Introduction to Algebraic Geometry

Lothar Göttsche

1. Introduction

In linear algebra one wants to find the solutions of a system of linear equations, i.e.

$$\begin{array}{ccccccc} a_{11}x_1 & + & \dots & + & a_{1m}x_m & = & b_1 \\ \vdots & & & & \vdots & & \dots \\ a_{n1}x_1 & + & \dots & + & a_{nm}x_m & = & b_n, \end{array}$$

where the a_{ij} and the b_i are elements in a field k.

In a course in algebra, one studies among other things the set of zeros of polynomials of arbitrary degree:

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0, \quad (a_i \in k).$$

In algebraic geometry one studies a common generalization of these two: algebraic sets, which are the solution sets (in k^n) of systems of polynomial equations in several variables.

$$\begin{array}{ccc} f_1(x_1, \dots, x_n) & = & 0 \\ \vdots & & \vdots \\ f_1(x_1, \dots, x_n) & = & 0. \end{array}$$

Already the ancient Greeks studied the conic sections, i.e. the solutions of polynomial equations of degree 2 in two variables:

$$\begin{array}{rl} x^2 + y^2 = 1 & \text{circle} \\ xy = 1 & \text{hyperbola} \\ y = x^2 & \text{parabola.} \end{array}$$

Here we are looking at the solutions over the real numbers, e.g.

$$\left\{(a, b) \in \mathbb{R}^2 \;\middle|\; a^2 + b^2 = 1\right\}.$$

One can also look at the solutions over other fields. The famous conjecture of Fermat just recently proved by Wiles is that for $n > 2$ the only solutions to $x^n + y^n = z^n$ in rational numbers (i.e. triples $(a, b, c) \in \mathbb{Q}^3$ with $a^n + b^n = c^n$) are the obvious ones with $a = 0$ or $b = 0$.

In fact it turns out that it is simpler to study the solution sets over an algebraically closed field k. In general it also is better to not just look at the solutions in k^n. One wants to complete the solution set by also allowing points at infinity. This is done by studying the solutions to the equations in projective space.

Algebraic geometry is a very active subject with a very long history. Modern Algebraic geometry truely got started with the introduction of Cartesian coordinates in the seventeenth century.

It was a very active subject throughout the nineteen century, for instance Riemann showed that compact Riemann surfaces (i.e. complex manifolds of dimension 1) can always be described as solution sets of polynomial equations. There was also the very important Italian school of algebraic geometry in the late nineteenth and early twentieth century. The subject however had some problems of foundation, so that one had to rely on more or less intuitive arguments, which lead to a crisis. This was solved and the foundations were laid, by developping algebra and commutative algebra, for instance by Hilbert and Emmy Noether. The work on foundations was finished by Oscar Zariski and André Weil in the middle of the twentieth century. Recently, starting in the 1950s the theory was enormously generalized and made more powerful by the introduction of schemes and cohomology by Grothendieck. Now Algebraic Geometry has connections to many parts of mathematics. In particular with the modern formulation of Algebraic Geometry most of Number Theory can be viewed as part of Algebraic Geometry and many of the most powerful methods of Number theory are Algebraic Geometry methods. For instance in the proof of Fermat's Last Theorem mentioned above, schemes play an important role. There are also very close connections to Algebra, Complex Analyis, Topology, Differential Geometry, Partial differential equations, Mathematical Physics but also to applied subjects such as Coding theory and Cryptography.

One might think that it is not very interesting to study zero sets of polynomials, as they appear to be very special. However this is misleading. It turns out that for many of the important phenomena one wants to study e.g. in Differential Geometry, algebraic varieties are very important examples, and using the much more powerful and precise tools of algebraic geometry one can understand them much better.

In these lectures we will not be able to discuss schemes. We do however use the modern language which should make it possible to study e.g. the book [**Hartshorne**] afterwards. We also will not introduce cohomology of sheaves that are a basic tool in modern algebraic geometry. Again after this course one can study this subject in [**Hartshorne**] or [**Kempf**].

The approach to algebraic geometry in this course is based on commutative algebra. This has the disadvantage that one needs some background in algebra and that it is maybe sometimes a bit dry in the beginning. I will use only elementary properties of rings, ideals and polynomials and introduce whatever I need as I go along. There is another approach to algebraic geometry over the complex numbers via complex analysis and complex differential geometry, partial differential equations and topology. The standard advanced textbook for this approach is [**Griffiths-Harris**], but there is also a newer more elementary book [**Huybrechts**]. The point is that over the complex numbers we can view nonsingular algebraic varieties as complex analytic manifolds (with particularly nice properties).

2. Algebraic preliminaries

We want to briefly recall a few elementary facts from algebra that we will use and also fix some notations. For us a **ring** is a commutative ring with 1, and a **homomorphism** of rings must map 1 to 1. Let k be a field. A k-**algebra** is a ring R with $k \subset R$. A **homomorphism** $\varphi : A \to B$ of k-algebras is a ring homomorphism that is the identity on k. If A and B are k-algebras, it follows that they are k-vector spaces and a homomorphism of k-algebras is a ring homomorphism that is also k-linear.

2.1. Polynomials. The typical examples of k-algebras are polynomial rings over k. Let k be a field. We denote by $k[x]$ the **ring of polynomials** with coefficients in k, i.e. expressions $f = \sum_{i=0}^{d} a_i x^i$ with $a_i \in R$. The **degree** of the polynomial f is the largest integer d such that $a_d \neq 0$. a_d is then called the **leading coefficient** of f. The **polynomial ring in** n **variables** is defined inductively by

$$k[x_1, \dots, x_n] := k[x_1, \dots, x_{n-1}][x_n].$$

We usually write $k[x, y]$ and $k[x, y, z]$ in case $n = 2$ and 3. Any polynomial $f \in k[x_1, \dots, x_n]$ can be written as

$$f = \sum_{i_1, \dots, i_n \geq 0} a_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n} \qquad , \quad a_{i_1, \dots, i_n} \in k.$$

The $x_1^{i_1} \cdot \ldots \cdot x_n^{i_n}$ are called **monomials**. Their **degree** is $i_1 + \ldots + i_n$. The degree of f is the maximal degree of a monomial $x_1^{i_1} \cdot \ldots \cdot x_n^{i_n}$ with $a_{i_1, \dots, i_n} \neq 0$. We write $deg(f)$ for the degree of f. f is called **homogeneous** of degree d if every monomial with $a_{i_1, \dots, i_n} \neq 0$ has degree d.

2.2. Ideals. A subset I of a ring is called **ideal** if it is a subgroup of the additive group of R and $fg \in I$ for $f \in R$ and $g \in I$. An ideal $I \subsetneq R$ is called a **proper ideal**. If $f : R \to S$ is a ring homomorphism, then the **kernel** $ker(f) = f^{-1}(0)$ is an ideal in R. On the other hand if $I \subset R$ is an ideal, then the set R/I of residue classes $[g] = g + I$ is with the induced addition and multiplication a ring, and the map $\pi : R \to R/I$ which sends $g \in R$ to its residue class $[g]$ is a ring homomorphism with kernel I. Thus the ideals in a ring R are precisely the kernels of ring homomorphisms starting from R.

Let $S \subset R$ be a subset. The **ideal generated by** S is

$$\langle S\rangle := \Big\{ \sum_{i=1}^{n} a_i s_i \;\Big|\; n \geq 0,\ a_i \in R,\ s_i \in S \Big\}.$$

It is easy to check that this is an ideal in R. If $S = \{f_1, \dots , f_n\}$ is a finite set, we write $\langle S\rangle = \langle f_1, \dots , f_r\rangle$ and say that $\langle S\rangle$ is finitely generated.

An ideal of the form $\langle f\rangle$ for $f \in R$ is called a **principal ideal**. An integral domain R is called a **principal ideal domain** if every ideal $I \subset R$ is principal. A typical example of a principal ideal domain is $k[x]$ for k a field.

Let $I, J \subset R$ be ideals. The **sum** of I and J is

$$I + J := \big\{ a + b \in R \;\big|\; a \in I, b \in J \big\}.$$

It is easy to see that $I + J$ is an ideal and $I + J = \langle I \cup J\rangle$. The **product** of I and J is

$$IJ := \big\langle ab \;\big|\; a \in I,\ b \in J \big\rangle,$$

i.e. it is the ideal generated by the products of an element of I and an element of J. Thus by definition it is an ideal.

An ideal $M \subsetneq R$ is called **maximal**, if it is not contained in any proper ideal $I \neq M$. Any ideal is contained in a maximal ideal. It is easy to see that

$$I \subset R \text{ maximal ideal} \iff R/I \text{ field.}$$

An ideal $I \subsetneq R$ is called a **prime ideal** if the following holds: If $f, g \in R$ with $fg \in I$ then $f \in I$ or $g \in I$. Maximal ideals are prime ideals. A ring A is called a **integral domain** if for any $f, g \in R$ with $fg = 0$ we have $f = 0$ or $g = 0$. By definition

$$R/I \text{ integral domain} \iff I \text{ prime ideal.}$$

A typical example of an integral domain is $k[x_1, \dots , x_n]$ for k a field.

If R is an integral domain, we can define the **quotient field** $Q(R)$ as follows: $Q(R)$ is the set of equivalence classes $\frac{f}{g}$ of pairs $(f, g) \in R \times R$ with $g \neq 0$, where $(f_1, g_1) \sim (f_2, g_2) \iff f_1g_2 = f_2g_1$. Addition and multiplication are defined by

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1g_2 + f_2g_1}{g_1g_2}, \quad \frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1f_2}{g_1g_2}.$$

It is easy to see that $Q(R)$ is a field. We identify $f \in R$ with $\frac{f}{1} \in Q(R)$. Thus R is a subring of $Q(R)$.

In particular, if $R = k[x_1, \ldots, x_n]$, the quotient field is denoted by $k(x_1, \ldots, x_n)$ and called the **ring of rational functions** in $x_1, \ldots, x_r$. It is the set of quotients $\frac{f}{g}$ of polynomials f, g in $x_1, \ldots, x_n$ with the usual addition and multiplication.

Contents

CHAPTER 1

Affine and projective varieties

In this whole course (unless said otherwise) let k be an algebraically closed field. To help your intuition, you can think of k as the complex numbers. In fact I think one looses very little if one assumes throughout that k is the field of complex numbers.

In this chapter we will introduce affine and projective varieties, which are the subject of this course, and study their first properties. We will start with affine algebraic sets, i.e. solutions of polynomial equations in k^n. Then we will introduce projective varieties, which are zero sets of polynomial equations in projective space $\mathbb{P}^n$. One can view them as "compactifications" of affine algebraic sets by adding some points at infinity.

1. Affine varieties

In this section we will introduce and study affine algebraic sets and affine varieties. An affine algebraic set is the zero set of a set of polynomials in n variables in k^n. k^n will be called affine space and denoted by $\mathbb{A}^n$. For these affine algebraic sets, we will see many of the concepts and results that in the rest of the course we want to study more profoundly and in greater generality. This includes

(1) The Zariski topology. This is a topology on $\mathbb{A}^n$ whose closed sets are the affine algebraic sets. This will be an important language for the rest of the course.
(2) Irreducible components. Every affine algebraic set can be written as a union of finitely many pieces, which cannot be further decomposed, these are called the irreducible components. Later we will often restrict out attention to irreducibles: the varieties.
(3) Dimension. This is an important invariant of varieties and will be one of the main subjects of Chapter 3.

The idea is that we first want to understand some of the main ideas in a simpler case, before going to the general definitions and results.

1.1. Affine algebraic sets. An affine algebraic set is the zero set of a set of polynomials in n variables in k^n. We will see that indeed every affine algebraic set can be obtained as the zero set of an ideal in $k[x_1, \dots, x_n]$. This will allow us to use commutative algebra to study algebraic sets.

DEFINITION 1.1. n-dimensional **affine space** is

$$\mathbb{A}^n = k^n = \big\{(a_1 \dots, a_n) \bigm| a_i \in k\big\}.$$

Polynomials $f \in k[x_1, \dots, x_n]$ define in the obvious way functions $f : \mathbb{A}^n \to k$; if $p = (a_1, \dots, a_n) \in \mathbb{A}^n$ is a point, then $f(p) = f(a_1, \dots, a_n)$.

Let $S \subset k[x_1, \dots, x_n]$ be a set of polynomials. The **zero set** of S is

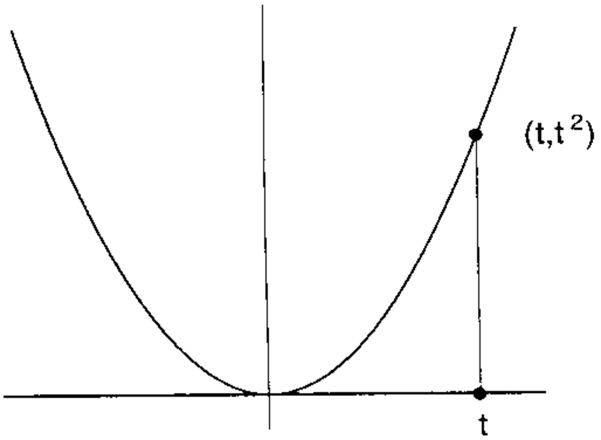
$$Z(S) := \big\{p \in \mathbb{A}^n \bigm| f(p) = 0 \text{ for all } f \in S\big\} \subset \mathbb{A}^n.$$

A subset of the form $Z(S)$ for $S \subset k[x_1, \dots, x_r]$ is called an **affine algebraic set**. We write $Z(f_1, \dots, f_r)$ for $Z(\{f_1, \dots, f_r\})$.

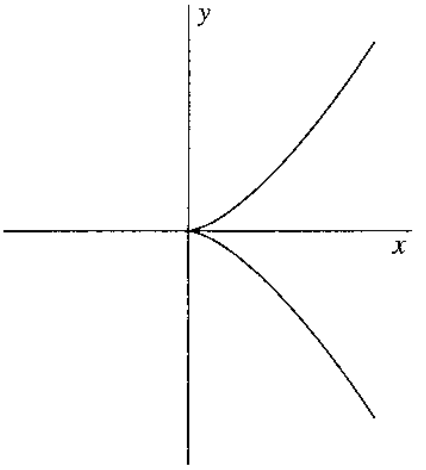
If $n \leq 3$ we usually write x, y, z for the variables.

EXAMPLE 1.2. When we make drawings of affine algebraic sets, we will usually draw the points over $\mathbb{R}$.

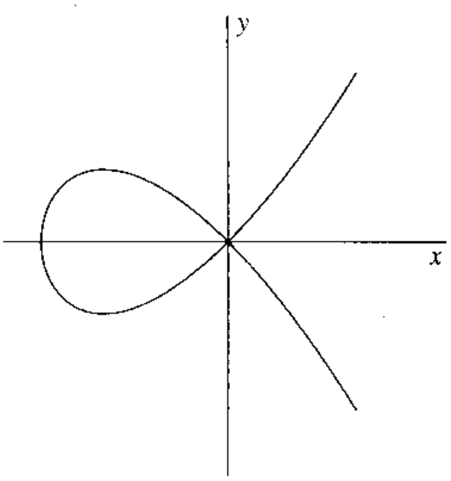
(1) $\mathbb{A}^n = Z(0)$ and $\emptyset = Z(1)$ are affine algebraic sets.
(2) A point $p = (a_1, \dots, a_n) = Z(x_1 - a_1, \dots, x_n - a_n)$ is an affine algebraic set.
(3) An **affine plane curve** is the zero set $Z(F)$ of a polynomial $F \in k[x, y]$ in $\mathbb{A}^2$.
   (a) $Z(y - x^2) \subset \mathbb{A}^2$ is a conic.



(b) $Z(y^2 - x^3) \subset \mathbb{A}^2$ is the cuspidal cubic.
(c) $Z(y^2 - (x^3 + x^2)) \subset \mathbb{A}^2$ is the nodal cubic.



$y^2 = x^3$



$y^2 = x^2(1 + x)$

(4) The zero set $Z(f)$ of a nonconstant polynomial $f \in k[x_1, \dots, x_n]$ is called a **hypersurface**.

(5) The zero set of a polynomial of degree 1 is called an **affine hyperplane**. For example the line defined by $5x + 6y = 4$ is a hyperplane in $\mathbb{A}^2$.

(6) The common zero set in $\mathbb{A}^n$ of a set of polynomials of degree 1 is called an **affine subspace**. By definition it is the intersection of affine hyperplanes.

(7) The set of $n \times n$ matrices with coefficients in k can be identified with $\mathbb{A}^{n^2}$. Let $\{x_{ij}\}_{i,j=1}^n$ denote the coordinates on $\mathbb{A}^{n^2}$. Then the determinant

$$det(x_{ij}) := det \begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \dots & x_{nn} \end{pmatrix}$$

is a polynomial. Thus we see that $SL(n, k)$, the set of all matrices of determinant 1, is the hypersurface defined by $det - 1$.

(8) A **determinantal variety** is the set of all $n \times n$ matrices of rank $\leq l$ for some $l \leq n$. The rank of a matrix A is $\leq l$ if and only if all $(l + 1)$ minors vanish (i.e. the $(l + 1) \times (l + 1)$ subdeterminants). These are polynomials in the x_{ij}. Thus determinantal varieties are affine algebraic sets in $\mathbb{A}^{n^2}$.

Now we want to see that every affine algebraic set in $\mathbb{A}^n$ is the zero set of an ideal in $k[x_1, \dots, x_n]$. This means that in future we can restrict our attention to the zero sets of ideals. This will allow us to use commutative algebra to study affine varieties: we can use the properties of ideals and quotient rings by ideals.

LEMMA 1.3. *Let $S, T \subset k[x_1, \dots, x_n]$.*

(1) *If $S \subset T$, then $Z(S) \supset Z(T)$.*
(2) *$Z(S) = Z(\langle S \rangle)$ (where $\langle S \rangle$ is the ideal generated by S). So every affine algebraic set $X \subset \mathbb{A}^n$ is the zero set of an ideal in $k[x_1, \dots, x_n]$.*

PROOF. (1) is clear: If $p \in Z(T)$, then $f(p) = 0$ for all $f \in T$, thus for all $f \in S$, so $p \in Z(S)$.

(2) $Z(\langle S \rangle) \subset Z(S)$ is clear by $S \subset \langle S \rangle$. Conversely let $p \in Z(S)$ and $g = \sum_i h_i f_i \in \langle S \rangle$ with $f_i \in S$. Then $g(p) = \sum_i h_i(p) f_i(p) = 0$ because all $f_i(p) = 0$. □

1.2. Zariski topology. The affine algebraic sets are the closed sets of a topology on $\mathbb{A}^n$. This is very useful for us, because it allows us to use the language of topology (open sets, closed sets, continuous maps) in our arguments. This language will be extremely useful for us and later we will use it all the time. Thus it is very important that you get used to the Zariski topology as soon as possible.

We will see that this topology is quite strange. The open subsets are very big and very few.

PROPOSITION 1.4. (1) *If $\{S_\alpha\}$ is a family of subsets of $k[x_1, \dots, x_n]$, then*

$$\bigcap_\alpha Z(S_\alpha) = Z\Big(\bigcup_\alpha S_\alpha\Big) = Z\Big(\sum_\alpha \langle S_\alpha \rangle)\Big) \subset \mathbb{A}^n.$$

(2) *If $S, T \subset k[x_1, \dots, x_n]$, then $Z(S) \cup Z(T) = Z(ST) = Z(\langle ST \rangle)$ (where $ST = \{fg \mid f \in S, \ g \in T\}$).*

Thus arbitrary intersections and finite unions of affine algebraic sets are affine algebraic sets.

PROOF. (1) Is clear: By definition $p \in \bigcap_\alpha Z(S_\alpha)$, if and only if $f(p) = 0$ for all f in any of the S_α. This is equivalent to $p \in Z(\bigcup_\alpha S_\alpha)$. The last equality follows by $\big\langle \bigcup_\alpha S_\alpha \big\rangle = \sum_\alpha \langle S_\alpha \rangle$ and Lemma 1.3.

(2) Let $p \in Z(S) \cup Z(T)$, let $f \in S$, $g \in T$. Then $f(p) = 0$ or $g(p) = 0$, i.e. $(fg)(p) = 0$, i.e. $p \in Z(ST)$. Conversersely let $p \in Z(ST)$, assume $p \notin Z(S)$. Then we have to see $p \in Z(T)$. Let $f \in S$ with $f(p) \neq 0$. We have $(fg)(p) = 0$ for all $g \in T$, thus $g(p) \neq 0$ for all $g \in T$, i.e. $p \in Z(T)$. The last equality follows by Lemma 1.3. □

By this result we can use the affine algebraic sets as the closed sets of a topology on $\mathbb{A}^n$.

Reminder 1.5. Recall that a **topology** on a set X is a collection of subsets called **open sets**, such that

(1) $\emptyset$ and X are open.
(2) A finite intersection of open sets is open.
(3) An arbitrary union of open sets is open.

A set X with a topology is called a **topological space**. A subset $A \subset X$ is called **closed**, if and only if $X \setminus A$ is open. The three axioms for a topological space are then obviously equivalent to

(1) $\emptyset$ and X are closed.
(2) A finite union of closed sets is closed.
(3) An arbitrary intersection of closed sets is closed.

Now let X be a topological space. The **closure** $\overline{U}$ of a subset $U \subset X$ is the intersection of all closed sets $A \subset X$ with $U \subset A$. We say that U is **dense** in X, if $\overline{U} = X$. A subset $W \subset X$ is called **locally closed** if it is the intersection of an open and a closed subset. A set $\{U_i\}_i$ of open sets $U_i \subset X$ with $\bigcup_i U_i = X$ is called an **open cover** of X.

For a subset $Y \subset X$ of a topological space X the **induced topology** (or subspace topology) on Y has as open sets the $U \cap Y$ with $U \subset X$ open. Equivalently the closed sets of Y are the $A \cap Y$ with $A \subset X$ closed. If $Y \subset X$ is a subset with the induced topology we also say Y is a **subspace** of X.

A map $f : X \to Y$ between topological spaces is called **continuous** if the inverse image of any open set is open (or equivalent if the inverse image of every closed set is closed).

Definition 1.6. The **Zariski topology** on $\mathbb{A}^n$ is the topology whose closed sets are the affine algebraic sets or equivalently the open sets are the complements of the affine algebraic sets. By Proposition 1.4 this is a topology on $\mathbb{A}^n$. If $X \subset \mathbb{A}^n$ is a subset, we give it the induced topology. It is called the **Zariski topology on** X.

Remark 1.7. If $X \subset \mathbb{A}^n$ is an affine algebraic set, the closed sets of X are precisely the affine algebraic sets $Y \subset \mathbb{A}^n$ contained in X. (By definition they are the intersections $A \cap X$ of X with closed subsets $A \subset \mathbb{A}^n$, but then $A \cap X$ is closed in $\mathbb{A}^n$ as the intersection of two closed subsets).

Example 1.8. (1) All finite subsets of $\mathbb{A}^n$ are closed.
(2) The closed subsets of $\mathbb{A}^1$ are $\mathbb{A}^1$, $\emptyset$ and the finite subsets of $\mathbb{A}^1$: Let $I \subset k[x]$ be an ideal. Obviously if $I = 0$, $Z(I) = \mathbb{A}^1$. Thus assume $0 \neq f \in I$.

Then $Z(I) \subset Z(f)$. We can write $f = (x - a_1)^{n_1} \cdot \ldots \cdot (x - a_l)^{n_l}$. So $Z(I) \subset Z(f) = \{a_1, \ldots, a_l\}$.

REMARK 1.9. One can see from the second example that the Zariski topology is quite coarse, i.e. it has very few (and very small) closed sets and therefore very few (and very large) open sets. One also sees that the Zariski topology is not Hausdorff. If $k = \mathbb{C}$ it is much coarser than the standard (Euclidean) topology, i.e. all Zariski open sets are open in the Euclidean topology, but most sets which are open in the Euclidean topology are not open in the Zariski topology (open balls are not open in the Zariski topology.

However the Zariski topology will be very useful to us because it allows us to introduce continuous functions and maps in a way which is meaningful for algebraic geometry. The main point here is that polynomials $F \in k[x_1, \ldots, x_n]$ are continuous maps $F : \mathbb{A}^n \to \mathbb{A}^1$ for the Zariski topology (this is an exercise below).

REMARK 1.10. In the future we will use the Zariski topology extensively in our arguments. Thus we can talk about open and closed sets and continuous maps and functions. However one should keep in mind that the Zariski topology is mostly just a convenient language. It allows us to make some arguments shorter and clearer, but one is not really doing any nontrivial topology.

1.3. The ideal and the coordinate ring of an affine algebraic set. We have found that to each ideal $I \subset k[x_1, \ldots, x_n]$ we can associate an affine algebraic set $Z(I) \subset \mathbb{A}^n$. In general there will be many ideals with the same set of zeros, but there is one **largest** ideal with a given zero set X, i.e. the set $I(X)$ of all polynomials vanishing on X. As $I(X)$ is determined by X in a canonical way, we can hope that it reflects the geometric properties of X. The ideal $I(X)$ determines the coordinate ring $A(X) = k[x_1, \ldots, x_n]/I(X)$ of X. We can view $A(X)$ as the ring of polynomial functions on X. We will see that it is extremely important in the study of the properties of X. One can say that if one knows $A(X)$, one knows everything about X.

DEFINITION 1.11. Let $X \subset \mathbb{A}^n$ be a subset. The **ideal of** X is

$$I(X) := \big\{ f \in k[x_1, \ldots, x_n] \bigm| f(p) = 0 \text{ for all } p \in X \big\}.$$

That is $I(X)$ is the ideal of all polynomials vanishing on X.

REMARK 1.12. It is clear that $X \subset Y$ implies $I(X) \supset I(Y)$ and we know from above that $I \subset J$ implies $Z(I) \supset Z(J)$.

Definition 1.13. Let $X \subset \mathbb{A}^n$ be an affine algebraic set. The **coordinate ring** of X is $A(X) := k[x_1, \dots, x_n]/I(X)$. By definition it is a k-algebra. We will often denote the class of $F \in k[x_1, \dots, x_n]$ in $A(X)$ by the same letter F, but sometimes also by $[F]$.

Example 1.14. If $X = Z(x - y^2) \subset \mathbb{A}^2$, then $A(X) = k[x, y]/(x - y^2) \simeq k[x]$.

We can view $A(X)$ as a ring of functions on X:

Remark 1.15. A **polynomial function** on X is a function of the form $F|_X$ for $F \in k[x_1, \dots, x_n]$. Polynomial functions obviously form ring (and even a k-algebra): constant functions are polynomial functions and if F, G are polynomial functions then

$$F + G : X \to k, p \mapsto F(p) + G(p), \qquad FG : X \to k, p \mapsto F(p)G(p)$$

are polynomial functions.

Proposition 1.16. *The map*

$$F \in k[x_1, \dots, x_n] \mapsto F|_X$$

induces an isomorphism of k-algebras from $A(X)$ to the ring of polynomial functions on X.

Proof. By definition the map $\varphi : F \to F|_X$ is a surjective homomomorphism of k-algebras from $k[x_1, \dots, x_n]$ to the polynomial functions on X. By definition $ker(\varphi) = \{F \in [x_1, \dots, x_n] \bigm| F|_X = 0\} = I(X)$. Thus we get an induced isomorphism from $A(X)$ to the polynomial functions on X. □

In future we will identify the coordinate ring $A(X)$ with the ring of polynomial functions on X via $[F] = F|_X$.

Finally we want to see that the zero set of polynomial functions is closed.

Definition 1.17. Let $X \subset \mathbb{A}^n$ be an affine algebraic set and let $f \in A(X)$. The zero set of f is

$$Z(f) := \{p \in X \bigm| f(p) = 0\}.$$

If $f = F|_X$ for $F \in k[x_1, \dots, x_n]$, we see by definition that $Z(f) = Z(F) \cap X$. Thus $Z(f)$ is closed in X.

1.4. Hilbert Basis Theorem. An affine algebraic set $X \subset \mathbb{A}^n$ is the zero set of an arbitrary set of polynomials $S \subset k[x_1, \dots, x_n]$. We now want to see that it is always the zero set of a **finite set** of polynomials. This has geometric consequences: every affine algebraic set can be decomposed into a finite number of "pieces", the irreducible components, that cannot be further decomposed. Later we will then want to restrict our attention to such irreducible algebraic sets, the affine varieties. We need to introduce some algebra.

LEMMA AND DEFINITION 1.18. *For a ring R the following are equivalent:*

1. *Every ideal $I \subset R$ is finitely generated, i.e. of the form $\langle f_1, \dots, f_k \rangle$.*
2. *R satisfies the* **ascending chain condition***: Every chain $I_1 \subset I_2 \subset \dots$ of ideals in R becomes stationary (i.e. $I_N = I_{N+1} = \dots$ for some N).*

A ring R that satisfies these conditions is called **Noetherian***.*

PROOF. (1) $\Rightarrow$ (2). Let $I_1 \subset I_2 \subset \dots$ be a chain of ideals in R. Put $I = \bigcup_i I_i$. Then I is obviously an ideal. By (1) we can write $I = \langle f_1, \dots, f_k \rangle$. These f_i must all be already contained in some I_N, thus $I_N = I_{N+1} = \dots$.

(2) $\Rightarrow$ (1). Let $I \subset R$ be an ideal, which is not finitely generated. Let $f_0 \in I$. Then for each $n \geq 1$ there exists $f_n \in I \setminus \langle f_0, \dots, f_{n-1} \rangle$. Then $\langle f_0 \rangle \subset \langle f_0, f_1 \rangle \subset \dots$ is a chain of ideals that does not become stationary. □

THEOREM 1.19. *Every algebraic set $X \subset \mathbb{A}^n$ is the intersection of finitely many hypersurfaces.*

PROOF. Let $X = Z(I)$ for I an ideal in $k[x_1, \dots, x_n]$. It is enough to show that I is finitely generated: If $I = \langle f_1, \dots, f_r \rangle$, then $X = Z(f_1, \dots, f_r) = Z(f_1) \cap \dots \cap Z(f_r)$. So it is enough to show that $k[x_1, \dots, x_n]$ is Noetherian. Any field k is Noetherian, because $\{0\}$ and k are the only ideals. Therefore the theorem follows from the Hilbert Basis Theorem. □

THEOREM 1.20. *(Hilbert Basis Theorem) R Noetherian $\Longrightarrow R[x_1, \dots, x_n]$ Noetherian.*

PROOF. As $R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$, it is enough to show: R Noetherian $\Rightarrow R[x]$ Noetherian. We assume $R[x]$ is not Noetherian and show that R is not Noetherian. Let $I \subset R[x]$ be an ideal which is not finitely generated. The trick is to look at the leading terms of elements in I. Let $f_1 \in I \setminus \{0\}$ be a polynomial of minimal degree. Inductively let f_n be a polynomial of minimal degree in $I \setminus \langle f_1, \dots, f_{n-1} \rangle$. Let $n_k = deg(f_k)$ and let a_k be the coefficient of x^{n_k} in f_k. Then $n_1 \leq n_2 \leq \dots$ and

$\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \dots$ is a chain of ideals in R. We claim that it does not become stationary. Assume otherwise; then for some k we get $\langle a_1, \dots , a_k \rangle = \langle a_1, \dots , a_{k+1} \rangle$. Therefore we can write

$$a_{k+1} = \sum_{i=1}^{k} b_i a_i, \qquad b_i \in R. \tag{1}$$

Then

$$g := f_{k+1} - \sum_{i=1}^{k} b_i x^{n_{k+1}-n_i} f_i$$

lies in $I \setminus \langle f_1, \dots , f_k \rangle$ (otherwise $f_{k+1} = g + \sum b_i x^{n_{k+1}-n_i} f_i$ would lie in $\langle f_1, \dots , f_k \rangle$). On the other hand we see that all the summands of g have degree n_{k+1} and by (1) the coefficients of $x^{n_{k+1}}$ cancel. Thus $deg(g) < n_{k+1}$, which contradicts the choice of f_{k+1}, as having minimal degree. □

1.5. Irreducible components. The algebraic set $Z(xy) \subset \mathbb{A}^2$ can be written as the union of the two coordinate axis $Z(x)$ and $Z(y)$. On the other hand one can show that $Z(x)$ and $Z(y)$ cannot be written as the union of two smaller closed subsets. An affine algebraic set will be called irreducible (or a variety) if it cannot be written as the union of two smaller affine algebraic sets. We want to show that every affine algebraic set can be written in a unique way as a union of affine varieties, its irreducible components. We make our definitions more generally for topological spaces. Thus they apply also to open subsets of affine algebraic sets and later to projective algebraic sets.

Definition 1.21. A topological space X is called **reducible** if we can write $X = X_1 \cup X_2$, where both X_1 and X_2 are closed subsets of X not equal to X. Otherwise X is called **irreducible**.

Remark 1.22. Let X be an irreducible topological space and let $U \subset X$ be nonempty and open.

(1) U is dense in X. (Because $X = X \setminus U \cup \overline{U}$ is a decomposition into closed subsets and by assumption $X \setminus U \neq X$, thus by irreducibility $\overline{U} = X$).

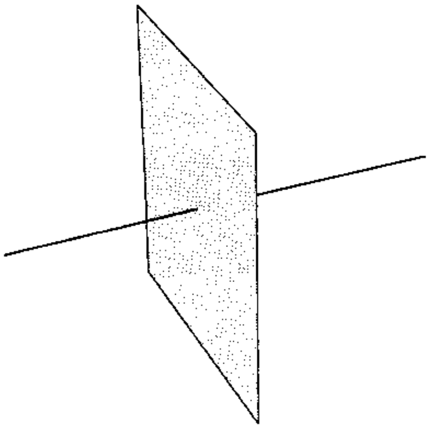
(2) U is irreducible. (If $U = U_1 \cup U_2$, with $U_i \subset U$ closed, then $U_i = U \cap X_i$ for $X_i \subsetneq X$ closed. Then $X_1 \cup X_2$ is a closed subset of X containing U, thus it contains $\overline{U} = X$. Therefore $X = X_1 \cup X_2$ and by irreducibility $X = X_1$ or $X = X_2$ and thus $U = U_1$ or $U = U_2$.)

The notion of irreducibility does not make much sense in the analytic topology. The only irreducible subsets of a Hausdorff space are the points. In future we often restrict attention to irreducible algebraic sets.

Example 1.23. (1) A point $p \in \mathbb{A}^n$ is irreducible.

(2) $Z(xy) \subset \mathbb{A}^2$ is the union of the lines $Z(x)$ and $Z(y)$, so it is reducible.

(3) $Z(xy, xz) = Z(y, z) \cup Z(x) \subset \mathbb{A}^3$ is the union of a plane and a line, thus it is reducible.



Now we want to show that every affine algebraic set is the union of finitely many irreducible affine algebraic sets. Again we want to more generally prove a statement about topological spaces, so that it applies more generally for instance also to projective varietes. A topological space is Noetherian if every descending chain of closed subsets becomes stationary. We will prove the result for Noetherian topological spaces. Then it is easy to see every affine algebraic set is Noetherian because $k[x_1, \dots, x_n]$ is a Noetherian ring.

Definition 1.24. A topological space X is called **Noetherian**, if every descending chain $X \supset X_1 \supset X_2 \supset \dots$ of closed subsets becomes stationary.

Remark 1.25. (1) Any subspace Y of a Noetherian topological space X is Noetherian: A descending chain $Y \supset Y_1 \supset Y_2 \supset \dots$ of closed subsets in Y is of the form $Y_i = Y \cap X_i$ with X_i closed subsets in X. By replacing X_i by $\bigcap_{j \leq i} X_j$, which has the same intersection with Y, we can assume that $X \supset X_1 \supset X_2 \supset \dots$ is a descending chain of closed subsets in X. Thus it becomes stationary.

(2) Let $X_1 \supset X_2 \supset \dots$ be a descending chain of closed subsets in $\mathbb{A}^n$. Then $I(X_1) \subset I(X_2) \subset \dots$ is an ascending chain of ideals in the Noetherian ring $k[x_1, \dots, x_n]$. Thus it becomes stationary and therefore also the original

chain of closed subsets. Thus $\mathbb{A}^n$ is Noetherian. By (1) also any (open subset of) an affine algebraic set is Noetherian.

Theorem and Definition 1.26. *Every Noetherian topological space X is up to reordering in a unique way a finite union $X = X_1 \cup \ldots \cup X_r$ of irreducible closed subsets with $X_i \not\subset X_j$ for $i \neq j$.*

The X_i are called the **irreducible components** *of X.*

Proof. **(Existence)** It is enough to prove the existence of a decomposition into finitely many irreducible closed subsets. The condition $X_i \not\subset X_j$ can then be satisfied by leaving out all X_i with $X_i \subset X_j$ for some $j \neq i$. Assume X does not have such a decomposition. Then X is in particular reducible. Thus we can write $X = X_1 \cup Y_1$ for closed subsets $X_1, Y_1 \subsetneq X$. Furthermore one of the two (say X_1) cannot have a finite decomposition into irreducible closed subsets, in particular it is reducible. Thus the same assumtions as for X also hold for X_1. Therefore we can repeat the argument with X_1. Continuing in this way we obtain a descending chain $X \supsetneq X_1 \supsetneq X_2 \supsetneq \ldots$ of closed subsets, which is a contradiction to X being Noetherian.

(Uniqueness) Let $X = X_1 \cup \ldots \cup X_r = Y_1 \cup \ldots \cup Y_s$ be two such decompositions. Then $X_i = \bigcup_j (Y_j \cap X_i)$ so by the irreducibility of X_i we get $X_i \subset Y_j$ for some j. Similarly $Y_j \subset X_k$ for some k. Thus $X_i \subset X_k$, which implies $i = k$ and $X_i = Y_j$. So each X_i is equal to one of the Y_j. Similarly each Y_j is equal to one of the X_i. Therefore the X_i are just a reordering of the Y_j. □

As every affine algebraic set is the union of irreducible affine algebraic sets we can restrict our attention to these irreducibles. We can study a reducible affine algebraic set by studying its irreducible components one by one. We will therefore give a special name to affine algebraic sets.

Definition 1.27. An **affine variety** is an irreducible affine algebraic set.

We will also often look at open subsets of affine varieties.

Definition 1.28. An open subset of an affine variety is called a **quasiaffine** variety.

As mentioned before, the algebraic properties of the ideal $I(X)$ of a closed set X should reflect the geometric properties of X. Here we see one instance: X is irreducible if and only if $I(X)$ is a prime ideal.

Proposition 1.29. *Let $X \subset \mathbb{A}^n$ be an affine algebraic set. Then X is irreducible if and only if $I(X)$ is prime.*

Proof. "$\Rightarrow$" Let X be irreducible, and let $fg \in I(X)$. Then $X \subset Z(fg) = Z(f) \cup Z(g)$, thus $X = (Z(f) \cap X) \cup (Z(g) \cap X)$. As X is irreducible, we must have $X = (Z(f) \cap X)$ or $X = (Z(g) \cap X)$, i.e $f \in I(X)$ or $g \in I(X)$.

"$\Leftarrow$" Assume $X = X_1 \cup X_2$ for closed subsets $X_1, X_2 \subsetneq X$. Then $Z(I(X_1)) = X_1 \subsetneq X = Z(I(X))$ implies $I(X) \subsetneq I(X_1)$, i.e. there exists $f_1 \in I(X_1) \setminus I(X)$. Similarly there exists $f_2 \in I(X_2) \setminus I(X)$. Then $f_1 f_2$ vanishes on all points of $X_1 \cup X_2 = X$. So $f_1 f_2 \in I(X)$. Therefore $I(X)$ is not a prime ideal. □

Remark 1.30. Let $X \subset \mathbb{A}^n$ be an affine algebraic set. Note that $I(X)$ is a prime ideal if and only if $A(X) = k[x_1, \ldots, x_n]/I(X)$ is an integral domain. Thus X is a variety if and only if $A(X)$ is an integral domain. The coordinate ring $A(X)$ is one of the main tools via which we want to study X. Integral domains are much more easy to work with than rings with zero divisors, this is the main reason why most of the time we will restrict our attention to varieties.

One of the nice properties of an integral domain is that one can form its quotient field. It will turn out that this quotient field will be very important for us to define and study regular functions and morphisms.

1.6. Dimension. As an application of the notion of irreducibility we can define the dimension of an irreducible affine variety or more generally of a Noetherian topological space. The idea is the following: A closed subset $Y \subsetneq X$ in an irreducible closed subvariety of $\mathbb{A}^n$ is given by at least one equation, so we should have $dim(Y) < dim(X)$.

Definition 1.31. Let $X \neq \emptyset$ be a irreducible topological space. The **dimension** $dim(X)$ of X is the largest integer n such that there is an ascending chain

$$\emptyset \neq X_0 \subsetneq X_1 \subsetneq \ldots \subsetneq X_n = X$$

of irreducible closed subsets of X. For a nonempty Noetherian topological space X the **dimension** of X is defined to be the maximum of the dimensions of the irreducible components of X.

Remark 1.32. (1) Points have dimension 0.

(2) $\mathbb{A}^1$ has dimension 1, as points are the only irreducible closed subsets of $\mathbb{A}^1$ not equal to $\mathbb{A}^1$.

(3) If the definition of dimension has anything to do with our intuition, then $\mathbb{A}^n$ must have dimension n. This is indeed the case, but in the moment we do not have the tools to prove this. Obviously we have $dim(\mathbb{A}^n) \geq n$, because

of the ascending chain

$$\{(0,\dots,0\} \subsetneq Z(x_2,\dots,x_n) \subsetneq \dots \subsetneq Z(x_2,\dots,x_n) \subsetneq \mathbb{A}^n.$$

Later when we have developed the theory further, we will study dimension carefully.

1.7. Hilbert Nullstellensatz. To an ideal $I \in k[x_1,\dots,x_n]$ we can associate its zero set $Z(I) \subset \mathbb{A}^n$ and to an affine algebraic set $X \subset \mathbb{A}^n$ we can associate its ideal $I(X)$. This gives inclusion reversing maps.

$$\left\{\begin{matrix}\text{affine algebraic sets}\\ \text{in } \mathbb{A}^n\end{matrix}\right\} \underset{Z}{\overset{I}{\rightleftarrows}} \left\{\begin{matrix}\text{ideals in}\\ k[x_1,\dots,x_n]\end{matrix}\right\}.$$

Question: To what extend are these two maps inverse to each other?

It is easy to see that $Z \circ I$ is the identity:

Remark 1.33. (1) By definition for any ideal I we have $I(Z(I)) \supset I$.

(2) For any affine algebraic set $X \subset \mathbb{A}^n$ we have $Z(I(X)) = X$.

Proof. (1) is obvious. (2) By definition $Z(I(X)) \supset X$. To prove the other inclusion, we know that $X = Z(I)$ for some ideal I. Thus by (1) $I \subset I(Z(I)) = I(X)$ and therefore $Z(I(X)) \subset Z(I) = X$. □

We will first deal with a much simpler version of the question: What is the condition that $Z(I) \subset \mathbb{A}^n$ is nonempty? We know that $Z(k[x_1,\dots,x_n]) = \emptyset$. We claim that for all other ideals the zero set is nonempty.

Theorem 1.34. *(Weak Hilbert Nullstellensatz). Let $I \subsetneq k[x_1,\dots,x_n]$ be a proper ideal. Then $Z(I) \neq \emptyset$.*

This is purely a statement of algebra, whose proof does not fit well with the rest of the course, therefore we will skip it. You can find it in Chapter 3 of these notes (but we will not do it).

Remark 1.35. The weak Nullstellensatz is most of the time used in the following form: Let $I \subset k[x_1,\dots,x_n]$ be an ideal with $Z(I) = \emptyset$. Then $1 \in I$.

Remark 1.36. We have made the assumption that k is algebraically closed. In fact the weak Nullstellensatz is false otherwise. E.g. $\langle x^2+1\rangle$ is a maximal ideal in $\mathbb{R}[x]$ because $\mathbb{R}[x]/\langle x^2+1\rangle \simeq \mathbb{C}$, but $Z(x^2+1) = \emptyset$.

Now we want to come back to our original question and study the relation between ideals and their zero sets. For an ideal in $J \subset k[x_1, \dots, x_n]$ it is in general not true that $I(Z(J)) = J$. For instance in $\mathbb{A}^1$ we have $I(Z(\langle x^n \rangle)) = I(\{0\}) = \langle x \rangle$. The point is that a polynomial f and a power f^n have the same zero set. Now we want to see that this is in fact the only thing that can happen: if $f \in I(Z(J))$, then a positive power f^n lies is I.

Definition 1.37. Let I be an ideal in a ring A. The **radical** of I is

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

$\sqrt{I}$ is an ideal: If $f^n \in I$, $a \in A$, then obviously $(af)^n = a^n f^n \in I$. If $f^n, g^m \in I$, then the binomial formula $(f+g)^{n+m} = \sum_i \binom{n+m}{i} f^i g^{n+m-i}$ implies that $(f+g)^{n+m} \in I$, because each summand $f^i g^{n+m-i}$ has either $i \geq n$ or $n+m-i \geq m$.

An ideal $I \subset A$ is called a **radical ideal**, if $I = \sqrt{I}$, or equivalently $I = \sqrt{J}$ for some ideal J.

Remark 1.38. Let $X \subset \mathbb{A}^n$ be an affine algebraic set. Then $I(X)$ is a radical ideal.

Proof. Let $f \in k[x_1, \dots, x_n]$ with $f^n \in I(X)$. Then for all $p \in X$ we have $f^n(p) = f(p)^n = 0$. Therefore $f(p) = 0$. Therefore $f \in I(X)$. □

The strong version of the Nullstellensatz gives the precise relation between I and $I(Z(I))$, namely $I(Z(I))$ is the radical of I.

Theorem 1.39. *(Hilbert Nullstellensatz) Let $I \subset k[x_1, \dots, x_n]$ be an ideal, then $I(Z(I)) = \sqrt{I}$.*

Proof. Write $I = \langle f_1, \dots, f_r \rangle$. We have seen that $I(Z(I))$ is a radical ideal containing I. Therefore $\sqrt{I} \subset I(Z(I))$. Let $f \in I(Z(I))$. We need to show that $f^N \in I$ for some $N > 0$. This is not obvious. We need to use a trick. We apply the weak Nullstellensatz in $k[x_1, \dots, x_n, t]$.

Let

$$J := \langle f_1, \dots, f_r, (ft-1) \rangle \subset k[x_1, \dots, x_n, t].$$

If $p \in \mathbb{A}^n$, $a \in k$, then $(p, a) \in \mathbb{A}^{n+1}$ and we get that $(p, a) \in Z(J)$, if and only if $p \in Z(I)$ and $f(p)a = 1$. But this is impossible because f vanishes on $Z(I)$, thus $f(p) = 0$. Thus $Z(J) = \emptyset$. By the weak Nullstellensatz $J = k[x_1, \dots, x_n, t]$. Thus we can write

$$1 = g_0(ft-1) + \sum_{i=1}^{r} g_i f_i \in k[x_1, \dots, x_n, t], \quad \text{for } g_i \in k[x_1, \dots, x_n, t],\ f_i \in I.$$

Now we need to go back to $k[x_1,\dots,x_n]$. Define a ring homomorphism

$$\varphi : k[x_1,\dots,x_n,t] \to k(x_1,\dots,x_n),\ f(x_1,\dots,x_n,t) \mapsto f(x_1,\dots,x_n,1/f),$$

this is obviously a ring homomorphism. As the f_i do not contain t, we have $\varphi(f_i) = f_i$, where we identify f_i with $\frac{f_i}{1} \in k(x_1,\dots,x_n)$. Furthermore $\varphi(ft-1) = \varphi(\frac{f}{f}-1) = 0$. Thus we get $1 = \sum_i \varphi(g_i) f_i$ in $k(x_1,\dots,x_n)$. Note that the only denominators that occur in the image of φ are powers f^n of f (as image of t^n). Thus we can write $\varphi(g_i) = \frac{G_i}{f^{n_i}}$ with $G_i \in k[x_1,\dots,x_n]$. Let N be the maximum of the n_i. Multiply this equation by f^N to get an equation in $k[x_1,\dots,x_n]$: $f^N = \sum_i G_i f^{N-n_i} f_i$. Thus $f^N \in \langle f_1,\dots,f_r\rangle = I$. □

Corollary 1.40. *We have mutually inverse inclusion-reversing bijections*

$$\left\{\begin{matrix}\textit{affine varieties}\\ \textit{in } \mathbb{A}^n\end{matrix}\right\} \underset{Z}{\overset{I}{\rightleftarrows}} \left\{\begin{matrix}\textit{radical ideals in}\\ k[x_1,\dots,x_n]\end{matrix}\right\}.$$

Corollary 1.41. *If $f \in k[x_1,\dots,x_n]$ is irreducible, then $Z(f)$ is irreducible.*

Proof. Let f be irreducible. Then, as $k[x_1,\dots,x_n]$ is a unique factorization domain, we know that $\langle f\rangle$ is a prime ideal. As prime ideals are radical it follows that $I(Z(f)) = \langle f\rangle$. Thus $Z(f)$ is irreducible. □

1.8. Exercises.

(1) Show that $\{(\cos(t),\sin(t)) \in \mathbb{A}^2_{\mathbb{R}} \mid t \in \mathbb{R}\}$ is an affine algebraic set.

