset m.M$. Let us assume this and show how to conclude the proof. We can write $\mu_i = \sum_{j=1}^{n} \alpha_{ij}\mu_j$ for all $i = 1, \dots, n$, where $\alpha_{ij} \in m$. Let $f(t)$ be the characteristic polynomial of the matrix (α_{ij}). Then $f(1) \in R$ annihilates M (Hamilton–Cayley). But $f(t)$ is monic with coefficients in m, hence $f(1)$ is invertible modulo m, hence $f(1) \neq 0$. Since R is an integral domain we conclude that $M = 0$.

The proof of the claim. Here is a proof borrowed from [Van der Waerden]. We first prove that every ideal in a Noetherian ring can be represented as the intersection of finitely many *primary* ideals. (An ideal $I \subset R$ is called primary if every zero divisor in R/I is nilpotent. For example, prime ideals are primary.)

Let us call an ideal I *irreducible* if whenever $I = J_1 \cap J_2$ we have $I = J_1$ or $I = J_2$. By Noetherian induction one proves that every ideal is an intersection of finitely many irreducible ideals (the set of ideals that do not have this property contains a maximal element). Now it suffices to show that every irreducible ideal I is primary. [Otherwise we can find $a \notin I$, and $b^i \notin I$ for all i such that $ab \in I$. Let $J_i := \{x \in R | xb^i \in I\}$. The ascending chain of ideals $J_1 \subset J_2 \subset \dots$ stabilizes, say, at $J_l = J_{l+1}$. We trivially have $I \subset (a, I) \cap (b^l, I)$. Let us show that the inverse inclusion is also true. Let $x + b^l r$ be an element of this ideal, where $x \in I$. Then $bx + b^{l+1}r \in (ab, bI) \subset I$, hence $b^{l+1}r \in I$. This means that $r \in J_{l+1} = J_l$, thus $b^l r \in I$. Hence $x + b^l r \in I$. Now $I = (a, I) \cap (b^l, I)$, hence I is reducible. Contradiction.]

We write $m.M = I_1 \cap \dots \cap I_s$, where all the I_j are primary. Then for every j we have either $m^s \subset I_j$ for some s, or $M \subset I_j$. In both cases we conclude that $M \subset I_j$. Therefore $M \subset m.M$. QED

A.2 Completion

Let R be a local ring with maximal ideal m. We have a topology on R such that the ideals m^i form a base of neighbourhoods of 0 (i.e., $x \in R$ is close to

0 is x belongs to a high power of m). Let the ring $\hat{R}$ be the completion of R with respect to this topology (defined via Cauchy sequences, as usual). Then $\hat{R}$ is also a local ring, with maximal ideal $m\hat{R}$, and has the same dimension as R.

A standard example of a complete local ring is the ring of formal power series $k[[x_1, \dots, x_n]]$. It is regular of dimension n. The units of this ring are the power series with non-zero constant term.

Theorem A.2 (Weierstrass preparation theorem) *Let $F \in k[[x_1, \dots, x_n]]$ be such that the lowest non-zero homogeneous form of F contains the monomial cx_1^m, $c \neq 0$. Then $F = UG$, where $U \in k[[x_1, \dots, x_n]]^*$ and G is a monic polynomial in x_1 of degree m over $k[[x_2, \dots, x_n]]$.*

It can be deduced form this result (by induction in n) that $k[[x_1, \dots, x_n]]$ is a UFD.

Note by the way that there is not much variety of complete local rings of geometric origin. This is shown by the following result, which shall not be used.

Theorem A.3 (Cohen structure theorem) *A complete regular local ring R of dimension n containing some field is isomorphic to $k[[x_1, \dots, x_n]]$, where k is the residue field of R.*

Idea of proof of Theorem 4.4. Let P be a smooth point of a variety X, $\mathcal{O}_P$ the local ring of P in X, and $\hat{\mathcal{O}}_P$ be the completion of $\mathcal{O}_P$. The canonical homomorphism $\mathcal{O}_P \to \hat{\mathcal{O}}_P$ is injective by Theorem A.1. It is clear that this map associates to a function its Taylor series with respect to a system of local parameters at P, that is, n functions $u_1, \dots, u_n$ such that $n = dim(X)$ and $(u_1, \dots, u_n)$ is the maximal ideal of $\mathcal{O}_P$. This also proves that $\hat{\mathcal{O}}_P = k[[x_1, \dots, x_n]]$. This is a UFD. Finally, it can be deduced from here that $\mathcal{O}_P$ is also a UFD.

