Introduction to Algebraic Geometry

Lothar Göttsche

1. Introduction

In algebraic geometry one studies sets of solutions to systems of polynomial equations. The topic is very old: already the ancient Greeks studied the conic sections, i.e. the solutions of polynomial equations of degree 2 in two variables:

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

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

$$\{(a,b) \in \mathbb{R}^2 \mid a^2 + b^2 = 1\}.$$

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 $a^2 + b^2 = c^2$) 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 made a lot of progress in the last century and the beginning of this century, in part due to the so-called Italian school. However the arguments of the Italian school were based in part on intuitive arguments and lacked solid foundations. In the 1920s and the 1930s the foundations of algebraic geometry were laid based on commutative algebra by van der Waerden, Zariski and Weil.

Recently, starting in the 1950s the theory was enormously generalized and made more powerful by the introduction of schemes by Grothendieck. We will not be able to discuss schemes in these lectures. We do however use the modern language which should make it possible to study e.g. the book of Hartshorne afterwards.

The approach to algebraic geometry in this course is based on commutative algebra. This has the disadvantage that one needs some background in algebra. 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 and topology. The point is that over the complex numbers we can view nonsingular algebraic varieties as complex analytic manifolds (with particularly nice properties). Furthermore the famous Theorem of Chow says that any complex analytic sub-manifold X of projective space is a nonsingular algebraic subvariety of projective space, i.e. the zero set of some polynomials. And the famous GAGA theorems of Serre show that all important properties of X remain the same whether we look at X in the complex analytic or the algebraic category.

2. Books

Atiyah-Macdonald, *Commutative Algebra*: A very useful place to learn the necessary background in commutative algebra for doing algebraic geometry.

Fulton, *Algebraic curves*: A nice introduction to algebraic geometry, which then specializes to curves.

Griffiths-Harris, *Principles of Algebraic Geometry*: This is the standard textbook for the approach via complex analysis and complex differential geometry.

Kempf. *Algebraic varieties.* An introduction to algebraic geometry at a somewhat more advanced level. 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). It also does not cover schemes.

Hartshorne, *Algebraic Geometry*: The standard advanced textbook for people wanting to become research mathematicians in algebraic geometry. Chapter one covers very fast (also without 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.

Shafarevich, *Basic Algebraic Geometry*: Another standard textbook, with a more elementary approach then Hartshorne. It can be used for additional reading for this course.

Reid, *Undergraduate Algebraic Geometry*: A nice elementary introduction. For most of the course it can also be used as background reading. This course covers similar material, but it covers more and also more advanced material.

Kirwan, *Complex Algebraic curves*, 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.

3. Algebraic preliminaries

We want to very briefly recall a few elementary facts from algebra that we will use and we 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.

3.1. Polynomials. Let k be a field. We denote by $k[x]$ the ring of polynomials with coefficients in k, i.e. expressions

$$f = \sum_{i=1}^{d} a_i x^i$$

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. We denote by $k[x_1, \dots, x_n]$ the ring of polynomials in n variables. 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

$$f = \sum_{i_1,\dots,i_n}^{d} a_{i_1,\dots,i_n} x_1^{i_1} \dots x_n^{i_n}$$

with $a_{i_1,\dots,i_n} \in k$. 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.

3.2. 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. 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.

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 $I + J = \langle I \cup J \rangle$.

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 an ideal I is maximal if and only if R/I is a 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 $A = R/I$ is an integral domain if and only if I is a 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 $(f, g) \in R$ with $g \neq 0$, where $(f, g) \sim (h, l)$

if $fl = hg$. Addition and multiplication are defined by

$$\frac{f}{g} + \frac{h}{l} = \frac{fl + gh}{gl}, \quad \frac{f}{g} \cdot \frac{h}{l} = \frac{fh}{gl}.$$

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.

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.

Contents

CHAPTER 1

Affine and projective varieties

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, for k an algebraically closed field.