(2) Is $\{(t,\sin(t)) \in \mathbb{A}^2_{\mathbb{R}} \mid t \in \mathbb{R}\}$ an affine algebraic set?

(3) Show that every affine algebraic set in $\mathbb{C}^n$ is closed in the standard Euclidean topology (Hint: Polynomials are continuous).

(4) Let $X \subset \mathbb{A}^n$ be an affine algebraic set, and $p \in \mathbb{A}^n \setminus X$.
Show there exists an $f \in k[x_1,\dots,x_n]$ with $f(p) = 1$ and $f|_X = 0$.

(5) Let $F_1,\dots,F_m \in k[x_1,\dots,x_n]$. Let $\varphi : \mathbb{A}^n \to \mathbb{A}^m$ be defined by $\varphi(p) = (F_1(p),\dots,F_m(p))$.
Show: The **graph** $\Gamma_\varphi := \{(p,q) \in \mathbb{A}^{n+m} \mid q = \varphi(p)\}$ is an affine algebraic set.

(6) Give an example of a countable collection of affine algebraic sets in $\mathbb{A}^n$ whose union is not an affine algebraic set.

(7) Show that the Zariski topology on $\mathbb{A}^n$ is strictly coarser than the Euclidean topology, i.e. all Zariski closed sets are closed in the Euclidean topology, but not all sets which are closed in the Euclidean topology are also closed in the Zariski topology.

(8) Identifying $\mathbb{A}^2$ with $\mathbb{A}^1 \times \mathbb{A}^1$, show that the Zariski topology on $\mathbb{A}^2$ is not the product topology of the Zariski topologies on two copies of $\mathbb{A}^1$.

(9) Let X be a topological space, $Y \subset X$ and $\{U_i\}_i$ an open cover of X. Show that Y is closed in X if and only if $Y \cap U_i$ is closed in U_i for all i.

(10) Show that polynomials $F \in k[x_1, \ldots, x_n]$ are continuous maps $f : \mathbb{A}^n \to \mathbb{A}^1$ (for the Zariski topology on $\mathbb{A}^n$ and on $\mathbb{A}^1$).

(11) Prove that the map $\varphi : \mathbb{A}^1 \to \mathbb{A}^3; t \mapsto (t, t^2, t^3)$ is continuous for the Zariski topology.

(12) Let $X, Y \subset \mathbb{A}^n$ be affine algebraic sets. Show that $X = Y$ if and only if $I(X) = I(Y)$.

(13) Let $I = \langle x^2 + y^2 - 1, x - 1\rangle$. Determine $X := Z(I)$, determine $I(X)$. Show that $I(Z(I)) \neq I$.

(14) Let 0 be the origin in $\mathbb{A}^n$. Show that $I(0) = \langle x_1, \ldots, x_n\rangle$ and $A(0) = k$.

(15) For $X = Z(x - y^2) \subset \mathbb{A}^2$, show $A(X) = k[x, y]/(x - y^2) \simeq k[x]$.

(16) Let X be an affine variety. Show that polynomial functions on X are continuous.

(17) Show that $Z(xy - z^2, y^5 - x^3) \subset \mathbb{A}^3$ has two irreducible components.

(18) Let $C = Z(F) \in \mathbb{A}^2$, for $F \in k[X, Y]$ an irreducible polynomial of degree $n > 1$. Let $L = Z(Y - aX - b)$ be a line in $\mathbb{A}^2$. Show that $L \cap C$ is a finite set, consisting of at most n points. (Hint: Consider $F(X, aX + b)$).

(19) Let $X, Y \subset \mathbb{A}^n$ be affine algebraic sets with $X \subset Y$. Show: Every irreducible component of X is contained in an irreducible component of Y.

(20) Recall that a topological space X is connected if the only subsets of X which are both open and closed are $\emptyset$ and X.

Let $X \neq \emptyset$ be a topological space. Prove that X is irreducible if and only if all nonempty open subsets of X are connected.

(21) A hypersurface $C \subset \mathbb{A}^2$ we call a plane curve. Show:
   (a) Any infinite subset of an irreducible plane curve $C \subset \mathbb{A}^2$ is dense in C.
   (b) Any bijective map between irreducible plane curves is a homeomorphism.

(22) Give an example of two irreducible subvarieties of $\mathbb{A}^3$ whose intersection is reducible.

(23) Let Z be a topological space and $\{U_\alpha\}$ be an open covering of Z such that $U_\alpha \cap U_\beta \neq \emptyset$ for $\alpha \neq \beta$ and that all U_α's are irreducible.

Prove that Z is irreducible.

(24) Show that a Noetherian topological space is quasicompact, i.e. every open cover has a finite subcover.

(25) Show that a Hausdorff Noetherian topological space is a finite set with the discrete topology.

(26) If two affine algebraic sets are isomorphic show that they have the same dimension.

(27) Let $\varphi : X \to Y$ be a surjective morphism of irreducible affine algebraic sets. Show that $dim(X) \geq dim(Y)$.

(28) Show: $\mathbb{A}^1$ has dimension 1.

(29) Let $C \subset \mathbb{A}^2$ be an irreducible plane curve. Show: C has dimension 1.

(30) Show that $Z(y - x^2) \subset \mathbb{A}^2$ is irreducible, in fact $I(Z(y - x^2)) = \langle y - x^2 \rangle$.

(31) Prove that the map $\varphi : \mathbb{A}^1 \to \mathbb{A}^3; t \mapsto (t, t^2, t^3)$ is continuous for the Zariski topology.

(32) Give an example of an irreducible $f \in \mathbb{R}[x, y]$ whose zero set in $\mathbb{A}^2_{\mathbb{R}}$ is not irreducible.

(33) Prove that the **cuspidal cubic** $C := Z(x^3 - y^2) \subset \mathbb{A}^2$ is irreducible.

2. Projective varieties

Let $X = Z(x - 1) \subset \mathbb{A}^2$ and for $a \in k$ let $Y_a = Z(x - ay) \subset \mathbb{A}^2$. Then X and Y_a are two lines in $\mathbb{A}^2$. For $a \neq 0$ we see that the intersection of X and Y_a is one point $(1, \frac{1}{a})$. For $a = 0$ however the intersection is empty. Intuitively the intersection point runs off to infinity as a goes to 0 and for $a = 0$ the lines are parallel. In some sense these parallel lines should still intersect, but "at infinity". Therefore we want to add some points at infinity to affine space and to affine varieties. This is done by introducing projective space $\mathbb{P}^n$ and defining projective algebraic sets as the zero sets of homogeneous polynomials on projective space. We will see that the elementary theory of projective algebraic sets is very similar to that of affine algebraic sets. Most of the definitions and results that we had in the affine case also work in the projective case. Thus we can introduce the Zariski topology on projective algebraic sets, we can consider their ideal. We can decompose them into irreducible components and can consider projective varieties, which are the irreducible projective algebraic sets. Finally there is also a projective version of the Nullstellensatz.

One can also view projective algebraic sets as compactifications of affine algebraic sets: Over the complex numbers and with the analytic topology we see that $\mathbb{A}^n$ and affine varieties (except for points) are not compact. But compact spaces are much nicer than non-compact ones. We want to "compactify" affine varieties by adding points at infinity. Over the complex numbers these are now compact in the analytic topology. We we will see later (at the end of chapter 2) that even with the Zariski topology they have a very similar property to compactness, which is called completeness.

2.1. Projective varieties. We introduce projective space $\mathbb{P}^n$ as the space of lines in k^{n+1} through the origin. We will in a moment see that $\mathbb{A}^n$ can be identified with a subset of $\mathbb{P}^n$.

Definition 2.1. On $k^{n+1} \setminus \{0\}$ we introduce an equivalence relation by

$$(a_0, \dots, a_n) \sim (\lambda a_0, \dots, \lambda a_n), \qquad \text{for all } \lambda \in k^* := k \setminus \{0\}.$$

The quotient set $\mathbb{P}^n := (k^{n+1}\setminus\{0\})/\sim$ is called **projective n-space**. The equivalence class of $(a_0, \dots, a_n)$ is denoted by $[a_0, \dots, a_n]$. The a_i are called the **homogeneous coordinates** of the point $p = [a_0, \dots, a_n] \in \mathbb{P}^n$. Note that giving the equivalence class $[a_0, \dots, a_n]$ is the same as giving the line $\big\{(\lambda a_0, \dots, \lambda a_n) \bigm| \lambda \in k\big\} \subset k^{n+1}$. Thus $\mathbb{P}^n$ is the space of lines in k^{n+1} through the origin.

We can see that $\mathbb{P}^n$ is the union of $n+1$ subsets which "look like $\mathbb{A}^n$". Choosing one of them, we can view $\mathbb{P}^n$ as being obtained from $\mathbb{A}^n$ by adding points at infinity.

Definition 2.2. Let $U_i := \big\{[a_0, \dots, a_n] \in \mathbb{P}^n \bigm| a_i \neq 0\big\}, \quad i = 0, \dots, n$. The map

$$\varphi_i : U_i \to \mathbb{A}^n,\ [a_0, \dots, a_n] \mapsto \big(\frac{a_0}{a_i}, \dots, \frac{\widehat{a_i}}{a_i}, \dots, \frac{a_n}{a_i}\big)$$

is obviously a bijection with inverse

$$u_i : \mathbb{A}^n \to U_i,\ (b_0, \dots, \widehat{b_i}, \dots, b_n) \mapsto [b_0, \dots, 1, \dots, b_n].$$

(As usual $\widehat{b_i}$ means that we remove b_i, so that we get a vector in $\mathbb{A}^n$). We call the $\frac{a_j}{a_i}$ the **affine coordinates** of $p = [a_0, \dots, a_n]$ with respect to U_i.

In particular we will want to use u_0 to view $\mathbb{P}^n$ as $\mathbb{A}^n$ with some points at infinity added. Thus sometimes we want to identify $\mathbb{A}^n$ and U_0 by identifying $(a_1, \dots, a_n)$ with $[1, a_1, \dots, a_n]$. Thus $\mathbb{A}^n$ becomes a subset of $\mathbb{P}^n$. For any subset $X \subset \mathbb{P}^n$ we thus have $X \cap \mathbb{A}^n = \varphi_0(X)$. In particular $\mathbb{P}^n = \mathbb{A}^n \cup H_\infty$, with $H_\infty := \mathbb{P}^n \setminus U_0 =$

$\big\{[a_0, a_1, \dots, a_n] \bigm| a_0 = 0\big\}$ the **hyperplane at infinity**. In case $n = 2$ we also call it the line at infinity. In case $n = 1$ we write $\infty := [0, 1]$. Thus $\mathbb{P}^1 = \mathbb{A}^1 \cup \infty$.

Now we want to define projective algebraic sets in $\mathbb{P}^n$ as zero sets of polynomials in $k[x_0, \dots, x_n]$. There is however a problem: Unlike the affine case, a polynomial $g \in k[x_0, \dots, x_n]$ does not define a function on $\mathbb{P}^n$: In general $g(a_0, \dots, a_n) \neq g(\lambda a_0, \dots, \lambda a_n)$. For instance for $f = x_1^2 - x_0$ we have $f(1, 1) = 0$ but $f(-1, -1) \neq 0$ although $[1, 1] = [-1, -1]$. If f is homogeneous this is not a problem, because whether f vanishes at a point $p \in \mathbb{P}^n$ does not depend on the representative.

Remark 2.3. If $g \in k[x_0, \dots, x_n]$ is homogeneous of degree d, then for all $\lambda \in k$,

$$g(\lambda a_0, \dots, \lambda a_n) = \lambda^d g(a_0, \dots, a_n).$$

This is because every monomial of g evaluated at $(a_0, \dots, a_n)$ is the product of d of the a_i. Thus replacing the a_i by the λa_i, each monomial is multiplied by λ^d. So the question whether $g(a_0, \dots, a_n) = 0$ depends only on $[a_0, \dots, a_n]$.

Definition 2.4. Let $g \in k[x_0, \dots, x_n]$ be homogeneous of degree d. One also says that g is a **form** of degree d. A point $p = [a_0, \dots, a_n]$ is a **zero** of g and we write $g(p) = 0$, if and only if $g(a_0, \dots, a_n) = 0$. By the above this is independent of the representative $(a_0, \dots, a_n)$. Let $S \subset k[x_0, \dots, x_n]$ be a set of homogeneous polynomials. The **projective zero set** of S is

$$Z(S) := \big\{p \in \mathbb{P}^n \bigm| f(p) = 0 \text{ for all } f \in S\big\}.$$

A subset of the form $Z(S)$ is called a **projective algebraic set**. If $S = \{f_1, \dots, f_r\}$, we write $Z(f_1, \dots, f_r) := Z(S)$. If f is a form of degree $d > 0$, then $Z(f)$ is called the **hypersurface** defined by f.

If we want to distinguish between the projective zero set and the affine zero set, we write $Z_p(S)$ for the projective zero set and $Z_a(S)$ for the affine zero set.

Example 2.5. (1) $\emptyset = Z(1)$; $\mathbb{P}^n = Z(\emptyset)$ are projective algebraic sets.

(2) If f is a homogeneous polynomial of degree 1, then $Z(f)$ is called a hyperplane.

(3) More generally, if $V \subset k^{n+1}$ is a sub-vector space of dimension $l + 1$, then $\mathbb{P}(V) := \big\{[a_0, \dots, a_n] \bigm| (a_0, \dots, a_n) \in V\ \big\}$ is called a **projective subspace** of $\mathbb{P}^n$ of dimension l. A projective subspace of dimension 1 is also called a **line**. V can be written as the intersection of $n - l$ hyperplanes, i.e. the zero set $\mathbb{P}(V) = Z(f_1, \dots, f_{n-l})$ of $n - l$ linear forms. Conversely every zero set $Z(f_1, \dots, f_r)$ of linear forms f_i is a projective subspace. In particular if

$f_1, \dots, f_{n-1}$ are linearly independent linear forms, then $Z(f_1, \dots, f_{n-1})$ is a **line**.

(4) Let $X = Z(x_1 - x_0)$ and $Y_a = Z(x_1 - ax_2)$ for $a \in k$ be two lines in $\mathbb{P}^2$. It is easy to see that $X \cap \mathbb{A}^2 = Z(x_1 - 1)$ and $Y_a \cap \mathbb{A}^2 = Z(x_1 - ax_2)$. Thus this is the example from the introduction to this section. We see that

$$X \cap Y_a = \{[b, b, c] \mid ac = b\} = \begin{cases} (1, \frac{1}{a}) & a \neq 0, \\ [0, 0, 1] & a = 0. \end{cases}$$

Thus the lines always intersect; in case $a = 0$ the intersection point is on the line at infinity.

Like in the affine case, all projective algebraic sets are the zero sets of ideals, and we can look at the ideal of a projective algebraic set. We only have to be slightly more careful, as we need to use homogeneous polynomials. Thus we want to use homogeneous ideals, i.e. ideals generated by homogeneous polynomials.

Definition 2.6. Any polynomial $f \in k[x_0, \dots, x_n]$ can be written in a unique way as a sum $f = f^{(0)} + \ldots + f^{(d)}$ of forms $f^{(i)}$ of degree i. The $f^{(i)}$ are called the **homogeneous components** of f.

An ideal $I \subset k[x_0, \dots, x_n]$ is called a **homogeneous ideal**, if for every $f \in I$, all the homogeneous components $f^{(i)}$ are in I.

Proposition 2.7. *An ideal $I \in k[x_0, \dots, x_n]$ is homogeneous, if and only if it is generated by homogeneous elements.*

Proof. Assume I is homogeneous. Let $\{f_\alpha\}_\alpha$ be generators of I. Then the $\{f_\alpha^{(i)}\}_{\alpha,i}$ are a set of homogeneous generators.

Let I be generated by homogeneous polynomials $\{g_i\}$. Then any $f \in I$ can be written as a finite sum $f = \sum_i a_i g_i$ for some $a_i \in k[x_0, \dots, x_n]$ (which need not be homogeneous). As g_i is homogeneous, the part of degree d of $a_i g_i$ is $a_i^{(d-deg(g_i))} g_i$. Thus we get $f^{(d)} = \sum_i a_i^{(d-deg(g_i))} g_i \in I$. □

Definition 2.8. For $I \subset k[x_0, \dots, x_n]$ a homogeneous ideal, the **zero set of** I is

$$Z(I) := \{p \in \mathbb{P}^n \mid f(p) = 0 \text{ for all homogeneous } f \in I\}.$$

For a subset $X \subset \mathbb{P}^n$ the **(homogeneous) ideal of** X is

$$I(X) := \langle f \in k[x_0, \dots, x_n] \text{ homogeneous} \mid f(p) = 0 \text{ for all } p \in X \rangle.$$

By definition this is a homogeneous ideal. If we want to distinguish it from the ideal of an affine algebraic set, we denote it by $I_H(X)$.

Remark 2.9. Even if $f \in k[x_0, \dots, x_n]$ is not homogeneous, we define $f(p) = 0$ if and only if $f(a_0, \dots, a_n) = 0$ for all representatives $(a_0, \dots, a_n)$ of p. Let $I \subset k[x_0, \dots, x_n]$ be any ideal. Let $I \subset k[x_0, \dots, x_n]$ be a homogeneous ideal. It is easy to check that with this definition

$$\begin{aligned} Z(I) &= \{p \in \mathbb{P}^n \mid f(p) = 0 \ \forall f \in I\}, \\ I(X) &= \{f \in k[x_0, \dots, x_n] \mid f(p) = 0 \ \forall p \in X\}. \end{aligned}$$

2.2. Zariski topology. The following is proven in the same way as for affine algebraic sets:

Proposition 2.10. (1) *If $X \subset Y$, then $I(X) \supset I(Y)$.*
(2) *If $Y \subset \mathbb{P}^n$ is a projective algebraic set, then $Z(I(Y)) = Y$.*
(3) *For any homogeneous ideal $I \subset k[x_0, \dots, x_n]$ we have $I \subset I(Z(I))$.*
(4) *If $S \subset T$ then $Z(S) \supset Z(T)$.*
(5) *Let $S \subset k[x_0, \dots, x_n]$ be a set of forms. Then $Z(S) = Z(\langle S \rangle)$.*
(6) *For a family $\{S_\alpha\}$ of sets of forms in $k[x_0, \dots, x_n]$ we have $Z\left(\bigcup_\alpha S_\alpha\right) = \bigcap_\alpha Z(S_\alpha)$.*
(7) *Let S, $T \subset k[x_0, \dots, x_n]$ be sets of forms. Then $Z(ST) = Z(S) \cup Z(T)$.*

In particular we see that finite unions and arbitrary intersections of projective algebraic sets are projective algebraic sets. As in the affine case, this allows us to introduce a topology on $\mathbb{P}^n$ for which the closed subsets are the projective algebraic sets.

Definition 2.11. The **Zariski topology** on $\mathbb{P}^n$ is the topology whose closed sets are the projective algebraic sets. If $X \subset \mathbb{P}^n$ is a subset, the induced topology on X (i.e. the one whose closed subsets are the intersections of X with closed subsets of $\mathbb{P}^n$) is called the **Zariski topology on** X.

Thus again we can talk about open and closed subsets, closure, continuous maps etc.

Definition 2.12. An open subset of a projective algebraic set is called **quasiprojective algebraic set**.

Remark 2.13. As $k[x_0, \dots, x_n]$ is Noetherian, we prove in the same way as in the affine case that that $\mathbb{P}^n$ and thus any subspace of $\mathbb{P}^n$ is a Noetherian topological space: if $X_1 \supset X_2 \supset \dots$ is a descending chain of closed subset of $\mathbb{P}^n$, then $I(X_1) \subset I(X_2) \subset \dots$ is an ascending chain of ideals in $k[x_0, \dots, x_n]$, which thus becomes stationary and thus also the original chain $X_1 \supset X_2 \supset \dots$ becomes stationary. In particular every quasiprojective algebraic set has a decomposition into irreducible components.

Again the irreducible quasiprojective algebraic sets are called varieties.

Definition 2.14. An irreducible projective algebraic set is called **projective variety** an irreducible quasiprojective algebraic set is called **quasiprojective variety** or also just **variety**.

Remark 2.15.

(1) Often in the literature a quasiprojective variety is not required to be irreducible.
(2) Often in the literature by variety one means an **abstract variety**, which is something more general than a quasiprojective variety. We will however only consider quasiprojective varieties.
(3) By our identification $\mathbb{A}^n$ is the open subset $\mathbb{P}^n \setminus Z(x_0)$ of $\mathbb{P}^n$. Thus $\mathbb{A}^n$, any affine variety and any quasiaffine variety are quasiprojective varieties.

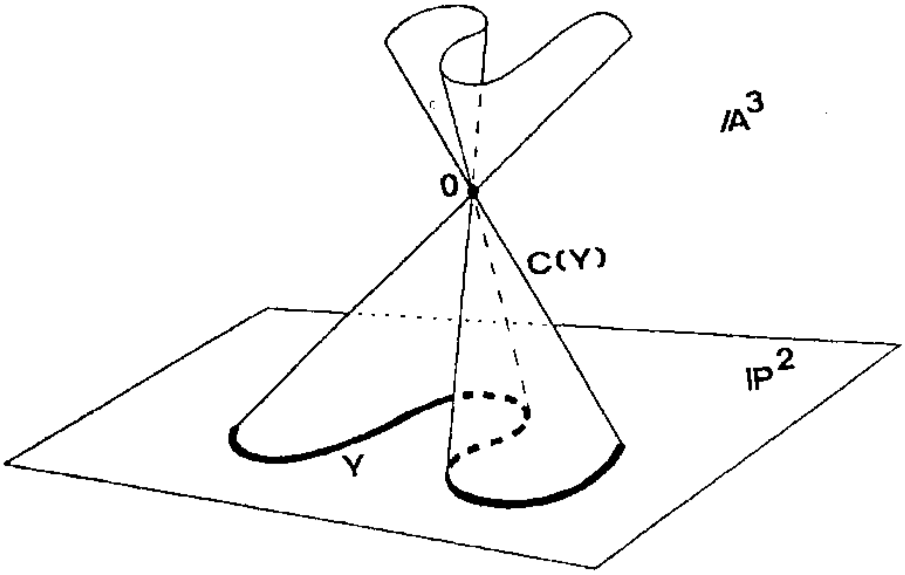
Remark 2.16. The definition of dimension for Noetherian topological spaces applies to irreducible quasiprojective varieties. We will see later that $dim(\mathbb{P}^n) = n$.

2.3. Affine cones and the projective Nullstellensatz. Now we prove the projective version of the Nullstellensatz, which gives a correspondence between the projective varieties in $\mathbb{P}^n$ and the homogeneous ideals in $k[x_0, \dots, x_n]$, very similar to the affine case. The proof is reduced to the affine case by making use of cones.

Definition 2.17. An nonempty affine algebraic set $X \subset \mathbb{A}^{n+1}$ is called a **cone**, if for all $\lambda \in k$, $p = (a_0, \dots, a_n) \in X$, we have $\lambda p = (\lambda a_0, \dots, \lambda a_n) \in X$, i.e. X contains the line through 0 and p. For $X \subset \mathbb{P}^n$ a projective algebraic set, the **affine cone** over X is

$$C(X) := \{(a_0, \dots, a_n) \in \mathbb{A}^{n+1} \mid [a_0, \dots, a_n] \in X\} \cup \{0\}.$$

Obviously this is a cone.



The cone over a curve in $\mathbf{P}^2$.

Lemma 2.18. *Let $X \neq \emptyset$ a projective algebraic set. Then*

(1) *$I(C(X))) = I_H(X)$,*
(2) *If $X = Z_p(I)$ for a homogeneous ideal I, then $C(X) = Z_a(I)$.*

In other words there is a one-one correspondence between nonempty projective algebraic sets and affine cones by taking the zero locus in $\mathbb{P}^n$ and $\mathbb{A}^{n+1}$ of the same homogeneous ideal.

Proof. Both (1) and (2) are reformulations of Remark 2.9. □

Now we can easily prove the projective version of the Nullstellensatz.

Theorem 2.19. *(Projective Nullstellensatz) Let $I \subset k[x_0, \dots, x_n]$ be a homogeneous ideal.*

(1) *$Z_p(I) = \emptyset$ if and only if I contains all forms of degree N for some N.*
(2) *If $Z_p(I) \neq \emptyset$ then $I_H(Z_p(I)) = \sqrt{I}$.*

Proof. Let $X := Z_p(I)$. (1) Then $X = \emptyset$ if and only if $C(X) = \{0\}$. As $C(X) = Z_a(I) \cup \{0\}$, we see that this means that $Z_a(I)$ is either empty or $\{0\}$. By the Nullstellensatz, this is equivalent to $\sqrt{I} = I(C(X)) \supset \langle x_0, \dots, x_n \rangle$. Therefore for each $i = 0, \dots, n$ there exists j_i with $x_i^{j_i} \in I$. We can take $N := j_0 + \ldots + j_n$, then every monomial of degree N is contained in I.

(2) Let $X = Z_p(I)$. Then (as $X \neq \emptyset$) we have $I_H(X) = I(C(X)) = I(Z_a(I)) = \sqrt{I}$, by the affine Nullstellensatz. □

So we get a very similar version of the Nullstellensatz, only the ideal $\langle x_0, \dots, x_n \rangle$ leads to exceptions. It is called the **irrelevant ideal**.

Corollary 2.20. *I_H and Z_p are mutually inverse bijections between non-irrelevant homogeneous radical ideals $I \subset k[x_0, \dots x_n]$ and projective algebraic sets $X \subset \mathbb{P}^n$.*

We can also see that, analogously to the affine case, projective varieties correspond to homogeneous prime ideals.

Proposition 2.21. (1) *A projective algebraic set $X \subset \mathbb{P}^n$ is irreducible if and only if $I_H(X)$ is a prime ideal.*

(2) *If $f \in k[x_0, \dots, x_n]$ is irreducible and homogeneous, then $Z_p(f) \subset \mathbb{P}^n$ is irreducible.*

Proof. (1) If $X \subset \mathbb{P}^n$ is reducible, then $X = X_1 \cup X_2$ for closed subsets $X_i \subsetneq X$. Then $C(X) = C(X_1) \cup C(X_2)$ is a reducible subset of $\mathbb{A}^{n+1}$ and thus $I_H(X) = I(C(X))$ is not prime.

Now assume that $I := I_H(X)$ is not prime. Then there exist $f, g \notin I$ with $fg \in I$. Let i, j be minimal with $f^{(i)}, g^{(j)} \notin I$. By subtracting homogeneous parts of f and g of lower degree, we can assume i and j are the lowest degrees occurring in f and g. Then $f^{(i)}g^{(j)}$ is the homogeneous component of minimal degree of the element fg of the homogeneous ideal I. Thus $f^{(i)}g^{(j)} \in I$, Let $X_1 = Z_p(I \cup \{f^{(i)}\})$, $X_2 = Z_p(I \cup \{g^{(j)}\})$. Then $X_1, X_2 \subsetneq X$ and $X = X_1 \cup X_2$. Thus X is reducible. (2) follows in the same way as in the affine case. □

2.4. Exercises.

(1) What points of $\mathbb{P}^2$ do not belong to two of the three sets U_0, U_1, U_2?

(2) Let I be a homogeneous ideal in $k[x_0, \dots, x_n]$. Show that I is prime if and only if: for any two forms $F, G \in k[x_0, \dots, x_n]$ with $FG \in I$, either $F \in I$ or $G \in I$.

(3) Let $I \in k[x_0, \dots, x_n]$ be a homogeneous ideal. Then $\sqrt{I}$ is a homogeneous ideal.

(4) Let $I, J \subset k[x_0, \dots, x_n]$ be homogeneous ideals. Show IJ and $I \cap J$ are homogeneous ideals.

(5) Show that every irreducible component of a cone is also a cone.

(6) Let $F \in k[x_0, \ldots, x_n]$ be homogeneous. Show the irreducible factors of F are homogeneous.

(7) Let V, W be algebraic sets and let $V \subset W$. Show: Each irreducible component of V is contained in an irreducible component of W.

(8) Let $C := Z(y^2z - (x^3 + axz^2 + bz^3)) \subset \mathbb{P}^2$. Under the isomorphisms $\varphi_i : U_i \to \mathbb{A}^2$ for $i = 0, 1, 2$ write down the equations of $\varphi_i(U_i \cap C)$. Determine the intersection of C with the $Z(x), Z(y), Z(z)$.

(9) Show that any two distinct lines in $\mathbb{P}^2$ intersect in one point.

(10) Let $Q_1 := Z(x^2 - yw), Q_2 := Z(xy - zw) \subset \mathbb{P}^3$. Show: Q_1 and Q_2 are irreducible, but $Q_1 \cap Q_2$ is the union of a twisted cubic and a line. This shows that the intersection of irreducible projective varieties need not be irreducible.

(11) Let $C = Z(x^2 - yz) \subset \mathbb{P}^2$. Let $L = Z(y) \subset \mathbb{P}^2$. Show that $C \cap L$ is one point p, but $I(p) \neq I(C) + I(L)$.

CHAPTER 2

Functions and Morphisms

We have now introduced affine and projective varieties and studied their first properties. In order to make any further progress in the theory we need to define and study the maps between these varieties which are compatible with the structure. These will be called morphisms. There is an easy way to define morphisms $f : X \to Y$ between affine varieties $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$; one can define them as polynomial maps $F = (F_1, \dots , F_m)$, given by an m-tuple of polynomials $F_i \in k[x_1, \dots , x_n]$. One can check that the pullback of $g \circ F$ of a polynomial function on Y is a polynomial function on X, that it polynomial maps preserve polynomial functions. We will take this as the most important defining property of morphism of more general quasiprojective varieties. We first define for each open set of a quasiprojective variety the regular functions on this open set. Then a morphism $F : X \to Y$ of quasiprojective varieties is defined as a continuous map, which is compatible with regular functions, i.e. if g is a regular function on an open subset $U \subset Y$, we require $g \circ F$ to be regular on $F^{-1}(U)$.

1. Regular and rational functions

Now we want to define regular functions on quasiaffine and quasiprojective varieties, the analogues of differentiable functions in differential geometry. As algebraic varieties are zero sets of polynomials, one should expect that the functions should just be the restrictions of polynomials. It turns out that these are not quite enough, we also need quotients of polynomials.

1.1. Regular functions on quasiaffine varieties. In this section let $X \subset \mathbb{A}^n$ be a closed subvariety of $\mathbb{A}^n$ and let $V \subset X$ be open. Thus V is a quasiaffine variety. We have already introduced the coordinate ring $A(X) = k[x_1, \dots , x_n]/I(X)$, and seen that it can be identified with the ring of polynomial functions

$$\big\{F|_X \;\big|\; F \in k[x_1, \dots , x_n]\big\}.$$

We will also write $A(V) := A(X)$ and call it the **coordinate ring** of V. We want to define regular functions on all open subsets of V. Naively one could think that this should just be the restrictions of polynomial functions, but this is not enough because we want regular functions to distinguish between different open subsets of V. We will therefore consider quotients of polynomial functions, by using the quotient field $Q(A(V))$. Note that here we are using that X (and thus V) is irreducible, because this is equivalent to $A(V)$ being an integral domain.

Reminder 1.1. Recall that the **quotient field** K of an integral domain R is the set of equivalence classes $\frac{f}{g}$ of pairs $(f,g) \in R$ with $g \neq 0$ via the equivalence relation

$$(f,g) \sim (f',g') \iff fg' = gf'.$$

Addition and multiplication are defined by

$$\frac{f}{g} + \frac{f'}{g'} = \frac{fg' + gf'}{gg'}, \quad \frac{f}{g} \cdot \frac{f'}{g'} = \frac{ff'}{gg'}.$$

It is easy to see that K is a field. Identifying $f \in R$ with $\frac{f}{1}$ we get that R is a subring of K.

Definition 1.2. The quotient field $K(V)$ of $A(V)$ is called the **field of rational functions** or just **function field** of V. Elements of $K(X)$ (resp. $K(V)$) are called **rational functions** on X (resp. on V).

We can use the rational functions to define the regular functions on open subsets of V.

Definition 1.3. Let $p \in V$. The **local ring** of V at p is

$$\mathcal{O}_{V,p} := \left\{ h \in K(V) \;\middle|\; \text{there exist } f,g \in A(X) \text{ s.th. } h = \tfrac{f}{g} \text{ and } g(p) \neq 0 \right\}.$$

In future we will just write this $\mathcal{O}_{V,p} := \left\{ \frac{f}{g} \in K(V) \;\middle|\; g(p) \neq 0 \right\}$. For $U \subset V$ an open subset, the **ring of regular functions** on U is the subring

$$\mathcal{O}_V(U) := \bigcap_{p \in V} \mathcal{O}_{V,p} \subset K(X).$$

Remark 1.4. By definition a regular function $h \in \mathcal{O}_V(U)$ is just an element $\frac{f}{g}$ in the quotient field $K(V)$ of $A(V)$. In what sense is a a function on U?

We will now check that $h \in \mathcal{O}_V(U)$ determines indeed a function $h : X \to k$. Furthermore we will also see that this function $h : X \to k$ determines the element $h \in \mathcal{O}_V(U)$, so we can (and will in future) identify elements of $\mathcal{O}_V(U)$ with the corresponding functions $U \to k$.

Let $h \in \mathcal{O}_V(U)$. Then h defines a function

$$h : U \to k,\ p \mapsto h(p) := \frac{f(p)}{g(p)} \text{ for any } f,g \in A(X) \text{ with } h = \tfrac{f}{g} \text{ and } g(p) \neq 0.$$

Note that this is well defined: If $\frac{f}{g} = \frac{f'}{g'}$ with $g'(p) \neq 0$, then $fg' = gf'$, thus $f(p)g'(p) = g(p)f'(p)$ and by $g(p) \neq 0 \neq g'(p)$ this implies $\frac{f(p)}{g(p)} = \frac{f'(p)}{g'(p)}$.

Conversely we want to see that the function $h : U \to k$ determines the corresponding element $h \in K(V)$. Let $h' \in \mathcal{O}_V(U)$ be another element with $h'(p) = h(p)$ for all $p \in U$. Then $(h - h')(p) = 0$ for all $p \in U$. We have to show that $l := h - h'$ is the zero element of $K(X)$. We can write $l = \frac{f}{g}$ with $f, g \in A(X)$, and $g \neq 0$. Let $W := U \setminus Z(g)$ which is a nonempty open subset of X. Then for $p \in W$ we have $0 = \frac{f(p)}{g(p)}$, i.e. $f(p) = 0$. Thus $W \subset Z(f)$. As W is dense in X we see that f is the zero function on X, thus f is the zero element of $A(X)$. Thus $l = \frac{0}{g}$ is the zero element of $K(X)$.

Note that this identification of elements of $\mathcal{O}_V(U)$ with functions $U \to k$ is compatible with with k-algebra structure on both sides. If $h = f + g$ (resp. $h = fg$) in $\mathcal{O}_V(U)$, then $h(p) = f(p) + g(p)$ (resp. $h(p) = f(p)g(p)$) for all $p \in U$.

Remark 1.5.
1. If $h \in K(V)$ is a rational function, then we can write $h = \frac{f}{g}$ with $f, g \in A(V)$ and $g \neq 0$. Thus $h \in \mathcal{O}_V(U)$ for the open set $U = V \setminus Z(g)$. Thus every rational function defines a regular function on an open dense subset of V.
2. If $h \in \mathcal{O}_{V,p}$, then we can choose g with $g(p) \neq 0$. Thus $p \in U$, i.e. an element of the local ring at p defines a regular function in a neighborhood of p.

One can show that the regular functions $f \in \mathcal{O}_V(U)$ are precisely the functions $f : U \to k$ which are **locally** quotients of polynomials.

Exercise 1.6. The above map $h \mapsto [p \mapsto h(p)]$ identifies $\mathcal{O}_V(U)$ with the ring of functions $h : U \to k$ with the following property: For each $p \in U$ there is an open neighborhood $W \subset U$ and $F, G \in k[x_1, \ldots, x_n]$, such that for all $q \in W$, $G(q) \neq 0$ and $h(q) = \frac{F(q)}{G(q)}$.

Remark 1.7. By the above we note that $\mathcal{O}_{V,p}$ is the ring of regular functions on a neighborhood of p. The **maximal ideal** at p is $\mathbf{m}_p := \{ f \in \mathcal{O}_{V,p} \mid f(p) = 0 \}$. It is the kernel of the evaluation morphism $ev_p : \mathcal{O}_{V,p} \to k; f \mapsto f(p)$. Therefore $\mathcal{O}_{V,p}/\mathbf{m}_p \simeq k$ and $\mathbf{m}_p$ is a maximal ideal.

If $h = \frac{f}{g} \in \mathcal{O}_{V,p}$ with $h(p) \neq 0$, then also its inverse $h^{-1} = \frac{g}{f}$ is in $\mathcal{O}_{V,p}$, thus h is a unit. So we see that $\mathbf{m}_p$ consists precisely of the non-units of $\mathcal{O}_{V,p}$.

Rings with this property have a name: A ring R is called **local ring** if it has precisely one maximal ideal consisting of all non-units.

The local ring at a point contains information about the properties of V near p. We will later see that we can determine the tangent space and singularities of V at p from $\mathcal{O}_{V,p}$.

On an affine variety the regular functions are just the polynomial functions: Recall that $A(X)$ is identified with the subring $\left\{\frac{f}{1} \mid f \in A(X)\right\}$ of $K(X)$.

Proposition 1.8. *Let X be an affine variety. Then $\mathcal{O}_X(X) = A(X)$.*

Proof. Obviously $A(X) \subset \mathcal{O}_X(X)$, so we need to show the other inclusion. Let $h \in \mathcal{O}_X(X)$. Then for any $p \in X$ we can write $h = \frac{[F]}{[G]}$, with $F, G \in k[x_1, \dots, x_n]$ and $G(p) \neq 0$. In other words there exists $G \in k[x_1, \dots, x_n]$ with $G(p) \neq 0$ and $h \cdot [G] \in A(X)$. Let

$$J := \left\{G \in k[x_1, \dots, x_n] \;\middle|\; h \cdot [G] \in A(X)\right\}$$

Then J is an ideal in $k[x_1, \dots, x_n]$, which contains $I(X)$. By the above we see $Z(J) \cap X = \emptyset$, and as $I(X) \subset J$, we see $Z(J) \subset X$. Thus $Z(J) = \emptyset$. By the Nullstellensatz $1 \in J$. Thus $h = h \cdot 1 \in A(X)$. □

We will see later that this result implies that the morphisms between affine varieties are precisely those given by polynomials.

1.2. Regular functions on quasiprojective varieties. For quasiprojective varieties we define regular and rational functions in a very similar way to the affine case. We have to replace polynomials by homogeneous polynomials. In this section let $X \subset \mathbb{P}^n$ be a projective variety, and let $V \subset X$ open, i.e. a quasiprojective variety. Like in the affine case the quotient of $k[x_0, \dots, x_n]$ by the ideal $I(X)$ of X will be very important for us.

Definition 1.9. Let $X \subset \mathbb{P}^n$ be a projective algebraic subset and let $I(X)$ be the homogeneous ideal of X. The **homogeneous coordinate ring** of X is $S(X) := k[x_0, \dots, x_n]/I(X)$.

$S(X)$ is an integral domain, because X is irreducible. We also write $S(V) := S(X)$.

Remark 1.10. Differently from the affine case, elements of $S(X)$ do not define functions on X because $f(\lambda a_0, \dots, \lambda a_n) \neq f(a_0, \dots, a_n)$. To get a well defined function one has to take the quotients $h = \frac{f}{g}$ of classes of polynomials of the same degree d, because then $\frac{f(\lambda a_0, \dots, \lambda a_n)}{g(\lambda a_0, \dots, \lambda a_n)} = \frac{\lambda^d f(a_0, \dots, a_n)}{\lambda^d g(a_0, \dots, a_n)}$.

Definition 1.11. For $f = [F] \in S(X)$ with $F \in k[x_0, \dots, x_n]$. The **homogeneous part of degree** d of f is $f^{(d)} := [F^{(d)}]$. Note that this is well defined: If $[F] = [G]$, then $[F - G] \in I(X)$. As $I(X)$ is a homogeneous ideal we have $F^{(d)} - G^{(d)} \in I(X)$ for all d, and thus $[F^{(d)}] = [G^{(d)}]$. We call

$$S(X)^{(d)} := \{f^{(d)} \mid f \in S(X)\}$$

the degree d part of $S(X)$.

Let $Q(S(X))$ be the quotient field of $S(X)$. The **field of rational functions** on V is defined as

$$K(V) = K(X) := \Big\{\frac{f}{g} \in Q(S(X)) \mid f, g \in S(X)^{(d)} \text{ for some } d\Big\}.$$

Thus the elements of $K(V)$ are quotients of elements of $S(X)$ which are homogeneous of the same degree. Elements of $K(V)$ are called **rational functions** on V.

For $f \in S(X)^{(d)}$ a homogeneous element the **zero set of** f is

$$Z(f) := \{p \in X \mid f(p) = 0\}.$$

This is a closed subset of X, because if $f = [F]$ for $F \in k[x_0, \dots, x_n]$, then $Z(f) = Z(F) \cap X$.

Definition 1.12. Let $p \in V$. The **local ring** of V at p is $\mathcal{O}_{V,p} := \big\{\frac{f}{g} \in K(V) \mid g(p) \neq 0\big\}$. For $U \subset V$ an open subset, the ring of regular functions on U is the subring

$$\mathcal{O}_V(U) := \bigcap_{p \in U} \mathcal{O}_{V,p} \subset K(V).$$

Again we will view regular functions on U as functions $U \to k$.

Remark 1.13. A regular function $h \in \mathcal{O}_V(U)$ defines a function

$$h : U \to k,\ p \mapsto h(p) := \frac{f(p)}{g(p)} \text{ for any } f, g \in S(X)^{(d)} \text{ with } h = \tfrac{f}{g} \text{ and } g(p) \neq 0.$$

In the same way as in the affine case we see that this is well-defined and identifies $\mathcal{O}_V(U)$ with the set of functions $h : U \to k$ with the following property: For any point $p \in X$ there exists an open neighbourhood $W \subset U$ and homogeneous polynomials $F, G \in k[x_0, \dots, x_n]$ of the same degree, with G nowhere zero on W, such that $h(q) = \frac{F(q)}{G(q)}$ for all $q \in U$.

For the rest of this section let V be a locally closed subvariety of $\mathbb{A}^n$ or of $\mathbb{P}^n$.

Remark 1.14. By the above a regular function $h \in \mathcal{O}_V(U)$ is determined by the corresponding function $U \to k$. Thus if $g, h \in \mathcal{O}_V(U)$ give the same function on an open subset $W \subset U$ then they are equal as elements of $\mathcal{O}_V(W) \subset K(X)$ and thus as elements of $\mathcal{O}_V(U)$, in particular they define the same function $U \to k$.

Now we want to show that regular functions fulfill some basic properties, that we will want to use all the time in future.

Proposition 1.15. *Let V be a quasiaffine or quasiprojective variety and let $U \subset V$ be open.*

(1) *(Regular functions are a k-algebra): Constant functions $a \in k$ are regular on U and if $f, g \in \mathcal{O}_V(U)$, then $f + g$, fg are regular functions.*
If furthermore $Z(g) = \emptyset$, then $f/g \in \mathcal{O}_V(U)$.
(2) *(Being regular is a local property): Let $\{U_i\}_i$ be an open cover of U. A function $h : U \to k$ is regular on U if and only if $h|_{U_i}$ is regular for all i.*
(3) *(Regular functions are continuous): Let $h \in \mathcal{O}_V(U)$. Then $h : U \to k$ is continuous ($k = \mathbb{A}^1$ is given the Zariski topology).*

Proof. (1) Obviously constant functions are regular. As $\mathcal{O}_V(U) = \bigcap_{p\in U} \mathcal{O}_{V,p}$, it is enough to see that for $f, g \in \mathcal{O}_{V,p}$ also $f + g$, $fg \in \mathcal{O}_{V,p}$. But this is clear, because $\mathcal{O}_{V,p}$ is a ring. Similarly, if $Z(g) = \emptyset$, then by definition $1/g \in \mathcal{O}_{V,p}$ for all $p \in U$. Thus $1/g \in \mathcal{O}_V(U)$ and therefore $\frac{f}{g} = f \cdot \frac{1}{g} \in \mathcal{O}_V(U)$.

(2) By definition a function $h : U \to k$ is regular if $h \in \mathcal{O}_{V,p}$ for all $p \in U$. Obviously this is equivalent to $h|_{U_i} \in \mathcal{O}_{V,p}$ for all $p \in U_i$ and for all i, i.e. to $h|_{U_i} \in \mathcal{O}_V(U_i)$ for all i.

(3) Obviously a map $U \to k$ is continuous if its restriction to a neighborhood of each $p \in U$ is continuous. Thus (by replacing U by such a neighborhood) we can assume that $h = \frac{f}{g}$ with f, g in $A(X)$ or $S(X)$ and $Z(g) \cap U = \emptyset$. Because the closed sets of k are just $\emptyset$, k and the finite sets, it is enough to show that $h^{-1}(a)$ is closed for all $a \in k$. But $h^{-1}(a) = \{q \in U \mid (f - ag)(q) = 0\} = Z(f - ag) \cap U$. □

Definition 1.16. Let $f \in \mathcal{O}_V(U)$. We put $Z(f) := \{p \in U \mid f(p) = 0\}$. By the last remark this is a closed subset of U.

Exercises.

(1) (a) Let $X = Z(y - x^2) \subset \mathbb{A}^2$. Show that $A(X)$ is isomorphic to $k[x]$.
(b) Let $X = Z(xy - 1) \subset \mathbb{A}^2$. Show that $A(X)$ is not isomorphic to $k[x]$.
(2) Let $Y := \{(t, t^2, t^3) \mid t \in \mathbb{A}^1\}$.
(a) Show that Y is an affine variety.

(b) Find generators for $I(Y)$.

(c) Show that $A(Y)$ is isomorphic to $k[x]$.

(3) Let $X \subset \mathbb{A}^n$ be an affine variety. A closed subvariety of X is an affine variety $Y \subset \mathbb{A}^n$ with $Y \subset X$. Show that the map

$$Y \mapsto I_X(Y) := \{f \in A(X) \mid f|_Y = 0\}$$

defines a natural bijection between irreducible closed subvarieties (resp. points) of X and prime ideals (resp. maximal ideals) of $A(X)$.

(4) Let $Y \subset X$ be an irreducible closed subvariety where $X \subset \mathbb{A}^n$ is an affine variety. Let $I_X(Y)$ be the ideal of Y in X as in the previous exercise. Show that $A(Y)$ is isomorphic to $A(X)/I_X(Y)$.