A.3 The topological space $Spec(R)$

Let R be a commutative ring with 1. We define the set $Spec(R)$ as the set of prime ideals of R. One endows $Spec(R)$ with the topological space structure, where a subset $Z \subset Spec(R)$ is *closed* if there is an ideal $I \subset R$ such that Z is the set of prime ideals that contain I. This identifies Z with $Spec(R/I)$. If $f : R_1 \to R_2$ is a ring homomorphism, then $f^{-1}(I)$, where $I \subset R_2$ is a prime ideal, is a prime ideal of R_1.

Exercise. Prove that this gives a continuous map of topological spaces $Spec(R_2) \to Spec(R_1)$.

Thus *Spec* is a functor from the category of rings and their homomorphisms to the category of topological spaces and their continuous maps.

Let us explore in more detail the topological space $Spec(k[X_1, \dots, X_n])$ where k is any field.

Definition. The topological space $Spec(k[X_1, \dots, X_n])$ is called the *affine space* over k, and is denoted by $\mathbf{A}^n_k$.

If $n = 0$ we obtain a one-point space $Spec(k)$, called a k-point. Let $n = 1$ and k is algebraically closed. The prime ideals of $k[X]$ (which is a principal ideal ring) are the zero ideal (0) and the principal ideals $(X - a)$, for $a \in k$. The ideals $(X - a)$ naturally correspond to the points of the usual affine line, with finite subsets as closed sets. The ideal (0) is called the generic point of $Spec(k[X])$: its closure is the whole space $Spec(k[X])$.

For $n > 1$ the situation becomes dramatically different. As for $n = 1$ we can consider k^n as the subset of $\mathbf{A}^n_k$ corresponding to maximal ideals $(X_1 - a_1, \dots, X_n - a_n) \subset k[X_1, \dots, X_n]$. Obviously the Zariski topology of k^n is induced by the topology of $\mathbf{A}^n_k$. When k is algebraically closed, then by Nullstellensatz the points of $Spec(k[X_1, \dots, X_n])$ bijectively correspond to irreducible closed subsets of k^n. Let us check when a point of $\mathbf{A}^n_k$ is closed. Let $I \subset k[X_1, \dots, X_n]$ be a prime ideal. Let $Z(J)$ be a closed set containing the point corresponding to I, where J is an ideal. Then I contains J. Hence the smallest closed subset corresponds to $I = J$, that is, $Z(I)$ is the closure of I. This means that only the maximal ideals correspond to closed points of $\mathbf{A}^n_k$, and all the other points, for example, those corresponding to principal ideals $(f(X))$, are not closed! If J is not a closed point, then the closed points of its closure correspond to maximal ideals containg J. If k is algebraically closed than this is precisely the closed subset $Z(J) \subset k^n$. The point J is called the generic point of $Z(J)$. For example, (0) is the generic point of $\mathbf{A}^n_k$.

A fundamental example of a scheme is $Spec(\mathbf{Z})$ (= (0) and (p), where p is a prime number, the closure of (0) is the whole space, other closed sets are finite unions of closed points). Note that $Spec(\mathbf{Z})$ is connected. Let us also consider $Spec(\mathbf{Z}[T])$. We have a natural continuous surjective map $Spec(\mathbf{Z}[T]) \to Spec(\mathbf{Z})$ (sending a prime ideal $I \subset \mathbf{Z}[T]$ to the prime ideal $I \cap \mathbf{Z}$). There are several kinds of prime ideals in $Spec(\mathbf{Z}[T])$: 0, then (p) and $(f(T))$, where p is a prime, and $f(T)$ is a polynomial (all these are not closed points!), and, finally, the closed points. Every closed point is located "over" a closed point of $Spec(\mathbf{Z})$, that is, over some prime p, and the quotient by the corresponding maximal ideal is a finite field $\mathbf{F}$ of characteristic p. Such an ideal of $\mathbf{Z}[T]$ can be given by $(p, f(T))$ for some polynomial $f(T) \in \mathbf{Z}[T]$, where $\mathbf{F} = \mathbf{F}_p[T]/(f(T))$. The closure of (p) is $\mathbf{A}^1_{\mathbf{F}_p}$

(the "fibre" of $Spec(\mathbf{Z}[T]) \to Spec(\mathbf{Z})$ at p). The closure of $(f(T))$ consists of $(p, g(T))$ where $g(T) \in \mathbf{Z}[T]$, considered modulo p, is an irreducible divisor of $f(T)$.