1. Affine 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.

1.1. Affine algebraic sets. An affine algebraic set is the zero set of a set of polynomials in n variables on k^n.

DEFINITION 1.1. n-dimensional *affine space* is $\mathbb{A}^n = \{(a_1 \dots, a_n) \mid a_i \in k\}$. 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

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

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 $f \in k[x_1, \dots, x_n]$ is a non-constant polynomial, then $Z(f)$ is called the *hypersurface* defined by f.

EXAMPLE 1.2. (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 algebraic set.
(3) $Z(x^2 - y^3) \subset \mathbb{A}^2$ is an algebraic set, called the cuspidal cubic.
(4) $Z(y^2 - (x^3 + x^2)) \subset \mathbb{A}^2$ is an algebraic set, called the nodal cubic.

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

(6) Sub-vectorspaces of $\mathbb{A}^n$ are algebraic sets. They are of the form $Z(f_1, \dots, f_r)$ where the f_i are polynomials of degree 1.

Every affine algebraic set in $\mathbb{A}^n$ is the zero set of an ideal in $k[x_1, \dots, x_n]$.

LEMMA 1.3. *(1) if $S \subset T$, then $Z(S) \supset Z(T)$.*
(2) Let $S \subset k[x_1, \dots, x_n]$. Then $Z(S) = Z(\langle S\rangle)$ (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 $\mathbb{A}^n$.

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

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

(2) If $S, T \subset k[x_1, \dots, x_n]$, then $Z(S) \cup Z(T) = Z(ST)$ (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 $p \in Z(\bigcup_\alpha S_\alpha)$.
(2) We have $p \in Z(S) \cup Z(T)$ if and only if for all $f \in S$ and $g \in T$ we have $f(p) = 0$ or $g(p) = 0$. This is equivalent to $(fg)(p) = 0$ for all $f \in S$, $g \in T$, and this is equivalent to $p \in Z(ST)$. □

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 spaces. 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.

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. 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 algebraic set, the closed sets of X are precisely the algebraic sets $Y \subset \mathbb{A}^n$ contained in X.

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 $\mathbb{A}^1$: Recall that $k[x]$ is a principal ideal domain. So every ideal $I \subset k[x]$ is of the form $I = \langle f \rangle$ for a polynomial $f \in k[x]$. Therefore every closed subset of $\mathbb{A}^1$ is of the form $X = Z(f)$. If f is constant, then $Z(f) = \emptyset$ or $\mathbb{A}^1$. Otherwise, as k is algebraically closed, $f = (x - a_1)^{n_1} \cdot \ldots \cdot (x - a_l)^{n_l}$. So $Z(f) = \{a_1, \ldots, a_l\}$.

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 (strong) topology, i.e. all Zariski open sets are open in the strong topology, but most sets which are open in the strong topology are not open in the Zariski topology. Nevertheless the Zariski topology will be useful.

1.3. Hilbert's Nullstellensatz. We have found that to each ideal $I \subset k[x_1, \ldots, x_n]$ we can associate an 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.

DEFINITION 1.10. Let $X \subset \mathbb{A}^n$ be a subset. The *ideal of* X is

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

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

REMARK 1.11. It is clear that $X \subset Y$ implies $I(X) \supset I(Y)$ and we know from above that $I \subset J$ implies $Z(I) \supset Z(J)$. Thus we have inclusion-reversing maps

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

We want to understand to what extend these two maps are inverse to each other. It is easy to see that $Z \circ I$ is the identity:

REMARK 1.12. (1) By definition for any ideal I we have $I(Z(I)) \supset I$.
(2) For any 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 start by looking at the simplest algebraic sets, the points in $\mathbb{A}^n$. As they are the smallest algebraic sets, they should correspond to maximal ideals. If $p = (a_1, \dots, a_n)$ is a point in $\mathbb{A}^n$, then $p = Z(I)$ for $I = \langle x_1 - a_1, \dots, x_n - a_n \rangle$. Furthermore I is a maximal ideal, because $k[x_1, \dots, x_n]/I$ is isomorphic to k and thus is a field. Because I is maximal and $I \subset I(p) \subsetneq k[x_1, \dots, x_n]$, we get $I = I(p) = I(Z(I))$. The weak form of the Hilbert Nullstellensatz now says that these are all the maximal ideals in $k[x_1, \dots, x_n]$.