(5) Let $X := Z(x_1x_4 - x_2x_3) \subset \mathbb{A}^4$. You can assume as known that $x_1x_4 - x_2x_3$ is irreducible. Show $f := \frac{x_1}{x_2} = \frac{x_3}{x_4}$ is defined at (a_1, a_2, a_3, a_4) if and only if $a_2 \neq 0$ or $a_4 \neq 0$.

2. Morphisms

Now we define morphisms between varieties. The idea is that a variety X is completely determined by the regular functions on all open subsets of X. So a morphism should be a continuous map that preserves regular functions on open subsets. Also in differential geometry one could define a differentiable map as a continuous map that preserves differentiable functions on open subsets. We will show that the morphisms $X \to Y$ between affine varieties are just the polynomial maps, and that they are in one-one correspondence with the k-algebra homomorphism $A(Y) \to A(X)$.

Then we look at morphism to quasiprojective varieties. We will show that $\mathbb{A}^n$ is isomorphic to the open subset U_0 of $\mathbb{P}^n$ and thus every variety is isomorphic to a quasiprojective variety. Finally we will see that the morphisms between projective varieties are **locally** polynomial maps.

2.1. Polynomial maps. We have introduced affine algebraic sets. To study them, we need to know what the morphisms between affine algebraic sets are. That is, what are the maps compatible with the structure? Thus let $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ be affine algebraic sets. As X and Y are the zero sets of polynomials, the most natural definition is that the morphisms $\varphi : X \to Y$ should be given by an m-tuple of polynomials $F_1, \dots, F_m \in k[x_1, \dots, x_n]$ by $p \mapsto (F_1(p), \dots, F_m(p))$. These will be called polynomial maps. Once we have defined polynomial maps, we can also say when two algebraic sets X and Y are isomorphic, namely when there are polynomial maps $\varphi : X \to Y$ and $\psi : Y \to X$, which are inverse to each other. We will see that polynomial maps are compatible with polynomial functions: the pullback $\varphi^*(f) := f \circ \varphi$ of a polynomial function by a polynomial map is a polynomial function. Thus to every polynomial map $\varphi : X \to Y$, the pullback $\varphi^* : A(Y) \to A(X)$ is a homomorphism of k-algebras. We will see later that φ and φ^* determine each other. Later when we have introduced more tools, we will study morphisms much more carefully.

Definition 2.1. Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be affine algebraic sets. A map of the form

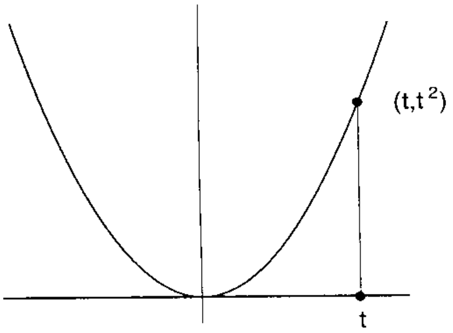
$$(F_1, \dots, F_m) : X \to Y, p \mapsto (F_1(p), \dots, F_m(p)), \qquad F_1, \dots, F_m \in k[x_1, \dots, x_n]$$

is called a **polynomial map**.

Note that $(F_1, \dots, F_m)$ and $(F_1|_X, \dots, F_m|_X)$ define the same map, thus we can also say that a polynomial map is given by an m-tuple of elements of $A(X)$. A bijective polynomial map whose inverse is also a polynomial map is called an **isomorphism** and in this case X and Y are called **isomorphic**.

Example 2.2. (1) The projection $\mathbb{A}^2 \to \mathbb{A}^1, (x, y) \to (x)$ is a polynomial map. It is not as isomorphism because it is not bijective.

(2) Let C be the plane parabola $Z(y-x^2) \subset \mathbb{A}^2$. The polynomial map $(t, t^2); A^1 \to C$ is an isomorphism, whose inverse is the projection $(x, y) \mapsto (x)$.



(3) Let X be an affine algebraic set. Then the polynomial maps $X \to \mathbb{A}^1$ are precisely the polynomial functions.

Now we want to see that polynomial maps are compatible with polynomial functions.

Definition 2.3. Let $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ be affine algebraic sets, and $\varphi := (F_1, \dots, F_m) : X \to Y$ a polynomial map. The **pullback** of $h \in A(Y)$ is $\varphi^*(h) := h \circ \varphi$. Note that $\varphi^*(h) \in A(X)$: If $h = H|_Y$ for $H \in k[y_1, \dots, y_m]$, then

$$\varphi^*(h)(a_1, \dots, a_n) = h(F_1(a_1, \dots, a_n), \dots, F_m(a_1, \dots, a_n)).$$

Thus $\varphi^*(h) = H(F_1, \dots, F_m)|_X$, where $H(F_1, \dots, F_m) \in k[x_1, \dots, x_n]$ is the polynomial obtained by replacing the y_i by $F_i(x_1, \dots, x_n)$.

It is clear from the definition, that the pullback of a constant function is a constant function and that $\varphi^*(f+g) = \varphi^*(f)+\varphi^*(g)$, $\varphi^*(fg) = \varphi^*(f)\varphi^*(g)$. Thus $\varphi^* : A(Y) \to A(X)$ is a homomorphism of k-algebras.

2.2. Definition of a morphisms.

Definition 2.4. Let X, Y be varieties. A map $\varphi : X \to Y$ is called a **regular map** or a **morphism** if

(1) φ is continuous;
(2) φ preserves regular functions, i.e. $\varphi^*(f) := f \circ \varphi \in \mathcal{O}_X(\varphi^{-1}(U))$ for all open subsets $U \subset Y$ and all $f \in \mathcal{O}_Y(U)$. (The condition that φ is continuous was put precisely so that $\varphi^{-1}(U)$ is open).

Thus for each open subset $U \subset X$ we get a k-algebra homomorphism $\varphi^* : \mathcal{O}_Y(U) \to \mathcal{O}_X(\varphi^{-1}(U))$. φ^* is called the **pullback** by φ.

Remark 2.5. (1) The identity map $id_X : X \to X$ is regular, and $id_X^* = id_{\mathcal{O}_X(U)}$ for all U.
(2) If $\varphi : X \to Y$ are morphisms of varieties, then the composition $\psi \circ \varphi$ is a morphism and $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.

Definition 2.6. An **isomorphism** $\varphi : X \to Y$ of varieties, is a bijective morphism whose inverse φ^{-1} is also a morphism. By the above we see that in this case $\varphi^* : \mathcal{O}_Y(U) \to \mathcal{O}_X(\varphi^{-1}(U))$ is an isomorphism; thus in particular $\mathcal{O}_X(X) \simeq \mathcal{O}_Y(Y)$.

Remark 2.7. (1) Let $\varphi : X \to Y$ be a map between varieties and assume that there is an open cover $(U_i)_i$ of X such that $\varphi|_{U_i}$ is a morphism for all i, then φ is a morphism.
(2) Let $Z \subset X$ and $W \subset Y$ be varieties, and let $\varphi : X \to Y$ be a morphism with $\varphi(Z) \subset W$. Then $\varphi|_Z : Z \to W$ is a morphism.

Proof. (1) Let $W \subset Y$ be open. Then $\varphi^{-1}(W) = \bigcup_i \varphi^{-1}(U_i \cap W)$ is open, and if $f \in \mathcal{O}_Y(W)$, then $f \circ \varphi$ is regular on all $\varphi^{-1}(U_i \cap W)$. Thus it is regular on W.

(2) $\varphi|_Z$ is continuous as the restriction of a continuous map. Let $h \in \mathcal{O}_W(U)$ be regular in a neighborhood of a point $h(p) \in W$. Then, making U possibly smaller, $h = \frac{[F]}{[G]}$ for polynomials F, G with G nowhere vanishing on U. This quotient also defines a regular function H in an open neighborhood $\widetilde{U}$ of $f(p)$ in Y. Then $H \circ \varphi \in \mathcal{O}(\varphi^{-1}(\widetilde{U}))$ and $h \circ \varphi = H \circ \varphi|_{\varphi^{-1}(U)} \in \mathcal{O}(\varphi^{-1}(U))$. □

If two varieties are isomorphic, we can consider them as being essentially the same.

Definition 2.8. A variety X is called **affine variety** if it is isomorphic to a an irreducible closed subset of affine space $\mathbb{A}^n$.

2.3. Morphisms to subvarieties of $\mathbb{A}^n$. We want to describe morphisms in a more explicit way. First we do this for morphisms to subvarieties of $\mathbb{A}^n$. They are just given by n-tuples of regular functions.

Theorem 2.9. *Let X, Y be varieties and assume $Y \subset \mathbb{A}^n$. A map $\varphi : X \to Y$ is a morphism, if and only if there exist regular functions $f_1, \dots, f_n \in \mathcal{O}_X(X)$ with $\varphi(p) = (f_1(p), \dots, f_n(p))$ for all $p \in X$. (We write $\varphi = (f_1, \dots, f_n)$).*

Proof. Let $\varphi : X \to Y$ be a morphism. Let $y_1, \dots, y_n$ be the restrictions of the coordinates on $\mathbb{A}^n$ to Y. If $q = (a_1, \dots, a_n) \in Y$, then $a_i = y_i(q)$. Then $f_i := \varphi^*(y_i) = y_i \circ \varphi \in \mathcal{O}_X(X)$. For $p \in X$ write $\varphi(p) = (b_1, \dots, b_n)$, then $b_i = y_i(\varphi(p)) = f_i(p)$. Thus $\varphi = (f_1, \dots, f_n)$.

Conversely let $\varphi = (f_1, \dots, f_n)$ with $f_i \in \mathcal{O}_X(X)$. φ is continuous: Let $B = X \cap Z(G_1, \dots, G_m)$ be closed in Y, for G_i polynomials. If $G = \sum a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$ is any of the G_i, then $G \circ \varphi = G(f_1, \dots, f_n) = \sum a_{i_1 \dots i_n} f_1^{i_1} \dots f_n^{i_n} \in \mathcal{O}_X(X)$, because $\mathcal{O}_X(X)$ is a k-algebra. Thus $\varphi^{-1}(B) = Z(G_1 \circ \varphi, \dots, G_m \circ \varphi) \cap Y$ is closed in X.

Now let $h \in \mathcal{O}_Y(U)$. We write $W = \varphi^{-1}(U)$. We have to show that $\varphi^*(h) \in \mathcal{O}_X(W)$. We can replace U by a smaller open neighboughhood of any $p \in U$, and thus assume that $h(p) = \frac{F(p)}{G(p)}$ for all $p \in U$ and $G(p) \neq 0$, with polynomials F, G. Thus on W we have $\varphi^*(h) = \frac{F(f_1, \dots, f_n)}{G(f_1, \dots, f_n)}$. As $\mathcal{O}_X(W)$ is a k-algebra, we have that $F(f_1, \dots, f_n), G(f_1, \dots, f_n) \in \mathcal{O}_X(W)$ and as $G(f_1, \dots, f_n)$, has no zero in W, we get $\varphi^*(h) \in \mathcal{O}_X(W)$. □

Corollary 2.10. *In particular regular functions $f \in \mathcal{O}_X(X)$ are the same as morphisms $f : X \to \mathbb{A}^1$.*

It follows also that morphisms between closed subvarieties of affine spaces are the polynomial maps.

Corollary 2.11. *Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be closed subvarieties. The morphisms $\varphi : X \to Y$ are precisely the polynomial maps.*

Proof. This follows immediately because $\mathcal{O}_X(X) = A(X)$. □

We can also see that for affine varieties X, Y, morphisms $X \to Y$ are the same as homomorphisms of k-algebras $A(Y) \to A(X)$.

Theorem 2.12. *Let X, Y varieties and assume $Y \subset \mathbb{A}^n$ closed. Then there is a natural $1:1$ correspondence*

$$\textit{(morphisms } X \to Y\textit{)} \leftrightarrow \textit{(}k\textit{-algebra homomorphisms } A(Y) \to \mathcal{O}_X(X)\textit{)}$$
$$\varphi \mapsto \varphi^*$$

In particular if also X is affine, there is a natural bijection between morphisms $X \to Y$ and homomorphisms $A(Y) \to A(X)$.

Proof. If $\varphi : X \to Y$ is a morphism, $\varphi^* : A(Y) \to \mathcal{O}_X(X)$ is obviously a k-algebra homomorphism. Now let $\Phi : A(Y) \to \mathcal{O}_X(X)$ be a k-algebra homomorphism. Let $y_1, \dots, y_n$ be the restrictions of the coordinate functions to Y. We put $f_i := \Phi(y_i) \in \mathcal{O}_X(X)$. Then $\varphi := (f_1, \dots, f_n) : X \to \mathbb{A}^n$ is a morphism. To see that φ is a morphism $X \to Y$ we need to show that $\varphi(X) \subset Y$. Let $h \in I(Y)$. Then

$$h \circ \varphi = h(f_1, \dots, f_n) = \Phi(h(y_1, \dots, y_n)) = 0,$$

because $h(y_1, \dots, y_n) = h|_Y = 0$. Thus $\varphi(X) \subset Z(I(Y)) = Y$. Thus we get a morphism $\varphi : X \to Y$.

It is straightforward to check that the maps $\varphi \mapsto \varphi^*$, $\Phi \mapsto \varphi$ are inverse to each other. □

So studying affine varieties is equivalent to studying finitely generated k-algebras.

Example 2.13.

(1) Let $\varphi : \mathbb{A}^1 \to \mathbb{A}^3, a \mapsto (a, a^2, a^3)$. Then $\varphi = (t, t^2, t^3)$ is a polynomial map. The image is the rational normal curve $C = Z(x_2 - x_1^2, x_3 - x_1^3)$. So we can view φ also as a polynomial map $\varphi : \mathbb{A}^1 \to C$. This is an isomorphism. The inverse morphism is the projection (x_1).

(2) A bijective polynomial map need not be an isomorphism: Let $C := Z(x^2 - y^3) \subset \mathbb{A}^2$. C is called the **cuspidal cubic**. There is a polynomial map $\varphi = (t^2, t^3) : \mathbb{A}^1 \to C$. It is easy to see that C is bijective with inverse $g(a, b) = b/a$ for $a \neq 0$, $g(0, 0) = 0$. φ is not an isomorphism because

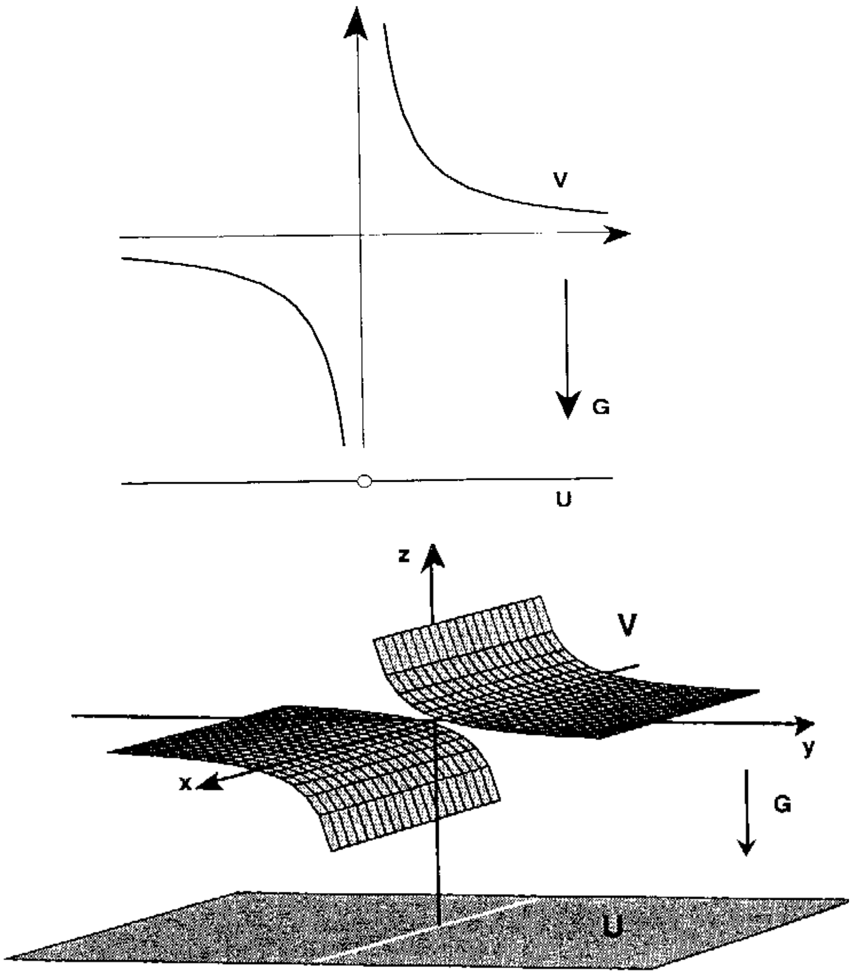
$$\varphi^* : k[C] = k[x, y]/(x^2 - y^3) \to k[t]; x \mapsto t^2,\ y \mapsto t^3$$

is not surjective: t is not in the image. We will see later that $\mathbb{A}^1$ is "smooth" and C has a "singularity" at $(0,0)$.

Now we want to show that there are more affine varieties than just the closed subvarieties of $\mathbb{A}^n$.

Definition 2.14. Let $X \subset \mathbb{A}^n$ be a closed subvariety, and let $F \in k[x_1, \dots, x_n]$ with $X \not\subset Z(F)$. The **principal open** defined by F is $X_F = X \setminus Z(F)$.

Proposition 2.15. *X_F is an affine variety.*



Proof. Let $Z := Z(I(X) + (Fx_{n+1} - 1)) \subset \mathbb{A}^{n+1}$. We want to show that Z is a subvariety of $\mathbb{A}^{n+1}$ isomorphic to X_F. Let $\varphi : (x_1, \dots, x_n, \frac{1}{[F]}) : X_F \to \mathbb{A}^{n+1}$. $[F]$ has no zero on X_F, thus $\frac{1}{[F]}$ is regular and φ is a morphism. It is obvious that φ is bijective with image Z. As X_F is irreducible, it follows that Z is irreducible (if $Z = Z_1 \cup Z_2$ with $Z_i \subsetneq Z$ closed, then $X_F = \varphi^{-1}(Z_1) \cup \varphi^{-1}(Z_2)$ with the $\varphi^{-1}(Z_i) \subsetneq X_F$ closed). Thus Z is a closed subvariety of $\mathbb{A}^{n+1}$ and $\varphi : X_F \to Z$ is a morphism. Obviously $\varphi^{-1} := (x_1, \dots, x_n) : Z \to X_F$ is also a morphism. □

2.4. Morphisms of quasiprojective varieties. Now we want to study morphisms of quasiprojective varieties. We will show that $\mathbb{A}^n$ is isomorphic to the open subset U_0 of $\mathbb{P}^n$ and thus every variety is isomorphic to a quasiprojective variety. We will use this to show that a morphisms between quasiprojective varieties is locally a polynomial map.

We can use the homogeneous coordinate ring to define the analogue of polynomial maps for projective algebraic sets.

Definition 2.16. Let $X \subset \mathbb{P}^n$, $Y \subset \mathbb{P}^m$ be projective algebraic sets. A map $\varphi : X \to Y$ is called a **polynomial map** if there are homogeneous polynomials $F_0, \dots, F_m \in k[x_0, \dots, x_n]$ with no common zero on X, such that for all $p \in X$ we have $\varphi(p) = [F_0(p), \dots, F_m(p)]$. We write $\varphi = [F_0, \dots, F_m]$. Instead of polynomials one can also use elements of the homogeneous polynomial ring $S(X)$.

Remark 2.17. Note that $F_i(p)$ is not well defined, as it depends on the representative of p, however the point

$$[F_0(p), \dots, F_m(p)] = [F_0(a_0, \dots, a_n), \dots, F_m(a_0, \dots, a_n)]$$

is independent of the representative $(a_0, \dots, a_n) \in k^{n+1}$. The condition that the F_i have no common zero on X ensures that $[F_0(p), \dots, F_m(p)]$ is a well-defined point of $\mathbb{P}^m$ for all $p \in X$.

Example 2.18. $[x_0^2, x_0x_1, x_1^2] : \mathbb{P}^1 \to \mathbb{P}^2$ is a polynomial map. One sees that the image is $Z(y_0y_2 - y_1^2)$.

Above we defined the open cover of $\mathbb{P}^n$ by subsets $U_i := \{[a_0, \dots, a_n] \in \mathbb{P}^n \mid a_i \neq 0\}$ and showed that $\varphi_i : U_i \to \mathbb{A}^n, [a_0, \dots, a_n] \mapsto (\frac{a_0}{a_i}, \dots, \widehat{\frac{a_i}{a_i}}, \dots, \frac{a_n}{a_i})$ is a bijection with inverse $u_i : (a_0, \dots, \widehat{a}_i, \dots, a_n) \mapsto [a_0, \dots, 1, \dots, a_n]$. Now we show that φ_i is an isomorphism.

Definition 2.19. The **dehomogenization** of $F \in k[x_0, \dots, x_n]$ is $F_a := F(1, x_1, \dots, x_n) \in k[x_1, \dots, x_n]$.

Theorem 2.20. (1) *$\varphi_i : U_i \to \mathbb{A}^n$ is an isomorphism.*

(2) *Every variety is isomorphic to a quasiprojective variety.*

(3) *Every variety has an open conver by affine varieties.*

Proof. (1) We can assume $i = 0$, we write $\varphi = \varphi_0$ and $U = U_0$. We can write $\varphi = (\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0})$, and the $\frac{x_i}{x_0}$ are regular on U. Thus φ is a morphism. We know that φ is bijective with inverse $u_0(a_1, \dots, a_n) = [1, a_1, \dots, a_n]$. φ^{-1} **is continuous:** Let $W = Z(F_1, \dots, F_m) \cap U$ for $F_i \in k[x_0, \dots, x_n]$ homogeneous. Then

$$\varphi(W) = \big\{(a_1, \dots, a_n) \in \mathbb{A}^n \bigm| F_i(1, a_1, \dots, a_n) = 0 \text{ for all } i\big\} = Z((F_1)_a, \dots, (F_n)_a)$$

is closed in $\mathbb{A}^n$ Finally let $h \in \mathcal{O}_U(V)$. By making V smaller, we can write $h = \frac{F}{G}$ for $F, G \in k[x_0, \dots, x_n]$ forms of the same degree with G nowhere zero on V. Then

$$(\varphi^{-1})^* h = \frac{F \circ \varphi^{-1}}{G \circ \varphi^{-1}} = \frac{F_a}{G_a} \in \mathcal{O}_{\mathbb{A}^n}(\varphi(U)).$$

(2) Let X be a variety, we can assume $X \subset \mathbb{A}^n$ is locally closed, because otherwise there is nothing to prove. Then $Y := \varphi^{-1}(X)$ is locally closed in U_0 and thus in $\mathbb{P}^n$, and, as φ is a homeomorphism, it is also irreducible, i.e. a quasiprojective variety. Then $\varphi : Y \to X$ is an isomorphism as a restriction of an isomorphism.

(3) If $X \subset \mathbb{P}^n$ is a quasiprojective variety, then $X = \bigcup_{i=0}^n X \cap U_i$ is an open cover of X by varieties isomorphic to locally closed subvarieties of $\mathbb{A}^n$. So we can assume that $X \subset \mathbb{A}^n$ is a locally closed subvariety, i.e. $X = Y \setminus Z$ with Y, Z closed subsets of $\mathbb{A}^n$. Let $p \in X$. It is enough to find an open affine subset of X containing p. As $p \in Y \setminus Z$, there exists $F \in I(Z)$ with $F(p) \neq 0$. Then $p \in Y_F \subset X$ and Y_F is affine. □

Remark 2.21.

(1) Above we said that we sometimes want to identify $(a_1, \dots, a_n) \in \mathbb{A}^n$ with $[1, a_1, \dots, a_n] \in \mathbb{P}^n$, so that $\mathbb{A}^n$ is a subset of $\mathbb{P}^n$. Now see we that $\mathbb{A}^n$ is an open subvariety of $\mathbb{P}^n$. In particular the Zariski topology on $\mathbb{A}^n$ is the induced topology of the Zariski topology on $\mathbb{P}^n$. Any closed subvariety X of $\mathbb{A}^n$ is an open subvariety of its closure $\overline{X}$ in $\mathbb{P}^n$. $\overline{X}$ is called the **projective closure** of X. We view it as compactification of X.
(2) Note that with this identification locally closed subvarieties of $\mathbb{A}^n$ are quasiprojective varieties. Thus all varieties are quasiprojective varieties.

We give a simple description of morphisms to quasiprojective varieties, similar to the affine case. Locally they are polynomial maps.

Theorem 2.22. *Let $X \subset \mathbb{P}^m$ and $Y \subset \mathbb{P}^n$ be quasiprojective varieties and $\varphi : X \to Y$ a map. The following are equivalent:*

(1) *φ is a morphism.*

(2) *φ is locally a polynomial map: For all $p \in X$ there exists an open neighbourhood $U \subset X$ and polynomials $F_0, \dots, F_n \in k[x_0, \dots, x_m]$ of the same degree, with no common zero on U such that*

$$\varphi(q) = [F_0(q), \dots, F_n(q)] \text{ for all } q \in U.$$

We write $\varphi = [F_0, \dots, F_n]$ on U.

(3) *φ is locally given by regular functions: For all $p \in X$ there exists an open neighbourhood $U \subset X$ and $h_0, \dots, h_n \in \mathcal{O}_X(U)$ with no common zero such that $\varphi = [h_0, \dots, h_n]$ on U.*

Proof. (1)⇒(2) Let $\varphi : X \to \mathbb{P}^n$ be a morphism and $p \in X$. Then $\varphi(p) \in U_i$ for some i. For simplicity of notation assume $i = 0$, i.e. $p \in \mathbb{A}^n$. Let U be a neighborhood of p with $\varphi(U) \subset \mathbb{A}^n$. Then $\varphi|_U : U \to \mathbb{A}^n$ is a morphism. Thus $\varphi|_U = (h_1, \dots, h_n) = [1, h_1, \dots, h_n]$, $\quad h_i \in \mathcal{O}_X(U)$.

(2)⇒(3) By making U possibly smaller, we can assume that for all i we have $h_i = \frac{F_i}{G_i}$, with F_i, G_i polynomials of the same degree and G_i nonzero on U. We put $L_i := F_i G_0 \dots \widehat{G_i} \dots G_n$. Then the L_i are homogeneous polynomials of the same degree, and $\varphi|_U = [h_0, \dots, h_n] = [L_0, \dots, L_n]$.

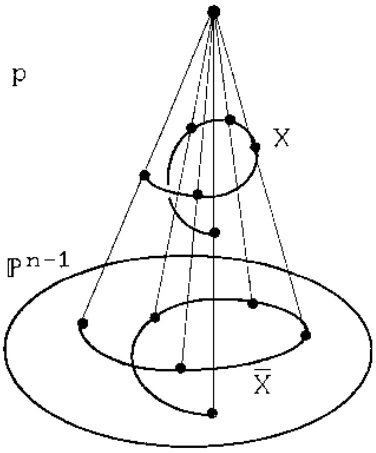
(3)⇒(1) Let $\varphi|_U = [H_0, \dots, H_n]$, where H_i are homogeneous polynomials of the same degree with no common zero on U. By making U smaller we can assume one of the H_i, say H_0, is nowhere vanishing on U. Then $h_i = \frac{H_i}{H_0} \in \mathcal{O}_X(U)$. Therefore $\varphi|_U = (h_1, \dots, h_n) : U \to \mathbb{A}^n$. Thus φ is a morphism in a neighborhood of every point, thus it is a morphism. □

Example 2.23. Let $X = \mathbb{P}^1$, $Y = Z(y_0 y_2 - y_1^2) \subset \mathbb{P}^2$. $\varphi = [x_0^2, x_0x_1, x_1^2] : X \to Y$ is an isomorphism and the inverse is $\varphi^{-1} = \begin{cases} [y_0, y_1] & , y_0 \neq 0 \\ [y_1, y_2] & , y_2 \neq 0 \end{cases}$. Where $x_0 \neq 0$ we get $\varphi^{-1} \circ \varphi = [x_0^2, x_0 x_1] = [x_0, x_1]$, and where $y_0 \neq 0$ we get $\varphi \circ \varphi^{-1} = [y_0^2, y_0y_1, y_1^2] = [y_0^2, y_0y_1, y_0y_2] = [y_0, y_1, y_2]$.

Definition 2.24. Let $A = \begin{pmatrix} a_{00} & \dots & a_{0n} \\ & \dots & \\ a_{m0} & \dots & a_{mn} \end{pmatrix}$ be an $(n+1) \times (n+1)$-matrix with coefficients in k, and assume $ker(A) = 0$. Then the map $[A] : \mathbb{P}^n \to \mathbb{P}^n, [b_0, \dots, b_n] \mapsto [A(b_0, \dots, b_n)]$ is called a **projective transformation** or a **projective change of coordinates**.. Note that $[A] = [a_{00}x_0 + \dots + a_{0n}x_n, \dots, a_{n0}x_0 + \dots + a_{nn}x_n]$, thus $[A]$ is a morphism. It is an isomorphism, its inverse is $[A^{-1}]$. One can show (but we will not) that all automorphisms of $\mathbb{P}^n$ are projective transformations.

Definition 2.25. (Projections) Let $X \subset \mathbb{P}^n$ be a subvariety and let $W \subset \mathbb{P}^n$ be a projective linear subspace of dimension k. Assume $W \cap X = \emptyset$. Then there exist $n-k$ linearly independent linear forms $H_0, \ldots, H_{n-k-1}$ such that $W = Z(H_0, \ldots, H_{n-k-1})$. The **projection from** W is the morphism $\pi_W = [H_0, \ldots, H_{n-k-1}] : X \to \mathbb{P}^{n-k-1}$. That $W \cap X = \emptyset$ means precisely that the H_i never vanish simultaneously on X. Note that the projection $\pi_W : X \to \mathbb{P}^{n-k-1}$ does not only depend on W, but on the choice of $H_0, \ldots, H_{n-k-1}$. However for any other choice $L_0, \ldots, L_{n-k-1}$, we see that both the L_i and the H_i are a basis of the vector space of linear forms vanishing on W. Thus there is an invertible $(n-k) \times (n-k)$-matrix A such that $L_i = \sum_j a_{ij} H_j$. Thus $[L_0, \ldots, L_{n-k}] = [A] \circ [H_0, \ldots, H_{n-k}]$ for the projective transformation $[A] : \mathbb{P}^{n-k-1} \to \mathbb{P}^{n-k-1}$. Thus projections from linear subspaces are uniquely determined up to projective transformations.

The most important case is the **projection from a point**. In particular the projection from $P = [0, \ldots, 0, 1] \in \mathbb{P}^n$ is $\pi_P = [x_0, \ldots, x_{n-1}]$.



Remark 2.26. (1) We can identify $\mathbb{P}^{n-1}$ with $Z(x_n) \subset \mathbb{P}^n$, via $[a_0, \ldots, a_{n-1}] \mapsto [a_0, \ldots, a_{n-1}, 0]$. Then π_p sends each point $q \in \mathbb{P}^n \setminus \{p\}$ to the intersection point of the line $\overline{pq}$ through p and q with $Z(x_n)$.

(2) The projection from a linear subspace is the composition of projections from a point: e.g.

$$\pi_{Z(x_0,\ldots,x_k)} = \pi_{p_{k+1}} \circ \ldots \circ \pi_{p_n}, \quad p_l = [0, \ldots, 0, 1] \in \mathbb{P}^l.$$

Exercises.

(1) X, Y be affine varieties and let $\varphi : X \to Y$ be a polynomial map. Show that φ is continuous.

(2) The twisted cubic in $\mathbb{A}^3$ is $C := Z(y-x^2, z-x^3)$. Show that C is isomorphic to $\mathbb{A}^1$.

(3) Show that $Z(xy) \subset \mathbb{A}^2$ is not isomorphic to $\mathbb{A}^1$.

(4) Let $C := Z(y^2 - (x^3 + x^2))$ be the nodal cubic. You can assume as known that $I(C) = \langle y^2 - (x^3 + x^2)\rangle$. Show that C is not isomorphic to $\mathbb{A}^1$.

(5) Let $\varphi = (F_1, \dots, F_n) : \mathbb{A}^n \to \mathbb{A}^n$ is an isomorphism. Show that the **Jacobian determinant**

$$det \begin{pmatrix} \frac{\partial F_1}{\partial x_1} & \cdots & \frac{\partial F_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial F_n}{\partial x_1} & \cdots & \frac{\partial F_n}{\partial x_n} \end{pmatrix}$$

is a nonzero constant polynomial. In case $k = \mathbb{C}$ the converse is a famous open problem, called the **Jacobian Conjecture**.

(6) If two affine algebraic sets are isomorphic show that they have the same dimension.

(7) Let $\varphi : X \to Y$ be a surjective morphism of irreducible affine algebraic sets. Show that $dim(X) \geq dim(Y)$.

(8) Let $\varphi : \mathbb{A}^1 \to \mathbb{A}^n$ be the map defined by $t \to (t, t^2, \dots, t^n)$.
   (a) Prove that φ is regular and describe $\varphi(\mathbb{A}^1)$.
   (b) Prove that $\varphi : \mathbb{A}^1 \to \varphi(\mathbb{A}^1)$ is an isomorphism.

(9) Show that $C := Z(xy - 1) \subset \mathbb{A}^2$ and $\mathbb{A}^1$ are not isomorphic.

(10) Which of the following affine varieties are isomorphic?
   (a) $\mathbb{A}^1$,
   (b) $Z(x^2 + y^2) \subset \mathbb{A}^2$,
   (c) $Z(x^2 - y^3) \subset \mathbb{A}^2$,
   (d) $Z(xy) \subset \mathbb{A}^2$,
   (e) $Z(y - x^2, z - x^3) \subset \mathbb{A}^3$

(11) Let $GL_n(k)$ be the set of invertible $n \times n$ matrices with entries in k. Prove that $GL_n(k)$ can be given the structure of an affine variety.

(12) Let $f : \mathbb{A}^2 \to \mathbb{A}^2$ be defined by: $(x, y) \to (x, xy)$. Describe $f(\mathbb{A}^2)$ and prove that it is not locally closed in $\mathbb{A}^2$.

(13) Show that $[0, x_0, \dots, x_{n-1}] : \mathbb{P}^{n-1} \to H_\infty$ is an isomorphism.

(14) Let $\varphi : X \to Y$ be a surjective morphism of varieties. Let $Z \subset Y$ be closed. Show: If $\varphi^{-1}(Z)$ is irreducible, then Z is irreducible.

(15) A conic in $\mathbb{A}^2$ is $Z(f)$ where $f \in k[x,y]$ is an irreducible polynomial of degree 2. A conic in $\mathbb{P}^2$ is $Z(F)$ where $F \in k[x,y,z]$ is irreducible and homogeneous of degree 2.

(a) Show that any conic in $\mathbb{A}^2$ is either isomorphic to $\mathbb{A}^1$ or to $\mathbb{A}^1 \setminus \{0\}$.

(b) Any conic in $\mathbb{P}^2$ is isomorphic to $\mathbb{P}^1$.

(16) Show that every isomorphism of $\mathbb{A}^1$ is of the form $t \mapsto at + b$, for some $a, b \in k$.

(17) Show that every isomorphism $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ is of the form $\varphi(x) = \frac{ax+b}{cx+d}$ for some $a, b, c, d \in k$, where x is the coordinate on $\mathbb{A}^1$. (This means that $\varphi([x_0, x_1]) = [cx_1 + dx_0, ax_1 + bx_0]$).

(18) Given tree distinct points $p, q, r \in \mathbb{P}^1$, there is a unique isomorphism $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ with $\varphi(p) = 0$, $\varphi(q) = 1$, $\varphi(r) = \infty = [0, 1]$.

(19) Let x, y, z, t be the homogeneous coordinates on $\mathbb{P}^3$. Let r_1, r_2 be two quadratic forms in x, y, z, and assume that for $q_1 := tx - r_1$, $q_2 := ty - r_2$ we have $Z(q_1, q_2) \subset \mathbb{P}^3$ is an irreducible curve C. Show that $[x, y, z] : C \to \mathbb{P}^2$ is an isomorphism of C with $Z(xq_2 - yq_1) \subset \mathbb{P}^2$.

(20) Let $\varphi : X \to Y$ be a morphism between affine varieties. Let $\varphi^* : \mathcal{O}_Y(Y) \to \mathcal{O}_X(X)$ the corresponding map. Which of the following is true?

(a) φ^* is injective if and only if φ is surjective.

(b) φ^* is surjective if and only if of φ is injective.

(c) φ^* is an isomorphism if and only if φ is an isomorphism.

Give proofs or counterexamples. If a statement is false, can you change it a little bit, so that it becomes true?

(21) Let $\pi : \mathbb{A}^{n+1} \setminus \{(0, \dots, 0)\} \to \mathbb{P}^n, (a_0, \dots, a_n) \mapsto [a_0, \dots, a_n]$. Show that π is a regular map.

(22) Let $C := Z(x_1^2 - x_0x_2) \subset \mathbb{P}^2$, $D := Z(x_1^2 - x_0x_2, x_1x_2 - x_0x_3, x_2^2 - x_1x_3) \subset \mathbb{P}^3$, $D_0 := \{[a_0, a_1, a_2, a_3] \in D \mid a_0 \neq 0\}$. Show that the map

$$\varphi_0 : D_0 \to C, [a_0, a_1, a_2, a_3] \mapsto [a_0, a_1, a_2]$$

can be extended to a morphism $\varphi : D \to C$.

(23) With the notation of the previous exercise, show that $\varphi : D \to C$ is an isomorphism.

(24) For a polynomial $f \in k[x_1, \dots, x_n]$, the **homogenization** $f^H \in k[x_0, \dots, x_n]$ is defined by

$$f^H(x_0, \dots, x_n) = x_0^{deg(f)} f(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}).$$

For an ideal $I \subset k[x_1, \dots, x_n]$ the homogenization of I is $I^H := \{f^H \mid f \in I\}$.

Let $Y \subset \mathbb{A}^n$ be a closed subvariety. Identify as usual $\mathbb{A}^n$ with U_0 via φ_0. Let $\overline{Y}$ be the closure of Y in $\mathbb{P}^n$, called the projective closure of Y.

(a) Show $I_H(\overline{Y})) = I(Y)^H$.

(b) Let $C := Z(x_2 - x_1^2, x_3 - x_1^3)$ be the twisted cubic in $\mathbb{A}^3$. Show that $Z(x_0x_2 - x_1^2, x_0^2x_3 - x_1^3)$ is reducible, and $\overline{C} \neq Z(x_0x_2 - x_1^2, x_0^2x_3 - x_1^3)$. Thus it is not always true that, $\langle f_1, \dots, f_n\rangle^H = \langle f_1^H, \dots, f_n^H\rangle$.

3. Products

Many important properties of varieties and morphisms $\varphi : X \to Y$ of varieties are best understood in terms of the product $X \times Y$. Once one understands the product $X \times Y$, one can understand φ via its graph. Below we will see two important properties of varieties, that are best stated in terms of products.

(1) Separatedness, which replaces the Haussdorff property of manifolds. In fact we will show that all quasiprojective varieties are separated.
(2) completeness, which corresponds to the compactness for manifolds. A morphism starting from complete variety maps closed sets to closed sets. We will show that the complete quasiprojective varieties are precisely the projective varieties.

3.1. Products of affine varieties.

We will first introduce the product of affine varieties, which turns out to be very simple, because for $X \subset \mathbb{A}^n$, $Y \subset A^m$ closed subsets, $X \times Y$ is a closed subset of $\mathbb{A}^{n+m}$.

Definition 3.1. Let $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ be affine varieties. The *product* of X and Y is

$$X \times Y := \{(p, q) \in \mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m} \mid p \in X,\ q \in Y\}.$$

Denote by $x_1, \dots, x_n, y_1, \dots, y_m$ the coordinates on $\mathbb{A}^n$ respectively $\mathbb{A}^m$, then $x_1, \dots, x_n$, $y_1, \dots, y_m$ are coordinates on $\mathbb{A}^{n+m}$, and we can write

$$X = Z(F_1, \dots, F_k),\ F_i, \in k[x_1, \dots, x_n], \quad Y = Z(H_1, \dots, H_s),\ H_i, \in k[y_1, \dots, y_m],$$
$$X \times Y = Z(F_1, \dots, F_k, H_1, \dots, H_s) \subset \mathbb{A}^{n+m},$$

where now the F_i, H_j are viewed as elements of $k[x_1, \dots, x_n, y_1, \dots, y_m]$. Thus $X \times Y$ is a closed subset of $\mathbb{A}^{n+m}$.

Now we want to see that $X \times Y$ is a variety, i.e. irreducible. To make our argument applicable also to quasiprojective varieties, we prove a topological statement.

LEMMA 3.2. *Let X, Y be irreducible topological spaces. Assume $X \times Y$ has a topology for which the inclusions $j_p : Y \to X \times Y, b \mapsto (p, b)$ and $i_q : X \to X \times Y, a \mapsto (a, q)$ are continuous for all $p \in X$ and for all $q \in Y$. Then $X \times Y$ is irreducible.*

PROOF. Assume $X \times Y = S_1 \cup S_2$ with $S_i \neq X \times Y$ closed. For $i = 1, 2$ let

$$T_i := \{p \in X \mid \{p\} \times Y \subset S_i\}.$$

As all i_q are continuous, $T_i = \bigcap_{q \in Y} i_q^{-1}(S_i)$ is closed in X. As j_p is continuous, and Y is irreducible, its image $\{p\} \times Y$ is irreducible for all $p \in X$. Thus $\{p\} \times Y \subset S_1$ or $\{p\} \times Y \subset S_2$. Thus $X = T_1 \cup T_2$ and $T_i \neq X$, i.e. X is reducible. □

COROLLARY 3.3. *Let X, Y be affine varieties, then $X \times Y$ is a affine variety.*

PROOF. Let $q = (b_1, \dots, b_m) \in X$. Then $i_p : X \to X \times Y, a \mapsto (a, q)$ is the regular map $(x_1, \dots, x_n, b_1, \dots, b_m)$ and thus continuous, similarly j_p is continuous. The result follows from the lemma. □

PROPOSITION 3.4. *(Universal property of the product)*

(1) *The projections*

$$p_1 = (x_1, \dots, x_n) : X \times Y \to X, \quad p_2 = (y_1, \dots, y_m) : X \times Y \to Y$$

are morphisms.

(2) *Let Z be a variety. The morphisms $Z \to X \times Y$ are precisely the*

$$(f, g) : Z \to X \times Y, p \mapsto (f(p), g(p))$$

for morphisms $f : Z \to X$, $g : Z \to Y$.

PROOF. (1) is obvious. (2) Let $h : Z \to X \times Y$ be a morphism. Then $f := p_1 \circ h$ and $g := p_2 \circ h$ are morphisms, and for all $p \in Z$ we get $h(p) = (p_1(h(p)), p_2(h(p))) = (f(p), g(p))$.

Conversely let $f = (f_1, \dots, f_n) : Z \to X$, $g = (g_1, \dots, g_m) : Z \to Y$ with $f_i, g_j \in \mathcal{O}_Z(Z)$. Then $(f, g) = (f_1, \dots, f_n, g_1, \dots, g_m)$ is a morphism. □

REMARK 3.5. This is the universal property of the product. It determines $X \times Y$ up to isomorphism. It is what really makes $X \times Y$ into a product. E.g. in topology the product topology on the product $X \times Y$ of topological spaces is defined precisely in such a way that the universal property holds.

3.2. The Segre embedding. Now we want also to look at the product of quasiprojective varieties. This is not as easy as the affine case, because $\mathbb{P}^n \times \mathbb{P}^m$ is not in an obvious way a quasiprojective variety. We will show that there is an injection $\sigma : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^N$ ($N = (n+1)(m+1) - 1$) with image a closed subset $\Sigma_{n,m}$ of $\mathbb{P}^N$. Later we will want to identify $\mathbb{P}^n \times \mathbb{P}^m$ with $\Sigma_{n,m}$, so that $\mathbb{P}^n \times \mathbb{P}^m$ is a projective variety. Similarly for $X \subset \mathbb{P}^n$, $Y \subset \mathbb{P}^m$ quasiprojective varieties, we will identify $X \times Y$ with its image, a quasiprojective variety.

Definition 3.6. (Segre Embedding) Let $N := (n+1)(m+1) - 1$. Let $x_0, \dots, x_n$ be the coordinates on $\mathbb{P}^n$, $y_0, \dots, y_m$ the coordinates on $\mathbb{P}^m$ and $(z_{ij})_{i=0,\dots,n; j=0,\dots m}$ the coordinates on $\mathbb{P}^N$. We define a map

$$\sigma : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^N; ([a_0, \dots, a_n], [b_0, \dots, b_n]) \mapsto [a_i b_j]_{ij}.$$

Note that σ is well-defined. If $\lambda, \mu \in k^*$, then

$$\sigma([\lambda a_0, \dots, \lambda a_n], [\mu b_0, \dots, \mu b_n]) = [\lambda \mu a_i b_j]_{ij} = [a_i b_j]_{ij}.$$

σ is called the *Segre embedding*. We denote by $\Sigma_{n,m}$ the image $\sigma(\mathbb{P}^n \times \mathbb{P}^m)$. Now we fix n, m and write Σ instead of $\Sigma_{n,m}$.

For $i \in \{1, \dots, n\}$, $j \in \{1, \dots, m\}$ let

$$U_i := \{[a_k]_k \in \mathbb{P}^n \mid a_i \neq 0\}, \ U_j := \{[a_l]_l \in \mathbb{P}^m \mid a_j \neq 0\},$$
$$U_{ij} := \{[a_{kl}]_{kl} \in \mathbb{P}^N \mid a_{ij} \neq 0\}.$$

We denote the corresponding isomorphisms by

$$u_i : \mathbb{A}^n \to U_i, \ u_j : \mathbb{A}^m \to U_j, \ u_{ij} : \mathbb{A}^N \to U_{ij}$$

with inverses φ_i, φ_j and φ_{ij}. Note that the index i always refers to $\mathbb{P}^n$ and the index j always to $\mathbb{P}^m$. $\mathbb{P}^N$ is covered by the $U_{ij} \simeq \mathbb{A}^N$ and Σ is covered by the $\Sigma^{ij} := \Sigma \cap U_{ij}$. Write

$$\sigma^{ij} := \mathbb{A}^{n+m} \to U_{ij}; (p, q) \mapsto \sigma(u_i(p), u_j(q)),$$

so that $\Sigma^{ij} = \sigma^{ij}(\mathbb{A}^{n+m})$.

Theorem 3.7. (1) *σ is injective and Σ is closed in $\mathbb{P}^N$:*

$$\Sigma = Z\big(z_{ij} z_{kl} - z_{ik} z_{jl} \mid i, k = 0, \dots, n; \ j, l = 0, \dots, m\big). \qquad (1)$$

(2) *$\sigma^{ij} : \mathbb{A}^{n+m} \to \Sigma^{ij}$ is an isomorphism. In particular Σ has on open cover by subsets isomorphic to $\mathbb{A}^{n+m}$.*

(3) *For any $q \in \mathbb{P}^m$, the map $i_q : \mathbb{P}^n \to \mathbb{P}^N; p \mapsto \sigma(p, q)$ is a morphism, in fact it is a linear map, embedding $\mathbb{P}^n$ as a linear subspace of $\mathbb{P}^N$.*

(4) *For $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$ quasiprojective varieties, $\sigma(X \times Y) \subset \mathbb{P}^N$ is a quasiprojective variety. It is projective if both X and Y are projective.*

Proof. (1) If $\sigma([a_0, \dots, a_n], [b_0, \dots, b_m]) = \sigma([a'_0, \dots, a'_n], [b'_0, \dots, b'_m])$, then there exists $\lambda \in k \setminus \{0\}$ with $\lambda a'_i b'_j = a_i b_j$ for all i, j. Choose i_0, j_0 with $a_{i_0} b_{j_0} \neq 0$. Then also $a'_{i_0} b'_{j_0} \neq 0$, in particular $b'_{j_0} \neq 0$. Therefore we get $a'_i = \big(\lambda \frac{b_{j_0}}{b'_{j_0}}\big) a_i$ for all i, i.e. $[a_0, \dots, a_n] = [a'_0, \dots, a'_n]$. Similarly one proves that $[b_0, \dots, b_m] = [b'_0, \dots, b'_m]$. This shows that σ is injective.