Other instructive examples are $Spec(O_k)$ where O_k is the ring of integers in a number field k. The natural map $\mathbf{Z} \to O_k$ gives rise to a surjection $Spec(O_k) \to Spec(\mathbf{Z})$. The inverse image of $(p) \in Spec(\mathbf{Z})$ consists of the prime ideals of O_k that lie over p.

Exercise: make this explicit when $k = \mathbf{Q}(\sqrt{-1})$.

Let X be a topological space. The *dimension* of X can be defined as the supremum of all integers n such that there exists a chain $Z_0 \subset Z_1 \subset \ldots \subset Z_n$ of distinct closed irreducible subsets of X. Then trivially $dim(Spec(R))$ is the Krull dimension of R.

B More geometry

B.1 Finite morphisms

We begin with defining finite morphisms of affine varieties.

Definition. A dominant morphism $f : X \to Y$ of affine varieties is called *finite* if $k[X]$ is *integral* over $f^*(k[Y]) \simeq k[Y]$.

Proposition B.1 *Let $f : X \to Y$ be a finite morphism of affine varieties, then*

(i) for any $P \in Y$ the set $f^{-1}(P)$ is finite,

(ii) f is surjective.

Proofs. (i) Coordinates of points in $f^{-1}(P)$, as elements of $k[X]$, satisfy monic polynomial equations, and hence for any values of (non-leading) coefficients have only finitely many roots.

(ii) Let $m_P \in k[Y]$ be the maximal ideal of $P \in Y$. Then $f^{-1}(P) = \emptyset$ iff $1 \in m_P k[X]$, that is, $m_P k[X] = k[X]$. But by assumption $k[X]$ is a $k[Y]$-module of finite type, and Nakayama's Lemma leads to contradiction. (Let $f_1, \ldots, f_n$ be a basis of the $k[Y]$-module $k[X]$, then $f_i = \sum_{j=1}^n m_{ij} f_j$ for all $i = 1, \ldots, n$, where $m_{ij} \in m_P$. Let $f(t)$ be the characteristic polynomial of the matrix (m_{ij}). Then $f(1) \in k[Y]$ annihilates $k[X]$. Since $k[X]$ contains 1, we must have $f(1) = 0$. But $f(t)$ is monic with non-leading coefficients in $m_P \neq k[Y]$, hence $f(1)$ is non-zero. Contradiction.) QED

One checks that finiteness is a local property, that is, a morphism is finite if and only if it has this property in a neighbourhood of any point

(see [Shafarevich]). Then one uses this to define finite morphisms of quasi-projective varieties. (Another general property of finite morphisms is that they send closed subsets to closed subsets.)

Definition. A morphism of quasi-projective varieties $f : X \to Y$ is called *finite* if every point $y \in Y$ has an affine neighbourhood U such that $f^{-1}(U)$ is affine, and $f : f^{-1}(U) \to U$ is finite.

Definition. The *degree* of a finite morphism $f : X \to Y$ is the degree of the field extension $k(X)/k(Y)$.

Theorem B.2 *A dominant morphism of smooth projective curves is finite.*

Proof. See [Shafarevich], Ch. 2.

Example. The affine variety X with equation $y^n = f(x_1, \ldots, x_n)$, where f is a polynomial in n variables, is equipped with a morphism $\pi : X \to \mathbf{A}^n_k$ which forgets the coordinate y. This morphism is finite of degree n.

Now we sketch the proof of Theorem 5.6. This theorem is proved as a corollary of Theorems A and B below. We note that by Theorem B.2 f is a finite morphism.

Let $P \in Y$, and $f^{-1}(P) = \{Q_1, \ldots, Q_r\}$. This is a finite set by Proposition B.1 (ii). The ring

$$\tilde{\mathcal{O}} = \cap_{i=1}^r \mathcal{O}_{Q_i}$$

is called *the semi-local ring of* $\{Q_1, \ldots, Q_r\}$. The first of two following theorems describes the algebraic structure of the semi-local ring $\tilde{\mathcal{O}}$, which is very similar to that of a local ring. The second theorem describes the structure of $\tilde{\mathcal{O}}$ as a module over the local ring $\mathcal{O}_P$.