THEOREM 1.13. *(Weak Hilbert Nullstellensatz). The maximal ideals in $k[x_1, \dots, x_n]$ are precisely the ideals of the form $I(p) = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ for some point $p = (a_1, \dots, a_n) \in \mathbb{A}^n$.*

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 an appendix to these notes.

COROLLARY 1.14. (1) *The maps $p \mapsto I(p)$, $M \mapsto Z(M)$ define inverse bijections*

$$\{\textit{points of } \mathbb{A}^n\} \longleftrightarrow \{\textit{maximal ideals of } k[x_1, \dots, x_n]\}$$
$$p = (a_1, \dots, a_n) \leftrightarrow I(p) = \langle x_1 - a_1, \dots, x_n - a_n \rangle$$

(2) *Every ideal $I \subsetneq k[x_1, \dots, x_n]$ has $Z(I) \neq \emptyset$.*

PROOF. (1) follows directly from the weak Nullstellensatz. (2) I is contained in a maximal ideal $M = I(p)$, thus $Z(I) \supset Z(M) = \{p\}$. □

REMARK 1.15. We have made the assumption that k is algebraically closed. In fact the weak Nullstellensatz and the above Corollary are 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 $Z(x^2 + 1) = \emptyset$.

We have found that I and Z define a bijective correspondence between the points in $\mathbb{A}^n$ and the maximal ideals in $k[x_1, \dots, x_n]$. Now we want to extend this to all algebraic sets.

REMARK 1.16. 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 $I(Z(\langle x^n \rangle)) = I(\{0\}) = \langle x \rangle$.

DEFINITION 1.17. 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 $f^n, g^n \in I$, then the binomial formula $(f+g)^n = \sum_i \binom{n}{i} f^i g^{n-i}$ implies that $(f+g)^{2n} \in I$.

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

REMARK 1.18. Let $X \subset \mathbb{A}^n$ be an 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 $f \in I(X)$. $\square$

Now we show the strong version of the Nullstellensatz, which gives the precise relation between I and $I(Z(I))$.

THEOREM 1.19. *(Strong Hilbert Nullstellensatz) Let $I \subset k[x_1, \dots, x_n]$ be an ideal, then $I(Z(I)) = \sqrt{I}$.*

PROOF. 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. This requires a trick, we apply the weak Nullstellensatz in $k[x_1, \dots, x_n, t]$. Let

$$J := \langle I \cup \{(ft-1)\}\rangle \subset k[x_1, \dots, x_n, t].$$

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

$$1 = g_0(ft-1) + \sum_{i>0} g_i f_i \in k[x_1, \dots, x_n, t], \quad \text{for } g_i \in k[x_1, \dots, x_n, t],\ f_i \in I.$$

Let t^N be the highest power of t occurring in the g_i. Then $g_i f^N$ can be written as $G_i(x_1, \dots, x_n, ft)$ for some polynomial $G_i \in k[x_1, \dots, x_n, u]$. Thus we obtain

$$f^N = (u-1)G_0(x_1, \dots, x_n, u) + \sum_{i>0} f_i G_i(x_1, \dots, x_n, u) \text{ in } k[x_1, \dots, x_n, u],$$

As f does not contain u, we get $f^N = \sum_{i>0} f_i G_i(x_1, \dots, x_n, 1) \in I$ by putting $u := 1$. $\square$

COROLLARY 1.20. *We have mutually inverse inclusion-reversing bijections*

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

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 a finite set of polynomials is always enough. We will then see that this has also geometric consequences for algebraic sets: every affine algebraic set can be decomposed into a finite number of "pieces" which cannot be further decomposed. We need to introduce some algebra.