Let W be the zero set of the right hand side of (1). It is clear that $\Sigma \subset W$. Let $[a_{ij}]_{ij} \in W$. Choose k, l such that $a_{kl} \neq 0$. Then

$$[a_{ij}]_{ij} = [a_{ij} a_{kl}]_{ij} = [a_{il} a_{kj}]_{ij} = \sigma([a_{il}]_i, [a_{kj}]_j).$$

(2) We can assume that $i = j = 0$. Then $\sigma^{00}(a_1, \dots, a_n, b_1, \dots, b_m) = [c_{ij}]_{ij}$ with $c_{00} = 1$ and for $i, j > 0$: $c_{i0} = a_i$, $c_{0j} = b_j$, $c_{ij} = a_i b_j$. In particular σ^{00} is a morphism. The inverse morphism is given by $(z_{10}/z_{00}, \dots z_{n0}/z_{00}, z_{01}/z_{00}, \dots, z_{0m}/z_{00})$.

(3) Let $q = [b_0, \dots, b_m]$. Then $i_q = [b_j x_i]_{ij}$, which is a projective linear map, and thus a morphism, which embeds $\mathbb{P}^n$ as a projective linear subspace $\mathbb{P}\big(\big\{[b_j a_i]_{ij} \bigm| a_0, \dots, a_n \in k\big\}\big)$.

(4) Let X and Y be projective algebraic sets. We first show that $\sigma(X \times Y)$ is a projective algebraic set. The quasiprojective case is similar.

$$\sigma(X \times Y) = \bigcup_{i,j} \sigma^{ij}(\varphi_i(X) \times \varphi_j(Y)).$$

$\varphi_i(X) \times \varphi_j(Y)$ is a closed subset in $\mathbb{A}^{n+m}$. As σ^{ij} is an isomorphism, we get that $\sigma^{ij}(\varphi_i(X) \times \varphi_j(Y)) = \sigma(X \times Y) \cap \Sigma^{ij}$ is a closed subset of Σ^{ij}. As the $\sigma(X \times Y) \cap \Sigma^{ij}$ are an open cover of $\sigma(X \times Y)$, it follows that $\sigma(X \times Y)$ is a closed subset of $\mathbb{P}^N$.

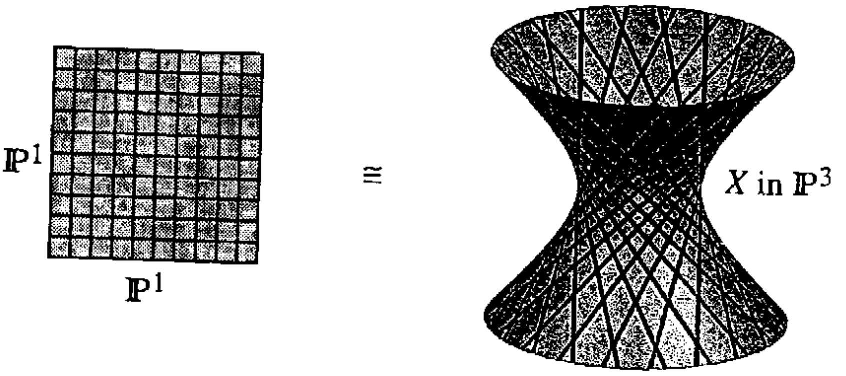
To show that $\sigma(X \times Y)$ is irreducible, we use Lemma 3.2. As $\sigma : X \times Y \to \sigma(X \times Y)$ is a bijection, we need that $\sigma \circ i_q : X \to \sigma(X \times Y), p \mapsto \sigma(p, q)$ is continuous (and similarly for $j_p : q \mapsto \sigma(p, q)$). But this follows immediately from (3) because it is the restriction of $i_q : \mathbb{P}^n \to \mathbb{P}^N$. □

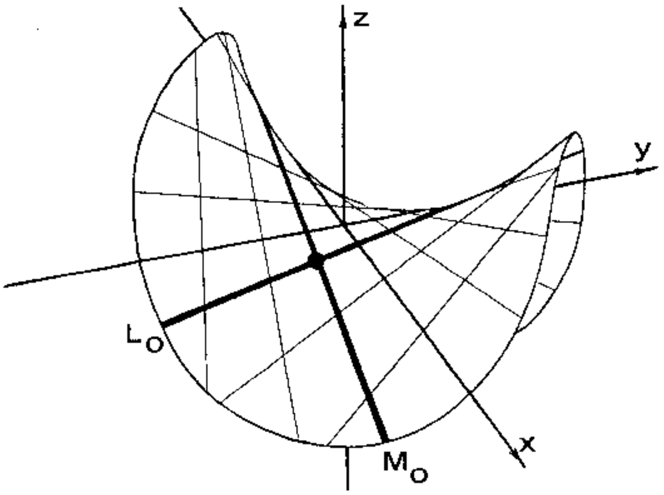
3.3. Products of quasiprojective varieties.

Definition 3.8. In future we will identify $\mathbb{P}^n \times \mathbb{P}^m$ with its image $\Sigma \subset \mathbb{P}^N$. So $\mathbb{P}^n \times \mathbb{P}^m$ becomes a projective variety. If $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$ are quasiprojective varieties, we identify $X \times Y$ with $\sigma(X \times Y) \subset \mathbb{P}^N$. So $X \times Y$ is a quasiprojective variety, and projective if X and Y are projective.

Remark 3.9. Note that by part (2) of the previous theorem, with this definition $U_i \times U_j$ is an open subset of $\mathbb{P}^n \times \mathbb{P}^m$, and $\varphi_i \times \varphi_j : U_i \times U_j \to \mathbb{A}^{n+m}$ is an isomorphism. Thus $(U_i \cap X) \times (U_j \cap Y)$ is an open affine subset of $X \times Y$.

Example 3.10. For $\mathbb{P}^1 \times \mathbb{P}^1$ the only nontrivial equation in (1) is $z_{00}z_{11} - z_{01}z_{10}$. So $\mathbb{P}^1 \times \mathbb{P}^1 = Z(z_{00}z_{11} - z_{01}z_{10}) \subset \mathbb{P}^3$ is a quadric. By the above $\mathbb{P}^1 \times \mathbb{P}^1$ contains two families of lines in $\mathbb{P}^3$: $p \times \mathbb{P}^1$ and $\mathbb{P}^1 \times q$ for all $p, q \in \mathbb{P}^1$.





Now we show the universal property of the product.

Proposition 3.11. *(Universal property) Let X, Y be varieties.*

1. *$p_1 : X \times Y \to X$, $p_2 : X \times Y \to Y$ are morphisms.*
2. *For any variety Z, the morphisms $Z \to X \times Y$ are precisely the $(f, g) : Z \to X \times Y, p \mapsto (f(p), g(p))$ for morphisms $f : Z \to X$ and $g : Z \to Y$.*

Proof. (1) It is enough to see that $p_1|_{Z\cap(U_i\times U_j)} \to X\cap U_i$ is an isomorphism. But note that it is just the restriction of the composition $U_i \times U_j \simeq \mathbb{A}^{n+m}\xrightarrow{p_1}\mathbb{A}^n \simeq U_i$. Thus it is a morphism.

(2) If $h : Z \to X \times Y$ is a morphism, then $f := p_1 \circ h$ and $g := p_2 \circ h$ are morphisms, and $h = (f, g)$. Let $f : Z \to X$, $g : Z \to Y$ be morphisms.

Let $Z^{ij} = (f, g)^{-1}(U_i \times U_j) = f^{-1}(U_i) \cap g^{-1}(U_j)$. Then Z^{ij} is open in Z and (f, g) is a morphism if and only for all i, j the composition

$$Z_{ij}\xrightarrow{(f,g)}(X \times Y) \cap (U_i \times U_j) \to \varphi_i(X) \times \varphi_j(Y).$$

is a morphism. As $\varphi_i(X) \subset \mathbb{A}^n$ and $\varphi_j(Y) \subset \mathbb{A}^m$ this follows from the affine case. □

Example 3.12. Let $f : X \to Y$, $g : Z \to W$ be morphisms of varieties. Then $f \times g : X \times Z \to Y \times W, (p, q) \mapsto (f(p), g(q))$ is a morphism, because $f \times g = (f \circ p_1, g \circ p_2)$.

Taking the product is compatible with isomorphism:

Corollary 3.13. *Let X, Y, X', Y' be varieties and assume that $X \simeq X'$, $Y \simeq Y'$. Then $X \times Y \simeq X' \times Y'$. In particular, the product of affine varieties (i.e. varieties isomorphic to closed subvarieties of affine space) is affine.*

Proof. Let $f : X \to X'$, $g : Y \to Y'$ be the isomorphisms. Then $f\times g : X\times Y \to X' \times Y'$ is an isomorphism whose inverse is $f^{-1} \times g^{-1}$. □

Lemma 3.14. *The closed subsets W of $\mathbb{P}^n \times \mathbb{P}^m$ are precisely the zero loci of sets of polynomials $f \in k[x_0, \dots , x_n, y_0, \dots , y_m]$ that are bihomogeneous in the x_i and y_j (i.e. they are homogeneous in the x_i and homogeneous in the y_i, but not necessarily of the same degree).*

Proof. Let $W \subset \mathbb{P}^n \times \mathbb{P}^m$ be closed. Then $W = \sigma^{-1}(A)$ where $A \subset \mathbb{P}^N$ is closed. Thus $A = Z(f_1(z_{ij}), \dots , f_r(z_{ij}))$ where the f_i are homogeneous polynomials in the z_{ij} and $W = Z(f_1(x_iy_j), \dots , f_r(x_iy_j))$ where the $f_k(x_iy_j)$ are bihomogeneous in the x_i and the y_j (even of the same degree). Conversely assume that $W = Z(f_1(x_i, y_j), \dots , f_r(x_i, y_j))$, with the $f_k(x_i, y_j)$ bihomogeneous. Then

$$(\varphi_i\times\varphi_j)(W\cap(U_i\times U_j)) = Z\big(f_k(x_0, \dots , x_i = 1, \dots , x_n, y_0, \dots , y_j = 1, \dots , y_m) \bigm| k = 1, \dots , r\big)$$

is closed in $\mathbb{A}^{n+m}$ for all i, j. As the $U_i \times U_j$ are an open cover of $\mathbb{P}^n \times \mathbb{P}^m$, it follows that W is closed. □

We can look at the diagonal in $X \times X$.

Definition 3.15. Let X be a variety. The *diagonal* is $\Delta_X := \{(p,p) \mid p \in X\}$. The *diagonal morphism* is $\delta_X = (id_X, id_X) : X \to X \times X$. Obviously the image of δ_X is Δ_X.

Lemma 3.16. *$\Delta_X \subset X \times X$ is closed and $\delta_X : X \to \Delta_X$ is an isomorphism.*

Proof. First we show $\Delta_X \subset X \times X$ is closed. As every variety is isomorphic to a locally closed subvariety of projective space, we can assume $X \subset \mathbb{P}^n$. Then $\Delta_X = \Delta_{\mathbb{P}^n} \cap X \times X$, and $X \times X$ carries the induced topology from $\mathbb{P}^n \times \mathbb{P}^n$. Thus it is enough to show the result for $X = \mathbb{P}^n$. Then $\Delta_{\mathbb{P}^n} = Z\big(x_i y_j - x_j y_i \mid i,j = 1, \dots, n\big)$ because $([a_0, \dots, a_n], [b_0, \dots, b_n])$ is in this zero set if and only if the matrix $\begin{pmatrix} a_0 & \dots & a_n \\ b_0 & \dots & b_n \end{pmatrix}$ has rank 1, i.e. $[a_0, \dots, a_n] = [b_0, \dots, b_n]$.

$\delta_X : X \to \Delta_X$ is obviously an isomorphism, its inverse is the restriction of $p_1 : X \times X \to X$. □

Remark 3.17. The fact that Δ_X is closed in $X \times X$ is very important. It is what replaces the *Hausdorff* property in the analytic topology. If X is a topological space, then $\Delta_X \subset X \times X$ is closed (with the product topology) if and only if X is Hausdorff.

There is a more general notion of abstract varieties, which are spaces with an open cover by affine varieties (note that it is not obvious what is meant by this) plus the condition that the diagonal is closed. This is very analogous to the definition of manifolds, which are spaces with an open cover by open subsets of $\mathbb{R}^n$, with the additional condition that the space is Hausdorff.

Corollary 3.18. *Let $\varphi : X \to Y$, $\psi : X \to Y$ be two morphisms. Then $\{p \in X \mid \varphi(p) = \psi(p)\}$ is closed in X.*

Proof. Note that the set is $(\varphi, \psi)^{-1}(\Delta_Y)$, which is closed as the inverse image of a closed set by a morphism. □

Now we can also look at the graph of a morphism.

Definition 3.19. Let $f : X \to Y$ be a morphism of quasiprojective varieties. The *graph* of f is

$$\Gamma_f := \{(a, f(a)) \mid a \in X\} \subset X \times Y.$$

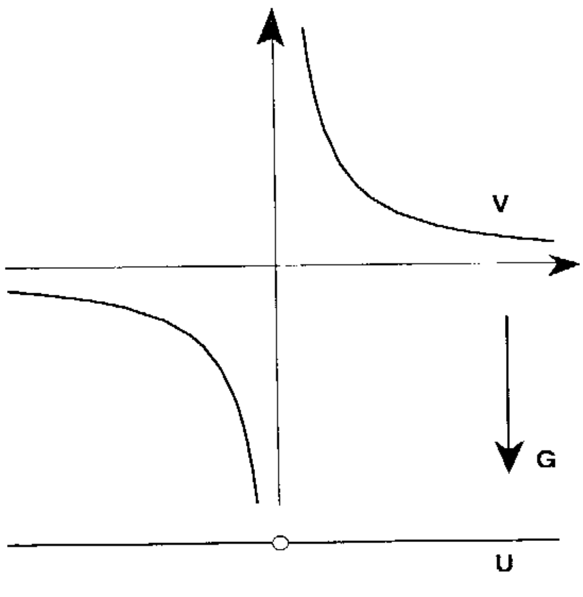
Corollary 3.20. *Γ_f is closed in $X \times Y$. The restriction of the projection $p_1 : X \times Y \to X$ is an isomorphism.*

Proof. By definition $\Gamma_f = (f \times id_Y)^{-1}(\Delta_Y)$, thus is is closed. The restriction of p_1 is an isomorphism, because its inverse is $(id_X, f) : X \to \Gamma_f$. □

3.4. Completeness. In this section we will show that projective varieties are complete: if X is a projective variety and Y is any variety, then $p_2 : X \times Y \to Y$ is a closed map, i.e. it maps closed subsets to closed subsets. Completeness corresponds to compactness in the analytic topology. If in the above X and Y are required to be Hausdorff topological spaces with countable basis, then X is complete if an only if it is compact. In particular projective varieties are compact in the analytic topology. Compact manifolds are in many ways much better behaved than noncompact ones. In the same way projective varieties are in many ways better than quasiprojective varieties.

DEFINITION 3.21. A map $\varphi : X \to Y$ between topological spaces is called **closed** if $\varphi(Z)$ is closed in Y for any closed subset $Z \subset X$. A variety X is called **complete** if $p_2 : X \times Y \to Y$ is a closed map for all varieties Y.

EXAMPLE 3.22. $\mathbb{A}^1$ is not complete: $p_2 : \mathbb{A}^1 \times \mathbb{A}^1 = \mathbb{A}^2 \to \mathbb{A}^1$ maps $C := Z(xy-1)$ onto $\mathbb{A}^1 \setminus \{0\}$, which is not closed in $\mathbb{A}^1$.



We want to see that this cannot happen for X projective. We start by proving an important special case.

THEOREM 3.23. *Any projective variety is complete.*

PROOF. (1) The main part is to show that $p_1 : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^n$ is closed. Let $X \subset \mathbb{P}^m \times \mathbb{P}^n$ be an algebraic set. Then X is the zero locus of polynomials $f_1(x, y), \dots, f_r(x, y)$

bihomogeneous in the x_i and the y_j (we use the shorthand x, y for $x_0, \dots, x_n, y_0, \dots, y_n$). We can assume that all f_i have the same degree d in the y_i (otherwise one replaces f_j with a lower degree by $y_0^e f_j, \dots, y_n^e f_j$, which have the same zero set).

Fix a point $P \in \mathbb{P}^n$. Then $P \in p_1(X)$ if and only if $Z(f_1(P,y), \dots, f_r(P,y)) \subset \mathbb{P}^m$ is not empty. By the projective Nullstellensatz this is equivalent to: for all $s > 0$

$$\langle f_1(P,y), \dots, f_r(P,y) \rangle \text{ contains not all monomials of degree } s \text{ in the } y_i \qquad (1)$$

The condition (1) is trivial for $s < d$. Thus it is enough that for all $s \geq d$ the set of all $P \in \mathbb{P}^n$ satisfying (1) is closed, because $p_1(X)$ is then closed as the intersection of all these closed sets.

Fix $s \geq d$. We denote the $\binom{m+s}{m}$ monomials in the y_i of degree s by $M_i(y)$ (in any order). Denote by $N_i(y)$ the homogeneous polynomials in the y_i of degree $s - d$ (in any order). The elements of degree s in $\langle f_1(P,y), \dots, f_r(P,y) \rangle$ are precisely the linear span of the $N_i(y) f_j(P,y)$. We denote the $N_i(y) f_j(x,y)$ by $G_k(x,y)$ $(k = 1, \dots, t)$ in any order. Then (1) is equivalent to the fact that the set of polynomials $\bigl\{G_k(P,y) \bigm| 1 \leq k \leq t\bigr\}$ does not generate the vector space of all polynomial of degree s. We write $G_j(x,y) = \sum_i A_{ij}(x) M_i(y)$ with $A_{ij}(x) \in k[x]$ homogeneous. Then the dimension of the linear span of the $G_k(P,y)$ is the rank of the matrix $(A_{ij}(P))_{i,j}$ $(i = 1, \dots, \binom{m+s}{m}$, $j = 1, \dots, t)$. Thus (1) is equivalent to $rk((A_{ij}(P))_{ij}) < \binom{m+s}{m}$. Thus the set of points where (1) holds is the zero set of all the $\binom{m+s}{m}$-minors of $(A_{ij}(x))_{ij}$, which are homogeneous polynomials in the x_i. Thus it is closed.

(2) It is now rather easy to deduce the general case. First we show that $\mathbb{P}^n$ is complete. Let Y be a variety. Let $\{Y_i\}_i$ be an open affine cover of Y and let $Z \subset \mathbb{P}^n \times Y$ be closed. Then $Z_i := Z \cap (\mathbb{P}^n \times Y_i)$ is closed in $\mathbb{P}^n \times Y_i$ and if $p_2(Z_i)$ is closed in Y_i for all i, then as the Y_i are an open cover of Y, Z is closed in Y. Thus we can assume that Y is affine. If $Y \subset \mathbb{A}^m$ is affine, we can view Y as a quasiprojective variety via the embedding $\mathbb{A}^m \to \mathbb{P}^m$. Thus we can assume that Y is quasiprojective. Let $Z \subset \mathbb{P}^n \times Y$ be closed. Let $\overline{Z}$ be its closure in $\mathbb{P}^n \times \mathbb{P}^m$. Then $p_2(\overline{Z})$ is closed in $\mathbb{P}^m$. Therefore $p_2(Z) = p_2(\overline{Z} \cap (\mathbb{P}^n \times Y)) = p_2(\overline{Z}) \cap Y$ is closed in Y.

Now let $X \subset \mathbb{P}^n$ be a projective variety. Let $Z \subset X \times Y$ be closed. Then Z is also closed in $\mathbb{P}^n \times Y$, thus $p_2(Z)$ is closed in Y, thus X is complete. □

This implies that the image of any morphism starting from a projective variety is closed.

Corollary 3.24. *Let $f : X \to Y$ be a morphism of varieties with X projective. Then $f(X) \subset Y$ is closed.*

Proof. We have $f(X) = p_2(\Gamma_f)$ and $\Gamma_f \subset X \times Y$ is closed. As X is complete, it follows that $f(X)$ is closed. □

This implies that projective varieties are very different from affine varieties.

Corollary 3.25. (1) *Every regular function on a projective variety is constant.*

(2) *Every morphism $f : X \to Y$ from a projective variety to an affine variety maps X to a point. In particular the only varieties which are affine and projective are points.*

Proof. (1) Let $f : X \to \mathbb{A}^1$ be a regular function. Then $f(X)$ is closed in $\mathbb{A}^1$. So, as X is irreducible, $f(X)$ is a point or $f(X) = \mathbb{A}^1$. Via the inclusion $\mathbb{A}^1 \subset \mathbb{P}^1$ we can view f as a map to $\mathbb{P}^1$, so $f(X)$ is closed in $\mathbb{P}^1$, which implies that $f(X) \neq \mathbb{A}^1$.

(2) We can assume $Y \subset \mathbb{A}^n$ and write $f = (f_1, \dots, f_n)$ for f_i regular functions. The f_i are constant and thus also f. □

The fact that the image of a map from a projective variety is closed allows us to construct many closed subvarieties of $\mathbb{P}^n$ as images of morphisms, even if it would be quite difficult to write down the equations.

Example 3.26. (The Veronese Embedding). Fix $n, m > 0$ and let $N = \binom{n+d}{d} - 1$. Let $M_i(x_0, \dots, x_n),\ 0 \leq i \leq N$ be the set of all monomials in $x_0, \dots, x_n$ of degree d. The **Veronese Embedding** of degree d is $v_d := [M_0, \dots, M_N]$. This is a morphism because among the M_i we have $x_0^d, \dots, x_n^d$ which do not vanish simultaneously. Thus $v_d(\mathbb{P}^n)$ is a closed subvariety of $\mathbb{P}^N$.

We claim that $v_d : \mathbb{P}^n \to v_d(\mathbb{P}^n)$ is an isomorphism. So we have to find an inverse morphism. It is enough to do this on an affine open. As the open sets where $x_i \neq 0$ cover $\mathbb{P}^n$, the open sets where $x_i^d \neq 0$ cover $v_d(\mathbb{P}^n)$. Consider the case $i = 0$, then the inverse morphism is given by $[\{x_0^d\}, \{x_0^{d-1}x\}, \dots, \{x_0^{d-1}x_n\}]$ (where I denote $\{M_i\}$ the coordinate on $\mathbb{P}^N$ corresponding to the monomial M_i.).

The simplest examples are the degree d embeddings of $\mathbb{P}^1$ given by

$$v_d : \mathbb{P}^1 \to \mathbb{P}^d, [a, b] \mapsto [a^d, a^{d-1}b, \dots, b^d].$$

The image is called a **rational normal curve** in $\mathbb{P}^d$.

Let $F = \sum a_i M_i$ be a homogeneous polynomial of degree d and $X \subset \mathbb{P}^n$ a closed subvariety. Then $v_d(X \cap Z(F))$ is the intersection of $v_d(X)$ with the hyperplane $Z(\sum a_i \{M_i\})$ in $\mathbb{P}^N$. As $v_d|_X$ is an isomorphism onto its image, we see that one can use the Veronese embedding to reduce problems about hypersurfaces to problems about hyperplanes.

Corollary 3.27. *Let $X \subset \mathbb{P}^n$ be a projective variety, and let $F \in k[x_0, \dots, x_n]$ be a nonconstant homogeneous polynomial. Then*

1. *$X \setminus Z(F)$ is an affine variety.*
2. *If X is not a point, then $X \cap Z(F) \neq \emptyset$.*

Proof. (1) If F is a hyperplane, then by a projective linear transformation we can assume that $Z(F) = Z(x_0)$, and $X \subset \mathbb{A}^n$. If F has degree d, then via the Veronese map $X \setminus Z(F)$ is isomorphic to $v_d(X) \cap H$ for H a hyperplane, thus it is affine.

(2) If $X \cap Z(F) = \emptyset$, then X is affine and projective, thus it is a point. □

Exercises.

(1) Assume $X \subset \mathbb{A}^n$ is an affine variety. Describe explicitely the homomorphism $\delta_X^* : A[X \times X] \to A[X]$ induced by $\delta_X : X \to X \times X; x \mapsto (x, x)$.

(2) Prove that a quasiprojective variety is complete if and only if it is projective.

(3) Prove that the Veronese variety $v_d(\mathbb{P}^n)$ is not contained in any hyperplane of $\mathbb{P}^N$ ($N = \binom{n+d}{d} - 1$).

(4) Let U and V be open subsets of a variety X. Show that $U \cap V$ is isomorphic to $(U \times V) \cap \Delta_X$.

(5) Under the assumptions of the previous exercise assume furthermore that U and V are affine (i.e. U is isomorphic to a closed subset of $\mathbb{A}^n$ and V isomorphic to a closed subset of $\mathbb{A}^m$). Then show that $U \cap V$ is affine (i.e. $U \cap V$ is isomorphic to a closed subset of $\mathbb{A}^{n+m}$). Use the previous exercise.

(6) Let $n \geq 1$, $N := \frac{(d+1)(d+2)}{2} - 1$ and let $M_0, \dots M_N$ be the monomials of degree d in x, y, z (in some order). Let $y_0, \dots, y_n$ be the homogeneous coordinates on $\mathbb{P}^N$. Let

$$Z := Z\Big(\sum_{i=0}^{N} M_i(x, y, z) y_i\Big) \subset \mathbb{P}^2 \times \mathbb{P}^N$$

with $\pi : Z \to \mathbb{P}^N$ the restriction of the second projection.

(a) Show that Z is an irreducible closed subvariety of $\mathbb{P}^2 \times \mathbb{P}^N$ and that π is a morphism.

(b) For each point $a := [a_0, \dots, a_N] \in \mathbb{P}^N$ let $C_a := Z(\sum_{i=0}^{N} a_i M_i(x, y, z)$. Show $\pi^{-1}(a) = C_a \times \{a\}$. Thus we can think of $\pi : Z \to \mathbb{P}^N$ as a universal family of curves of degree d in $\mathbb{P}^2$.

(7) In this exercise we give the space of lines in $\mathbb{P}^n$ (or equivalently the space of 2-dimensional vector subspaces of k^{n+1}) the structure of a projective variety.

Let $n \geq 1$. We define a set-theoretic map

$$\varphi : \{\text{lines in } \mathbb{P}^n\} \to \mathbb{P}^N, \qquad N := \binom{n+1}{2} - 1$$

as follows. For every line $L \subset \mathbb{P}^N$ choose two distinct points $p := [a_0, \ldots, a_n]$, $q := [b_0, \ldots, b_n]$ on L. Let $\varphi(L)$ be the point in $\mathbb{P}^N$ whose homogeneous coordinate are the $\binom{n+1}{2}$ maximal minors of the matrix $\begin{pmatrix} a_0 & \ldots & a_n \\ b_0 & \ldots & b_n \end{pmatrix}$ in any fixed order. Show that

(a) φ is well-defined (i.e. independent of the choice of p and q) and injective.

(b) The image of φ is an irreducible projective variety that has a finite cover by open subset isomorphic to $\mathbb{A}^{2n-2}$. It is called the Grassmannian of lines in $\mathbb{P}^n$ and denoted by $G(1,n)$.

Hint: We can choose p and q of the form

$$p = (a_2, \ldots, a_i, 1, a_{i+1}, \ldots, a_j, 0, a_{j+1}, \ldots, a_n)$$
$$q = (b_2, \ldots, b_i, 0, b_{i+1}, \ldots, b_j, 1, b_{j+1}, \ldots, b_n)$$

for suitable i, j.

(8) Let $G(1,n)$ be the Grassmannian of lines in $\mathbb{P}^n$ as in the previous exercise. Show that

(a) The set $\{(L, P) \mid p \in L\} \subset G(1,n) \times \mathbb{P}^n$ is closed. It is called the universal family.

(b) Let $Z \subset G(1,n)$ be a closed subset. Then the union of all lines $L \subset \mathbb{P}^n$ such that $L \in Z$ is closed in $\mathbb{P}^n$.

(c) Let $X, Y \subset \mathbb{P}^n$ be disjoint projective varieties. Then the union of all lines in $\mathbb{P}^n$ intersecting both X and Y is a closed subset of $\mathbb{P}^n$. It is called the join $J(X,Y)$ of X and Y.

4. Rational maps

Let X, Y be varieties. Rational functions on X are functions which are defined only on an open subset. Similarly now we want to study morphisms between X and Y that are only defined on open subsets. These are called rational maps. A rational map with an inverse rational map is called a birational map. In this case the varieties are called birational. Since any open set in a variety is dense, rational maps carry a lot of information. In particular birational varieties are isomorphic "almost everywhere" and we will later see that important properties of varieties, like the dimension are preserved by birational maps. It turns out that two varieties are birational if and only if their function fields are isomorphic. Finally we will look at blowups, which are the most important examples of birational morphisms.

4.1. Rational maps. Let X, Y be varieties. A rational map $\varphi : X \dashrightarrow Y$ is given by a morphism $\varphi : U \to Y$ from an open subset $U \subset Y$. An other such morphism $\psi : V \to Y$ gives the same rational map if $\varphi|_{U\cap V} = \psi_{U\cap V}$. This works because of the following lemma.

Lemma 4.1. *Let $\varphi, \psi : X \to Y$ be morphism between varieties. If $\varphi|_U = \psi|_U$ for a nonempty open subset $U \subset X$, then $\varphi = \psi$.*

Proof. We have seen that $Z := \{p \in X \mid \varphi(p) = \psi(p)\}$ is closed in X. It contains the dense open subset U. Thus $X = Z$. □

Definition 4.2. A **rational map** $f : X \dashrightarrow Y$ is an equivalence class $\langle U, \varphi\rangle$ of pairs (U, φ) where $U \subset X$ is a nonempty open subset and $\varphi : U \to Y$ is a regular map. The equivalence relation is

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

This is an equivalence relation, Lemma 4.1 implies the transitivity. We say the rational map $\langle U, \varphi\rangle$ is defined by (V, ψ) if $(V, \psi) \in \langle U, \varphi\rangle$.

We can also view rational maps $\varphi : X \dashrightarrow Y$ as regular maps $\varphi : dom(\varphi) \to Y$, where $dom(\varphi) = \bigcup_{\langle V,\psi\rangle\sim\langle U,\varphi\rangle} V$. Here $\varphi(p) := \psi(p)$ for any $\langle V, \psi\rangle \sim \langle U, \varphi\rangle$ with $p \in U$. It is easy to see that $\varphi : dom(\varphi) \to Y$ is a well-defined morphism. $dom(\varphi)$ is the largest open set on which φ can be defined. We say that φ is *defined at p* if $p \in dom(\varphi)$. We call $\varphi(dom(\varphi))$ the *image* of φ.

Remark 4.3.

1. The rational functions $f \in K(X)$ are natually identified with the rational maps $f : X \dashrightarrow \mathbb{A}^1$: If $f \in K(X)$ then $f \in \mathcal{O}_X(U)$ for some nonempty open set, and thus f defines a morphism $f : U \to \mathbb{A}^1$, i.e. a rational map $\langle U, f\rangle$. Conversely if $\langle U, f\rangle$ is a rational map, then $f \in \mathcal{O}_X(U) \subset K(X)$. It is easy to see that $f \in \mathcal{O}_X(U)$ and $g \in O_X(V)$ are the same element of $K(X)$ if and only if $f|_{U\cap V} = g|_{U\cap V}$.
2. Let X be a variety, let $f_1, \ldots, f_n \in K(X)$. Then $(f_1, \ldots, f_n) : X \dashrightarrow \mathbb{A}^n$ is a rational map defined on $\bigcap_{i=1}^n dom(f_i)$.
3. Let $X \subset \mathbb{P}^n$ be a quasiprojective variety.

(a) Let $F_0, \dots, F_m \in k[x_0, \dots, x_n]$ be homogeneous polynomials of the same degree, not all vanishing identically on X. Then $[F_0, \dots, F_m] : X \dashrightarrow \mathbb{P}^m$ is a rational map, defined at least on $X \setminus \bigcap_{i=0}^m Z(F_i)$.

(b) Let $h_0, \dots, h_m \in K(X)$ not all 0. Then $[h_0, \dots, h_m] : X \dashrightarrow \mathbb{P}^m$ is a rational map.

Example 4.4. Let $W \subset \mathbb{P}^n$ be a linear subspace of dimension k given by $W = Z(H_0, \dots, H_{n-k-1})$ for H_i linear forms. Then the linear projection $\pi_W = [H_0, \dots, H_{n-k-1}] : \mathbb{P}^n \dashrightarrow \mathbb{P}^{n-k-1}$ is a rational map defined outside W. In particular the projection $\pi_p : \mathbb{P}^n \dashrightarrow \mathbb{P}^{n-1}$ from a point is a rational map.

We would like to define the composition of rational maps $\varphi : X \dashrightarrow Y$, $\psi : Y \dashrightarrow Z$. This is in general not possible, even if φ is a morphism: It can very well be that the intersection of the image of φ and $dom(\psi)$ is empty. To remedy this, we only consider rational maps with dense image.

Definition 4.5. A rational map $\langle U, \varphi \rangle : X \dashrightarrow Y$ of varieties is called **dominant** if $\varphi(U)$ is dense in Y. It is straighforward to see that this is independent of the representative (U, φ). (If (V, ψ) is another representative and $\psi(V)$ is contained in a closed subset $Z \subsetneq Y$, then $\varphi^{-1}(Z)$ is closed in U and contains $U \cap V$, thus it is equal to U.) Let $\varphi : X \dashrightarrow Y$ be a dominant rational map and $\psi : Y \dashrightarrow Z$ a rational map, then the composition $\psi \circ \varphi$ is defined as follows. Let $\langle U, \varphi \rangle$, $\langle V, \psi \rangle$ be representatives. Then $\varphi^{-1}(V)$ is open and nonempty in X and $\langle U \cap \varphi^{-1}(V), \psi \circ \varphi \rangle$ is a representative of the composition.

This allows us to define the pullback of rational functions by rational maps. If $f \in K(Y)$ is regular on the open set $V \subset X$, and $\langle U, \varphi \rangle : X \dashrightarrow Y$ is a dominant rational map, then $\varphi^*(f) = \langle \varphi^{-1}(V), f \circ \varphi \rangle \in K(X)$. It is immediate that $\varphi^* : K(Y) \to K(X)$ is a homomorphism of k-algebras and that $(\varphi \circ \psi)^* = \psi^* \circ \varphi^*$.

Example 4.6. Let $\pi_W : \mathbb{P}^n \dashrightarrow \mathbb{P}^{n-k-1}$ be the projection from a linear subspace. Then π_W is dominant (in fact it is surjective).

Definition 4.7. A dominant rational map $\varphi : X \dashrightarrow Y$ is called **birational map** if there exists a dominant rational map $\varphi^{-1} : Y \dashrightarrow X$ with $\varphi \circ \varphi^{-1} = id_Y$, $\varphi^{-1} \circ \varphi = id_X$ (Note that these are identities of rational maps, thus it is enough they hold on nonempty open subsets of X and Y). If φ is in addition a morphism, it is called a **birational morphism**. X and Y are called **birationally equivalent** (or just **birational** if there exists birational map $\varphi : X \dashrightarrow Y$.

If X and Y are birational, then $K(X)$ and $K(Y)$ are isomorphic. Now we show that rational maps between varieties are really nothing else than homomorphisms between their function fields.

Theorem 4.8. *Let X and Y be varieties. The map $(\varphi : X \dashrightarrow Y) \mapsto (\varphi^* : K(Y) \to K(X))$ gives a bijection from the set of dominant rational maps from X to Y to the set of k-algebra homomorphisms from $K(Y)$ to $K(X)$.*

Proof. We have to construct an inverse to the map $\varphi \mapsto \varphi^*$. Let $\theta : K(Y) \to K(X)$ be a homomorphism of k-algebras. We want to construct a rational map $\varphi : X \dashrightarrow Y$. It is enough to construct a rational map to any open affine subset of Y, so we can assume that $Y \subset \mathbb{A}^n$ is a closed subvariety. Let $y_1, \dots, y_n$ be the coordinate functions. Then $\theta(y_1), \dots, \theta(y_n)$ are rational functions on X and we can find an open set $U \subset X$, so that the functions $\theta(y_i)$ are all regular on U. Then θ defines an injective homomorphism of k-algebras $\theta : A(Y) \to \mathcal{O}_U(X)$ (it is injective, because the original $\theta : K(Y) \to K(X)$ was injective as a nonzero homomorphism of fields). Thus by the characterization of morphisms to affine varieties, we get a morphism $\varphi : U \to Y$, such that $\varphi^* = \theta : A(Y) \to \mathcal{O}_U(X)$, and it is an exercise to show that the condition that φ^* is injective implies that the image of φ is dense in Y. Thus we have obtained a dominant rational map $\varphi : X \dashrightarrow Y$ and it is straightforward to check that $\theta \mapsto \varphi$ is inverse to $\varphi \mapsto \varphi^*$. □

In particular two varieties are birational if and only if their function fields are isomorphic.

Corollary 4.9. *Let X and Y be varieties. The following are equivalent.*

(1) *X and Y are birational,*
(2) *there are nonempty open subsets $U \subset X$, $V \subset Y$ with U isomorphic to V.*
(3) *$K(X)$ and $K(Y)$ are isomorphic as k-algebras.*

Proof. "(1)$\Longrightarrow$(2)" Let $\langle U, \varphi\rangle : X \dashrightarrow Y$ be a birational map, with inverse $\langle V, \psi\rangle : Y \dashrightarrow X$. Then $\psi \circ \varphi$ is defined on $U \cap \varphi^{-1}(V)$ and thus is the identity on $U \cap \varphi^{-1}(V)$. Similarly $\varphi \circ \psi$ is the identity on $V \cap \psi^{-1}(U)$. Thus $\varphi : U \cap \varphi^{-1}(V) \to V \cap \psi^{-1}(U)$ is an isomorphism, with inverse ψ.

"(2)$\Longrightarrow$(3)" is obvious because $K(U) = K(X)$ for U an open subset of X.

"(3)$\Longrightarrow$(1)" follows from the theorem. □

Example 4.10. The cuspidal cubic $C = Z(x^3 - y^2) \subset \mathbb{A}^2$ is not isomorphic to $\mathbb{A}^1$, but they are birational: $\varphi : \mathbb{A}^1 \to C,\ t \mapsto (t^2, t^3)$ is a birational morphism. Its inverse rational map is $\varphi^{-1} : C \dashrightarrow \mathbb{A}^1$, $(x, y) \mapsto \frac{y}{x}$. φ^{-1} is a morphism on $C \setminus \{(0, 0)\}$. $\varphi : \mathbb{A}^1 \setminus \{0\} \to C \setminus \{(0, 0)\}$ is an isomorphism.

Definition 4.11. A variety X is called **rational** if it is birational to $\mathbb{A}^n$ for some n. Note that by the previous corollary this is equivalent to $K(X) \simeq k(x_1, \dots, x_n)$.

Example 4.12. (1) $\mathbb{P}^n$ is rational.

(2) The cuspidal cubic is rational.
(3) It is easy to see that an irreducible curve of degree 2 (a conic) in $\mathbb{P}^2$ is isomorphic to $\mathbb{P}^1$ and thus rational. On the other hand one can show that a general (nonsingular) curve of degree $d > 2$ is never rational.
(4) $\mathbb{P}^n \times \mathbb{P}^m$ is rational, because it contains an open subset isomorphic to $\mathbb{A}^{n+m}$.

Remark 4.13. One of the aims of algebraic geometry is to classify algebraic varieties. It would be natural to classify them up to isomorphism, but this is a very fine equivalence relation. Thus one can first classify them up to birational equivalence, which is coarser. We see by the above that classifying algebriac varieties up to birational equivalence is equivalent to classifying finitely generated extension fields of k up to isomorphism of fields.

4.2. Blowups. We now come to the most important examples of birational morphisms: the blowups. One can define the blowup of any variety along any ideal. We will just look at the blow up of $\mathbb{A}^2$ in the origin $0 = (0, 0)$.

Definition 4.14. On $\mathbb{A}^2$ let the coordinates be x, y and on $\mathbb{P}^1$ let the homogeneous coordinates be t, u. The **blowup** of $\mathbb{A}^2$ at 0 is the closed subset

$$\widehat{\mathbb{A}}^2 := Z(xu - yt) \subset \mathbb{A}^2 \times \mathbb{P}^1.$$

Let $\pi : \widehat{\mathbb{A}}^2 \to \mathbb{A}^2$ be the projection. We call $E := \pi^{-1}(0)$ the **exceptional divisor**.

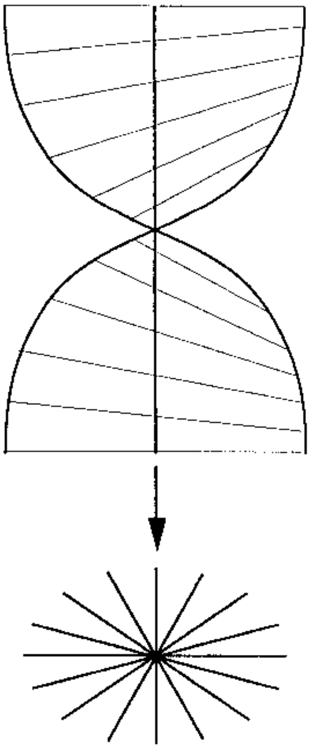
We shall see that blowing up 0 leaves $\mathbb{A}^2 \setminus \{0\}$ unchanged, but $\{0\}$ is replaced by $\mathbb{P}^1$, which we can identify with the space of lines through 0. In particular π is a birational morphism, but not an isomorphism.

(1) Let $((x, y), [t, u]) \in \widehat{\mathbb{A}}^{n+1} \setminus E$. Then $x \neq 0$ or $y \neq 0$, we can assume $x \neq 0$. Then $xu = ty$, i.e $u = \frac{y}{x}t$. Thus $[t, u] = [x, y]$. Thus we see that $\widehat{\mathbb{A}}^2 \setminus E$ is the graph of the morphism

$$[] : \mathbb{A}^2 \setminus \{0\} \to \mathbb{P}^1, (a_0, a_1) \mapsto [a_0, a_1],$$

which sends a point p to the line through p and 0. In particular the restriction $\pi : \widehat{\mathbb{A}}^2 \setminus E \to \mathbb{A}^2 \setminus \{0\}$ is an isomorphism. On the other hand it is clear that

$$E = \big\{((0,0),[t,u]) \bigm| 0 * u = 0 * t\big\} = \{0\} \times \mathbb{P}^1.$$



(2) Now we want to see that $\widehat{\mathbb{A}}^2$ has an open cover by two affine planes. Let $V_t = \widehat{\mathbb{A}}^2 \setminus Z(t)$. On V_t we can put $t = 1$, thus

$$V_t = \{\ ((x,y),[1,u]) \in \mathbb{A}^2 \times \mathbb{P}^1 \bigm| y = xu\big\}.$$

Thus we see that the map $((x,y),[1,u]) \to (x,u) : V_t \to \mathbb{A}^2$ is an isomorphism with inverse $(x,u) \mapsto ((x,xu),[1,u])$. Simiarly let $V_u = \widehat{\mathbb{A}}^2 \setminus Z(u)$. Then

$$V_u = \{\ ((x,y),[t,1]) \in \mathbb{A}^2 \times \mathbb{P}^1 \bigm| x = yt\big\}$$

and $((x,y),[t,1]) \to (x,t) : V_u \to \mathbb{A}^2$ is an isomorphism.

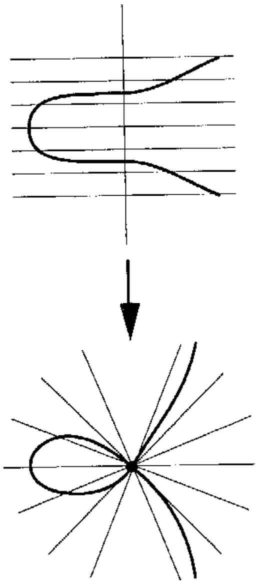
Thus on $\widehat{\mathbb{A}}^2$ we have two charts $(t \neq 0)$ and $(u \neq 0)$. The chart $t \neq 0$ is isomorphic to $\mathbb{A}^2$ with coordinates x, u. The exceptional divisor is $E = Z(x)$ and the projection π to $\mathbb{A}^2$ is given by $(x,u) \mapsto (x,xu)$. The chart $u \neq 0$ is isomorphic to $\mathbb{A}^2$ with coordinates t, y. The exceptional divisor is $E = Z(y)$ and the projection π to $\mathbb{A}^2$ is given by $(t, y) \mapsto (yt, y)$.

(3) Thus $\widehat{\mathbb{A}}^2$ has an open cover the affine spaces V_t,V_u, with nonempty intersection. Thus $\widehat{\mathbb{A}}^2$ is irreducible. As by (1) it contains the graph of [] as an open subset, it is its closure.

(4) We see that $\varphi_t(E \cap V_t) = Z(x) \subset \mathbb{A}^2$ and $\varphi_u(E \cap V_u) = Z(y) \subset \mathbb{A}^2$.

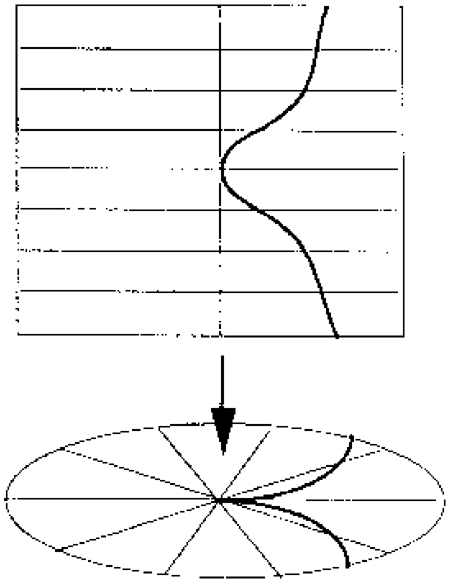
Example 4.15. Now we want to see what happens to curves in $\mathbb{A}^2$ under blowup.

(1) Let $C = Z(F)$ with $F = y^2 - x^2(x+1))$ be a nodal cubic. In the chart $t \neq 0$, the preimage of C is $Z(F(x, ux))$. We note that $F(x, ux)) = x^2(u^2 - (x+1))$. As $Z(x^2)$ is the exceptional divisor and $u^2 - (x+1)$ is irreducible, we see that $\widehat{C} = Z(u^2 - (x+1)$. Note that the intersection of $\widehat{C}$ with E consists of two points $(0, 1), (0, -1)$ corresponding to the slopes of the two different branches of C. By looking at the other chart $u \neq 0$ we see that $\widehat{C}$ is containded in the chart $t \neq 0$. Note that the map $\widehat{C} \to \mathbb{A}^1, (x, u) \mapsto u$ defines an isomorphsm of $\widehat{C}$ with $\mathbb{A}^1$, with inverse $t \mapsto (t^2 - 1, t)$. Thus $\widehat{C}$ is isomorphic to $\mathbb{A}^1$, whereas C is not.



(2) Let $C = Z(x^3 - y^2) \subset \mathbb{A}^2$ be the cuspidal cubic. In the chart $t \neq 0$, the preimage of C is $Z(x^2(x - u^2))$ and we see that $\widehat{C} = Z(x - u^2)$. Again it is easy to see that $\widehat{C}$ is completely contained in the chart $t \neq 0$ and that

$(x, u) \mapsto u$ defines an isomorphism $\widehat{C} \to \mathbb{A}^1$, while C is not isomorphic to $\mathbb{A}^1$.