Theorem A. (1) *$\tilde{\mathcal{O}}$ is a PID.*

(2) *The only prime ideals of $\tilde{\mathcal{O}}$ are the ideals $m_i := m_{Q_i} \cap \tilde{\mathcal{O}}$, where m_{Q_i} is the maximal ideal of $\mathcal{O}_{Q_i}$.*

(3) *There are elements $t_i \in \tilde{\mathcal{O}}$, $i = 1, \ldots, r$, such that $val_{Q_j}(t_i) = \delta_{ij}$, in other words, t_i is a local parameter at Q_i, $(t_i) = m_i$, and a unit at Q_j when $i \neq j$. Any element of $\tilde{\mathcal{O}}$ can be uniquely written as $ut_1^{a_1} \ldots t_r^{a_r}$, where $u \in \tilde{\mathcal{O}}^*$ is a unit, and $a_i \geq 0$.*

Theorem B. *Let n be the degree of the finite morphism f, $n = [k(X) : k(Y)]$. Then $\tilde{\mathcal{O}}$ is a free $\mathcal{O}_P$-module of rank n.*

Proof of Theorem 5.6. By definition, if $t \in \mathcal{O}_P$ is a local parameter, and we write $t = ut_1^{a_1} \ldots t_r^{a_r}$ as in Theorem A, then $deg(f^*(P)) = a_1 + \ldots + a_r$.

By the Chinese remainder theorem the ring $\tilde{\mathcal{O}}/(t)$ is isomorphic to the product of $\tilde{\mathcal{O}}/(t_i^{a_i}) \simeq \mathcal{O}_{Q_i}/(t_i^{a_i})$. This latter ring is the ring of power series

in t_i with coefficients in k, considered modulo $t_i^{a_i}$. As a vector space over k it has dimension a_i. Hence $dim_k(\tilde{\mathcal{O}}/(t)) = a_1 + \ldots + a_r$.

On the other hand, by Theorem B $\tilde{\mathcal{O}}/(t)$ is isomorphic to $(\mathcal{O}_P/(t))^n$ as a $\mathcal{O}_P/(t)$-module. Since t is a local parameter at P, we have $\mathcal{O}_P/(t) \simeq k$, and thus $\tilde{\mathcal{O}}/(t)$ is a vector space k^n. By comparing $dim_k(\tilde{\mathcal{O}}/(t))$ computed in two different ways we conclude that $n = a_1 + \ldots + a_r$. QED

B.2 Functoriality of Pic

Let $f : X \to Y$ be a morphism of smooth varieties. The construction of f^* relies on a so called "moving lemma".

Moving lemma. *Let X be a smooth variety, and $x_1, \ldots, x_n$ be points on X. In every class of divisors on X there exists a divisor whose support does not contain the points $x_1, \ldots, x_n$.*

The inverse image $f^*(D)$ of a divisor D on Y *such that* $Supp(D) \not\subset f(X)$ is defined as follows. We may assume that D is an irreducible subvariety of codimension 1. We know that locally D is given as the zero set of a rational function. Thus the variety Y can be covered by open affine subsets U_i such that $D \cap U_i$ is either empty or is the set of zeros of a rational function $\phi_i \in k(Y)$ in U_i. It is clear that the restrictions of ϕ_i and ϕ_j to the intersection $U_i \cap U_j$ differ by an invertible function. Since $Supp(D) \not\subset f(X)$ we observe that $\phi_i \circ f$ is a well defined rational function on X. Moreover, the restrictions of $\phi_i \circ f$ and $\phi_j \circ f$ to $f^{-1}(U_i) \cap f^{-1}(U_j)$ differ by an invertible function. Together these function define a divisor $f^*(D)$ on X:

$$f^*(D) = \sum_{Z \subset X,\ codim_X(Z)=1} val_Z(\phi_i \circ f)$$

Here $Z \subset X$ is irreducible and of codimension 1, val_Z is the valuation defined by the local ring $\mathcal{O}_Z$ of X at Z (recall that $\mathcal{O}_Z$ is a DVR by Corollary 4.6), and i is such that $Z \cap f^{-1}(U_i) \neq \emptyset$. It is easy to see that all such i give the same result. [Note that the verification that this defintion does not depend on the choice of the affine covering and the functions ϕ_i is non-trivial.]

Now by the moving lemma, we can modify D in its divisor class in $\mathrm{Pic}(Y)$ such that the condition $Supp(D') \not\subset f(X)$ is satisfied for some some $D' \sim D$. Then we define $f^*([D])$ as the class $[f^*(D')]$. (Note that in general this homomorphism $f^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$ is not induced by a homomorphism $\mathrm{Div}(Y) \to \mathrm{Div}(X)$!)