Exercises.

(1) Let X, Y be irreducible varieties, $p \in X$, $q \in Y$. Show that $\mathcal{O}_{X,p}$ is isomorphic to $\mathcal{O}_{Y,q}$ if and only if there is an isomorphism $\varphi : U \to V$ between neighbourhoods U of p in X and V of q in Y.

(2) Which of the following define a rational map $\mathbb{P}^n \to \mathbb{P}^m$ (for suitable n, m).

(a) $[x, y]$ on $\mathbb{P}^3$,

(b) $[x, y, 1]$ on $\mathbb{P}^2$,

(c) $[x, y, 0]$ on $\mathbb{P}^2$,

(d) $[1/x, 1/y, 1/z]$ on $\mathbb{P}^2$,

(e) $[(x^3 + y^3)/z^3, y^2/z^2, 1]$ on $\mathbb{P}^2$,

(f) $[x^2 + y^2, y^2, y^2]$ on $\mathbb{P}^2$.

In each case determine $dom(\varphi)$ and say whether φ is birational.

(3) (a) Let $f := \frac{x_1}{x_0}$, viewed as a rational function on $\mathbb{P}_2$. Determine the domain of f.

(b) Let $f = [x_0, x_1]$ viewed as a rational map $\mathbb{P}^2 \to \mathbb{P}^1$. Determine the domain of f and describe the corresponding morphism.

(4) Show that any nonsingular conic in $\mathbb{P}^2$ is rational.

(5) Prove that any nonsingular quadric $Q \in \mathbb{P}^{n+1}$ is rational. Show that if $p \in Q$ is a nonsingular point, then the projection from p gives a birational map $\pi : Q \to \mathbb{P}^n$.

(6) Show that the cuspidal cubic $Z(y^2 - x^3) \subset \mathbb{A}^2$ is rational.

(7) Let $C = Z(y^3 - x^4) \subset \mathbb{A}^2$. Show that the strict transform of C under blowup in $(0,0)$ is isomorphic to $\mathbb{A}^1$.

(8) Show that the nodal cubic $C := Z(y^2 z - x^2(x+z)) \subset \mathbb{P}^2$ is rational.

Hint: The projection from $[0,0,1]$ induces a birational map $C \dashrightarrow \mathbb{P}^1$.

(9) Show that the blowup of $\mathbb{A}^2$ in a point is not affine.

(10) A quadric in $\mathbb{P}^n$ is the zero set of an irreducible homogeneous polynomial of degree 2. Show that every quadric in $\mathbb{P}^n$ is birational to $\mathbb{P}^{n-1}$.

(11) Let C, C' be irreducible curves. Let $f : C \dashrightarrow C'$ be a rational map. Prove:

(a) Either f is dominant, or f is constant.

(b) If f is dominant, then $K(C)$ is a finite algebraic extension of $f^*(K(C'))$.

(12) Let $p_0 := [1,0,0], p_1 := [0,1,0], p_2 := [0,0,1] \in \mathbb{P}^2$ and let $U := \mathbb{P}^2 \setminus \{p_0, p_1, p_2\}$. Consider the rational map

$$f : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2, [a_0, a_1, a_2] \mapsto [a_1 a_2, a_0, a_2, a_0 a_1].$$

(a) Show that f is defined on U.

(b) Show that f cannot be extended to $\mathbb{P}^2$.

(c) Show that f is birational and it is its own inverse. This is called the **Cremona transformation**.

CHAPTER 3

Dimension and Nonsingularity

In this chapter we want to study two important invariants of a variety, its dimension and its tangent space at a given point. In differential geometry a manifold has an open cover by sets diffeomorphic to $\mathbb{R}^n$ for some n, and then n is called the dimension of the manifold. In algebraic geometry things are more difficult, because algebraic varieties are not locally isomorphic to some affine spaces.

1. Dimension

In the first chapter we briefly introduced the notion of dimension of a variety. Recall that the dimension of an algebric set is the maximum of the dimensions of its irreducible components. In order to study dimension, the main idea is to use morphisms to compare dimensions for different varieties. For instance, if $f : X \to Y$ is a **surjective** morphism, then we expect $dim(X) \geq dim(Y)$. If in addition all the fibres $f^{-1}(p)$ for $p \in Y$ are **finite**, then we expect that $dim(X) = dim(Y)$. We will check this for a particularly nice class of morphisms, the **finite morphisms**.

1.1. Finite morphisms. Finite morphism of affine varieties are morphisms $f : X \to Y$ such that $A(X)$ is finite over $f^*(A(Y))$. So we first introduce and study the concept of an algebra being finite over another.

Definition 1.1. Let $A \subset B$ be k-algebras. For $b_1, \dots, b_n \in B$ we denote

$$A[b_1, \dots, b_n] := \big\{ g(b_1, \dots, b_n) \in B \; \big| \; g \in k[x_1, \dots, x_n] \big\}$$

the A**-algebra generated by** $b_1, \dots, b_n$.

B is called **finite** over A if there exist finitely many elements $b_1, \dots, b_n \in B$ such that $B = Ab_1 + \dots + Ab_n$.

To explain the meaning of this definition, we recall the notion of a module over a ring, which is the analogue of a vector space over a field.

Definition 1.2. Let R be a ring with 1. An abelian group B together with an operation $\cdot : R \times M \to M$ is called an R**-module**, if for all $r, r_1, r_2 \in R$, $b, b_1, b_2 \in B$ the following holds

(1) $(r_1r_2)b = r_1(r_2b)$ (associativity),

(2) $r(b_1 + b_2) = rb_1 + rb_2$, $(r_1 + r_2)b = r_1b + r_2b$ (distributivity),

(3) $1b = b$.

These are the same axioms as that for a vector space over a field.

An R-module B is called **finitely generated** if there are finitely many elements $b_1, \dots, b_n \in B$ with $B = Rb_1 + \dots + Rb_n$.

Example 1.3. (1) If I is an ideal in a ring R, then I is an R-module, via the multiplication in R. The condition that I is an ideal says precisely that $rb \in I$ for all $r \in R$, $b \in I$.

(2) If I is an ideal in a ring R and $A = R/I$, then A is an R-module, via $ra = \overline{r}a$ for all $r \in R$, $a \in A$, where $\overline{r}$ denotes the class of r in R/I.

(3) If A is a subring of the ring B, then B is an A-module, via the usual multiplication in B.

Thus if $A \subset B$ are k algebras, then B is an A-module and by definition B is finite over A if and only if it is a finitely generated A-module.

Proposition 1.4. (1) *Let $A \subset B \subset C$ be k-algebras. If B is finite over A and C is finite over B, then C is finite over A. If C is finite over A, then C is finite over B.*

(2) *Let $B \supset A$ be a finite A-algebra, and assume B is an integral domain. Then any $x \in B$ satisfies a monic equation over A, i.e. an equation*

$$x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0, \ a_i \in A,$$

(note that the leading coefficient is 1).

(3) *If b satisfies a monic equation over A, then $B = A[b]$ is finite over A.*

Proof. (1) is easy. If $B = Ab_1 + \dots + Ab_n$, $C = Bc_1 + \dots + Bc_m$, then $C = \sum_{i=1}^n \sum_{j=1}^m Ab_ic_j$. If $C = \sum_{i=1}^n Ac_i$ with $c_i \in C$, then $C = \sum_{i=1}^n Bc_i$ because $A \subset B$. (3) is easy: If $b^n + a_{n-1}b^{n-1} + \dots a_0 = 0$, then $B = Ab + \dots + Ab^{n-1}$, because all higher powers of b can be expressed in terms of $b, \dots, b^{n-1}$.

(2) We will use the determinant: Let R be a ring. Let $D := (d_{ij})_{i,j=1}^n$ be an $n \times n$ matrix of elements of R. Recall that the determinant of D is

$$det(D) := \sum_{\sigma \in \mathfrak{S}_n} sign(\sigma) d_{1\sigma(1)} \dots d_{n\sigma(n)},$$

where $\mathfrak{S}_n$ is the symmetric group and $sign(\sigma) = \pm 1$ is the sign of the permutation. In particular for any element x in a ring $C \supset R$ we get

$$det((x\delta_{ij} - d_{ij})_{ij}) = x^n + \sum_{i=0}^{n-1} a_i x^i, \quad a_i \in R. \tag{1}$$

Assume $B = \sum Ab_i,\ b_i \in B$, then $xb_i = \sum_j a_{ij} b_j$ for $a_{ij} \in A$. Thus $\sum_j (x\delta_{ij} - a_{ij}) b_j = 0$, where $(\delta_{ij})_{ij}$ is the identity matrix. That is $(b_1, \dots, b_n)$ is a nonzero element in the kernel of the matrix $M = (x\delta_{ij} - a_{ij})_{ij}$. Viewing this as a matrix with entries in the quotient field of B, we see that $det(M) = 0$. $det(M)$ is a monic polynomial in x. □

Definition 1.5. Let X, Y be affine varieties. A morphism $\varphi : X \to Y$ is called **finite** if $A(X)$ is a finite $\varphi^*(A(Y))$-algebra.

Remark 1.6. (1) In general, a morphism $f : X \to Y$ of varieties is called **finite** if Y has an affine open cover $Y = U_1 \cup \ldots \cup U_n$, such that all $W_i = f^{-1}(U_i)$ are affine and the $f|_{W_i} : W_i \to U_i$ are finite. For us however a finite morphism will be **a morphism of affine varieties**.

(2) Let $Y \subset X$ be a closed subvariety of an affine variety. Then the inclusion $i : Y \to X$ is a finite morphism (because i^* is surjective).

(3) Let $\varphi : X \to Y$, $\psi : Y \to Z$ morphisms of affine varieties. If φ and ψ are finite, then the composition $\psi \circ \varphi$ is finite. If $\psi \circ \varphi$ is finite, then φ is finite. This follows directly from part (2) of Proposition 1.4. In particular if $\varphi : X \to Y$ is a finite morphism with $\varphi(X) \subset W$ for $W \subset Y$ closed, then $\varphi : X \to W$ is finite.

A very important topological property of finite morphisms is, that, like morphisms between projective varieties, they are closed.

Remark 1.7. Let $X \subset \mathbb{A}^n$ be an affine variety and let $I \subsetneq A(X)$ be a proper ideal. Then $Z(I) \neq \emptyset$.

Proof. This is a straightforward reformulation of the Nullstellensatz. Let $\pi : k[x_1, \dots, x_n] \to A(X)$ be the projection. Then $Z(\pi^{-1}(I))$ is a proper ideal of $k[x_1, \dots, x_n]$ and $Z(I) = Z(\pi^{-1}(I))$, which is nonempty by the Nullstellensatz. □

Theorem 1.8. *Finite morphisms are closed.*

Proof. Let $f : X \to Y$ be a finite morphism of affine varieties. Let $W \subset X$ be closed. Let Z be the closure of $f(W)$ in Y. Then $f|_W : W \to Z$ is a finite morphism, $f(W)$ is dense in Z and we have to show that $f|_W : W \to Z$ is surjective. Thus we can assume that $f(X)$ is dense in Y and have to show that f is surjective.

As $f(X)$ is dense in Y we get that $f^* : A(Y) \to A(X)$ is injective. We identify $A(Y)$ with $f^*(A(Y)) \subset A(X)$. Let $Y \subset \mathbb{A}^n$ and $p = (a_1, \dots, a_n) \in Y$. Let $M := \langle x_1 - a_1, \dots, x_n - a_n\rangle \subset A(Y)$. We denote by $A(X)M := \{am \mid a \in A(X), m \in M\}$ the ideal generated by M in $A(X)$. Then

$$\begin{aligned} f^{-1}(p) &= \{q \in X \mid f(p) = q\} \\ &= \{q \in X \mid (x_i - a_i) \circ f = 0 \quad \forall_i\} = Z(A(X)M). \end{aligned}$$

Thus by the above remark it is enough to show the following Lemma. □

LEMMA 1.9. *Let B be a finite A-algebra, assume also that B is an integral domain. Let $I \subsetneq A$ be a proper ideal. Then also BI is a proper ideal in B.*

PROOF. The proof is rather similar to that of part (2) of Lemma 1.4. Assume $BI = B$. Let $B = Ab_1 + \ldots + Ab_n$, with $b_i \in B$. Then $BI = Ib_1 + \ldots + Ib_n$, thus $B = Ib_1 + \ldots + Ib_n$. In particular we get

$$b_i = \sum_{j=1}^{n} a_{ij} b_j, \quad a_{ij} \in I.$$

Put $M := (\delta_{ij} - a_{ij})_{i,j=1}^{n}$. Then $(b_1, \dots, b_n)$ is a nonzero element in the kernel of M, thus, viewing M as a matrix in the quotient field of B, we get $det(M) = 0$. Again by the formula (1) for the determinant, we get $det(M) = 1 + \sum_l b_l$ with $b_l \in I$. Thus we get $1 \in I$ and therefore $I = A$, a contradiction. □

Now we prove the Noether Normalization Theorem, the main tool for our treatment of dimension.

REMARK 1.10. Let $f \in k[x_1, \dots, x_n] \setminus \{0\}$ be a polynomial. Then there exists a point $p \in \mathbb{A}^n$ with $f(p) \neq 0$.

PROOF. If $n = 0$, the result is clear. If $n = 1$, then f splits as

$$f(x) = (x - b_1)^{n_1} \cdot \ldots \cdot (x - b_l)^{n_l}.$$

Choose $b \in k$ with $b \notin \{b_1, \dots, b_l\}$ (this is possible because k is algebraically closed and therefore infinite). Then $f(b) \neq 0$.

Now let n be general. We can write

$$f = \sum_i f_i x_n^i, \qquad f_i \in k[x_1, \dots, x_{n-1}].$$

Then there exists a j with $f_j \neq 0$. By induction on n there exists an $(a_1, \dots, a_{n-1}) \in \mathbb{A}^{n-1}$ with $f_j(a_1, \dots, a_{n-1}) \neq 0$. Therefore $g(x) := f(a_1, \dots, a_{n-1}, x) \neq 0$. By the case $n = 1$ there is an element $b \in k$ with $g(b) = f(a_1, \dots, a_{n-1}, b) \neq 0$. □

Theorem 1.11. *(Noether Normalization Theorem)*

(1) *Let $Z(F) \subset \mathbb{A}^n$ be a hypersurface. Then there exists a finite surjective morphism $\pi : Z(F) \to \mathbb{A}^{n-1}$.*

(2) *Let X be an affine variety. Then there exists a finite surjective morphism $\pi : X \to \mathbb{A}^k$ for some k.*

Proof. (1) Let $F^{(d)}$ be the top-degree homogeneous part of F. Then, as $F^{(d)}$ is homogeneous $F^{(d)}(x_1, \dots, x_{n-1}, 1) \neq 0$. Thus there exist $b_1, \dots, b_{n-1} \in k$, such that $F^{(d)}(b_1, \dots, b_{n-1}, 1) \neq 0$. By a linear change of coordinates we can assume that $(b_1, \dots, b_{n-1}) = (0, \dots, 0)$ and by multiplying F with a constant we can assume that $F^{(d)}(0, \dots, 0, 1) = 1$; in other words the coefficient of x_n^d in F is 1. Let

$$\pi := (x_1, \dots, x_{n-1}) : Z(F) \to \mathbb{A}^{n-1}.$$

Let $w_n \in A(Z(F))$ be the class of x_n. Then $A(X) = \pi^*(k[x_1, \dots, x_{n-1}])[w_n]$. As the coefficient of x_n^d in F is 1, we have $F = x_n^d + \sum_{i=0}^{d-1} a_i x_n^i$ with $a_i \in k[x_1, \dots, x_{n-1}]$. Thus in $A(X)$ we have an equation $0 = w_n^d + \sum_{i=0}^{d-1} \pi^*(a_i) w_n^i$, and π is a finite morphism.

Now we show that π is surjective. Let $b := (b_1, \dots, b_{n-1}) \in \mathbb{A}^{n-1}$. Let $g := F(b_1, \dots, b_{n-1}, x) \in k[x]$. As the coefficient of x_n^d of F is 1, we see that g is a nonconstant polynomial, thus $Z(g) \neq \emptyset$. Therefore

$$\pi^{-1}(b) = \big\{(b_1, \dots, b_{n-1}, c) \,\big|\, F(b_1, \dots, b_{n-1}, c) = 0\big\} = \{b\} \times Z(g) \neq \emptyset.$$

(2) If $X = \mathbb{A}^n$ or $n = 0$, the claim is trivial. Thus we assume $\emptyset \neq X \subsetneq \mathbb{A}^n$ and use induction on n. Let $F \in I(X) \setminus 0$. Then by part (1) there exist a finite morphism $\pi : Z(F) \to \mathbb{A}^{n-1}$. The inclusion $X \hookrightarrow Z(F)$ is a finite morphism, thus the composition $\tilde{\pi} : X \to \mathbb{A}^{n-1}$ is finite, let $Y \subset \mathbb{A}^{n-1}$ be its image. Then by induction there is a finite surjective morphism $\varphi : Y \to \mathbb{A}^k$. The composition $\varphi \circ \tilde{\pi} : X \to \mathbb{A}^k$ is a finite surjective morphism. □

We now show that finite surjective morphisms preserve strict inclusion of closed subsets and have finite fibres.

Lemma 1.12. *Let $\varphi : X \to Y$ be a finite surjective morphism. Let $Z \subsetneq W$ be closed subvarieties of X. Then $f(Z) \subsetneq f(W)$.*

Proof. We can assume $X = W$ and $Y = f(W)$ because $W \hookrightarrow X \to Y$ is finite. Let $g \in A(X)$ with $g|_Z = 0$. Then g satisfies an equation

$$g^n + \sum_{i=0}^{n-1} \varphi^*(a_i) g^i = 0, \quad a_i \in A(Y). \tag{1}$$

Take such an equation with minimal n. Then $\varphi^*(a_0) \neq 0$ because otherwise we could divide by g. Thus

$$\varphi^*(a_0) = -g\big(g^{n-1} + \sum_{i=1}^{n-1} \varphi^*(a_i) g^{i-1}\big) \in \langle g \rangle.$$

Therefore $\varphi^*(a_0)|_Z = 0$ and thus $a_0|_{\varphi(Z)} = 0$, i.e. $\varphi(Z) \subsetneq Y$. □

Corollary 1.13. *Let $\varphi : X \to Y$ be a finite surjective morphism. Then all the fibres $\varphi^{-1}(y)$ for $y \in Y$ are finite.*

Proof. It is enough to show that every irreducible component Z of $\varphi^{-1}(y)$ is a point. Let $z \in Z$. Then $\varphi(z) = \varphi(Z) = y$. Thus $Z = \{z\}$. □

1.2. Proof of the weak Nullstellensatz. At this point it is easy to show the weak Nullstellensatz. Let $M \subset k[x_1, \dots, x_n]$ be a maximal ideal. $L = k[x_1, \dots, x_n]/M$ is a field, which contains k as a subfield. Assume we know $k = L$. Then there are $a_1, \dots, a_n \in k$ such that a_i is the class of x_i in L, i.e. $x_i - a_i \in M$. So $\langle x_1 - a_1, \dots, x_n - a_n \rangle \subset M$. As $\langle x_1 - a_1, \dots, x_n - a_n \rangle$ is maximal, we see that $M = \langle x_1 - a_1, \dots, x_n - a_n \rangle$. Thus we have to show that $k = L$. This will follow from the Noether Normalization theorem.

Theorem 1.14. *(Noether Normalization Theorem) Let $I \subsetneq k[x_1, \dots, x_n]$ be an ideal and $A := k[x_1, \dots, x_n]/I$. There exists an injective k-algebra homomorphism $\varphi : k[x_1, \dots, x_k] \to A$ for some $0 \leq k \leq n$, such that A is finite over $im(\varphi)$.*

Proof. If $I = \{0\}$ or $n = 0$ the result is trivial. Thus assume $I \neq \{0\}$ and $n \neq 0$. Let $0 \neq F \in I$. Let $F^{(d)}$ be the top degree homogeneous part of F. Then, as $F^{(d)}$ is homogeneous, $F^{(d)}(x_1, \dots, x_{n-1}, 1) \neq 0$. Thus there exist $b_1, \dots, b_{n-1}$ in k such that $F^{(d)}(b_1, \dots, b_{n-1}, 1) \neq 0$. Let w_i be the class of x_i in A, then $A = k[w_1, \dots, w_n]$. Let $\pi : k[x_1, \dots, x_{n-1}] \to A; g(x_1, \dots, x_{n-1}) \mapsto g(w_1 - b_1 w_n, \dots, w_n - b_{n-1} w_n)$. Let $B := im(\pi) = k[w_1 - b_1 w_n, \dots, w_{n-1} - b_{n-1} w_n]$. Then $A = B[w_n]$. Let $g := F(w_1 + b_1 x, \dots w_{n-1} + b_{n-1} x) \in B[x]$. Then $g(w_n) = F(w_1, \dots, w_n) = 0$. The leading term of g is $F^{(d)}(b_1 x, \dots, b_{n-1} x, x) = F^{(d)}(b_1, \dots, b_{n-1}, 1) x^d$. Therefore $g/F^{(d)}(b_1, \dots, b_{n-1}, 1)$ is a monic polynomial for w_n. Thus A is finite over B.

We can write $B := k[x_1, \dots, x_{n-1}]/ker(\pi)$. Thus by induction on n there is an injective homomorphism of k-algebras $\psi : k[x_1, \dots, x_k] \to B$, such that B is finite over $im(\psi)$. Thus the composition $\varphi := \pi \circ \psi$ is injective and A is finite over $im(\varphi)$. □

Proof. (of the weak Nullstellensatz). There is an injective homomorphism of k-algebras $\varphi : k[x_1, \dots, x_k] \to L$, such that L is finite over $B := im(\varphi)$.

Claim: B is a field. Let $b \in B$. We need to show that $b^{-1} \in B$. b^{-1} exist in L. Therefore b^{-1} satisfies a monic equation

$$b^{-n} + a_{n-1}b^{-(n-1)} + \ldots + a_0 = 0, \quad a_i \in B.$$

Multiplying by b^{n-1} gives $b^{-1} = -(a_{n-1} + a_{n-2}b + \ldots + a_0 b^{n-1}) \in B$. Thus B is a field.

This gives immediately that $k = 0$ (because a polynomial ring is not a field). So L is a field, which is a finite k-algebra, i.e. L is a finite extension of k. As k is algebraically closed, we get that $k = L$. □

1.3. Dimension. Now we want to use finite morphisms to study the dimension of varieties. The main point is that finite surjective morphisms preserve dimension. Then the Noether Normalization Theorem allows us to reduce questions about dimension to questions in $\mathbb{A}^k$. By definition the dimension of a possibly not irreducible algebraic set is the maximum of the dimensions of its irreducible components. Thus we can restrict our attention to varieties.

Definition 1.15. Let X be a variety. Let $\emptyset \neq X_0 \subsetneq X_1 \subsetneq \ldots \subsetneq X_n = X$ be a chain of irreducible closed subsets of X. We call $X_0 \subsetneq X_1 \subsetneq \ldots \subsetneq X_n$ **a chain in** X. We know that $dim(X)$ is the maximal n such that such a chain exists. In this case we call $X_0 \subsetneq X_1 \subsetneq \ldots \subsetneq X_n$ a **longest chain in** X.

Now we show that finite surjective morphisms preserve dimension. We start with some elementary statements about dimension.

Lemma 1.16. (1) *If $Y \subset X$ is a closed subvariety of the variety X, then $dim(Y) < dim(X)$.*

(2) *Let $f : X \to Y$ is a surjective closed morphism of varieties. Then $dim(X) \geq dim(Y)$.*

Proof. (1) We can extend a longest chain $Y_0 \subsetneq \ldots \subsetneq Y_k$ in Y to a chain $Y_0 \subsetneq \ldots \subsetneq Y_k \subsetneq X$, which is longer.

(2) Let $Y_0 \subsetneq \ldots \subsetneq Y_n$ be a longest chain in Y. We have to show there is a chain $X_0 \subsetneq \ldots \subsetneq X_n$ in X, with $f(X_i) = Y_i$ for all i. We use induction on n. If $n = 0$ there is nothing to show. Otherwise let $Z_1, \ldots, Z_r$ be the irreducible components of $f^{-1}(Y_{n-1})$ Thus $Y_{n-1} = f(Z_1) \cup \ldots \cup f(Z_r)$. Y_{n-1} is irreducible and the $f(Z_i)$ are closed. So one of the Z_i, say Z_1, must map surjectively to Y_{n-1}. We apply the induction hypothesis to $f|_{Z_1}$, to get a chain $X_0 \subsetneq \ldots \subsetneq X_{n-1} = Z_1$ with $f(X_i) = Y_i$. Extending the chain by X at the end we get a chain of length n. □

Theorem 1.17. *Let $f : X \to Y$ be a finite surjective morphism of varieties. Then $dim(X) = dim(Y)$.*

Proof. $dim(X) \geq dim(Y)$ because f is surjective and closed. We show the opposite inequality. Let $X_0 \subsetneq \dots \subsetneq X_n$ be a longest chain in X. We put $Y_i = f(X_i)$. Then the Y_i are closed and irreducible and $Y_i \subsetneq Y_{i+1}$ for all i because f preserves strict inclusion. Thus $Y_0 \subsetneq \dots \subsetneq Y_n$ is a chain in Y and $dim(Y) \leq dim(X)$. □

Now we can show that $\mathbb{A}^n$ has dimension n.

Theorem 1.18. (1) *$dim(\mathbb{A}^n) = n$.*

(2) *Let $F \in k[x_1, \dots, x_n]$ be an irreducible polynomial of positive degree. Then $dim(Z(F)) = n - 1$.*

(3) *Conversely any subvariety $X \subset \mathbb{A}^n$ with $dim(X) = n - 1$ is a hypersurface.*

Proof. (1)⇒(2) Let $F \in k[x_1, \dots, x_n]$ be a nonconstant polynomial. Then there is a finite surjective morphism $Z(F) \to \mathbb{A}^{n-1}$, thus $dim(Z(F)) = dim(\mathbb{A}^{n-1})$.

(1) We show the result by induction on n, the case $n = 0$ being trivial. Let $Z_i := Z(x_{i+1}, \dots, x_n) \subset \mathbb{A}^n$. Then $Z_i \simeq \mathbb{A}^i$, thus $Z_0 \subsetneq Z_1 \subsetneq \dots \subsetneq Z_n$ is a chain in $\mathbb{A}^n$. Thus $dim(\mathbb{A}^n) \geq n$.

The opposite inequality we prove by induction on n. The case $n = 0$ is trivial. Thus assume $dim(\mathbb{A}^{n-1}) = n - 1$. Let $X_0 \subsetneq X_1 \subsetneq \dots \subsetneq X = X_{k-1} \subsetneq \mathbb{A}^n$ be a maximal chain for $\mathbb{A}^n$. Then $X \subsetneq \mathbb{A}^n$ is a closed subset. Let $F \in I(X)$ be irreducible (first we take $G \in I(X)$, then one irreducible factor of G must lie in the prime ideal $I(X)$). As $X \subset Z(F)$, we know that $k - 1 \leq dim(Z(F)) = dim(\mathbb{A}^{n-1}) = n - 1$ by the part (1)⇒(2). Thus $dim(\mathbb{A}^n) = k \leq dim(Z(F)) + 1 = n$.

(3) As $X \subsetneq \mathbb{A}^n$, there is an irreducible $F \in I(X)$ with $X \subset Z(F)$. As $dim(X) = dim(Z(F))$ and both are irreducible, we have $X = Z(F)$ by Lemma 1.16. □

Now we show that the intersection of a closed subvariety $X \subset \mathbb{A}^n$ with a hypersurface has dimension $dim(X) - 1$.

Proposition 1.19. *Let $X \subset \mathbb{A}^N$ be an affine variety of dimension n. Let $F \in k[x_1, \dots, x_N] \setminus I(X)$. If $X \cap Z(F) \neq \emptyset$, then $dim(X \cap Z(F)) = n - 1$.*

Remark 1.20. If $X \cap Z(F)$ is reducible, then the statement says that $dim(X_i) \leq dim(X) - 1$ for all irreducible components X_i of $X \cap Z(F)$ and equality holds for at least one X_i. Later we will see that **all** components satisfy $dim(X_i) = dim(X) - 1$.

Proof. As $Y := X \cap Z(F) \subsetneq X$, we see that $dim(Y) \leq n-1$. Assume $dim(Y) \leq n-2$. Then we have to show $Y = \emptyset$. Let $f \neq 0$ be the class of F in $A(X)$. We reduce to the case $X = \mathbb{A}^n$. Let $\pi : X \to \mathbb{A}^n$ be a finite surjective morphism. We identify $k[x_1, \dots, x_n]$ with its image via π^* in $A(X)$. By finiteness there is a nonzero polynomial

$$H = x_{n+1}^d + \sum_{i=0}^{d-1} a_i x_n^i, \quad a_i \in k[x_1, \dots, x_n], \quad \text{with } H(x_1, \dots, x_n, f) = 0 \text{ in } A(X).$$

By replacing H by one of its irreducible factors we can assume that H is irreducible. Note that if $H = H_1 H_2$, then we must have that both H_1 and H_2 are of this form.

Let $\varphi : (\pi, F) : X \to \mathbb{A}^{n+1}$. As $\pi = (x_1, \dots, x_n) \circ \varphi$ is finite, also φ is finite. By definition $\varphi(X) \subset Z(H)$. Thus $\varphi(X)$ is a closed subset of dimension n of $Z(H)$. On the other hand $Z(H)$ is an irreducible hypersurface in $\mathbb{A}^{n+1}$. Thus $\varphi(X) = Z(H)$. Therefore $\varphi : X \to Z(H)$ is a finite surjective morphism. By definition

$$Z(F) \cap X = \varphi^{-1}(Z(H, x_{n+1})) = \varphi^{-1}(Z(a_0) \times \{0\}).$$

Thus $n - 2 \geq dim(Z(F) \cap X) = dim(Z(a_0))$. Thus, by Theorem 1.18, a_0 is constant and $Z(F) \cap X = Z(a_0) = \emptyset$. □

A variety X and dense open subset $U \subset X$ have the same dimension.

Theorem 1.21. *Let X be a variety, and let $U \subset X$ be a nonempty open subset. Then $dim(U) = dim(X)$.*

Proof. "$\leq$" Let $\emptyset \neq U_0 \subsetneq U_1 \subsetneq \dots \subsetneq U_n = U$ be a longest chain for U. Let $X_i = \overline{U}_i$ be the closure of U_i in X. Then $X_0 \subsetneq X_1 \subsetneq \dots \subsetneq X_n$ is a chain in X, and thus $dim(U) \leq dim(X)$.

"$\geq$" Let $X_0 \subsetneq X_1 \subsetneq \dots \subsetneq X_n$ be a maximal chain in X. Let $W \subset X$ be an open affine subset such that $X_0 \in W$. Let $W_i = X_i \cap W$ for all i. As $W_{i+1} \neq \emptyset$, it is dense in X_{i+1}. On the other hand $W_i \subset X_i$ which is not dense in X_{i+1}. Thus $W_i \subsetneq W_{i+1}$ and $W_0 \subsetneq W_1 \subsetneq \dots \subsetneq W_n$ is a chain in W. Thus $dim(W) \geq dim(X)$, i.e. $dim(W) = dim(X)$. Thus replacing X by W and U by $U \cap W$, we can assume that X is affine.

If $X = \mathbb{A}^n$, let X_0 a point in U, and X_{i+1} an affine linear subspace containing X_i. Put $U_i = X_i \cap U$. Then $U_0 \subsetneq U_1 \subsetneq \dots \subsetneq U_n$ is a chain in U, i.e. $dim(U) = n$. If X is affine, there is a finite surjective morphism $\varphi : X \to \mathbb{A}^n$ and $\varphi(X \setminus U)$ is a proper closed subset Z of $\mathbb{A}^n$, because φ preserves strict inclusion of closed subsets. Let $f \in I(Z)$. Then $V := \mathbb{A}^n \setminus Z(f)$ is open and dense in $\mathbb{A}^n$, thus $dim(V) = n$. Let $W := \varphi^{-1}(V)$. Then, as φ is surjective and closed, so is $\varphi|_W : W \to V$. Thus

$dim(W) \geq dim(V) = n$. Therefore $dim(U) \geq dim(W) \geq dim(V) = n = dim(X)$. Thus $dim(U) = dim(X)$. □

Corollary 1.22. *If the varieties X and Y are birational, then $dim(X) = dim(Y)$.*

Proof. Assume X and Y are birational. By Corollary 4.9 of Chapter 2 there are nonempty open subsets $U \subset X$ and $V \subset Y$ which are isomorphic. Then by the theorem $dim(X) = dim(U) = dim(V) = dim(Y)$. □

Corollary 1.23. (1) *$dim(\mathbb{P}^n) = n$.*

(2) *Let $F \in k[x_0, \ldots, x_n]$ be an irreducible homogeneous polynomial of positive degree. Then $dim(Z(F)) = n - 1$.*
(3) *Conversely any subvariety $X \subset \mathbb{P}^n$ with $dim(X) = n - 1$ is a hypersurface.*

Proof. (1) is clear, because $\mathbb{A}^n \subset \mathbb{P}^n$ is open and dense. (2) By a projective linear transformation we can assume $Z(F) \not\subset H_\infty$. Then $Z(F) \cap \mathbb{A}^n = Z(F(1, x_1, \ldots, x_n))$ has dimension $n - 1$ and is dense in $Z(F)$. (3) Is proven in the same way as in the affine case. □

Finally we can prove a stronger version of Proposition 1.19: Every component of $Z(F) \cap X$ has dimension $dim(X) - 1$.

Theorem 1.24. *Let $X \subset \mathbb{A}^n$ be an affine variety, and let $F \in k[x_1, \ldots, x_n] \backslash I(X)$. Then every irreducible component of $X \cap Z(F)$ has dimension $dim(X) - 1$.*

Remark 1.25. It can happen that $X \cap Z(F) = \emptyset$, e.g. $X = Z(x_1)$, $F = x_1 + 1$ in $\mathbb{A}^2$. There is no contradiction: then $X \cap Z(F)$ has no irreducible components.

Proof. Let Z be an irreducible component of $X \cap Z(F)$ and let W be the union of the other irreducible components. Let $g \in I(W) \setminus I(Z)$. Let $U := X \setminus Z(g)$. Then we know that U is an affine variety and $U \cap Z(F) = U \cap Z$ is irreducible. Thus $dim(Z) = dim(Z \cap U) = dim(X) - 1$. □

Theorem 1.21 and Theorem 1.24 are the main results about dimension that usually allow to compute the dimension of a variety. We give a number of consequences.

Corollary 1.26. *Let $f : X \to Y$ be a morphism of varieties, assume that there is a nonempty open subset of $U \subset Y$ so that $dim(f^{-1}(p)) = n$ for all $p \in U$. Then $dim(X) = dim(Y) + n$.*

PROOF. As morphisms are continuous and points are closed, the fibres of f are closed in X. $V := f^{-1}(U)$ is open and dense in X. $dim(Y) = dim(U)$ and $dim(X) = dim(V)$, so replacing X by V and Y by U we can assume all fibres have dimension n.

Now we prove the result by induction on $dim(Y)$. If Y is a point, there is nothing to show. Replacing Y by an affine open subset and X by an open affine in its preimage, we can assume $X \subset \mathbb{A}^l$, $Y \subset \mathbb{A}^m$ are affine varieties. Then $f = (F_1, \dots, F_m)$ with $F_i \in k[x_1, \dots, x_l]$. Let $g \in k[x_1, \dots, x_m]$ be a polynomial with $\emptyset \neq Z(g) \cap Y \neq Y$. Let Y' be an irreducible component of $Z(g) \cap Y$ and let $X' = f^{-1}(Y')$. Then X' is a union of components of $Z(g(F_1, \dots, F_m)) \cap X$. Thus by the previous theorem and the induction hypothesis we get

$$dim(X) = dim(X') + 1 = dim(Y') + n + 1 = dim(Y) + n$$

□

EXAMPLE 1.27.

(1) For varieties X, Y, we have $dim(X \times Y) = dim(X) + dim(Y)$ (apply the corollary to the projection $X \times Y \to Y$).

(2) Let $X \subset \mathbb{P}^n$ be a projective variety and let $C(X) \subset \mathbb{A}^{n+1}$ be its affine cone. Then $dim(C(X)) = dim(X) + 1$: The morphism

$$[x_0, \dots, x_n] : C(X) \setminus \{0\} \to X, (a_0, \dots, a_n) \mapsto [a_0, \dots, a_n]$$

has all fibres isomorphic to $\mathbb{A}^1 \setminus \{0\}$.

Now we are able to get a result about the intersection of two arbitrary closed subvarieties of $\mathbb{A}^n$ and $\mathbb{P}^n$.

THEOREM 1.28.

(1) *Let $X, Y \subset \mathbb{A}^n$ be affine varieties. Then every irreducible component of $X \cap Y$ has dimension at least $dim(X) + dim(Y) - n$.*

(2) *Let $X, Y \subset \mathbb{P}^n$ be projective varieties. Then every irreducible component of $X \cap Y$ has dimension at least $dim(X) + dim(Y) - n$. Furthermore, if $dim(X) + dim(Y) \geq n$, then $X \cap Y \neq \emptyset$.*

PROOF. (1) The trick is to use the diagonal to reduce to the intersection with hyperplanes. Let $\Delta \subset \mathbb{A}^n \times \mathbb{A}^n$ be the diagonal and let $\delta : \mathbb{A}^n \to \mathbb{A}^n \times \mathbb{A}^n$ be the diagonal morphism, which is an isomorphism onto Δ. We note that $\delta^{-1}(X \times Y) = X \cap Y$, thus

$$X \cap Y \simeq (X \times Y) \cap \Delta \subset \mathbb{A}^{2n}.$$

Let $x_1, \dots, x_n$ be the coordinates on the first factor $\mathbb{A}^n$ and $y_1, \dots, y_n$ the coordinates on the second. Then $\Delta = Z(x_1 - y_1, \dots, x_n - y_n)$ is the intersection of n hyperplanes. By Theorem 1.24 every irreducible component of an intersection of a variety $Z \subset \mathbb{A}^N$

of dimension k with a hypersurface f has dimension $\geq k-1$ (namely k in case $Z \subset Z(f)$ and $k-1$ otherwise). Therefore inductively every irreducible component of $X \cap Y$ has dimension $dim(X \cap Y) \geq dim(X) + dim(Y) - n$.

(2) We reduce to (1) by using the affine cones $C(X), C(Y) \subset \mathbb{A}^{n+1}$. By definition $C(X) \cap C(Y) = C(X \cap Y)$ and X is irreducible if and only if $C(X)$ is. We have $dim(C(X)) = dim(X)+1$ (and analogously for Y and $X \cap Y$). Let Z be an irreducible component of $X \cap Y$. Then

$$dim(Z) = dim(C(Z))-1 \geq dim(C(X))+dim(C(Y))-(n+1)-1 = dim(X)+dim(Y)-n.$$

Now assume $dim(X) + dim(Y) \geq n$. We note that $C(X) \cap C(Y) \neq \emptyset$ because it contains 0. Every irreducible component of $C(X \cap Y) = C(X) \cap C(Y)$ has dimension $dim(X) + dim(Y) - n + 1 \geq 1$. Thus $C(X \cap Y) \neq \{0\}$ and $X \cap Y \neq \emptyset$. □

Remark 1.29. We get a stronger result in the projective case. It is also guarantied that the intersection $X \cap Y$ is nonempty if $dim(X) + dim(Y) \geq n$. This is a strong existence result, which is not true in other varieties.

Corollary 1.30. *$\mathbb{P}^1 \times \mathbb{P}^1$ is not isomorphic to $\mathbb{P}^2$.*

Proof. Assume $\mathbb{P}^2 \simeq \mathbb{P}^1 \times \mathbb{P}^1$. Then any two subvarieties of $\mathbb{P}^1 \times \mathbb{P}^1$ of dimension 1 intersect. On the other hand for $p \neq q \in \mathbb{P}^1$, obviously $p \times \mathbb{P}^1$ and $q \times \mathbb{P}^1$ are disjoint. □

1.4. Dimension and Transzendence degree. We have seen that birational algebraic varieties have the same dimension. As two varieties are birational if and only if their function fields are isomorphic, it must be possible to define dimension of a variety X only in terms of the function field $K(X)$. In fact one of the standard definitions of the dimension of X in the literature is the transzendence degree of $K(X)$. Now I want to briefly sketch why this definition is equivalent to our definition. First I need to briefly recall (without proofs) the basic facts about transzendendence degree.

Definition 1.31. Let K/k be a **field extension**. This means that K and k are fields and k is a subring of K. Let $a_1, \dots, a_n \in K$. We denote $k(a_1, \dots, a_n)$ the smallest subfield of K containing k and $a_1, \dots, a_n$. We call $k(a_1, \dots, a_n)$ the field extension **generated by** $(a_1, \dots, a_n)$. If there exist finitely many elements $a_1, \dots, a_n$ such that $K = K(a_1, \dots, a_n)$ we say that K/k is a **finitely generated** field extension.

Now let K/k be a finitely generated field extension. Elements $b_1, \dots, b_m \in K$ are called **algebraically independent** over k if there is no polynomial $f \in k[x_1, \dots, x_m] \setminus \{0\}$ with $f(b_1, \dots, b_m) = 0$. Note that one element $b \in K$ is algebraically independent if and only if it is **transzendent**, i.e. not algebraic over k.

Assume $b_1, \dots, b_r$ are algebraically independent over k. Then it is easy to see that $k(b_1, \dots, b_n)$ is isomorphic to the field of rational functions $k(x_1, \dots, x_n)$.

A maximal set of algebrically independent elements of K over k is called a **transzendence basis**.

Theorem 1.32. *Let $K = k(a_1, \dots, a_m)/k$ be a finitely generated field extension*

1. *There exists a transzendence basis of K/k, it can be chosen as a subset of $a_1, \dots, a_m$.*
2. *Every transzendence basis of K/k has the same number of elements, called the* **transzendence degree** *of K/k.*
3. *Let $b_1, \dots, b_r$ be a transzendence basis of K/k. Then $K/k(b_1, \dots, b_r)$ is a finite algebraic extension.*

Now let X be an algebraic variety over k. Then X contains an open subset V which is affine and $K(X) = K(V)$. If $V \subset \mathbb{A}^n$, then $K(X) = k(y_1, \dots, y_n)$ where the y_i are the coordinate functions on X. Thus $K(X)$ is a finitely generated extension field of k and we denote by $trdeg(K(X))$ the transzendence degree of $K(X)/k$. If $X = \mathbb{A}^n$ or $X = \mathbb{P}^n$, we see that $k(X)$ is the field of rational $k(x_1, \dots, x_n)$ and thus $trdeg(K(X)) = n = dim(X)$. Our aim is to show:

Theorem 1.33. *Let X be a variety. Then $dim(X) = trdeg(K(X))$.*

Proof. We will show below that every variety is birational to a hypersurface in some $\mathbb{A}^n$. Thus we can assume that $X = Z(F)$ is a hypersurface in $\mathbb{A}^n$, where $F \in k[x_1, \dots, x_n]$ is an irreducible polynomial. Then $dim(X) = n - 1$. We denote $x_1, \dots, x_n$ the coordinates on $\mathbb{A}^n$. Let $y_1, \dots, y_n$ be the coordinate functions on X. Then we have $F(y_1, \dots, y_n) = 0$ in $K(X)$ and thus $trdeg(K(X)) \leq n - 1$. To show that $trdeg(K(X)) = n - 1$, we can assume that x_n occurs in F and show that $y_1, \dots, y_{n-1}$ are algebraically independent. If they were not algebraically independent, then there would be a polynomial $G \in k[x_1, \dots, x_{n-1}]$ with $G(y_1, \dots, y_{n-1}) = 0$. But then $G \in I(X) = \langle F \rangle$ in contradiction to our choice of F. Thus it remains to show that every variety X is birational to a hypersurface in some $\mathbb{A}^n$. □

We want to use another nontrivial result from algebra: the theorem of the primitive element. We state this only in characteristic 0, although the proof works in arbitrary characteristic when one takes a bit more care.

Theorem 1.34. *(of the primitive element) Let K be a field of characteristic* 0 *and let L/K be a finite field extension. Then there is an element $b \in L$ such that $L = K(b)$.*

Theorem 1.35. *Any variety X is birational to a hypersurface in some $\mathbb{A}^n$.*

Proof. Let $x_1, \dots, x_r$ be a transzendence basis of $K(X)/k$. $K(X)/k(x_1, \dots, x_r)$ is a finite algebraic extension, and thus there exists an element $y \in K(X)$, such that $K(X) = k(x_1, \dots, x_r; y)$. y is algebraic over $k(x_1, \dots, x_r)$, thus there is an irreducible polynomial $F \in k(x_1, \dots, x_r)[x]$, such that $F(y) = 0$.

Write

$$F = \sum_l \frac{G_l(x_1, \dots, x_n)}{H_l(x_1, \dots, x_n)} x^l, \quad G_l, H_l \in k[x_1, \dots, x_n].$$

Let $f \in k[x_1, \dots, x_n, x]$ be the polynomial obtained from f by multiplying with the product of the $H_l(x_1, \dots, x_n)$ and then dividing by the largest common factor of the coefficients of all the x^i. As F was irreducible, so is f (by the Gauss Lemma: Obviously f is irreducible in $k(x_1, \dots, x_r)[x]$. It is also a primitive polynomial in $k[x_1, \dots, x_n][x]$, thus is is irreducible in $k[x_1, \dots, x_n, x]$.) Then f defines a hypersurface Y in $\mathbb{A}^{r+1}$ and $K(Y) = Q(k[x_1, \dots, x_r, x]/(f)) = Q(k[x_1, \dots, x_r, x])/(f) = K(X)$. □

Exercises.

(1) Let $X = Z(x^3 - y^2) \subset \mathbb{A}^2$. Give a finite morphism $X \to \mathbb{A}^1$.

(2) Let $Y \subset \mathbb{P}^n$ be a closed subvariety. Assume that $[0, \dots, 0, 1] \not\in Y$. Let $X := Y \cap \mathbb{A}^n$. Show that $(x_1, \dots, x_{n-1}) : X \to \mathbb{A}^{n-1}$ is a finite morphism.

(3) Let $f : X \to Y$ be a finite morphism of affine varieties. Show that there is an n, such that $|f^{-1}(p)| \le n$ for all $p \in Y$.

(4) Give an example of a projective variety Z and closed subsets $X, Y \subset Z$ with $dim(X) + dim(Y) \ge dim(Z)$, and $X \cap Y = \emptyset$.

(5) Prove that a proper closed subset of an irreducible curve is a finite set. Deduce that any bijection between irreducible curves is a homeomorphism.

(6) Let X, Y be varieties, $f : X \to Y$ a dominant rational map. Show that $dim(X) \ge dim(Y)$.

2. Tangent Space and nonsingular varieties

We introduce tangent spaces of algebraic varieties and singular and nonsingular points. We will show that the nonsingular points of an irreducible variety X are an open dense subset, i.e. almost all point of X are nonsingular points. In the case $k = \mathbb{C}$ one can show that the nonsingular points of a variety form a complex manifold. We start with affine varieties, where the definition is more explicit. The tangent space of a variety X at p is the vector space that best approximates X near p.

2.1. Singular and nonsingular points of hypersurfaces. We briefly introduce singular and nonsingular points of hypersurfaces in $\mathbb{A}^n$. We will study these notions much more carefully and in more generality in chapter 3.

DEFINITION 2.1. For a polynomial $f \in k[x_1, \dots, x_n]$, we have the **partial derivatives** $\frac{\partial f}{\partial x_i} \in k[x_1, \dots, x_n]$.

Let $X = Z(f) \subset \mathbb{A}^n$ be a hypersurface with $f \in k[x_1, \dots, x_n]$ and assume that $I(X) = \langle f \rangle$. A point $p \in X$ is called a **singular point** of X if

$$\frac{\partial f}{\partial x_i}(p) = 0 \text{ for all } i = 1, \dots, n.$$

Otherwise X is called a **nonsingular point**.

We denote X_{reg} the set of nonsingular points of X and X_{sing} the set of singular points. If $X = X_{reg}$, then X is called **nonsingular** or **smooth**.

REMARK 2.2. If $X \subset \mathbb{A}^n$ is an affine hypersurface over $\mathbb{C}$, one can show that with the analytic topology X_{reg} is a complex submanifold of $\mathbb{C}^n$ of dimension $n-1$.

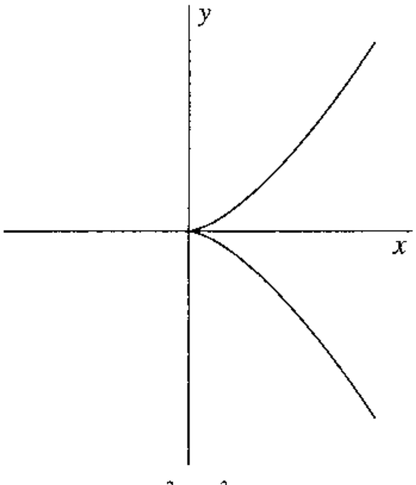
EXAMPLE 2.3.

(1) In the definition one needs that $I(X) = \langle f \rangle$ and not just that $X = Z(f)$, e.g. $Z(y^2) \subset \mathbb{A}^2$ is just the line $Z(y)$, which in nonsingular, but $\frac{\partial y^2}{\partial y}(p) = \frac{\partial y^2}{\partial x}(p) = 0$.

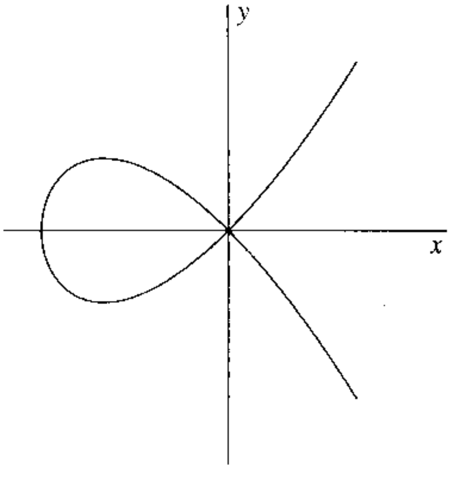
(2) $X = Z(y - x^2 + x) \subset \mathbb{A}^2$ be an irreducible conic. Then $(0,0)$ is a nonsingular point of X, in fact X is nonsingular.

(3) Let $X = Z(y^2 - x^2 - x^3) \subset \mathbb{A}^2$, be a nodal cubic, then $(0,0)$ is a singular point of X. One can check that it is the only singular point of X.

(4) Let



$y^2 = x^3$



$y^2 = x^2(1 + x)$

Proposition 2.4. *Let $X \subset \mathbb{A}^n$ be an irreducible hypersurface. Then X_{reg} is an open dense subset of X.*

Proof. For simplicty we assume $char(k) = 0$. Let $F \in k[x_1, \ldots, x_n]$ be irreducible with $Z(F) = X$.

Thus we obtain $X_{sing} = Z(F, \frac{\partial F}{\partial x_1}, \ldots, \frac{\partial F}{\partial x_n})$, which is closed in X, i.e. X_{reg} is open in X. If X_{reg} was empty, then $\frac{\partial F}{\partial x_i} \in \langle F \rangle$ for all i. As the degree of $\frac{\partial F}{\partial x_i}$ is smaller than that of F, the only possibility for this to happen is that $\frac{\partial F}{\partial x_i} = 0$ for all i. By the assumption that the characteristic of k is 0 this implies that F is constant, a contradiction. □

2.2. The tangent space of an affine algebraic set. Let $X \subset \mathbb{A}^n$ be an affine algebraic set. Note that we not not require X to be irreducible. The tangent space of $X \subset \mathbb{A}^n$ at a point p is the linear subspace $V \subset \mathbb{A}^n$ which best approximates X near p. If the dimension of the tangent space at p is the same as the dimension of X then p is called a nonsingular point of X.

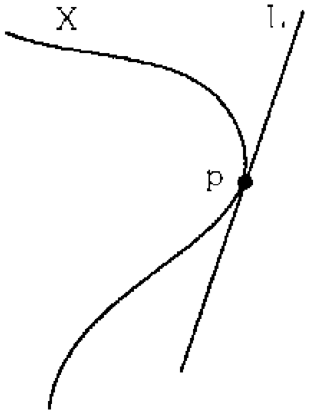
Definition 2.5. Let $f \in k[x_1, \ldots, x_n]$ and $p = (p_1, \ldots, p_n) \in \mathbb{A}^n$. The **differential** of f at p is the linear map

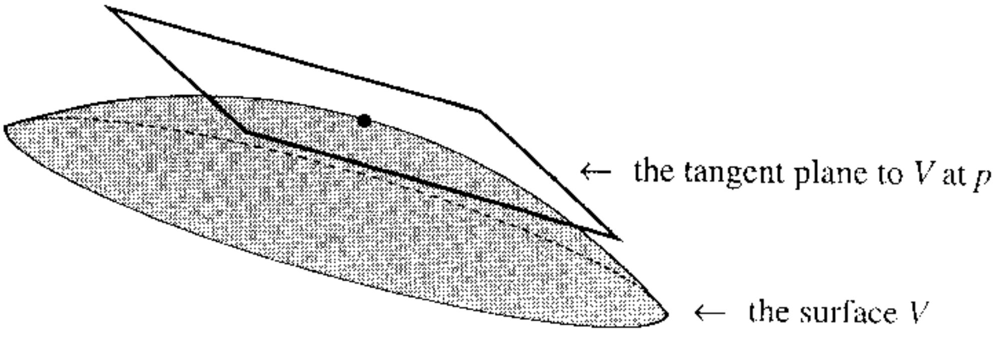
$$d_pf := \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(p)x_i = \Big(\frac{\partial f}{\partial x_1}(p), \ldots, \frac{\partial f}{\partial x_n}(p)\Big).$$

Let $X \subset \mathbb{A}^n$ be an affine algebraic set and let $p \in X$. Note that $d_p(fg) = (d_pf)g(p) + f(p)d_p(g)$.

The **tangent space** of X at p is

$$T_pX = Z\big(d_pf \mid f \in I(X)\big) = \bigcap_{f \in I(X)} ker(d_p(f)).$$





$p \in X$ is called a **nonsingular point**, if $dim(T_pX) = dim_p(X)$, i.e. the maximum of the dimensions of the components passing through p. Here we can take the dimension of T_pX either to be the dimension as a vector space, or equivalently as a variety. One can show, but we will not, that in this case there can be only one irreducible component of X passing through p. Otherwise p is called a **singular point**. We denote X_{reg} the set of nonsingular points of X and X_{sing} the set of singular points. If $X = X_{reg}$, then X is called **nonsingular** or **smooth**.

Remark 2.6. If $X \subset \mathbb{C}^n$ is an affine variety over $\mathbb{C}$, one can show that with the analytic topology X_{reg} is a complex submanifold of $\mathbb{C}^n$ of dimension $dim(X)$.

To determine the tangent space it is enough to look at the generators of $I(X)$.

Corollary 2.7. *Let $I(X) = \langle f_1, \dots, f_r \rangle$. Then*

$$T_pX = Z(d_pf_1, \dots, d_pf_r) \subset k^n.$$

Proof. The inclusion $T_pX \subset Z(d_pf_1, \dots, d_pf_r$ is obvious. If $h = \sum_i h_if_i \in I(X)$, then $f_i(p) = 0$ implies

$$d_ph = \sum_i h_i(p)d_pf_i + (d_ph_i)f_i(p) = \sum_i h_i(p)d_pf_i \in \langle d_pf_1, \dots, d_pf_r\rangle.$$

Thus $Z(d_ph) \supset Z(d_pf_1, \dots, d_pf_r)$. □

Like in differential geometry a morphism of affine varieties gives a linear map between tangent spaces.

Definition 2.8. The **Jacobian** of $f_1, \dots, f_r \in k[x_1, \dots, x_n]$ is the $r \times n$ matrix

$$J(f_1, \dots, f_r) := \begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \dots & \frac{\partial f_1}{\partial x_n} \\ & \dots & \\ \frac{\partial f_r}{\partial x_1} & \dots & \frac{\partial f_r}{\partial x_n} \end{pmatrix}.$$

with coefficients in $k[x_1, \dots, x_n]$.

Remark 2.9. Note that that $Z(d_pf_1, \dots, d_pf_r) = ker(J(f_1, \dots, f_r)(p))$.

Definition 2.10. Let $X \subset \mathbb{A}^n, Y \subset \mathbb{A}^m$ be affine varieties. Let $p \in X$, $q \in Y$. Let $\varphi = (f_1, \dots, f_m) : X \to Y$ be a morphism with $\varphi(p) = q$ given by $f_i \in k[x_1, \dots, x_n]$. The **differential** of φ at p is $d_p\varphi := (d_pf_1, \dots, d_pf_m) : T_pX \to T_qY$. Note that $d_p\varphi$ is the linear map $d_p\varphi : k^n \to k^m$ given by the Jacobian $J(f_1, \dots, f_r)(p) = \left(\frac{\partial f_i}{\partial x_j}(p)\right)_{ij}$. It is an easy exercise to check that $d_p\varphi$ indeed maps T_pX to T_qY.

Remark 2.11. Obviously we have $d_pid_X = id_{T_pX}$, and it is easy to see (exercise) that $d_p(\psi \circ \varphi) = d_{\varphi(p)}\psi \circ d_p\varphi$. In particular, if $\varphi : X \to Y$ is an isomorphism, then $d_p\varphi : T_pX \to T_{\varphi(p)}Y$ is an isomorphism for all $p \in X$.

Example 2.12.

(1) Very often, if a surjective morphism $\varphi : X \to Y$ is not an isomorphism, then either φ is not injective or $d_p\varphi$ is not injective for some p. So this is the first thing to check.

(2) Let $C := Z(y^2 - x^3) \subset \mathbb{A}^2$ be the cuspidal cubic. Then the bijective morphism $(t^2, t^3) : \mathbb{A}^1 \to C$ is not an isomorphism, because $d_0(t^2, t^3) : T_0\mathbb{A}^1 = k \to T_0C$ is the zero map.

(3) If $X \subset \mathbb{A}^r$ is a subvariety, then $dim(T_pX) \leq r$. So, if $dim(T_pX) > r$ for some $p \in X$, then X cannot be isomorphic to a subvariety of $\mathbb{A}^r$. For this reason $dim(T_pX)$ is also called the **embedding dimension** of X at p.

2.3. Nonsingular varieties. Now we define singular and nonsingular points of any variety. The definition is in terms of the local ring of $\mathcal{O}_{X,p}$. It has the advantage of being intrinsic, i.e. it does not use the embedding of X into any affine or projective space. We then show that for affine varieties it coincides with the previous definition, which is easier to compute. Then we show that in every variety the nonsingular points form an open dense subset.

Definition 2.13. Let X be a variety and let $p \in X$. Let $\mathcal{O}_{X,p}$ be the local ring at p with maximal ideal $\mathbf{m}_p$. The **tangent space** of X at p is the dual vector space

$$\begin{aligned} T_pX &:= (\mathbf{m}_p/\mathbf{m}_p^2)^\vee = \big\{\text{linear maps } v : (\mathbf{m}_p/\mathbf{m}_p^2) \to k\big\} \\ &= \big\{\text{linear maps } v : \mathbf{m}_p \to k \text{ with } v|_{\mathbf{m}_p^2} = 0\big\}. \end{aligned}$$

$p \in X$ is called a **nonsingular point** or **regular point** of X if the dimension of T_pX as k-vector space is equal to $dim(X)$. Otherwise p is called a **singular point**. Again we denote by X_{reg} the set of regular points of X and by X_{sing} the set of singular points. X is called **nonsingular** or **smooth** if $X = X_{reg}$.

Now we want to see that for affine varieties the two different definitions agree. We temporarily denote t_pX the old definition of a tangent space of an affine variety $X \subset \mathbb{A}^n$.

Definition 2.14. Let $a = (a_1, \dots, a_n) \in t_pX$. We want to associate to a a linear map $\partial_a : \mathbf{m}_p \to k \in T_pM$. We can write any element $h \in \mathbf{m}_p$ as $h := \frac{F}{G}|_X$, where $F, G \in k[x_1, \dots, x_n]$ and $F(p) = 0$, $G(p) = 1$. Then we put

$$\partial_a h := \sum_{i=1}^n a_i \frac{\partial F}{\partial x_i}(p) = d_pF(a).$$

We have to check that this is well-defined. If $\frac{F}{G}|_X = \frac{F'}{G'}|_X$, then $FG' - F'G \in I(X)$. Thus by $F(p) = 0 = F'(p)$ and $G(p) = 1 = G'(p)$, we get that

$$d_p(F)(a) = d_pF(a)G'(p) + F(p)d_pG'(a) = d_p(FG')(a) = d_p(F'G)(a) = d_p(F')(a).$$

Thus δ_a is well-defined.

Finally if $h \in \mathbf{m}_p^2$, then h is a linear combination of products $h = \frac{f}{g}\frac{f'}{g'}$ with $f(p) = f'(p) = 0$. Thus $d_p(ff') = \partial_a(f)f(p) + \partial_a(f')f(p) = 0$. Thus $\partial_a h = 0$. Thus we get a linear map $\partial : t_pM \to T_pM, a \mapsto \partial_a$.

We write t_i for the class of $x_i - x_i(p)$ in $\mathbf{m}_p$. Then $\delta_a(t_i) = a_i$.

Theorem 2.15. (1) *Let $X \subset \mathbb{A}^n$ be a closed subvariety and let $p \in X$. Then $\delta : t_pX \to T_pX$ is an isomorphism.*

(2) *Let $\varphi : X \to Y$ be a morphism, with $\varphi(p) = q$. Using δ to identify t_pX with T_pX and t_qY with T_qY, we get that $d_p\varphi : T_pX \to T_qY$ is the map $(v : \mathbf{m}_p \to k) \mapsto (v \circ \varphi^* : \mathbf{m}_q \to k)$.*

Proof. We only show (1), (2) is left as an exercise.

Injectivity: If $\partial_a = 0$, then $\partial_a f = 0$ for all $f \in \mathbf{m}_p$, in particular $a_i = \partial_a(t_i) = 0$. Thus $a = 0$.

Surjectivity: Now let $\delta \in T_pX$. We put $a_i := \delta(t_i)$, and $a := (a_1, \dots, a_n)$, and claim that $\delta = \partial_a$. By definition $\delta(t_i) = \partial_a(t_i)$. Thus it is enough to show that $\mathbf{m}_p/\mathbf{m}_p^2$ is generated by the t_i as a vector space. Let $f = \frac{g}{h} \in \mathbf{m}_p$. Then $f - \frac{g}{h(p)} = \frac{g(h(p)-h)}{hh(p)} \in \mathbf{m}_p^2$. Thus $\mathbf{m}_p/\mathbf{m}_p^2$ is generated by the classes of elements of $A(X)$. All elements of $A(X)$ are polynomials in the t_i, and a monomial of degree d is in $\mathbf{m}_p^d$. Thus the t_i generate $\mathbf{m}_p/\mathbf{m}_p^2$ as vector space. □

Theorem 2.16. (1) *Let X be a irreducible variety. Then X_{reg} is an open dense subset of X.*

(2) *For all $p \in X$ we have $dim(T_pX) \geq dim(X)$.*

Proof. As X has an open cover by affine varieties and the theorem holds if it holds for every open subset in the cover, we can assume that $X \subset \mathbb{A}^n$ is an irreducible affine variety. We know that $T_p(X) = ker(J(f_1, \dots, f_r)(p))$. Thus $dim(T_pX) = n - rk(J(f_1, \dots, f_r)(p))$. Thus for any d the locus

$$X_d := \big\{p \in X \bigm| dim(T_pX) \geq d\big\}$$

is closed in X as the zero locus of the $(n-d) \times (n-d)$ minors of $J(f_1, \dots, f_r)$. Choose the largest d with $X_d = X$. Then $X^0 := X \setminus X_{d+1}$ is open and dense in X. Thus $dim(T_pX) \geq d$ for all $p \in X$ and $dim(T_pX) = d$ for all $p \in X^0$. X is birational to a hypersurface Y in $\mathbb{A}^{dim(X)+1}$. Let $U \subset X$ be a nonempty open set which is isomorphic to an open set of Y_{reg}. Then $dim(T_pX) = dim(X)$ for all $p \in U$. On the other hand $U \cap X^0 \neq \emptyset$, thus $d = dim(X)$, i.e. $X_{reg} = X^0$. This shows both (1) and (2). □

Now we want to see that smoothness is easy to check. For $F_1, \dots, F_r \in k[x_0, \dots, x_n]$ the Jacobian is

$$J(F_1, \dots, F_r) := \begin{pmatrix} \frac{\partial F_1}{\partial x_0} & \dots & \frac{\partial F_1}{\partial x_n} \\ & \dots & \\ \frac{\partial F_r}{\partial x_0} & \dots & \frac{\partial F_r}{\partial x_n} \end{pmatrix}.$$

Corollary 2.17. (1) *Let $X \subset \mathbb{A}^n$ be an irreducible affine algebraic variety, with $I(X) = \langle f_1, \dots, f_r \rangle$. Then $p \in X$ is nonsingular if and only if $rk(J(f_1, \dots, f_r)(p)) \geq n - dim(X)$.*

(2) *Let $X \subset \mathbb{P}^n$ be an irreducible projective variety, with $I(X) = \langle F_1, \dots, F_r \rangle$, for $F_i \in k[x_0, \dots, x_n]$ homogeneous. Then $p \in X$ is nonsingular if and only if $rk(J(F_1, \dots, F_r)(p)) \geq n - dim(X)$.*

Proof. (1) We know that X is nonsingular at p if and only if $rk(J(f_1, \dots, f_r)(p) = n - dim(X)$. We already know that $dim(T_pX) \geq dim(X)$. Thus it is enough that $rk(J(f_1, \dots, f_r)(p)) \geq n - dim(X)$.

(2) We can assume $p = [1, a_1, \dots, a_n]$. We put $f_i(x_1, \dots, x_n) := F_i(1, x_1, \dots, x_n)$. Then p is a nonsingular point of X, if and only if $a = (a_1, \dots, a_n)$ is a nonsingular point of $Z(f_1, \dots, f_r)$. By definition $\frac{\partial F_i}{\partial x_j}(p) = \frac{\partial f_i}{\partial x_j}(a)$ for $j \geq 1$. As F_i is homogeneous of degree d_i, the Euler formula says that $\sum_{j=0}^n x_j \frac{\partial F_i}{\partial x_j} = d_i F_i$. Thus

$$\frac{\partial F_i}{\partial x_0}(p) = -a_1 \frac{\partial f_i}{\partial x_1}(a) - \dots - a_n \frac{\partial f_i}{\partial x_n}(a).$$

Thus the zeroth column in

$$J(F_1, \dots, F_r)(p) = \begin{pmatrix} \frac{\partial F_1}{\partial x_0}(p) & \frac{\partial f_1}{\partial x_1}(a) & \dots & \frac{\partial f_1}{\partial x_n}(a) \\ & \dots & & \\ \frac{\partial F_r}{\partial x_0}(p) & \frac{\partial f_r}{\partial x_1}(a) & \dots & \frac{\partial f_r}{\partial x_n}(a) \end{pmatrix}$$

is a linear combination of the others. Thus $rk(J(F_1, \dots, F_r)(p)) = rk(J(f_1, \dots, f_r)(a)$. □

Remark 2.18. The fact that X_{reg} is an open dense subset of X can be used to compute the dimension of varieties. The dimension of X is the dimension of the tangent space at a general point, or equivalently the minimum of the dimension of the tangent spaces of X. As tangent spaces are very easy to compute, this is often the fastest way to determine the dimension of a variety.

Remark 2.19. In the section on rational maps we have seen that the blowup of the nodal and the cuspidal cubic in the origin are isomorphic to $\mathbb{A}^1$. In particular they are nonsingular. If X is an irreducible variety and $\pi : Y \to X$ is a birational surjective morphism from a nonsingular irreducible variety, then π (or Y) is called a **resolution of singularities** of X. Thus we have seen that one can resolve the singularities of the nodal and the cuspidal cubic by blowing up a point. Indeed a very difficult and important theorem of Hironaka says that in characteristic 0 every irreducible variety admits a resolution of singularities by a succession of blowups of ideals.

2.4. Nonsingular curves. In this section a curve is a variety of dimension 1. In this subsection we want to study nonsingular points of curves and in particular their local ring $\mathcal{O}_{C,p}$. It turns out that they are discrete valuation rings, i.e. there exists a so-called uniformizing parameter t in the maximal ideal $\mathbf{m}$, so that every element of $\mathcal{O}_{C,p}$ can be written as ut^n for some $n \geq 0$ and u a unit in $\mathcal{O}_{C,p}$. This has a number of consequences. In particular a rational map from a nonsingular curve to a projective variety can always be extended to a morphism and two nonsingular projective birational curves are isomorphic.

Recall that a local ring is a ring A with a unique maximal ideal $\mathbf{m}$, so that all the elements of $A \setminus \mathbf{m}$ are units. Recall that a module over a ring is the analogue of a vector space over a field:

Definition 2.20. Let A be a ring. An abelian group M together with an operation $\cdot : A \times M \to M$ is called an **A-module**, if for all $u, u_1, u_2 \in M$, $a, a_1, a_2 \in A$ we have

(1) $(a_1a_2)u = a_1(a_2u)$ (associativity),
(2) $a(u_1 + u_2) = au_1 + au_2$, $(a_1 + a_2)u = a_1u + a_2u$ (distributivity),
(3) $1u = u$.

Let $S \subset M$. The A module **generated by** S is

$$\langle S\rangle := \{a_1s_1 + \ldots + a_ns_n \mid n > 0,\ a_i \in A,\ s_i \in S\}.$$

An A-module M is called **finitely generated** if there are finitely many elements $u_1, \ldots, u_n \in M$ with $M = \langle u_1, \ldots, u_n\rangle$.

Recall that an ideal I in A is an A-module, as well as A/I. The generators of I as an ideal are the same as that of I as an A module. If M is an A-module and I an ideal in A, we denote

$$IM := \langle\{bu \mid b \in I, u \in M\}\rangle.$$

If M, N are A-modules and $N \subset M$, the quotient M/N is in a natural way an A module via $a[u] = [au]$.

We start with a very useful lemma on local rings.

Lemma 2.21. *(Lemma of Nakajama) Let A be a local ring with maximal ideal $\mathbf{m}$ and let M be a finitely generated A module. If $M = \mathbf{m}M$, then $M = 0$.*

Proof. Assume $M \neq 0$. Let $u_1, \ldots, u_r$ be a minimal set of generators of M. Since $u_r \in M = \mathbf{m}M$, we can write $u_r = \sum_{i=1}^r m_iu_i$ with $m_i \in \mathbf{m}$. Thus $(1-m_r)u_r = \sum_{i=1}^{r-1} m_iu_i$. Note that $1-m_r$ is a unit in A, because otherwise $1-m_r \in \mathbf{m}$ and thus also $1 = 1-m_r+m_r \in \mathbf{m}$, a contradiction. Thus we can write $u_r = \sum_{i=1}^{r-1} m_i(1-m_r)^{-1}u_i$.

Therefore already $u_1, \dots, u_{r-1}$ is a set of generators for M, a contradiction to the minimality of $u_1, \dots, u_r$. □

COROLLARY 2.22. *Let A be a local ring with maximal ideal $\mathbf{m}$. Write $k := A/\mathbf{m}$. Let M be a finitely generated A module. Let $f_1, \dots, f_r \in M$, such that their classes $\overline{f}_1, \dots, \overline{f}_r$ generate $M/\mathbf{m}M$ as a k-vector space. Then $f_1, \dots, f_r$ generate M as A-module.*

PROOF. Let $N := \langle f_1, \dots, f_r \rangle$. We consider the A-module M/N. Note that $N/\mathbf{m}M = M/\mathbf{m}M$ is the k-vector space spanned by $\overline{f}_1, \dots, \overline{f}_r$. Thus $N + \mathbf{m}M = M$. Thus

$$\mathbf{m}(M/N) = (\mathbf{m}M + N)/N = M/N.$$

If M is generated by $g_1, \dots, g_s$, than M/N is generated by the classes of $g_1, \dots, g_s$ in M/N. Thus M/N is a finitely generated A-module and Nakajamas lemma applies. Thus $M/N = 0$, i.e. $M = N = \langle f_1, \dots, f_r \rangle$. □

DEFINITION 2.23. Let A a local ring which is also an integral domain, with maximal ideal $\mathbf{m}$. A is called a **discrete valuation ring** (DVR) if the following holds:

(1) $\mathbf{m}$ is a principal ideal, i.e. we can write $m = \langle t \rangle$ for some element $t \in \mathbf{m}$. t is called a **uniformizing parameter**

(2) If t is a uniformizing parameter, then every $a \in A$ can be written as $a = ut^n$, for $u \in A$ a unit and $n \in \mathbb{Z}_{\geq 0}$.

REMARK 2.24. Let t be a uniformizing parameter. We claim that $\langle t^n \rangle = \mathbf{m}^n$ for all $n \in \mathbb{Z}_{\geq 0}$. Obviously $\langle t^n \rangle \subset \mathbf{m}^n$. The converse is clear for $n = 0, 1$. Assume, we know $\langle t^{n-1} \rangle = \mathbf{m}^{n-1}$. Thus any element a of $\mathbf{m}^{n-1}$ can be written as $a = ct^{n-1}$ and any element b of $\mathbf{m}$ can be written as dt, for $b, d \in \mathcal{O}_{C,p}$. Thus $\mathbf{m}^n = \mathbf{m}(\mathbf{m}^{n-1})$ is generated by elements of the form bdt^n and the result follows.

This shows that the number n in $a = ut^n$, with u a unit is independent of the choice of uniformizing parameter. $a = ut^n$ if and only if $a \in \mathbf{m}^n \setminus \mathbf{m}^{n+1}$.

EXERCISE 2.25. (1) Let A be a ring, I and ideal in A. Let $\pi : A \to A/I$ be the projection. The map $J \mapsto \pi^{-1}(J)$ is an injective map from the ideals of A/I to the ideals of A.

(2) Let A be a Noetherian ring, $I \subset A$ an ideal. Show that A/I is Noetherian. Hint: If $J_1 \subset J_2 \subset \dots$ is a chain of ideals in A/I, then $\pi^{-1}(J_1) \subset \pi^{-1}(J_2) \subset \dots$ is a chain of ideals in A, which therefore becomes stationary, and thus also the original chain becomes stationary.

In particular we obtain: If $X \subset \mathbb{A}^n$ is an affine variety, then $A[X]$ is Noetherian.

(3) Now let X be a variety, $p \in X$. We want to show that $\mathcal{O}_{X,p}$ is Noetherian. As $\mathcal{O}_{X,p}$ depends only on an open neighbourhood of X, we can assume that X is affine. Show: The map $I \mapsto I \cap A[X]$ is an injective map from the ideals of $\mathcal{O}_{X,p}$ to the ideals of $A[X]$.

(4) In the same way as for A/I deduce that $\mathcal{O}_{X,p}$ is Noetherian.

Theorem 2.26. *Let p be a nonsingular point on a curve C. Then the local ring $\mathcal{O}_{C,p}$ is a discrete valuation ring.*

Proof. As $\mathcal{O}_{C,p}$ is a subring of the field $K(C)$, it is an integral domain. It is an exercise to show that $\mathcal{O}_{C,p}$ is Noetherian.

Let $\mathbf{m}$ be the maximal ideal of $\mathcal{O}_{C,p}$. We know that the tangent space of $(\mathbf{m}/\mathbf{m}^2)^\vee$ of C at p has dimension one. Thus $\mathbf{m}/\mathbf{m}^2$ has dimension 1 as a vector space over $k = A/\mathbf{m}$. Let $t \in \mathbf{m}$ be an element so that its class in $\mathbf{m}/\mathbf{m}^2$ is a basis. By the corollary to Nakajamas Lemma we get that $\mathbf{m} = \langle t \rangle$, i.e. t is a uniformizing parameter.

Now we want to see that $M := \bigcap_{n>0} \mathbf{m}^n = 0$. Obviously M is an ideal in $\mathcal{O}_{C,p}$, which is Noetherian, thus M is finitely generated. Note that by definition $\mathbf{m}M = M$. Thus by Nakajamas Lemma $M = 0$. This means in other words that every element a of $\mathcal{O}_{C,p}$ lies in $\langle t^n \rangle \setminus \langle t^{n+1} \rangle$ for some n, i.e. we can write $a = ut^n$ for u a unit. □

As $\mathcal{O}_{C,p}$ is a discrete valuation ring, we can associate to each $f \in \mathcal{O}_{C,p}$ a number, which measures to which order f vanishes at p.

Definition 2.27. Let p be a nonsingular point on a curve C. We define $v_p : \mathcal{O}_{C,p} \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ by $v_p(f) = n$ if and only if $f = ut^n$ for $u(p) \neq 0$ and t a uniformizing parameter.

Remark 2.28. v_p fulfills the following properties:

(1) $v_p(fg) = v_p(f) + v_p(g)$,
(2) $v_p(f+g) \geq min(v_p(f), v_p(g))$ with equality if $v_p(f) \neq v_p(g)$.
(3) f is a unit if and only if $v_p(f) = 0$.

Proof. Let $f = at^n$, $g = bt^m$ with a, b units. (1) Then $fg = abt^{n+m}$. (2) Assume $n \leq m$. Then $f+g = a(1+bt^{m-n})t^n$, thus $v_p(f+g) \geq n$. If $n > m$, then $(1+bt^{m-n})$ is a unit, because otherwise $1 = 1 + bt^{m-n} - bt^{m-n}$ would be in $\mathbf{m}$. Thus $v_p(f+g) = n$. (3) is clear. □

We can extend the valuation v_p to $K(C)$.

Definition 2.29. Note that $K(C)$ is also the quotient field of $\mathcal{O}_{C,p}$. We extend $v_p : \mathcal{O}_{C,p} \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ to

$$v_p : K(C) \setminus \{0\} \to \mathbb{Z};\ v_p(\frac{f}{g}) := v_p(f) - v_p(g).$$

This is well defined: if $\frac{f}{g} = \frac{f'}{g'}$, then $fg' = f'g$, thus $v_p(f) + v_p(g') = v_p(fg') = v_p(f'g) = v_p(f') + v_p(g)$, i.e. $v_p(f) - v_p(g) = v_p(f') - v_p(g')$.

Let C be a curve, p a nonsingular point of C and let $h \in K(C)$. Let $n := \nu_p(h)$. If $n > 0$ we say h has a **zero of order** n **at** p, if $n < 0$ we say h has a **pole of order** $-n$ **at** p.

Corollary 2.30. *Let p be a nonsingular point on a curve C.*

(1) *Let $f \in K(C) \setminus \{0\}$. Then $v_p(f) = n$ ($n \in \mathbb{Z}$) if and only if there exists a unit in $a \in \mathcal{O}_{C,p}$ such that $f = ut^n$.*

(2) $\mathcal{O}_{C,p} = \{f \in K(C) \setminus \{0\} \bigm| v_p(f) \geq 0\} \cup \{0\}$.

Proof. (1) We have $v_p(f) = n$ if and only if $f = \frac{g}{h}$ with $g, h \in \mathcal{O}_{C,p}$ and $v_p(h) - v_p(g) = n$. This is equivalent to $g = at^{m+n}$, $h = bt^m$ with a, b units and $m, m+n \geq 0$. This is equivalent to $f = ct^n$ with $c = a/b$ a unit. (2) By definition for $f \in \mathcal{O}_{C,p} \setminus \{0\}$, $v_p(f) \in \mathbb{Z}_{\geq 0}$. Now let $f \in K(C)$ with $v_p(f) \geq 0$. Then by (1) we can write $f = ct^{v_p(f)}$ for t a uniformizing parameter and c a unit in $\mathcal{O}_{C,p}$. Thus $f \in \mathcal{O}_{C,p}$. □

We want to use these results to study morphisms from nonsingular curves. We will show that any rational map from a nonsingular curve $C \dashrightarrow Y$ to a projective can be extended to a morphism $C \to Y$. This is another manifestation of the fact that projective varieties are complete. It implies that if two nonsingular projective curves are birational, then they are isomorphic.

Theorem 2.31. *Let C be a nonsingular curve and $\varphi_0 : C \dashrightarrow Y$ be a rational map to a projective variety. Then φ_0 can be extended to a morphism $\varphi : C \to Y$.*

Proof. φ_0 is a morphism on an open subset of C, thus we have $\varphi_0 : C \setminus \{p_1, \dots, p_r\} \to Y$. Assume we can extend φ_0 to a morphism $\varphi : C \to \mathbb{P}^n$. Then $\varphi^{-1}(Y)$ contains the open dense subset $C \setminus \{p_1, \dots, p_r\}$. As φ is continuous, we get $\varphi^{-1}(Y) = C$, i.e. $\varphi(C) \subset Y$. Thus we can assume that $Y = \mathbb{P}^n$.

To extend φ_0 to C it is enough to extend it to a neighbourhood to each of the p_i. Thus, replacing C by such a neighbourhood, we can assume that $\varphi_0 : C \setminus \{p\} \to \mathbb{P}^n$

is a morphism. Possibly replacing C by a smaller open neighbourhood, we can write $\varphi_0 = [f_0, \dots, f_n]$ with $f_i \in \mathcal{O}_C(C \setminus \{p\})$ without any common zeros. Let t be a uniformizing parameter at p. As $f_i \in K(C)$, we can write $f_i = a_i t^{m_i}$ with a_i a unit in $\mathcal{O}_{C,p}$ and $m_i \in \mathbb{Z}$. By replacing C by a smaller neighbourhood, we can assume that $t \in \mathcal{O}_C(C)$, $a_i \in \mathcal{O}_C(C)$ and a_i has no zero on C. As $t \neq 0$, t has only finitely many zeros on C, thus replacing C by a smaller neighbourhood, t is nowhere vanishing on $C \setminus \{p\}$. Let m_j be the minimum of $m_0, \dots, m_n$. For $i = 0, \dots, n$ we put $g_i := a_i t^{m_i - m_j}$ and define

$$\varphi = [g_0, \dots, g_n] : C \to \mathbb{P}^n.$$

As $m_i - m_j \geq 0$, we get $g_i \in \mathcal{O}_C(C)$ and as $g_j = a_j$ has no zero on C, the g_i have no common zero on C, and thus φ is a morphism. On the other hand, as t does not vanish anywhere on $C \setminus \{p\}$, we have

$$\varphi = [g_0, \dots, g_n] = [t^{m_j} f_0, \dots, t^{m_j} f_n] = [f_0, \dots, f_n] = \varphi_0$$

on $C \setminus \{p\}$. □

Corollary 2.32. *Let C, D be nonsingular projective curves. If C and D are birational, then they are isomorphic.*

Proof. As C and D are birational there exists an isomorphism $\varphi : U \to V$ between nonempty open subsets $U \subset C$ and $V \subset D$. By the theorem we can extend both φ and φ^{-1} to morphisms $\varphi : C \to D$, $\psi : D \to C$. Then on U we have $\psi \circ \varphi = id$ and on V we have $\varphi \circ \psi = id$. As two morphisms agree if they agree on an open subset we obtain $\psi \circ \varphi = id_C$ and $\varphi \circ \psi = id_D$, i.e $\varphi : C \to D$ is an isomorphism. □

In particular any nonsingular projective rational curve is isomorphic to $\mathbb{P}^1$.

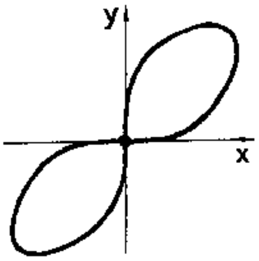
Example 2.33. Note that all the assumptions are necessary.

(1) Obviously the embedding $\mathbb{A}^1 \to \mathbb{P}^1$ is a birational morphism of nonsingular curves, but not an isomorphism, thus we need that the curves are projective.
(2) The curve $C := Z(x^3 - y^2 z) \subset \mathbb{P}^2$ is a cuspidal cubic. The map $\varphi : \mathbb{P}_1 \to C, [u, t] \mapsto [ut^2, t^3, u^3]$ is a birational morphism of projective curves. The rational inverse is given by $[x, y, z] \mapsto [x, y]$. It is not an isomorphism because $[0, 0, 1]$ is a singular point of C. In fact in the affine chart $z = 1$, we see that C is just the usual cuspidal cubic $Z(x^3 - y^2) \subset \mathbb{A}^2$.
(3) We know that $\mathbb{P}^n$ and $(\mathbb{P}^1)^n$ are birational and both nonsingular but not isomorphic, so this is only a result about curves.

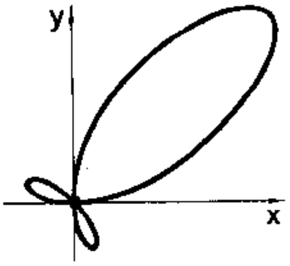
Remark 2.34. It can be shown that every curve is birational to a nonsingular projective curve. One can show that every curve has a resolution of singularities and every nonsingular curve is quasiprojective and in fact an open subset of a nonsingular projective curve. Thus classifying curves up to birational equivalence is equivalent to classifying nonsingular projective curves up to isomorphism.

Exercises.

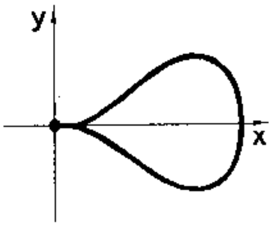
(1) Find the singular points of the following curves in $\mathbb{A}^2$ (assume $char(k) \neq 2$)
   (a) $Z(x^2 - x^4 - y^4)$,
   (b) $Z(xy - x^6 - y^6)$,
   (c) $Z(x^3 - y^2 - x^4 - y^4)$,
   (d) $Z(x^2y + xy^2 - x^4 - y^4)$.
   which is which in the figure below?



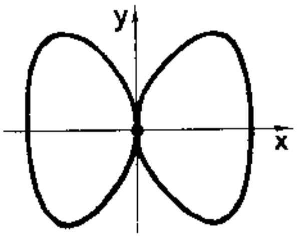
Node



Triple point



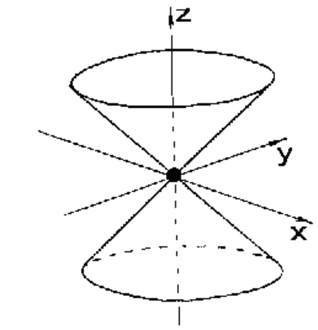
Cusp



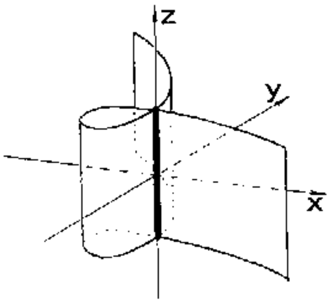
Tacnode

(2) Determine the singular points of the following curves in $\mathbb{A}^2$.
   (a) $Z(y^2 - (x^3 - x))$,
   (b) $Z(y^2 - (x^3 - 6x^2 + 9x))$,

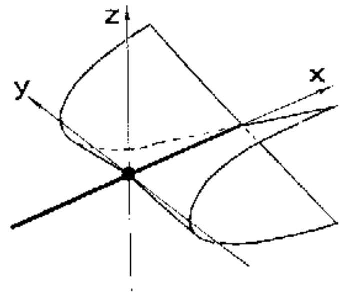
(3) Find the singular points of the following surfaces in $\mathbb{A}^3$
   (a) $Z(xy^2 - z^2)$,
   (b) $Z(x^2 + y^2 - z^2)$,
   (c) $Z(xy + x^3 + y^3)$.
   which is which in the figure below?



Conical double point



Double line



Pinch point

(4) Let $F \in k[x, y, z] \setminus \{0\}$ and let $C := Z(F) \subset \mathbb{P}^2$. Assume $I(C) = \langle F \rangle$ and that C is nonsingular.

Show that C (and thus also F) is irreducible.

(5) Let $C := Z(y - x^2) \subset \mathbb{A}^2$ and let $\varphi = (y) : \mathbb{A}^2 \to \mathbb{A}^1$. Show that $d_{(0,0)}\varphi$ is the zero map.

(6) Show that the cubic curve $Z(Y^2Z - (X^3 + aXZ^2 + bZ^3)) \subset \mathbb{P}^2$ is smooth if $4a^4 + 27b^2 \neq 0$.

(7) Show that a hypersurface of degree 2 in $\mathbb{A}^n$ with a singular point is a cone.

(8) Let $X \subset \mathbb{P}^n$ be a hypersurface of degree 3 with 2 singular points p, q. Show that X contains the line through p and q.

(9) Resolve the singularities of the following curves by subsequent blow-ups of the singular points (i.e. starting with C blowup all singular points and replace C with its strict transforms. Continue until the resulting curve is smooth).
(a) $C = Z(y^3 - x^4) \subset \mathbb{A}^2$,
(b) $C = Z(x^2 - x^4 - y^4) \subset \mathbb{A}^2$,
(c) $C = Z(y^3 - x^5) \subset \mathbb{A}^2$,

(10) Let $C_n := Z(y^2 - x^{2n+1}) \subset \mathbb{A}^2$. Show that O is the only singular point of C_n. Show that the strict transform of C_n under blowup at O is isomorphic to C_{n-1}. Deduce that C_{n-1} can be resolved in n blow-ups.

(11) Let $X = Z(F) \subset \mathbb{P}^n$ be a hypersurface with $F \in k[x_0, \dots, x_n]$ homogeneous and $I(X) = \langle F \rangle$.

Show: A point $p \in \mathbb{P}^n$ is a singular point of X if and only if $\frac{\partial F}{\partial x_i} = 0$ for $i = 0, \dots, n$ (Note: one also has to show that $p \in X$.)

(12) Let $X = Z(F), Y = Z(G) \subset \mathbb{P}^n$ be hypersurfaces, with $F, G \in k[x_0, \dots, x_n]$ homogeneous.

Show: All points of $X \cap Y$ are singular points of $Z(FG)$.

(13) Let $n \geq 2$ and let $X \subset \mathbb{P}^n$ be an reducible hypersurface.

Show: X is singular and the dimension of its singular locus is at least $n - 2$.

(14) Let $0 \leq m \leq n$ and let $Q_m := Z(x_0^2 + \dots + x_m^2) \subset \mathbb{P}^n$.

Show that Q_m is reducible if and only if $m = 1$.

(15) Let $C \subset \mathbb{A}^2$ be a plane curve of degree 3 with 3 singular points. Show: C is the union of 3 lines.

(16) For what values of a has the curve $C_a := Z(x_0^3 + x_1^3 + x_2^3 + a(x_0 + x_1 + x_2)^3) \subset \mathbb{P}^2$ a singular point. Is C_a irreducible?

(17) Show that the hypersurface $Z(x_0^d + x_1^d + \dots + x_n^d) \subset \mathbb{P}^n$ is nonsingular (if the characteristic of k does not divide d).

(18) Let $z_{00}, z_{01}, z_{10}, z_{11}$ be the homogeneous coordinates on $\mathbb{P}^3$. Let $\Sigma := Z(z_{00}z_{11} - z_{01}z_{10})$ be the image of $\mathbb{P}^1 \times \mathbb{P}^1$ under the Segre embedding. For which hyperplanes H in $\mathbb{P}^3$ is $\Sigma \cap H$ singular?

(19) Let $F_1, \dots, F_r \in k[x_0, \dots, x_n]$ be homogeneous. Write $X := Z(F_1, \dots, F_r) \subset \mathbb{P}^n$. Assume $rk(J(F_1, \dots, F_r)(p)) = n - r$ for all X. Then X is a complete intersection.

(20) Let $X = Z(F) \subset \mathbb{P}^n$ be a hypersurface. Show that a point $p \in \mathbb{P}^n$ is a singular point of $Z(F)$ if and only if $\frac{\partial F}{\partial x_i}(p) = 0$ for $i = 0, \dots, n$.

(21) Let C be a nonsingular rational curve which is not isomorphic to $\mathbb{P}^1$.
   (a) Show that C is isomorphic to an open subset of $\mathbb{A}^1$.
   (b) Show that C is affine.

(22) Give an example of a rational map $\varphi : X \dashrightarrow \mathbb{P}^n$, where X is a nonsingular surface, such that φ cannot be extended to morphism.

(23) Let C be a nonsingular projective curve. Show that every nonconstant rational function f on C defines a surjective morphism $\varphi : C \to \mathbb{P}^1$ and that for all $p \in \mathbb{P}^1$, $\varphi^{-1}(p)$ is a finite set.

CHAPTER 4

Curves

In this chapter we want to study nonsingular projective curves. The study of algebraic curves is an important and fundamental part of algebraic geometry. The main tool for understanding a curve C is the study of the divisors on C, i.e. formal linear combinations of finitely many points on C. To a divisor D on C we can associate the vector space $L(D)$ of rational functions with poles and zeros determined by D, and these give a morphism $\varphi_{|D|} : C \to \mathbb{P}^n$. This gives us a new way to construct and understand morphisms from curves. So in this chapter we will study curves via their divisors and the associated morphisms.

The most important tool in the study of divisors on curves is the Riemann-Roch Theorem, which allows us to compute the dimensions of the spaces $L(D)$. The most natural proof of the Riemann-Roch theorem is via cohomology of sheaves, in fact the theorem is an immediate consequence of standard results about cohomology. There is also an elementary proof available e.g. in the book [**Fulton**], but it is very long, and the approach using sheaves is much more natural and will give powerful results for varieties of any dimension.

Unfortunately the proper development of cohomology of sheaves would take a course in its own right, thus we cannot attempt to do this here. Instead I will just assume the Riemann-Roch Theorem, and we will see that it has very powerful applications to the geometry of curves. This should serve as a motivation for studying cohomology of sheaves in the future.

In this chapter we will also assume some further results from algebra without proof, so that we can concentrate on the geometrical applications.

In this whole chapter we just say curve for **nonsingular irreducible projective** curve. Most of the results of this chapter would be false otherwise.

1. Divisors

In this whole section C will be a curve. We will start our study of divisors on curves. A divisor on a curve C is a finite formal linear combination $D := n_1P_1 + \ldots + n_rP_r$ of points $P_i \in C$ with coefficients $n_i \in \mathbb{Z}$.

1.1. Divisors.

Definition 1.1. Let C be a curve. A **divisor** on C is a formal sum

$$\sum_{p\in C} a_P \cdot P, \quad a_P \in \mathbb{Z}, \text{ only finitely many } a_P \neq 0.$$

Let $D := \sum_{P\in C} a_P \cdot P$, $E := \sum_{P\in C} b_P \cdot P$ be divisors on C. We write

$$D + E := \sum_{P\in C} (a_P + b_P) \cdot P,$$
$$D - E := \sum_{p\in C} (a_P - b_P) \cdot P.$$

It is evident that the divisors on C form an abelian group with these operations, the neutral element is $0 := \sum_{P\in C} 0 \cdot P$.

For a point $Q \in C$ and $a \in \mathbb{Z}$ we also denote by $a \cdot Q$ the divisor $\sum_{p\in C} a_P \cdot P$ with $a_Q = a$ and all other $a_P = 0$. Thus e.g. $P_1 + \ldots + P_r$ is the divisor $\sum_{p\in C} a_P \cdot P$ with $a_P = \#\{i \mid P_i = P\}$. For a divisor $D = \sum_P a_P \cdot P$ and a point $P \in C$ we write $\nu_P(D) := a_P$ and call it the **multiplicity** of D at P.

D is called **effective** if $\nu_P(D) \geq 0$ for all P. We write $D \geq C$ if $D - C$ is effective. The **degree** of D is

$$deg(D) := \sum_{P\in C} \nu_P(D) \in \mathbb{Z}.$$

The group of divisors on C is denoted $Div(C)$. We denote by $Div^d(C)$ the set of divisors on C of degree d. The **support** of D is $supp(D) := \{P \in C \mid \nu_P(D) \neq 0\}$.

Now we introduce principal divisors which are the divisors associated to rational functions.

Definition 1.2. Let $h \in K(C) \setminus 0$ be a rational function. The **divisor of** h is

$$(h) := \sum_{P\in C} \nu_P(h) \cdot P.$$

Divisors of the form (h) for $h \in K(X) \setminus 0$ are called **principal divisors**. Note that these are indeed divisors, i.e. only finitely many of the $\nu_P(h)$ are nonzero: We can write $h = \frac{f}{g}$ with $f, g \in S(C)^{(d)} \setminus 0$ for some $d \geq 0$. If $\nu_P(h) > 0$, then $f(p) = 0$, and if $\nu_P(h) < 0$, then $g(p) = 0$, but f and g have only finitely many zeros on C.

Remark 1.3. Let $f, g \in K(C) \setminus \{0\}$. By Remark III.2.26 We have for all $P \in C$ that $\nu_P(fg) = \nu_P(f) + \nu_p(g)$. Thus we get $(fg) = (f) + (g)$, i.e. the map

$$(K(C) \setminus 0, \cdot) \to Div(C), f \mapsto (f)$$

is a group homomorphism. In particular the principal divisors are a subgroup of $Div(C)$.

Definition 1.4. Let C be a curves and let $\varphi : C \to \mathbb{P}^n$. We want to define the divisor $(\varphi^*(H))$ associated to a hyperplane $H = Z(a_0x_0 + \dots a_nx_n) \subset \mathbb{P}^n$ with $C \not\subset H$. Let $P \in C$ be a point. In a neighbourhood W of P write $\varphi := [g_0, \dots, g_n]$ with $g_i \in \mathcal{O}_C(W)$ with no common zeros. Then we put $(\varphi^*(H))_P := \nu_P(\sum_{i=0}^n a_ig_i)$. This is independent of the choice of the g_i because for any other choice g_i' would be of the form $g_i' = ug_i$ with $u \in \mathcal{O}_{C,P}$, thus $\sum_{i=0}^n a_ig_i' = u\sum_{i=0}^n a_ig_i$. We define $(\varphi^*(H)) := \sum_{P\in C}(\varphi^*(H))_P \cdot P$. By definition this is an effective divisor on C with support $\varphi^{-1}(H)$.

If in particular C is a curve in $\mathbb{P}^n$ and we denote by i the inclusion, we define the divisor (H) on C by $(H) := (i^*(H))$. In this case we can take the open set of the form $W = U_i$ for some i and $g_j := \frac{x_j}{x_i}$. By definition (H) is an effective divisor on C with support $C \cap Z(H)$. We call (H) the divisor of H. Thus (H) is a sum of the intersection points $H \cap C$ with positive multiplicities.

1.2. The Picard group. Two divisors will be called linearly equivalent if their difference is a principal divisor. This gives us a natural equivalence relation on divisors. The group of equivalence classes will be called the Picard group.

Definition 1.5. Let C be a nonsingular irreducible curve. Two divisors D, E on C are called **linearly equivalent**, denoted $D \sim E$, if $D - E$ is a principal divisor. We denote by $[D]$ the equivalence class of the divisor D. The **Picard group** of C is the group $Pic(C)$ of linear equivalence classes of divisors on C. The group operation is $[D] + [E] = [D + E]$. Thus **Picard group** $Pic(C)$ of C is the quotient of $Div(C)$ by the subgroup of principal divisors.

Now we want to see that divisors behave nicely under morphisms of curves: If D is a divisor on a curve C and $\varphi : X \to C$ is a dominant morphism from another curve, one can define the pullback $\varphi^*(D) \in Div(X)$.

We will use (without proof) a result from algebra, which implies that the degree of divisors behaves nicely under pullback. This will in particular imply that all principal divisors have degree 0. First we define the degree of a morphism of curves.

Definition 1.6. Let $\varphi : X \to C$ be a dominant morphism of curves. Then $\varphi^* : K(C) \to K(X)$ is an injective field homomorphism, thus we can view $K(X)$ as a finite field extension of $K(C)$. We define the **degree** of φ to be the degree of the field extension $[K(X) : K(C)]$.

Definition 1.7. Let $\varphi : X \to C$ be a dominant morphism of curves. We define a homomorphism $\varphi^* : Div(C) \to Div(X)$ as follows. Let $Q \in C$. Let $\varphi^{-1}(Q) = \{P_1, \dots, P_r\}$. Let $t \in \mathcal{O}_{C,Q}$ be a uniformizing parameter at Q. Thus $\varphi^*(t) \in O_{X,P_i}$ for all i. We define

$$\varphi^*(Q) := \sum_{i=1}^{r} \nu_{P_i}(\varphi^*(t)) \cdot P_i.$$

By definition this is an effective divisor on X. If t' is another uniformizing parameter at Q, then $t' = tu$ with $u(Q) \neq 0$. Thus $\varphi^*(t') = \varphi^*(t)\varphi^*(u)$ with $\varphi^*(u)(P_i) \neq 0$ for all i, Thus $\nu_{P_i}(\varphi^*(t')) = \nu_{P_i}(\varphi^*(t))$.

We extend the definition by linearity to all divisors on C, i.e.

$$\varphi^*\Big(\sum_i n_i \cdot Q_i\Big) := \sum_i n_i \varphi^*(Q_i).$$

It is clear that this gives a group homomorphism $\varphi^* : Div(C) \to Div(X)$. We call $\varphi^*(D)$ the **pullback** of D by φ.

Exercise 1.8. Let $\varphi : X \to C$ be a dominant morphism of curves.

(1) Let $f \in K(C) \setminus 0$. Then $\varphi^*((f)) = (\varphi^*(f))$.

(2) Assume $C \in \mathbb{P}^n$ and let $H \subset \mathbb{P}^n$ be a hyperplane not containing C. Then $(\varphi^*(H)) = \varphi^*((H))$.

Remark 1.9. Let $\varphi : X \to C$ be a dominant morphism of curves. By the above exercise we see that if $D \sim E$ in $Div(C)$, then $\varphi^*(D) \sim \varphi^*(E)$. Thus $\varphi^*([D]) := [\varphi^*(D)]$, defines a group homomorphism $\varphi^* : Pic(C) \to Pic(X)$.

The following is a result in algebra. It is not very difficult (see e.g. [**Hartshorne**] Prop.II.6.9) but we do not have the time to prove it.

Theorem 1.10. *Let $\varphi : X \to C$ be a dominant morphism of curves. For any divisor D on C we have $deg(\varphi^*(D)) = deg(\varphi) \cdot deg(D)$.*

Theorem 1.11. *Principal divisors on C have degree* 0.

Proof. Let $f \in K(C) \setminus 0$. If $f \in k$, then $(f) = 0$, so there is nothing to prove. If $f \notin k$, then f defines a morphism $\varphi : C \to \mathbb{P}^1$: on the open set where f has no poles it is given by $p \mapsto [1, f(p)]$ and on the open set where f has no zeros by $p \mapsto [\frac{1}{f(p)}, 1]$. Thus $(f) = \varphi^*(0 - \infty)$. As $0 - \infty$ has degree 0, we see that also $deg((f)) = 0$. □

In particular the principal divisors form a subgroup of $Div^0(C)$.

Definition 1.12. Let $Pic^0(C) \subset Pic(C)$ be the group of equivalence classes of divisors on C of degree 0.

Remark 1.13. By the definition we see that for dominant morphisms $\varphi : Y \to X$, $\psi : X \to C$ of curves we have $\varphi^* \circ \psi^* = (\psi \circ \varphi)^* : Pic^0(C) \to Pic^0(Y)$ and $id_C^* = id$. Thus if two curves C and X are isomorphic, then $Pic^0(C) \simeq Pic^0(X)$.

$Pic^0(C)$ is an important invariant of the curve C. For the moment we only want to see that it distinguishes rational curves the curves that are not rational.

Proposition 1.14. *A curve C is rational if and only if there are two distinct points $P, Q \in C$ with $P \sim Q$.*

Proof. Assume C is rational, then it is isomorphic to $\mathbb{P}^1$, and we can assume $C = \mathbb{P}^1$. On $\mathbb{P}^1$ let $P = [a, b]$, $Q = [c, d]$. Let $f = \frac{ax_0 - bx_1}{cx_0 - dx_1}$. Then $(f) = P - Q$, i.e. $P \sim Q$.

Conversely let C be a curve and $P \neq Q \in C$ with $P \sim Q$. Then there is a rational function $f \in K(C)$, with $(f) = P - Q$. Thus we have a morphism $f : C \to \mathbb{P}^1$ with $f^*(0) = P$. By Theorem 1.10 this implies that the degree of the morphism f is 1, i.e. $[K(C) : K(\mathbb{P}^1)] = 1$. Thus $f^* : K(\mathbb{P}^1) \to K(C)$ is an isomorphism and thus f is an isomorphism. □

Corollary 1.15. *C is rational if and only if $Pic^0(C) = \{0\}$.*

Definition 1.16. Let $C \subset \mathbb{P}^n$ be a curve. For any hyperplane $H \subset \mathbb{P}^n$, with $C \not\subset H$, we define the **degree** of C as $deg(C) := deg((H))$. Note that this is independent of the choice of H: Write $H = Z(F)$ for $F \in k[X_0, \ldots, X_n]^{(1)} \setminus I(C)$ for another choice $H' = Z(F')$ we put $(f) := \frac{F'}{F}|_C \in K(C) \setminus 0$. Then $(H') - (H) = (f)$ has degree 0. In fact this argument shows that for any two hyperplanes $H, H' \subset \mathbb{P}^n$ not containing C, the divisors (H) and (H') are linearly equivalent.

Remark 1.17. Let $C = Z(F)$ be a plane curve with $F \in k[x_0, x_1, x_2]$ irreducible of degree d. Then the degree of C is d. This can be seen as follows: We can find a $H \in k[x_0, x_1, x_2]$ which is not tangent to C (i.e. $T_P C \neq T_P H$ as subspaces of $T_P \mathbb{P}^2$). This is an Exercise. Then $F|_{Z(H)}$ is a polynomial of degree d on $\mathbb{P}^1$ with d simple zeros $P_1, \ldots, P_d$ and (by another exercise) $(H) = P_1 + \ldots + P_d$.

1.3. The spaces $L(D)$. To a divisor $D = \sum_i a_i \cdot P_i - \sum_j b_j \cdot Q_j$ with $a_i, b_j > 0$, we can associate the space $L(D)$ of rational functions $f \in K(C)$, which have poles of at most order a_i at the P_i, zeros of order at least b_j at all Q_j, and are regular everywhere else. These spaces $L(D)$ will turn out to be very important.

Definition 1.18. Let D be a divisor on C. Let

$$L(D) := \{f \in K(C) \mid f = 0, \text{ or } (f) + D \geq 0\}.$$

Note that $L(D)$ is a subvectorspace of $K(C)$: For a in $k \setminus 0$ we have $(af) = (f)$. If $f, g \in L(D)$, then $(f) \geq -D$, $(g) \geq -D$, and by Rem. III.2.26 $\nu_P(f+g) \geq min(\nu_P(f), \nu_P(g))$ for all $P \in C$. Therefore $(f+g) \geq -D$.

We denote by $l(D)$ the dimension of $L(D)$ as a k-vector space.

Lemma 1.19. (1) *If $deg(D) < 0$, then $L(D) = \{0\}$.*
(2) *If $deg(D) = 0$ and $L(D) \neq 0$, then $D \sim 0$.*

Proof. (1) Assume $deg(D) < 0$. Let $f \in K(C)^*$. Then $deg((f)) = 0$, thus $deg((f)+D) = deg(D) < 0$. But by definition, if $(f)+D \geq 0$, then $deg((f)+D) \geq 0$.

(2) Assume $deg(D) = 0$, then there is an $f \in K(C)^*$ with $D + (f) \geq 0$. As $deg(D + (f)) = 0$, this implies $D + (f) = 0$, i.e. $D \sim 0$. □

Lemma 1.20. *If $D \sim E$, then $L(D) \simeq L(E)$.*

Proof. Let $D \sim E$, i.e. there is $f \in K(C)^*$ with $E - D = (f)$. If $h \in L(D)$, then $(hf) = (h) + (f) \geq D + (f) = E$, thus $hf \in L(E)$. Thus $L(D) \to L(E); h \mapsto fh$ is an isomorphism with inverse $m \mapsto m/f$. □

Example 1.21. We want to compute $l(D)$ for all divisors D on $\mathbb{P}^1$. We know that on $\mathbb{P}^1$ for any point P we have $P \sim [0,1] = \infty$. Let D be a divisor on $\mathbb{P}^1$ of degree d. By induction we see immediately that $D \sim d \cdot \infty$. Thus $l(D) = l(d \cdot \infty)$. We put $x = x_1/x_0$, we know that $K(\mathbb{P}^1) = k(x)$. Let $h = \frac{f(x)}{g(x)} \in L(d \cdot \infty)$, we can assume that f and g have no common factors. Then g must have degree 0 (otherwise h would have a pole somewhere in $\mathbb{A}^1$). Thus $h \in k[x]$. Let $n := deg(h)$. The uniformizing parameter of $\mathbb{P}^1$ at ∞ is $z := \frac{1}{x}$. We can write $h = \sum_{i=0}^n \frac{a_i}{z^i}$ with $a_i \in k$ and $a_n \neq 0$. Thus $\nu_\infty(h) = (-n)$. Thus we see that $L(d \cdot \infty) = \{h \in k[x] \mid deg(h) \leq d\}$, and thus $l(D) = max(0, deg(D) + 1)$.

The aim of the Riemann-Roch Theorem will be to generalize this result to all curves. The formula will be a bit more complicated, there are additional terms related to differentials.

Exercises.

(1) Show by example that the degree of a nonsingular projective curve is not an invariant under isomorphism.

(2) Let $C = Z(F) \subset \mathbb{P}^1 \times \mathbb{P}^1$ be the zero set of a bihomogeneous polynomial of bidegree (a, b) with $I(C) = \langle F \rangle$. Via the Segre embedding $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ consider C as a curve in $\mathbb{P}^3$. Compute the degree of C.

(3) Let $C \subset \mathbb{P}^n$ be a rational normal curve, i.e. C is the image of the Veronese embedding $[x_0^n, x_0^{n-1}x_1, \dots, x_1^n] : \mathbb{P}^1 \to \mathbb{P}^n$. Show that $deg(C) = n$.

(4) More generally let $C \subset \mathbb{P}^n$ be a curve and let $v_d : \mathbb{P}^n \to \mathbb{P}^{\binom{n+d}{d}-1}$ be the Veronese embedding. Show that $deg(v_d(C)) = d \cdot deg(C)$.

(5) Let $C \subset \mathbb{P}^n$ be a curve of degree d. Show that there is a linear subspace of $\mathbb{P}^n$ of dimension d which contains C. Hint: Consider a linear subspace containing $d+1$ points of C.

(6) Let $\varphi : C \to \mathbb{P}^n$ be a morphism, and let $H \subset \mathbb{P}^n$ be a hyperplane with $C \not\subset H$. Show that $(\varphi^*(H))_P \geq 2$ if and only if $\varphi(P) \in H$ and $\varphi_*(T_PC) \subset T_{\varphi(P)}H$.

(7) Let $C = Z(F)$ be a smooth plane curve, with F irreducible. We say that line $L \subset \mathbb{P}^2$ is tangent to C at P, if $P \in C \cap L$ and and $T_PC = T_PL$ (as subspaces of $T_P\mathbb{P}^2$.

(a) Define the $\varphi : C \to \mathbb{P}^2$ as follows. At any point $P \in C$, show that there is a unique line $L = Z(a_0x_0 + a_1x_1 + a_2x_2)$, which is tangent to C at P. Put $\varphi(P) := [a_0, a_1, a_2] \in \mathbb{P}^2$.

(b) Show that φ is a morphism.

(c) Deduce that $dim(\varphi(C)) \leq 1$.

(d) We say that a line L is tangent to C, if there is a point $P \in C \cap L$ with $T_PC = T_PL$. Show that there are lines $L \subset \mathbb{P}^2$ which are not tangent to C.

(8) Let $C := Z(Y^2Z - X(X-Z)(X-\lambda Z)) \subset \mathbb{P}^2$, for $\lambda \in k \setminus \{0,1\}$. Let $x := \frac{X}{Z}$, $y := \frac{Y}{Z}$. Compute (x) and (y).

(9) Let $C \subset \mathbb{P}^n$ be a curve. For $F \in k[x_0, \dots, x_n]$ a homogeneous polynomial with $C \not\subset Z(F)$, define a divisor (F) on C as follows. For each $P \in C$ choose an i with $P \in U_i$. Then put $f := F(\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i})|_C \in K(C)$. Define $(F)_P := (f)_P$ and $(F) := \sum_P (F)_P \cdot P$.

(a) Show that this is well-defined.

(b) Prove Bézouts Theorem:

$$deg((F)) = deg(F) \cdot deg(C).$$

(c) Let $C \neq E \subset \mathbb{P}^2$ be smooth irreducible curves of degrees d and e. Write $E = Z(G)$ for an irreducible homogeneous polynomial of degree e. Show that $C \cap E$ is nonempty and has at most $d \cdot e$ elements, and that $(G) \in Div(C)$ is the sum of the intersection points $C \cap E$ with positive multiplicities.

2. Riemann-Roch Theorem

The divisor of a differential form on C will be called a canonical divisor and denoted by K_C. The genus of C is defined to be $g(C) = l(K_C)$. It turns out that $g(C)$ is an invariant of C under isomorphism. It is the most important invariant of a curve. It allows us finally to show that there are infinitely many isomorphism types of curves.

The Riemann-Roch theorem will allow us to compute the dimensions $l(D)$. Finally if $\varphi : X \to Y$ is a morphism of curves, the Hurwitz Theorem allows us to compute the genus of X in terms of that of Y and properties of φ.

2.1. Canonical Divisors. In this section we want to introduce differential forms and canonical divisors on C. In differential geometry one studies differential forms on manifolds. To a differential form ω on a curve C one can associate a divisor (ω), any such divisor is called a canonical divisor on C and denoted K_C. For different differential forms ω, η on C the corresponding divisors are linearly equivalent. The genus $g(C)$ of C is defined as $g(C) := l(K_C)$. We start by constructing the space of differential forms on C.

Definition 2.1. Let F be the $K(C)$-vector space with basis the symbols $\{[df] \mid f \in K(C)\}$. The $K(C)$-vector **space of differential forms** on C is the quotient of F by the subvectorspace generated by the following:

(1) $[d(f+g)] - [df] - [dg]$, for $f, g \in K(C)$,
(2) $[d(fg)] - f[dg] - g[df]$ for $f, g \in K(C)$,
(3) $[da]$ for $a \in K$.

We write df for the equivalence class of $[df]$. We denote by Ω_C the space of differential forms on C. By definition there is a k-vector space homomorphism $d : K(C) \to \Omega_C; f \mapsto df$. The elements of Ω_C are called **differential forms** on C.

Remark 2.2. (1) The definition is rather abstract so we will rephrase it: A differential form is a finite linear combination $\sum_i f_i dg_i$, with $f_i, g_i \in K(C)$. This is a $K(C)$-vector space by $h \cdot \sum_i f_i dg_i = \sum_i h f_i dg_i$. We have the following relations:
  (a) $d(f+g) = df + dg$, for $f, g \in K(C)$,
  (b) $d(fg) = f dg + g df$ for $f, g \in K(C)$,
  (c) $da = 0$ for $a \in k$.

(2) From the rules above we can easily find some rules for computation with differential forms. The rules are the same as for differentiation of functions in calculus.

(a) If $h = \frac{f}{g} \in K(C)$, then $f = gh$, thus $df = hdg + gdh$. Therefore $d(\frac{f}{g}) = \frac{1}{g^2}(gdf - fdg)$.
(b) If $t \in K(C)$ and $a \in k$, then we see that $at^n = nat^{n-1}dt$.
(c) Let $F \in k[x,y]$, and $f, g \in K(C)$. We write $F_f(f,g) := \frac{\partial F}{\partial x}(f,g)$, $F_g(f,g) := \frac{\partial F}{\partial y}(f,g)$. From (b) we see that

$$d(F(f,g)) = F_f(f,g)df + F_g(f,g)dg.$$

Note that a priori Ω_C could be anything between huge and 0. It is defined as a quotient of an infinite-dimensional vector space by an infinite-dimensional subspace. However it turns out that Ω_C is always a $K(C)$-vector space of dimension 1.

Theorem 2.3. (1) *Ω_C is a 1-dimensional $K(C)$-vector space. If t is a uniformizing parameter of C at any point $P \in C$, then dt is a basis of Ω_C.*
(2) *If s, t are uniformizing parameters at $P \in C$, then $ds = udt$ with u a unit in $\mathcal{O}_{C,P}$.*
(3) *If $f \in \mathcal{O}_{C,P}$ and t is a uniformizing parameter at P, then $df = gdt$ with $g \in \mathcal{O}_{C,P}$.*

Proof. Let $P \in C$. Let s, t be local parameters at P, and assume that (1) and (3) hold for t. Then $s = tu$ for u a unit it $\mathcal{O}_{C,P}$. We have $du = vdt$ for $v \in \mathcal{O}_{C,P}$. Therefore

$$ds = udt + tdu = udt + tvdt = (u + tv)dt.$$

As u is a unit and $tv \in \mathbf{m}_P$, it follows that $(u + tv)$ is a unit $\mathcal{O}_{C,p}$. This shows (2), and we see that (1) and (3) also hold for s. Thus it is enough to prove (1), (3) for **one** local parameter.

We know that there is a birational map $\varphi : C \to C'$ where C' is a hypersurface in $\mathbb{A}^2$. Given any point P in C, we can assume that φ is an isomorphism from an open neighbourhood of $P \in C$ to an open neighbourhood of $\varphi(P)$ in C'. We denote X, Y the coordinates of $\mathbb{A}^2$ and x, y the corresponding coordinate functions on C'. We can assume that x is a uniformizing parameter at P. Note that $K(C') = K(C)$, and $\mathcal{O}_{C,P} = \mathcal{O}_{C',\varphi(P)}$, so we can work on C'. We write C for C' and P for $\varphi(P)$.

Let $F \in k[X,Y]$ be the equation of C. Then we have $F(x,y) \equiv 0$. Thus

$$0 = dF(x,y) = F_x(x,y)dx + F_y(x,y)dy.$$

As x is a uniformizing parameter at 0 we see $F_y(P) \neq 0$. Thus we get $dy = -\frac{F_x(x,y)}{F_y(x,y)}dx$, and $-\frac{F_x(x,y)}{F_y(x,y)} \in \mathcal{O}_{C,P}$. Now let $h \in K(C)$ be general. Then we can write $h = \frac{G(x,y)}{H(x,y)}$, for $G, H \in k[X,Y]$. Thus $dh = \frac{1}{H(x,y)^2}\big(H(x,y)dG(x,y) - G(x,y)dH(x,y)\big)$. By the above we know that $dG(x,y) = G_x(x,y)dx + G_y(x,y)dy = udx$ for a suitable $u \in \mathcal{O}_{C,P}$, and similarly $dH(x,y) = vdx$ for some $v \in \mathcal{O}_{C,P}$. Thus $dh = \frac{uH(x,y)-vG(x,y)}{H^2(x,y)}dx$. If $h \in \mathcal{O}_{C,P}$ then $H(P) \neq 0$, thus $dh = fdx$ with $f \in \mathcal{O}_{C,p}$.

This shows the theorem except for the statement that $\Omega_C \neq 0$. This is shown by using that Ω_C fulfills a universal property. For the details see [**Fulton**]. □

Now we want to define canonical divisors as the divisors of differential forms.

Definition 2.4. Let $\omega \in \Omega_C \setminus 0$ be a differential form. Let $P \in C$. We can write $\omega = fdt$ for t a local parameter at P and $f \in K(C) \setminus 0$. Then we define $\nu_P(\omega) := \nu_P(f)$. Note that this is independent of the choice of t: If s is another local parameter at P, then $ds = udt$ for $u \in \mathcal{O}^*_{C,P}$. Thus $\nu_P(fu) = \nu_P(f)$. The **divisor** of ω is defined as

$$(\omega) := \sum_{P \in C} \nu_P(\omega) \cdot P.$$

Every divisor of the form (ω) is called a **canonical divisor** of C. We often write K_C for any canonical divisor on C.

If (ω) is a canonical divisor, then the canonical divisors are $\{(f\omega) = (f) + (\omega) \mid f \in K(C)^*\}$. Thus the canonical divisors form a linear equivalence class. In particular they are linearly equivalent and thus have the same degree.

Example 2.5. We want to compute the canonical divisors of $\mathbb{P}^1$. Let $x = \frac{x_1}{x_0}$. Then $x - a$ is a local parameter at $a := [1,a] \in \mathbb{A}^1$. On the other hand $z := 1/x$ is a local parameter at ∞. We compute (dx). At any $a \in \mathbb{A}^1$ we have $dx = d(x-a)$, thus $\nu_a(dx) = 0$. Finally at ∞ we have $dx = d(\frac{1}{z}) = -\frac{1}{z^2}dz$. Thus $\nu_\infty(dx) = -2$. Thus we get $(dx) = -2 \cdot \infty$. Thus the canonical divisors on $\mathbb{P}^1$ are the divisors of degree -2.

2.2. Riemann-Roch Theorem. We define the genus of a curve as $g(C) := l(K_C)$ for any canonical divisor K_C. It is the most important invariant of C. The celebrated Riemann Roch Theorem allows us to compute the dimensions of the spaces $L(D)$.

Definition 2.6. The **genus** of C is $g(C) := l(K_C)$.

As K_C was defined in terms of $K(C)$, we see that if $C \simeq C'$, then $g(C) = g(C')$. Therefore the genus will allow us to distinguish non-isomorphic curves. Now we state the Riemann-Roch theorem.

Theorem 2.7. *(Riemann-Roch) Let D be a divisor on a curve C of genus g. Then*

$$l(D) - l(K_C - D) = deg(D) + 1 - g.$$

Thus we do not get directly $l(D)$, but only the difference $l(D) - l(K_C - D)$.

Example 2.8. We want to check this result for $\mathbb{P}^1$. We know $g(\mathbb{P}^1) = l(-2 \cdot \infty) = 0$. If D is a divisor on $\mathbb{P}^1$, then $deg(K_{\mathbb{P}^1} - D) = -2 - deg(D)$, and we have seen that $l(D) = max(0, deg(D) + 1)$. Thus the Riemann-Roch Theorem says that

$$max(0, deg(D) + 1) - max(0, -(deg(D) + 1)) = deg(D) + 1,$$

which is clearly true.

Corollary 2.9. *(Riemann) $l(D) \geq deg(D) + 1 - g$.*

Remark 2.10. (1) The corollary is the original result of Riemann. His student Roch determined the missing term $l(K_C - D)$.

(2) The natural proof of this result is using cohomology of sheaves: To a divisor D on C one associates an “invertible sheaf” $\mathcal{O}_C(D)$ on C (whatever that might be). For such invertible sheaves one can define cohomology groups $H^i(C, \mathcal{O}_C(D))$, which a finite-dimensional k-vector spaces. The definition will imply that $H^0(C, \mathcal{O}_C(D)) \simeq L(D)$. The Riemann-Roch Theorem then is a formula for $dim_k(H^0(C, \mathcal{O}_C(D))) - dim_k(H^1(C, \mathcal{O}_C(D)))$. Finally there is the Serre-duality theorem, which implies that

$$dim_k(H^1(C, \mathcal{O}_C(D))) = dim_k(H^0(C, \mathcal{O}_C(K_C - D))) = l(K_C - D).$$

(3) The Riemann-Roch Theorem can be generalized from curves to nonsingular varieties of any dimension. This is the famous Hirzebruch-Riemann-Roch Theorem see ([**Hartshorne**], Appendix A).

(4) If X is a nonsingular variety over the complex numbers, one can view the Hirzebruch-Riemann-Roch Theorem as a result on the dimensions of spaces of solutions for a certain partial differential equation on the corresponding complex manifold. This result can be generalized to arbitrary so-called elliptic differential operators. This is the celebrated Atiyah-Singer index theorem.

We can now determine the degree of a canonical divisor.

Corollary 2.11. *$deg(K_C) = 2g - 2$.*

Proof. We apply the Riemann-Roch Theorem to K_C. Then $l(K_C) - l(0) = deg(K_C) + 1 - g$. But $l(K_C) = g$ and $l(0) = 1$, thus $deg(K_C) = 2g - 2$. □

If the degree of D is large, we get a precise formula for $l(D)$.

Corollary 2.12. *If $deg(D) > 2g - 2$, then $l(D) = deg(D) + 1 - g$.*

Proof. This is because $deg(K_C - D) < 0$, thus $l(K_S - D) = 0$. □

We know $g(\mathbb{P}^1) = 0$. But conversely any curve of genus 0 is isomorphic to $\mathbb{P}^1$.

Corollary 2.13. *Let C be a curve of genus 0. Then $C \simeq \mathbb{P}^1$.*

Proof. Let P, Q be two distinct points on C. Then by the Riemann-Roch theorem we have $l(P - Q) + l(K_C - Q + P) = 1$. But $deg(K_C - Q + P) = -2$, thus $l(P-Q) = 1$. As $P-Q$ is a divisor of degree 0, it follows that $P-Q \sim 0$, i.e. $P \sim Q$. But we have seen that this implies that $C \simeq \mathbb{P}^1$. □

Corollary 2.14. *Let C be a curve of genus 1. Then $K_C \sim 0$.*

Proof. We know that $deg(K_C) = 0$ and $l(K_C) = 1$, thus $K_C \sim 0$. □

As a final application we want to compute the genus of a smooth curve of degree d in $\mathbb{P}^2$. The result shows that if X and Y are curves of degrees $d_1 < d_2$ in $\mathbb{P}^2$, then they are not isomorphic unless $(d_1, d_2) = (1, 2)$. Thus suddenly we know that there are infinitely many isomorphism classes of curves.

Theorem 2.15. *Let C be a smooth curve of degree d in $\mathbb{P}^2$. Then $g(C) = \frac{1}{2}(d-1)(d-2)$.*

Proof. Let $F \in k[x_0, x_1, x_2]$ be the equation of C. Let $X := \frac{x_1}{x_0}$, $Y := \frac{x_2}{x_0}$. Put $f(X,Y) := F(1, X, Y)$. Let x, y be the restrictions of x, y to C. Then $f(x,y) \equiv 0$ on $C \cap \mathbb{A}^2$. Thus we have $0 = d(f(x,y)) = f_x(x,y)dx + f_y(x,y)dy$. Therefore $\omega := \frac{dx}{f_y(x,y)} = -\frac{dy}{f_x(x,y)}$. As C is smooth, for any point $P = (a,b)$ of $C \cap \mathbb{A}^2$ we have either $f_y(P) \neq 0$ and $x - a$ is a local parameter or $f_x(P) \neq 0$ and $y - b$ is a local parameter. Thus ω has no pole and no zero on $C \cap \mathbb{A}^2$

So it is enough to see what happens on $Z(x_0)$. We can assume that $[0,0,1] \notin C$. Let $U := \frac{x_0}{x_1}, V := \frac{x_2}{x_1}$, and denote by u, v their restrictions to $C \cap U_1$. We put $g(U,V) := F(U, 1, V)$, thus $C \cap U_1 = Z(g)$. Thus $g(u,v) = 0$. Note that $x = \frac{1}{u}$ and $y = \frac{v}{u}$. Thus

$$f_y(x,y) = \frac{\partial F}{\partial X_2}(1, \frac{1}{u}, \frac{v}{u}) = \frac{1}{u^{n-1}} \frac{\partial F}{\partial X_2}(u, 1, v) = \frac{g_v(u,v)}{u^{n-1}}.$$

Thus

$$\omega = \frac{dx}{f_y(x,y)} = \frac{d(\frac{1}{u})}{\frac{1}{u^{n-1}} g_v(u,v)} = -\frac{u^{n-3}du}{g_v(u,v)}.$$

As above we can see that also $\omega = \frac{u^{n-3}dv}{g_u(u,v)}$. As before we see that at each point $P = [a, 1, b]$ in $C \cap U_1$ we have $g_u(P) \neq 0$ and $v - b$ is a local parameter or $g_v(P) \neq 0$ and $u - a$ is a local parameter. Thus for all $P \in C \cap Z(x_0)$ we have $\nu_P(\omega) =$

$\mu_P(u^{n-3}) = (n-3)\nu_P(H\infty)$, where $H_\infty = Z(x_0)$ is the line at infinity. Thus we get $(\omega) = (n-3)H_\infty$ and thus $deg(\omega) = n(n-3)$. We conclude by the formula $deg(\omega) = 2g-2$. □

Remark 2.16. One can modify the above arguments to prove the following. Let $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ be a nonsingular curve given as a zero set of a polynomial $F \in k[x_0, x_1, y_0, y_1]$ of bidegree a, b. Then $deg(K_C) = 2(ab - a - b)$, and thus $g(C) = ab - a - b + 1$. In particular a nonsingular curve of bidegree $(2, a)$ has genus $a - 1$. Thus we see that there are curves of any genus $g \geq 0$.

2.3. Hurwitz Theorem. In this section we want to look at dominant morphisms $\varphi : X \to Y$ of curves. Recall that the degree of φ is the degree $[K(X) : K(Y)]$ of the corresponding extension of function fields. We will prove a formula that determines $g(X)$ in terms of $g(Y)$, $deg(\varphi)$ and the ramification divisor. We start out by defining ramification. Ramification can be more complicated if k has finite characteristic, therefore we will assume in this section that k has characteristic 0.

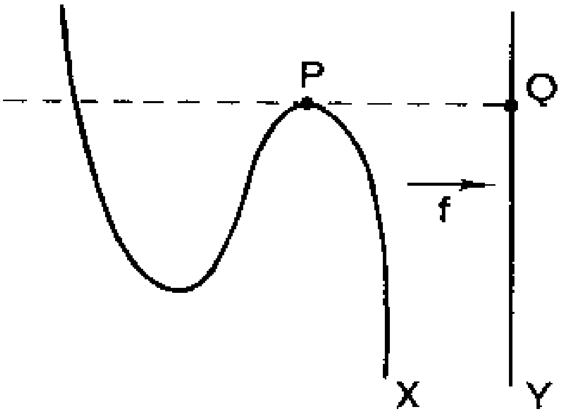
Definition 2.17. For a point $P \in X$ we define the **ramification index** e_P as follows: Let $Q := \varphi(P)$ and let $t \in \mathcal{O}_{Y,Q}$ be a local parameter. Then $\varphi^*(t) \in \mathcal{O}_{X,P}$ and we put

$$e_P := \nu_P(\varphi^*(t)).$$

Note that this is independent of the choice of the local parameter: if $s := ut$ for u a unit in $\mathcal{O}_{Y,Q}$, then $\varphi^*(u)$ is also a unit in $\mathcal{O}_{X,P}$ and thus $\nu_P(\varphi^*(ut)) = \nu_P(t)$. If $e_P > 1$, we say that φ is **ramified** at P and Q is a **branch point** of φ. If $e_P = 1$, we say that φ is **unramified** at P. We define the **ramification divisor** R of φ by

$$R := \sum_{P \in X} e_P \cdot P.$$

(We will assume that φ has only finitely many ramification points, so that R is a well-defined divisor. In fact under our assumption that k has characteristic 0 this is always true, but we do not have the time to prove it).



ıre 13 A finite morphism of curves

Recall that we defined a homomorphism $\varphi^* : Div(Y) \to Div(X)$ by setting

$$\varphi^*(Q) = \sum_{P \in \varphi^{-1}(Q)} e_P \cdot P,$$

and extending by linearity. We saw that $deg(\varphi^*(D)) = deg(\varphi) \cdot deg(D)$, and $\varphi^*((f)) = (\varphi^*(f))$ for a function $f \in K(Y) \setminus 0$.

Theorem 2.18. *(Hurwitz) Let $\varphi : X \to Y$ be a dominant morphism of curves of degree n (with only finitely many ramification points). Then $K_X \sim \varphi^* K_Y + R$, in particular*

$$2g(X) - 2 = n(2g(Y) - 2) + deg(R).$$

Proof. Let $\omega \neq 0$ be a differential form on Y, we can assume $\omega = dg$ for $g \in K(Y)$ as these generate Ω_Y as a $K(C)$-vector space. We put $\eta := d(\varphi^*(g))$. This is a differential form on X, and we want to compute (η). Let $P \in X$, $Q = \varphi(P) \in Y$, we write $e := e_P$. Let t be a local parameter in $\mathcal{O}_{Y,Q}$. We can write $g = ut^m$ with u a unit and $m \in \mathbb{Z}$. Then $\omega = mut^{m-1}dt + t^m du$ and thus $\nu_Q(\omega) = m - 1$ (note that here we have used characteristic 0). By definition of e, there is a local parameter $s \in \mathcal{O}_{X,P}$ with $\varphi^*(t) = as^e$ for a unit $a \in \mathcal{O}_{C,P}$. Thus $dt = as^{e-1}ds + s^e da$. Thus for suitable elements $b_1, b_2 \in \mathcal{O}^*_{C,P}$, $c \in \mathcal{O}_{C,P}$, we get $d(\varphi^*(g)) = b_1 s^{(m-1)e} s^{e-1} ds + b_2 s^{me} dc$. Thus $\nu_P(\eta) = (m-1)e + e - 1 = e \cdot \nu_Q(\omega) + (e-1)$. Note that by definition $e \cdot \nu_Q(\omega) = \nu_P(\varphi^*(\omega))$. Therefore

$$(\eta) = \varphi^*((\omega)) + \sum_{P \in X} (e_P - 1) \cdot P = \varphi^*((\omega)) + R,$$

and the result follows. □

An important special case is that of dominant morphisms to $\mathbb{P}^1$. If $C \to \mathbb{P}^1$ is a dominant morphism of degree n, we see that $2g(C) - 2 = -2n + R$.

EXAMPLE 2.19. Let C be a curve of bidegree $(2, a)$ in $\mathbb{P}^1 \times \mathbb{P}^1$. We know that $g(C) = a - 1$. The second projection gives a morphism $\pi : C \to \mathbb{P}^1$. We can see that a general fibre is not tangent to C and intersects C in 2 points. Thus $\pi : C \to \mathbb{P}^1$ is a finite morphism of degree 2 with finitely many ramification points. As $deg(\pi) = 2$, we see that $e_P = 2$ for all ramification points. By the Hurwitz formula we see that $2a - 4 = -4 + deg(R)$. Thus if $P_1, P_2 \in C$ are two points lying in the same fibre, then $\pi^*(K_{\mathbb{P}^1}) \sim -2(P_1 + P_2)$, and if $R_1, \ldots, R_{2a}$ are the ramification points, then $K_C \sim -2 \cdot (P_1 + P_2) + R_1 + \ldots + R_{2a}$.

DEFINITION 2.20. A curve C of genus $g \geq 2$ is called **hyperelliptic** if there is a dominant morphism $\varphi : C \to \mathbb{P}^1$ of degree 2.

Thus all curves in $\mathbb{P}^1 \times \mathbb{P}^1$ of bidegree $(2, a)$ with $a \geq 3$ are hyperelliptic of genus $a - 1$. Thus there are hyperelliptic curves of any genus $g \geq 2$.

Exercises

(1) Let $C := Z(Y^2Z - X(X - Z)(X - \lambda Z)) \subset \mathbb{P}^2$, for $\lambda \in k \setminus \{0, 1\}$. Let $x := \frac{X}{Z}$, $y := \frac{Y}{Z}$. Let $\omega := \frac{dx}{y}$. Show that $(\omega) = 0$.

(2) (Reciprocity Theorem of Brill-Noether). Let D, E be divisors on a curve C so that $D + E$ is a canonical divisor. Then $l(D) - l(E) = \frac{1}{2}(deg(D) - deg(E))$.

(3) Let D be a divisor of degree $2g - 2$ on a curve C of genus g and assume that $l(D) = g$. Show that D is a canonical divisor.

(4) Let C be a curve and $P \in X$ be a point. Show that there exists a nonconstant rational function $f \in K(C)$, which is regular everywhere except at P.

(5) Use Corollary 2.11 and Corollary 2.12 to show that $l(D)$ is finite for any divisor D on C.

(6) Let D be an effective divisor on a curve C of genus g. Show that $l(D) \leq deg(d) + 1$. Furthermore equality holds if and only if $g = 0$ or $D = 0$.

(7) Let X, Y curves and assume $g(Y) > g(X)$. Then every morphism $\varphi : X \to Y$ maps X to a point.

(8) Let X, Y curves and assume there is a morphism $\varphi : X \to Y$ of degree $n > 0$. Then $g(X) > g(Y)$ or $g(Y) \leq 1$.

(9) Show that there are dominant morphisms $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ of any degree $d \geq 1$.

3. Applications to the geometry of curves

3.1. Embeddings in projective space. For divisor classes $[D] \in Pic(C)$ we define a morphism $\varphi_{|D|} : C \to \mathbb{P}^r$, where $r = dim(l(D)) - 1$. We will see that the effective divisors linearly equivalent to D are precisely the inverse images of the hyperplanes in $\mathbb{P}^r$. We will show that if $deg(D) \geq 2g + 1$, then $\varphi_{|D|}$ is an embedding and the image is a curve of degree $deg(D)$.

Definition 3.1. Let D be a divisor on C. The **linear system** $|D|$ is the set of all effective divisors E with $E \sim D$. By definition

$$|D| = \{D + (f) \mid (f) \in L(D) \setminus 0\}.$$

A point $Q \in C$ is called **base point** of $|D|$ if for all $E \in |D|$, we have $E \geq P$ (thus it is a point that all elements of $|D|$ have in common. We say that $|D|$ is **base point free** if it has no basepoints. Note that by definition $|D|$ depends only on the class $[D] \in Pic(C)$.

To $[D] \in Pic(C)$ with $|D|$ base point free we want to associate a morphism $\varphi_{|D|} : C \to \mathbb{P}^r$, with $r = l(D) - 1$ (well defined up to a projective linear transformation of $\mathbb{P}^r$).

Definition 3.2. Let $D = \sum_{i=1}^{s} a_i P_i$ be a divisor with $|D|$ base point free. For each P_i we choose a local parameter t_i at P_i and an open neighbourhood W_i of P_i, not containing any other of the P_j, so that t_i has no other zeros or poles on W_i. We put $s_i := t_i^{a_i}$. We put $W_0 := C \setminus \{P_1, \dots, P_s\}$, and $s_0 := 1$.

Let $h_0, \dots, h_r$ be a basis of $L(D)$. We define $\varphi_{|D|} : C \to \mathbb{P}^r$ on each W_i by $\varphi_{|D|} := [h_0 s_i, \dots, h_r s_i]$.

We need to check that this is a well-defined morphism: For all j, we have $(h_j) + D \geq 0$. By the definition we see that $\nu_P(h_j s_i) = \nu_P(D) + \nu_P(h_j) \geq 0$ for all $P \in W_i$. As $|D|$ is base point free, for any point $P \in W_i$ at least one of the $(h_j s_i) = 0$ does not vanish at P. Thus $\varphi_{|D|}$ is locally given by an $(r + 1)$-tuple of regular functions with no common zeros and on the intersection of any two of these open sets $\varphi_{|D|}$ defines the same map. Thus $\varphi_{|D|}$ is a morphism.

We still have to see that $\varphi_{|D|} = \varphi_{|E|}$ if $D \sim E$. Let $f \in K(C)^*$ with $D + (f) = E$. Then we know that $h \mapsto fh$ is an isomorphism $L(D) \to L(E)$. Choose $h_0 f, \dots, h_r f$ as a basis of $L(E)$, and define $\varphi_{|E|}$ using this basis. Then on the open set $W_0 \setminus supp(f)$ we have $\varphi_{|D|} = [h_0, \dots, h_r] = [fh_0, \dots, fh_r] = \varphi_{|E|}$. So the morphisms $\varphi_{|D|}$ and $\varphi_{|E|}$ coincide on a nonempty open subset, so they are equal.

We call D **very ample** if $|D|$ is base point free and $\varphi_{|D|} : C \to \mathbb{P}^r$ is an imbedding (i.e. an isomorphism to $\varphi(C) \subset \mathbb{P}^r$).

By definition $\varphi_{|D|}$ does not just depend on D, but also on a choice of a basis of $L(D)$. For any other choice of basis the corresponding morphism $\psi_{|D|}$ will be $F \circ \varphi_{|D|}$, where F is a projective linear transformation of $\mathbb{P}^r$, thus the morphism is essentially the same.

The nice fact about these morphisms $\varphi_{|D|}$ is that we can understand them in terms of the geometry of $|D|$. The elements of $|D|$ will be precisely the inverse images of the hyperplanes in $\mathbb{P}^r$.

Remark 3.3. We use the notations of Definition 3.2

(1) We write $\varphi := \varphi_{|D|}$. Let $E \in |D|$. Then $E = D+h$ for $h := b_0h_0+\ldots+b_rh_r \in L(D)\setminus 0$. Let $H := b_0x_0+\ldots+b_rx_r$, which is a linear form on $\mathbb{P}^r$. Let $P \in C$, then $P \in W_i$ for some i and by definition

$$\nu_P(\varphi^*(H)) = \nu_P(s_ib_0h_0 + \ldots + s_ib_rh_r)) = \nu_p(s_i) + \nu_P(h) = \nu_P(D + (h)) = \nu_P(E).$$

Thus $(\varphi^*(H)) = E$. So we get that

$$|D| = \big\{(\varphi^*(H)) \bigm| H \text{ linear form on } \mathbb{P}^r\big\}.$$

In particular the supports of the elements of $|D|$ are precisely the inverse images of the hyperplanes $Z(H)$ in $\mathbb{P}^r$.

(2) If φ is an embedding with image $X \subset \mathbb{P}^r$, then $deg(D) = deg(X)$.

Now we will show that every divisor D on C of sufficiently high degree defines an embedding $\varphi_{|D|} : C \to \mathbb{P}^r$.

We use the following result from algebra, that we will not prove. For a proof see [**Hartshorne**], Prop.II.7.3:

Theorem 3.4. *A morphism $\varphi : X \to Y$ of projective varieties is an embedding if and only if*

(1) *φ is injective,*

(2) *$d_p\varphi : T_pX \to T_pY$ is injective for all $p \in X$.*

Theorem 3.5. *Let D be a divisor on a curve C.*

(1) *$|D|$ is base point free (and thus D defines a morphism) if and only if for all $P \in C$,*

$$l(D - P) = l(D) - 1.$$

(2) *D is very ample if and only if for all $P, Q \in C$ (including the case $P = Q$),*

$$l(D - P - Q) = l(D) - 2.$$

Proof. By definition $f \in L(D - P)$ if and only if then $D + (f) - P \geq 0$ i.e. if and only if $D + (f) \geq P$. Thus $L(D - P)$ is the subset of all $(f) \in L(D)$ with $D+(f) \geq P$, and $L(D-P-Q)$ is the subset of all $(f) \in L(D)$ with $D+(f) \geq P+Q$.

(1) The Riemann Roch Theorem implies

$$1 = l(D)-l(K-D)-(l(D-P)-l(K-D+P)) = (l(D)-l(D-P))+(l(K-D+P)-l(K-D).$$

By the above we know that $l(D) \geq l(D - P)$ and $l(K - D + P) \geq l(K - D)$. Thus either $l(D) = l(D) - 1$ or otherwise $L(D) = L(D - P)$, i.e. P is a base point.

(2) By the above we know that $l(D - P - Q) = l(D) - 2$ if and only if $l(D) - l(D - P) = 1$ and $l(D - P) - l(D - P - Q) = 1$. By (1) this is equivalent to

(1) $|D|$ has no basepoints. Thus it defines a morphism $\varphi : C \to \mathbb{P}^r$.
(2) For all P, Q there is an element $f \in L(D - P) \setminus L(D - P - Q)$, i.e. there is an element $E \in |D|$ with $E \geq P$, but not $E \geq P + Q$.

Assume that $P \neq Q$. Then this means that $P \in supp(E)$ but not $Q \in supp(E)$. We have seen that the supports of the elements of $|D|$ are the inverse images of the hyperplanes in $\mathbb{P}^r$. Thus this is is equivalent to the existence of a hyperplane H in $\mathbb{P}^r$ with $\varphi(P) \in H$ and $\varphi(Q) \notin H$, and this is equivalent to $\varphi(P) \neq \varphi(Q)$. Thus we see that the condition of (2) for all $P \neq Q$ is equivalent to φ being injective.

Now assume $P = Q$. By the exercise above for a hyperplane $H \subset \mathbb{P}^r$ we have $(\varphi^*(H)) \geq 2P$ if and only if $\varphi(P) \in H$ and $d_P\varphi(T_PC) \subset T_{\varphi(P)}H$. Thus the existence of $E \in |D|$ with $E \geq P$ but not $E \geq 2P$ means that there exists a hyperplane $H \in \mathbb{P}^r$ with $\varphi(P) \in H$ and $d_P\varphi(T_PC) \not\subset T_{\varphi(P)}H$. This is equivalent to $d_P\varphi : T_PC \to T_P\mathbb{P}^r$ being injective. □

Theorem 3.6. *Let D be a divisor on a curve X of genus G.*

(1) *If $deg(D) \geq 2g$, then $|D|$ has no basepoints.*
(2) *If $deg(D) \geq 2g + 1$ then D is very ample and embeds C as a curve of degree $deg(D)$ in $\mathbb{P}^{deg(D)-g}$.*

Proof. (1) As $deg(D) \geq deg(K) + 2$, we see that $l(K - D) = 0 = l(K - D + P)$, for any $P \in X$. Thus by the Riemann-Roch Theorem $l(D) = deg(D) + 1 - g = l(D - P) + 1$.

(2) As $deg(D) \geq deg(K) + 3$, we get $l(K - D) = 0 = l(K - D + P + Q)$, for any $P, Q \in X$, Thus by Riemann-Roch $l(D) = deg(D) + 1 - g = l(D - P - Q) + 2$. □

EXAMPLE 3.7.

1. On a curve C of genus 1 any divisor D of degree 3 is very ample. Thus any curve of genus 1 can be embedded in $\mathbb{P}^2$ as a cubic. and we know already that nonsingular cubics in $\mathbb{P}^2$ have genus 1. If D is a divisor of degree 2 on C, then as $deg(K_C) = 0$, we see that $l(D) = 2$. Thus D defines a morphism $C \to \mathbb{P}^1$, of degree 2.
2. If $g(C) = 2$, then any divisor of degree 5 is very ample. Thus every curve of genus 2 can be embedded as a curve of degree 5 in $\mathbb{P}^3$.
3. The bound $deg(D) \geq 2g + 1$ is not always optimal. If $C \subset \mathbb{P}^2$ is a smooth curve of degree d in $\mathbb{P}^2$, then the divisor of a line is very ample and has degre d, whereas $2g + 1 = d^2 - 3d + 3$, which is larger for $d \geq 4$.

3.2. Riemann surfaces and algebraic curves. We want to briefly sketch the relation of compact Riemann surfaces and algebraic curves. For more details see for instance Part X of [**Fulton1**].

A **Riemann surface** X is a complex manifold of dimension 1. This means that X has an open cover $(V_\alpha)_\alpha$ and there are homeomorphisms $\varphi_\alpha : U_\alpha \to V_\alpha$ from open subsets $U_\alpha \subset \mathbb{C}$. We call the φ_α the **coordinate charts** of X.

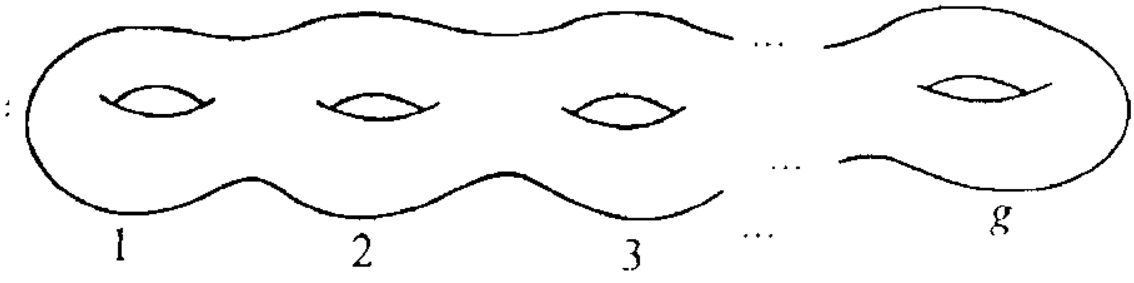
$$\begin{tikzcd}
V_\alpha & \subset & X \\
U_\alpha \arrow[u, "\varphi_\alpha"'] & \subset & \mathbb{C}
\end{tikzcd}$$

For all α, β let $U_{\alpha\beta} := \varphi_\alpha^{-1}(V_\alpha \cap V_\beta)$. Then it is required that for all α, β, the **coordinate change** $\varphi_{\beta\alpha} := \varphi_\beta^{-1} \circ \varphi_\alpha : U_{\alpha\beta} \to U_{\beta\alpha}$ is a holomorphic (i.e. complex differentiable) map of open subsets of $\mathbb{C}$

A function $f : X \to \mathbb{C}$ is called **holomorphic** (resp. **meromorphic**), if $f \circ \varphi_\alpha : U_\alpha \to \mathbb{C}$ is holomorphic (resp. meromorphic) for all α. We denote $\mathcal{M}(X)$ the field of meromorphic functions on X. A point $p \in X$ is called a **pole** of order m (resp. a **zero** of order m) of f if $\varphi_\alpha^{-1}(p)$ is a pole (resp. a zero) of order m of $f \circ \varphi_\alpha$ for an α with $p \in V_\alpha$ (it is straightforward to check that this is independent of the choice of α).

More generally if X and Y are Riemann surfaces, a map $h : X \to Y$ is called **holomorphic** if for any point $p \in X$ there are coordinate charts φ of X in a neighbourhood of p and ψ on Y in a neighbourhood of $h(p)$, such that $\psi^{-1} \circ h \circ \varphi$ is holomorphic.

From now on let X be a compact Riemann surface. It is known that a compact Riemann surface X is topologically a sphere with g handles. Here g is called the **genus** of X.



A divisor D on X is a formal sum $\sum_{p\in X} a_p \cdot P$, with coefficients $a_p \in \mathbb{Z}$ and only finitely $a_p \neq 0$. For a meromorphic function f on X (with no essential singularities), the **divisor** of f is defined as

$$(f) := \sum_{p\in X} \nu_p(f) \cdot X,$$

where $\nu_p(f) := k$ if f has a zero of order k at p, $\nu_p(f) = -k$ if f has a pole of order k and $\nu_p(f) = 0$ otherwise. For a divisor D on X we define

$$L(D) := \big\{ f \in \mathcal{M}(X) \bigm| (f) + D \geq 0 \big\}.$$

Let $l(D)$ be the dimension of $L(D)$ as $\mathbb{C}$-vector-space. As before we see that $L(D) = 0$ if $deg(D) < 0$, and $l(0)$ consists only of the constant functions.

If $X \subset \mathbb{P}^n$ is a nonsingular algebraic curve over $\mathbb{C}$, then X is in a natural way a complex submanifold of $\mathbb{P}^n$, and thus a Riemann surface. Then a rational function on X is in particular a meromorphic function on X. It is a nontrivial fact that in this case the two different definitions of $L(D)$ coincide.

A **meromorphic differential form** on X is given by a tuple $(f_\alpha)_\alpha$, of meromorphic functions f_α on $U_\alpha \subset \mathbb{C}$ for all α with the following condition: For all α, β we have that

$$f_\beta \circ \varphi_{\beta\alpha} = \frac{d\varphi_{\beta\alpha}}{dz} f_\alpha$$

on $U_{\alpha\beta}$. We write $f_\alpha dz$ for the differential form.

Let $\omega = f_\alpha dz$ be a meromorphic differential form on X. For any $p \in X$ let $\nu_p(\omega) := \nu_p(f_\beta)$ for any β with $p \in V_\beta$ (it is easy to see that this is independent of β). The **divisor** of ω is $(\omega) := \sum_{p\in X} \nu_p(\omega) \cdot p$. The divisor of a meromorphic differential form on X is called a **canonical divisor**.

In this context one can prove the Riemann-Roch Theorem

Theorem 3.8. *Let D be a divisor on a compact Riemann surface X of genus g, and let K be Then*

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

Remark 3.9. (1) Note that by definition here g is the number of handles of X. But by the Riemann Roch theorem we see that $g = l(K)$. Thus if X is the Riemann surface associated to a projective algebraic curve, then the two different definitions of genus coincide.

(2) The corollaries 2.9, 2.11, 2.12, 2.13, 2.14 to the Riemann-Roch theorem still hold in this context. In particular the degree of a canonical divisor is $2g - 2$.

Let X be a compact Riemann surface and let D be a divisor on X. Analogously to Definition 3.1 above we say that p is a basepoint of $|D|$ if $D + (f) \geq p$ for all $(f) \in L(D)$. If $|D|$ has no basepoints, we can in the same way in Definition 3.2 define an analytic map $\varphi_{|D|} : C \to \mathbb{P}^{r-1}$, (it is now given locally by an r-tuple of holomorphic functions. The arguments of the proof of Theorem 3.5 still work to show that for $|D| > 2g + 1$, $\varphi_{|D|}$ will be an embedding (i.e. the image will be a complex submanifold of $\mathbb{P}^n$ isomorphic to X), and in fact one can show that the image will be even a projective algebraic curve. Thus every compact Riemann surface is a projective algebraic curve over $\mathbb{C}$.

3.3. Elliptic curves. A pair of a curve C of genus 1 and a point $O \in C$ is called an elliptic curve. By the results of the last section we know that every elliptic curve can be embedded as a cubic in $\mathbb{P}^2$. We will first show that (C, O) is in a natural way an abelian group, in fact it is isomorphic to $Pic^0(C)$. In case C is a cubic in $\mathbb{P}^2$ we will give a geometric description of the group structure.

Definition 3.10. An **elliptic curve** is a pair (C, O) of a curve C of genus 1 and a point $O \in C$.

Now we show that an elliptic curve is an abelian group.

Theorem 3.11. *The map $\epsilon : C \to Pic^0(C), P \mapsto [P - O]$ is a bijection.*

Proof. Let D be a divisor of degree 0 on C. We have to show that there is a unique point $P \in C$ with $D \sim P - O$. We apply Riemann-Roch to $D + O$, to get $l(D + O) - l(K - D - O) = 1$. We know that $deg(K) = 0$, thus $l(K - D - O) = 0$. Thus $l(D + O) = 1$. For f the generator of $L(D + O)$, we have that $D + O + (f)$ is the unique effective divisor linearly equivalent to $D + O$. As it has degree 1, we have $D + O + (f) = P$ for some point P. Thus there is a unique point $P \in C$ with $D + O \sim P$ or equivalently $D \sim P - O$. □

Therefore we can transport the group structure to C.

Definition 3.12. Let (C, O) be an elliptic curve. We define the addition of $P, Q \in C$ as follows: We put $P \oplus Q := R$, for the unique $R \in C$ with $P + Q - O \sim R$.

Corollary 3.13. *$(C, \oplus)$ is an abelian group with neutral element O. We denote the inverse of $P \in C$ with $\ominus P$. The map $\epsilon : C \to Pic^0(C); P \mapsto [P - O]$ is an isomorphism of groups.*

Proof. By definition $\epsilon(O) = 0$, and for $P, Q \in C$

$$\epsilon(P \oplus Q) = [P + Q - 2O] = \epsilon(P) + \epsilon(Q).$$

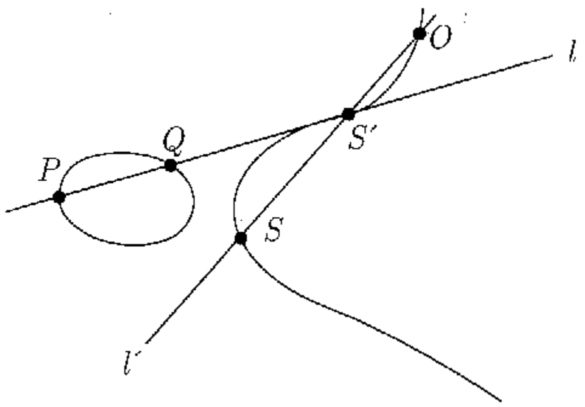
□

Remark 3.14. A smooth projective variety, which is an abelian group is called an abelian variety. The study of abelian varieties is an important subject of algebraic geometry. We have thus seen that an elliptic curve C is in a natural way an abelian variety. We can also say this differently: for an elliptic curve C the group $Pic^0(C)$ is in a natural way an abelian variety of dimension 1. For a curve C of genus g, one can show that $Pic^0(C)$ is in a natural way an abelian variety of dimension g. It is called the Jacobian variety of C. The proof is much more difficult. In case $k = \mathbb{C}$, one can view C as a Riemann surface. In this case the proof is simpler. One can find it in Part X of [**Fulton1**].

Now we use the morphism $\varphi := \varphi_{|3 \cdot O|}$ to embed C into $\mathbb{P}^2$. Let E denote the image and 0 the image of O. We want to give a geometric description of the group structure of E.

Theorem 3.15. (1) *The group structure of E is determinied by $P \oplus Q \oplus R = 0$ if and only if P, Q, R lie on a line. (here P, P, Q to lie on a line means that the tangent line to E at P intersects E at L, and P, P, P to lie on a line means that the tangent line has second order contact).*

(2) *Explicitely $P \oplus Q$ is determined as follows: Let L be the line through P, Q. Let R be the third intersection point. Let M be the line through R and 0. Then the third intersecion point of M with E is $P \oplus Q$.*



$\ominus P$ is the third intersection point of the line through $P, 0$ with E.

Proof. As E is the image of C under $\varphi_{3 \cdot O}$, we see that 3 points P, Q, R (with multiplicities) lie on a line if and only if $P + Q + R \sim 3 \cdot 0$. This is equivalent to $[P - 0] + [Q - 0] + [R - 0] = 0$ in $Pic^0(E)$, which by definition of the group structure on E is equivalent to $P \oplus Q \oplus R = 0$. This shows (1). Let now M be the line through R and 0 and let S be the third intersection point. Then $R \oplus 0 \oplus S = 0$, i.e. $S = \ominus R = P \oplus Q$. Let R be the third intersection point of the line through P and 0. Then $P \oplus 0 \oplus R = 0$, i.e. $R = \ominus P$. □

The embedding $\varphi_{|3 \cdot O|} : C \to \mathbb{P}^2$ is only well defined up linear change of coordinates. By choosing the coordinates carefully we can bring the equations into a particularly nice form.

Theorem 3.16. *Let (C, O) be an elliptic curve. Then there is a $\lambda \in k \setminus \{0, 1\}$, such that C is isomorphic to the curve*

$$y^2 = x(x-1)(x-\lambda),$$

(we mean by this that this is the intersection with $\mathbb{A}^2$), and the isomorphism sends O to $[0, 0, 1]$.

Proof. Now we will see that one can use the spaces $L(D)$ to actually find the equation of the image under $\varphi_{|D|}$. Embed C into $\mathbb{P}^2$ via $\varphi := \varphi_{|3 \cdot O|}$. The embedding depends on the choice of a basis of $L(3 \cdot O)$, and we want to choose this basis carefully. We know that

$$k = L(0 \cdot O) \subset L(O) \subset L(2 \cdot O) \subset \dots ,$$

and by Riemann-Roch we have $l(n \cdot O) = n$ for $n \geq 1$. We have $1 \in L(0 \cdot O)$. Choose $x \in L(2 \cdot O)$, such that $1, x$ are a basis of $L(2 \cdot O)$ and choose $y \in L(3 \cdot O)$, such that $1, x, y$ are a basis of $L(3 \cdot O)$. Note that the seven elements $1, x, y, x^2, xy, x^3, y^2$ are all in $L(6 \cdot O)$, which has dimension 6, thus there is a linear relation among them. Furthermore in this linear relation both x^3 and y^2 have to appear with a nonzero coefficient, because they are the only functions with a pole of order 6 at O. Replacing x and y by scalar multiples, we can assume that their coefficients are 1. Thus we get a relation

$$y^2 + b_1 xy + b_2 y = x^3 + a_1 x^2 + a_2 x + a_3.$$

Note the following: If we use $1, x, y$ as our basis for the embedding φ, then denoting $X := \frac{x_1}{x_0}$, $Y := \frac{x_2}{x_0}$ the coordinates of $\mathbb{A}^2$, then

$$\varphi(C) \cap \mathbb{A}^2 \subset Z\big(Y^2 + b_1 XY + b_2 Y - (X^3 + a_1 X^2 + a_2 X + a_3)\big),$$

because by definition $X(\varphi(p)) = x(p)$ and $Y(\varphi(p)) = y(p)$ for all $p \in C$. We know that $\varphi(C)$ is a cubic, so $\varphi(C) \cap \mathbb{A}^2 = Z\big((Y^2 + b_1 XY + b_2 Y - (X^3 + a_1 X^2 + a_2 X + a_3)\big)$.

We make further linear change of the basis: Replace y by $y + \frac{1}{2}(b_1 x + b_2)$. Then the equation becomes of the form

$$y^2 = (x - a)(x - b)(x - c).$$

Note that this equation defines a nonsingular cubic only if a, b, c are distinct. As this is still the equation of $\varphi(C)$, which is smooth, we thus know that a, b, c are distinct. Finally we replace x by $x + a$, to get the equation $y^2 = x(x - b')(x - c')$, and then x by $b'x$ and y by $b''y$ for any $b'' \in k$ with $(b'')^2 = (b')^3$, to obtain $y^2 = x(x-1)(x-\lambda)$ for some $\lambda \in k \setminus \{0, 1\}$. By definition we see that $\varphi = [1, x, y] = [\frac{1}{y}, \frac{x}{y}, 1]$ and thus $\varphi(O) = [0, 0, 1]$. □

Remark 3.17. Let us denote by E_λ the elliptic curve given by $y^2 = x(x-1)(x-\lambda)$. For an elliptic curve $X = (C, 0)$, which is isomorphic to E_λ, The j-**invariant** $j(X)$ is defined as $j((C, 0)) := 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$. One can show ([**Hartshorne**] Thm.IV.4.1) that

(1) $j(X)$ depends only on X,
(2) two elliptic curves X, Y are isomorphic, if and only if $j(X) = j(Y)$,
(3) every $a \in \mathbb{A}^1$ is of the form $j(X)$ for an elliptic curve X.

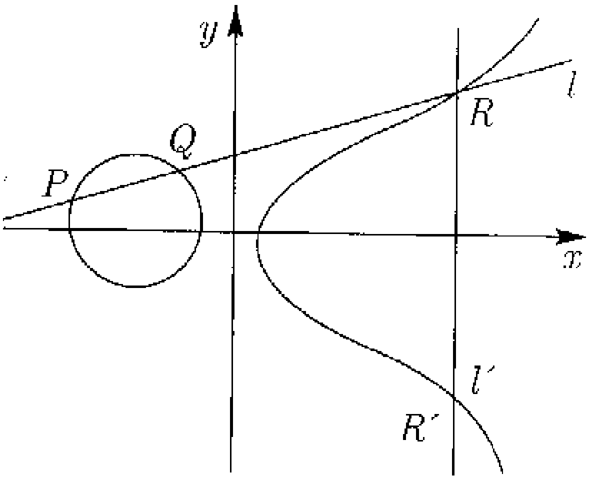
So we see that the isomorphism classes of elliptic curves are parametrized by $\mathbb{A}^1$.

We have a simpler description of the group structure of the elliptic curve $E \subset \mathbb{P}^2$ if it is of the form above.

Remark 3.18. Let $E := Z(y^2 - x(x-1)(x-\lambda)$ for $\lambda \in k \setminus \{0,1\}$. Then one checks immediately that $E \cap Z(x_0) = 0 := [0,0,1]$ and the group structure can be described as follows.

(1) If $(a,b) \in E \setminus \{0\}$, then $\ominus(a,b) = (a,-b)$. Thus the negative is obtained by reflection at the x-axis. This is because by the equation, if $(a,b) \in E$, then also $(a,-b) \in E$ and the line through (a,b) and $[0,0,1]$ is just the vertical line $\{(a,t) \mid t \in k\}$, which intersects E in $(a,b),(a,-b),[0,0,1]$.

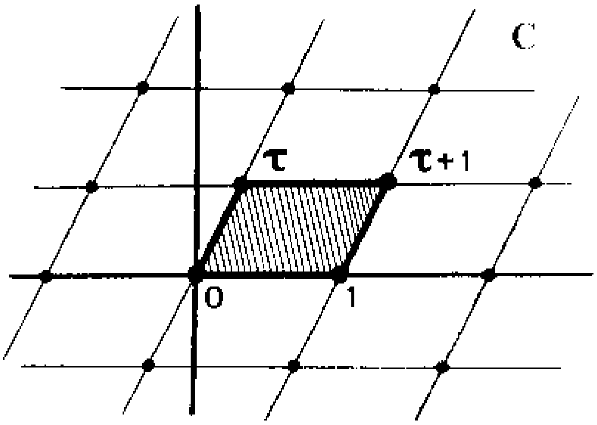
(2) Thus $(a,b) \oplus (c,d)$ is obtained as follows. Let (e,f) be the third intersection point with E of the line through $(a,b),(c,d)$. Then $(a,b) \oplus (c,d) = (e,-f)$. Thus we take the third intersection point and reflect it at the x-axis.



Elliptic curves over the complex numbers. We will very briefly sketch without proofs how elliptic curves arise in complex analysis. This also gives another explanation for the group law on an elliptic curve. The proofs of the results below are not difficult and only use the results that you have learned in your first course in complex analysis. It would however take a few hours to carry them out. This approach leads naturally to the theory of modular forms see e.g. [**Serre**].

Let $U \subset \mathbb{C}$ be open in the analytic topology. Recall that a function $f : U \to \mathbb{C}$ is **holomorphic** if it is complex differentiable, i.e. $f'(z) := \lim\limits_{w \to z} \frac{f(z)-f(w)}{z-w}$ exists for all $z \in U$. Then $g := (z-w)^{-n} f : U \setminus \{w\} \to \mathbb{C}$ is called **meromorphic**, and if $f(w) \neq 0$, we say that g has a **pole of order** n at w.

Definition 3.19. Fix a complex number τ with positive imaginary part $\Im(\tau) > 0$. Then 1 and τ are linearly independent over $\mathbb{R}$. The subgroup $\Lambda_\tau := \mathbb{Z} + \mathbb{Z}\tau$ is called a **lattice** in $\mathbb{C}$.



Theorem and Definition 3.20. *We fix $\Lambda = \Lambda_\tau$. A meromorphic function $f : \mathbb{C} \to \mathbb{C}$ is called* **elliptic** *with respect to Λ if $f(z+\omega) = f(z)$ for all $z \in \mathbb{C}, \omega \in \Lambda$.*

Write $\Lambda' = \Lambda \setminus \{0\}$. The **Weierstrass $\wp$-function** *for Λ is*

$$\wp(z) = \wp_\tau(z) := \frac{1}{z^2} + \sum_{\omega \in \Lambda'} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

It is an elliptic function with only poles of order 2 at all $\omega \in \Lambda$.

The derivative of $\wp$ is

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

$\wp'(z)$ is elliptic with only poles of order 3 at all $\omega \in \Lambda$.

The relation with elliptic curves comes from the differential equation for $\wp$.

Theorem 3.21.

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3, \qquad g_2 = 60 \sum_{\omega \in \Lambda'} \frac{1}{\omega^4}, \quad g_3 = 140 \sum_{\omega \in \Lambda'} \frac{1}{\omega^6}.$$

Therefore we can define a map

$$\varphi = \varphi_\tau : \mathbb{C} \to \mathbb{P}^2_{\mathbb{C}}, z \mapsto \begin{cases} [\wp(z), \wp'(z), 1], & z \notin \Lambda \\ [0,1,0] & z \in \Lambda. \end{cases}$$

THEOREM 3.22. *φ is a continuous and holomorphic map. Let C be the elliptic curve $Z(y^2z - 4x^3 + g_2xz^2 + g_3z^3) \subset \mathbb{P}^2_{\mathbb{C}}$ (with the analytic topology). Then φ induces a homeomorphism $\overline{\varphi} : \mathbb{C}/\Lambda \to C$.*

If we endow C with its natural structure of Riemann surface, then $\overline{\varphi}$ is an analytic isomorphism.

Note that $\mathbb{C}/\Lambda$ is homeomorphic to $S^1 \times S^1$, so we see that topologically C is a torus $S^1 \times S^1$. $\mathbb{C}/\Lambda$ is also a group as a quotient of the additive group of $\mathbb{C}$ by the subgroup Λ. In fact it is isomorphic to $\mathbb{R}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Z}$.

THEOREM 3.23. *$\overline{\varphi}$ is an isomorphism of groups. Thus as a group C is isomorphic to $\mathbb{R}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Z}$ and the subgroup of n-division points is isomorphic to $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.*

REMARK 3.24. The **complex upper half plane** $\mathcal{H}$ is the set of all complex numbers with $\Im(\tau) > 0$. We have seen that to any point $\tau \in \mathcal{H}$ can associate an elliptic curve E_τ. Some of the holomorphic functions $\mathcal{H} \to \mathbb{C}$, will depend only on the corresponding elliptic curve, thus they can be viewed as holomorphic functions on the space of elliptic curves. These are called **modular functions** and a generalization of these are the **modular forms**. Modular forms and functions play an enormous role in the study of elliptic curves and are by themself quite important (see [**Serre**] for an introduction).

Elliptic curves in number theory. Let $(C, \mathbf{0})$ be an elliptic curve over $\mathbb{Q}$. This means that $C = Z(F) \subset \mathbb{P}^2$ where F is a cubic whose coefficient are in $\mathbb{Q}$. In number theory one studies the set

$$C(\mathbb{Q}) := \big\{[a,b,c] \in C \;\big|\; a,b,c \in \mathbb{Q}\big\}$$

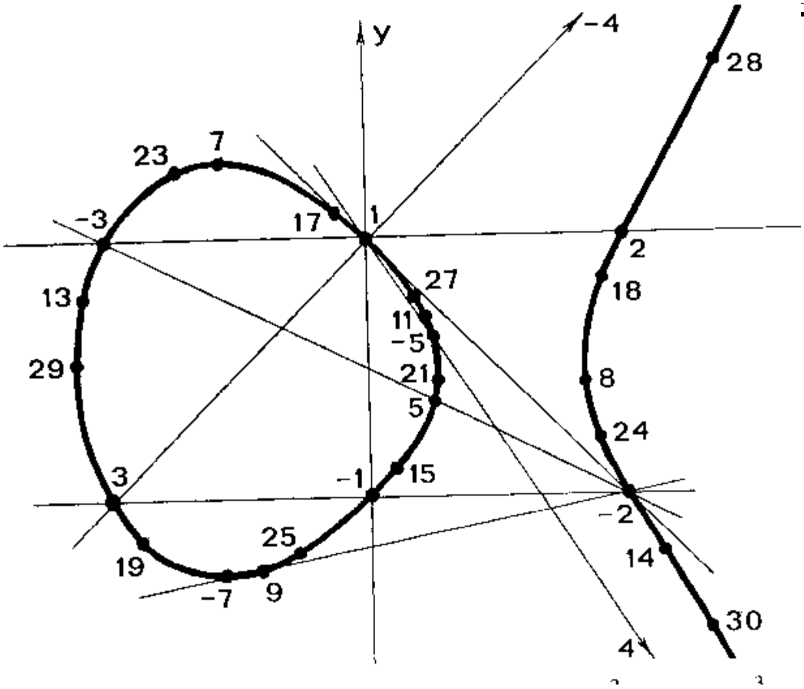
of **rational points** of C. We require $\mathbf{0} \in C(\mathbb{Q})$ and, by the geometric definition of the addition, it is easy to see that with $P, Q \in C(\mathbb{Q})$ also $\ominus P$ and $P \oplus Q$ are rational points. Thus $C(\mathbb{Q})$ is a subgroup of C. One of the most important and most difficult parts of number theory is the study of these sets $C(\mathbb{Q})$. The theorem of Mordel says that $C(\mathbb{Q})$ is a finitely generated abelian group, i.e. $C(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus \bigoplus_{i=1}^s \mathbb{Z}/n_i\mathbb{Z}$. The number $r \geq 0$ is called the **rank** of C. Note that $r > 0$ if and only if $C(\mathbb{Q})$ is infinite. One of the most difficult questions is to determine the rank of C.

EXAMPLE 3.25. (1) The Fermat cubic $C = Z(x^3 + y^3 - z^3)$. Fermats last theorem (which is easy for $n = 3$), says that $C(\mathbb{Q}) = \big\{[1,-1,0],[1,0,1],[0,1,1]\big\}$. Choosing one of these points as $\mathbf{0}$ we get $C(\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$.

(2) Let $C := Z(y^2z+yz^2-(x^3-xz^2))$. Let $\mathbf{0} := [0,1,0]$. Then it has been shown

l $\underbrace{\oplus\ldots\oplus P}_{n}$

i



If $(C, \mathbf{0})$ is an elliptic curve over $\mathbb{Q}$, we can also assume that the coefficients of the equation for $C = Z(F)$ are in $\mathbb{Z}$. Then we can look at the set of solutions $C(F_q)$ of $F = 0$ over finite fields F_q with q elements. One of the most difficult conjectures of mathematics is the **Birch and Swinnerton-Dyer** conjecture, with determines the rank of C in terms of the numbers $\#C(F_q)$ for all q.

Applications to public key cryptography. Elliptic curves are not just interesting mathematical objects, but they have also many applications to practical questions; just to name two examples coding theory and cryptography. I will just briefly talk about the application to cryptography.

The idea of public key cryptography is the following: One wants to send through a public channel (so that other people can hear it) to another person some information that only this person should understand. This is used very much in practice for bank transfers, communication via internet, bancomat and many others.

One can always assume that the information to be sent is a number. How can person A send the number N to person B so that only B so that only B can understand it? For this one uses a public key. This is just another number K on which A and B have to agree. Then A sends $N+K$ instead of N and B subtracts K. However the problem has only been shifted: How do A and B agree on K without everybody else knowing K too? For this one needs an operation on numbers that is very easy to perform, but very difficult to undo. For elliptic curves this is the following. If P is a point on an elliptic curve it is very easy to compute $n \odot P := \underbrace{P \oplus \ldots \oplus P}_{n}$. But if one has two points P, Q on an elliptic curve and Q is a multiple $n \odot P$ of P, then there is no efficient method of finding n. This is applied as follows:

(1) A and B agree publicly on an elliptic curve E and a point $P \in E$.
(2) A (secretly) chooses a number $a \in \mathbb{Z}$, and sends the coordinates of $a \odot P = \underbrace{P \oplus \ldots \oplus P}_{a}$ to B.
(3) B (secretly) chooses a number $b \in \mathbb{Z}$ and sends the coordinates of $b \odot P$ to A.
(4) Both can compute the coordinates of $(ab) \odot P$: A has to multiply $(b \odot P)$ by a and B has to multiply $(a \odot P)$ by b. The key K is the x-coordinate of $(ab) \cdot P$.

Note that, although everything was public, if anybody else wants to find the key he has to find one of the numbers a, b from P, $a \odot P$, $b \odot P$, which as mentioned before is practically impossible.

3.4. The Canonical Embedding. Let C be a curve of genus $g \geq 1$. We will just write K for its canonical divisor. Now we will look at the morphism associated to K. We will see that if C is non-hyperelliptic of genus $g \geq 3$, then $\varphi_{|K|}$ is an embedding, which embedds C as a curve of degree $2g-2$ in $\mathbb{P}^{g-1}$. It is called the canonical embedding. Note that $\varphi_{|K|}$ depends only on C and not on any further choices, thus every non-hyperelliptic curve is in a natural way a curve of degree $2g-2$ in $\mathbb{P}^{g-1}$.

Let C be a curve of genus g. If $g = 0$, then $l(K) = 0$. If $g = 1$, then K_C is trivial, thus φ_K is the constant map to a point. For $g \geq 2$ we will see that $|K|$ is base point free, thus we get a morphism $\varphi_{|K|} : C \to \mathbb{P}^{g-1}$ called the **canonical morphism**.

Lemma 3.26. *If $g \geq 2$, then $|K|$ is base point free.*

Proof. We have to show that for all $P \in C$, $l(K-P) = l(K) - 1 = g - 1$. As C is not rational, we know that $l(P) = 1$ for all $P \in C$. Thus by Riemann-Roch $1 - l(K-P) = l(P) - l(K-P) = 1 + 1 - g$, thus $l(K-P) = g - 1$. □

Recall that a curve C of genus $g \geq 2$ is called hyperelliptic if there is a morphism $\varphi : C \to \mathbb{P}^1$ of degree 2.

Theorem 3.27. *Let C be a curve of genus $g \geq 2$. Then $|K|$ is very ample if and only if X is not hyperelliptic.*

PROOF. As $l(K) = g$, we see that $|K|$ is very ample if and only if for all $P, Q \in X$ (possibly equal) $l(K - P - Q) = g - 2$. We apply Riemann-Roch to $P + Q$. This gives

$$l(P + Q) - l(K - P - Q) = 2 + 1 - g.$$

Thus K is very ample if and only if $l(P+Q) = 1$ for all $P, Q \in C$. If C is hyperelliptic, let $\psi : C \to \mathbb{P}^1$ be the map of degree 2. Let $M \in \mathbb{P}^1$, write $\psi^*(M) = P + Q$, then $\psi = \varphi_{|P+Q|}$. Thus $l(P + Q) = 2$, thus K is not very ample.

Conversely assume that K is not very ample. Thus there exist $P, Q \in C$, such that $l(P + Q) = 2$. As C is not rational, we know that $l(P) = l(Q) = 1$. Thus $|P + Q|$ is base point free and defines a morphism $\varphi_{|P+Q|} : C \to \mathbb{P}^1$. Thus C is hyperelliptic. □

DEFINITION 3.28. Let C be a non-hyperelliptic curve of genus $g \geq 3$. The embedding $\varphi_K : C \to \mathbb{P}^{g-1}$ is called the **canonical embedding** of C it is well-defined up to a projective linear transformation of $\mathbb{P}^{g-1}$. Its image, which is a curve of degree D is called a **canonical curve**.

On the classification of curves. We have shown a number of facts about curves. We have introduced the genus, which is an isomorphism invariant: curves of different genus are not isomorphic, more strongly: if $g(X) < g(Y)$, then all morphism $X \to Y$ must map X to a point.

Thus the next question to ask is whether any two curves of the same genus are isomorphic. We know that all curves of genus 0 are isomorphic to $\mathbb{P}^1$. However we have seen, that there are curves of any genus $g \geq 2$ which are hyperelliptic and on the other hand an exercise below shows that plane curves of degree $d \geq 4$ can never by hyperelliptic, thus we know that at least for infinitely many values of g there are non-isomorphic curves of the same genus. So one can ask: How many different isomorphism types of curves of a given genus g are there.

One can show that for any genus g there is a so called **moduli space** M_g of curves of genus g. This means that there is a quasiprojective variety M_g, such that the points of M_g can **in a natural way** be identified with the isomorphism classes of curves of genus g. Here in a natural way means in particular

(1) There is a natural bijection

$$\{\text{isom. classes of curves of genus } g\} \to M_g, E \mapsto [E].$$

Thus M_g parameterizes isomorphism classes of curves of genus g.

(2) If $\pi : X \to Y$ is a morphism of nonsingular quasiprojective varieties, such that all the fibres of $F_y := \pi^{-1}(y)$ are smooth projective curves of genus g (one could call this a family of curves of genus g over Y), then the map $Y \to$

$M_g, y \mapsto [F_y]$ is a morphism. Thus families of curves of genus g correspond to maps to M_g.

Then one can show:

(1) M_0 is a point (this we know).
(2) $M_1 \simeq \mathbb{A}^1$ (in fact the isomorphism is given by the j-invariant).
(3) For $g \geq 2$, M_g is an irreducible quasiprojective variety of dimension $3g-3$.
(4) If $g \geq 2$, then the set of hyperelliptic curves forms a closed subvariety of dimension $2g-1$.

Thus we see in particular that for any genus $g \geq 1$ there are infinitely many isomorphism classes of curves of that genus. We also see in particular that the hyperelliptic curves of genus 2 are a closed subvariety of dimension 3 of M_2, which is irreducible of dimension 3, thus any curve of genus 2 is hyperelliptic. For any genus $g > 2$ there are non-hyperelliptic curves.

An important classical invariant of a curve C is the **gonality**. It is the minimal number n, such that there is a finite morphism $\varphi : C \to \mathbb{P}^1$ of degree n. An exercise below shows that the gonality of any curve of genus g is at most $g+1$.

Exercises.

(1) Let C be a curve of genus g. Show that there is a finite morphism $\varphi : C \to \mathbb{P}^1$ of degree $\leq g+1$.
(2) Show that every curve of genus 2 is hyperelliptic.
(3) Let $\varphi : X \to Y$ be a finite morphism of degree n of curves. We define a homomorphism $\varphi_* : Div(X) \to Div(Y)$ by $\varphi_*(\sum n_i \cdot P_i) := \sum n_i \cdot f(P_i)$.

    Show that $\varphi_* \varphi^*(D) = nD$ for all divisors D on Y.
(4) Let X be a curve of genus 2. Show that a divisor D on X is very ample if and only if $deg(D) \geq 5$.
(5) Let (C, O) be an elliptic curve. Let $P \in C$.
    (a) Show that the map $C \to C; Q \mapsto Q \oplus P$ is an isomorphism.
    (b) Show that the map $\ominus : C \to C, Q \mapsto \ominus Q$ is an isomorphism.
(6) Let C be a nonsingular cubic. Suppose that $\mathbf{0}$ is a flex.
    (a) Show that the flexes of C form a subgroup of C.
    (b) Show that a point $p \in C$ is of order 2 in the group if and only if the tangent line to C at p passes through $\mathbf{0}$.
    (c) Let $C = y^2z = x(x-z)(x-\lambda z)$, with $\lambda \neq 0, 1$ and $\mathbf{0} = [0,1,0]$. Find the points of order 2.

(7) Let C be a nonsingular cubic in given by $y^2z-(x^3+axz^2+bz^3)$, $\mathbf{0}=[0,1,0]$. Let $p_i=(x_i,y_i,1)$ for $i=1,2,3$. Suppose $p_1\oplus p_2=p_3$. Assume $x_1\neq x_2$. Let

$$\lambda := \frac{y_1-y_2}{x_1-x_2}, \quad \mu := y_1-\lambda x_1 = y_2-\lambda x_2.$$

Show that

$$x_3=\lambda^2-x_1-x_2, \quad y_3=-\lambda x_3-\mu.$$

This gives a simple method for computing in the group.

(8) Let $E=y^2z-x^3-4xz^2$, $\mathbf{0}=[0,1,0]$. Let $A:=[0,0,1], B:=[2,4,1], C:=[2,-4,1]$. Show that $\mathbf{0},A,B,C$ form a cylic subgroup of E of order 4.

(9) For which points p on a nonsingular cubic C does there exist a nonsingular conic which intersects C only at p.

(10) Let $C\subset\mathbb{P}^2$ be a smooth cubic curve and let $p,q\in C$ be two points. Show that there is an isomorphism $\varphi: C\to C$ with $f(p)=q$.

(11) A nonsingular point O on a plane curve C is called a flex if $I_O(L,C)\geq 3$ where L is the line tangent to C at O. Let $C=Z(z^{n-1}y-x^n)\subset\mathbb{P}^2$. For which n is $[0,0,1]$ a flex?

(12) Let $C,D\subset\mathbb{P}^2$ be cubic curves and assume that C is nonsingular. Assume that on C we have $(D)=p_1+\ldots+p_9$ for p_i not necessarily distinct points. Let D' be a cubic with $(D')=p_1+\ldots+p_8+q$ on C. Show that $q=p_9$.

(13) Let $[0,1,0]$ be a flex on an irreducible cubic $C=Z(F)$ in $\mathbb{P}^2$. and let $z=0$ be the tangent line at the flex.

Show that

$$F=zy^2+byz^2+cxyz+\text{ polynomial in } x,z.$$

Find a projective change of coordinates to bring F into the form

$$zy^2-\text{cubic in } x,z.$$

(14) Show that a line through two flexes on a cubic passes through a third flex.

(15) This exercise shows that there are nonhyperelliptic curves.

(a) Let C be a curve of degree 4 in $\mathbb{P}^2$. Show that $|K_C|$ is very ample and deduce that C is not hyperelliptic.

(b) More generally, if C is a curve of degree $d\geq 4$ in $\mathbb{P}^2$. Show that C is not hyperelliptic.

References

Introductory Textbooks

[Atiyah-Macdonald] Atiyah, M.F., Macdonald, I.G.*Introduction to commutative algebra*, Addison-Wesley Pub. 1969.
A very useful place to learn the necessary background in commutative algebra for doing algebraic geometry, and also a very good reference book for results of commutative algebra that one might want to use in algebraic geometry.

[Fulton] W. Fulton, *Algebraic curves: an introduction to algebraic geometry*, Benjamin, 1969.
A nice introduction to algebraic geometry, which then specializes to curves. It culminates in a classicalproof of the Riemann-Roch Theorem for curves.

[Kirwan] F. Kirwan, *Complex Algebraic curves*, London Mathematical Society. Student texts. v.23.
This is a nice introduction to algebraic curves over the complex numbers, where one sees the methods of complex algebraic geometry, topology and differential geometry in a relatively simple situation.

[Kunz] E. Kunz, Introduction to commutative algebra and algebraic geometry, Birkhauser 1985.
This is mostly a book on commutative algebra, although it takes its motivation from questions of algebraic geometry.

[Perrin] Perrin, *Geometrie algebrique: une introduction*, InterEditions/CNRS Editions, 1995.
Like the book of Kempf mentioned below it covers abstract varieties and also sheaves and cohomology. It is however considerable easier then the book of Kempf, and therefore still can be considered an introductory book. Many of the more difficult results are not proven or only in special cases.

[Reid] M. Reid, *Undergraduate Algebriaic Geometry*, London Mathematical Society. Student texts. v.12.

An elementary introduction. For most of the course it can also be used as background reading. This course covers similar material.

[Shafarevich] I.R. Shafarevich, *Basic Algebraic Geometry*, Springer-Verlag, 1994.
A standard textbook. It can be used for additional reading for this course.

[Smith et. al] K.E. Smith, L. Kahanpaa, P. Kekalainen, W.N. Traves, *An invitation to Algebraic Geometry*, Springer-Verlag, 2000.
A nicely written book, which gives very good motivation. It is easy to read and succeeds all the same to explain some current research problems of Algebraic Geometry. The price for this is that it does not contain many complete proofs and that some of the statements are unexact. It is as its title says, an invitation to algebraic geometry showing why the subject is interesting.

Advanced Textbooks

[Beauville] A. Beauville, *Complex Algebraic Surfaces*, London Mathematical Society. Student texts. v.34.
In this book the basic tools from sheaves and cohomology are briefly introduced in the beginning, basically without proofs. Then they are put to work to study and classify algebraic surfaces. The book is well-written and gives you a good “hands-on” knowledge on how to use and understand the more advanced tools of algebraic geometry. One finds that these methods are easier to apply, than one would think. The book is very well suited for a second semester in algebraic geometry.

[Eisenbud-Harris1] D. Eisenbud, J. Harris, *The Geometry of Schemes*, Graduate texts in mathematics. v.197, Springer Verlag, 2000.
This book is an introduction to the language of schemes on a more elementary level that the book of Hartshorne. It is well-written and contains nice motivation. It does not develop very much theory.

[Eisenbud-Harris2] D. Eisenbud, J. Harris, *Schemes: the language of modern algebraic geometry*, Wadsworth and Brooks/Cole Advanced Books & Software, 1992.
A shorter version of the previous book, which I actually like more. It gives nice motivation for schemes.

[Griffiths-Harris] P. Griffiths and J. Harris, *Principles of Algebraic Geometry*, Wiley, 1978.
This is the standard advanced textbook for the approach to algebraic geometry via complex analysis and complex differential geometry. Nicely motivated

but rather advanced. One should have previous knowledge in complex analysis, algebraic topology and differential geometry, differential topology.

[Hartshorne] R. Hartshorne, *Algebraic geometry*, Graduate texts in mathematics. v.52, Springer-Verlag, 1977.
The standard advanced textbook for people wanting to become research mathematicians in algebraic geometry. Chapter I covers very fast (also with rather little motivation) material similar to that of this course. The modern techniques (schemes and cohomology) of advanced algebraic geometry are developed in Chapters 2 and 3, which one can try to study after this course. This is a quite advanced book. Chapters 4 and 5 which cover curves and surfaces are much easier to read. The appendices are quite interesting and to some extend readable independently.

[Huybrechts] D. Huybrechts *Complex geometry: an introduction*, Universitext, Springer-Verlag, 2005.
Like the book of Griffiths-Harris it covers the approach to algebraic geometry via complex analysis. The book is however much more elementary and much more readable than Griffiths-Harris. It also covers some problems of current research.

[Kempf] G. Kempf, *Algebraic varieties*, London Mathematical Society. Lecture note series v.172.
An introduction to algebraic geometry at a more advanced level. It covers abstract varieties and also sheaves and cohomology. One can use it instead of Hartshorne as an introduction to the modern techniques. It is easier to read and much shorter than Hartshorne (obviously it also covers less). The book is written a bit terse, so one has to try hard. It does not cover schemes.

[Mumford] D. Mumford, *The Red Book on Varieties and Schemes*, Lecture notes in mathematics. v.1358, Springer-Verlag, 1999.
A very good advanced introduction, not really finished.

Background reading for special topics

[Arbarello et al] E. Arbarello, M. Cornalba, P. Griffiths, J. Harris, *Geometry of algebraic curves*, Grundlehren der mathematischen Wissenschaften, Springer.
This is an advanced book on algebraic curves.

[Cox-Little-O'Shea] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties and Algorithms*, Undergraduate Texts in Mathematics, Springer.
A nice and elementary introduction to computational algebraic geometry. It also develops many of the things that we develop in these notes, but much slower and with many examples. There are also some applications, e.g. to robotics.

[Dieudonne] J. Dieudonne, *History of Algebraic Geometry*, Chapman and Hall, 1985.
For those who want to know about the history of the problems and methods in algebraic geometry.

[Eisenbud] D. Eisenbud, *Commutative Algebra, with a view towards Algebraic Geometry*, Graduate texts in mathematics. v.150, Springer Verlag, 1995.
An advanced book on commutative algebra which contains all the material, that one needs for advanced algebraic geometry.

[Fulton1] W. Fulton, *Algebraic Topology, a first course*, Graduate texts in mathematics. v.153, Springer Verlag, 1995.
This is a very readable book. It is a book on algebraic topology, however in Part X the analytic theory of Riemann surfaces and algebraic curves of $\mathbb{C}$ is developed. In particular it is shown that an algebraic curve of genus g over $\mathbb{C}$ is a surface with g handles. It also contains a construction of the Jacobian of a curve. In Chapter 21 a rather short proof of the Riemann-Roch theorem is given using Adeles.

[Serre] J. P. Serre, *A course in Arithmetic*, Graduate texts in mathematics. v.7, Springer-Verlag, 1973.
The second half of this book is very very short and very clear introduction to modular forms.

[Silverman] J. Silverman, *The arithmetic of elliptic curves*, Graduate texts in mathematics. v.106, Springer-Verlag 1986. This is a very good introduction to the arithmetic of elliptic curves.