LEMMA AND DEFINITION 1.21. *The following conditions for a ring R 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 1.22. *Every affine algebraic set $X \subset \mathbb{A}^n$ is the intersection of finitely many hypersurfaces.*

PROOF. It is enough to show that $I(X)$ is finitely generated: If $I(X) = \langle f_1, \dots, f_r \rangle$, 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 1.23. *(Hilbert Basis Theorem) Let R be a Noetherian ring. Then $R[x_1, \dots, x_n]$ is 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

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

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} would lie in $\langle f_1, \dots, f_k \rangle$). On the other hand $deg(g) < n_{k+1}$, which contradicts the choice of f_{k+1}. □

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 $Z(y)$. An affine algebraic set will be called irreducible if it cannot be written as the union of two smaller algebraic sets. We want to show that every affine algebraic set can be written in a unique way as a union of irreducible algebraic sets, 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 1.24. 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 1.25. Let X be an irreducible topological space and let $U \subset X$ be a nonempty open subset.

(1) U is dense in X. (Because otherwise $X = X \setminus U \cup \overline{U}$).
(2) U is irreducible. (If $U = U_1 \cup U_2$, with $U_i \subsetneq U$ closed, then put $X_i = \overline{U}_i$, the closure in X. Then $X_i \subsetneq X$ because $U_i = U \cap X_i \neq U$, and $X_1 \cup X_2 = \overline{U} = X$.)

The notion of irreducibility does not make much sense in the strong topology. The only irreducible subsets of a Hausdorff space are the points. In future we will mostly want to study irreducible algebraic sets. They are called closed subvarieties of $\mathbb{A}^n$.

DEFINITION 1.26. An irreducible affine algebraic set is called a *closed subvariety* of $\mathbb{A}^n$. An open subset of an affine variety is called a *locally closed subvariety* of $\mathbb{A}^n$.

EXAMPLE 1.27. (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.

We said that the algebraic properties of $I(X)$ should reflect the geometric properties of $X \subset \mathbb{A}^n$. The first instance of this is the following.

PROPOSITION 1.28. (1) *An algebraic set $X \subset \mathbb{A}^n$ is a closed subvariety if and only if $I(X)$ is a prime ideal, or equivalently if $X = Z(I)$ for I a prime ideal.*
(2) *If $f \in k[x_1, \dots, x_n]$ is irreducible, then $Z(f)$ is irreducible.*

PROOF. (1) The two statements are equivalent, because every prime ideal is a radical ideal, thus if I is a prime ideal, then by the Nullstellensatz $I = I(Z(I))$.

"$\Leftarrow$" 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 $g \in I(X)$.

"$\Rightarrow$" Assume $X = X_1 \cup X_2$ for algebraic subsets $X_1, X_2 \subsetneq X$. Then $X_1 \subsetneq X$ implies that 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.

(2) 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. Thus the result follows from (1). □

Now we want to show that every affine algebraic set X is the union of finitely many irreducible algebraic sets. We use that the Zariski topology is Noetherian.

DEFINITION 1.29. 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 1.30.
(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 $Y_i = Y \cap X_i$ for $X \supset X_1 \supset X_2 \supset \dots$ a descending chain of closed subsets in X, thus it becomes stationary.
(2) As $k[x_1, \dots, x_n]$ is a Noetherian ring, every ascending chain of ideals becomes stationary, and thus any descending chain $\mathbb{A}^n \supset Z(I_1) \supset Z(I_2) \supset \dots$ of closed subsets becomes stationary, i.e. $\mathbb{A}^n$ is a Noetherian topological space. By (1) also any (open subset of) an affine algebraic set is Noetherian.

THEOREM AND DEFINITION 1.31. *Every Noetherian topological space X is up to reordering in a unique way a finite union $X = X_1 \cup \dots \cup X_r$ 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 $X_1, X_2 \subsetneq X$. Furthermore one of the two (say X_1) cannot a finite decomposition into irreducible closed subsets, in particular it is reducible. Continuing in this way we obtain a descending chain $X \subsetneq X_1 \subsetneq X_2 \subsetneq \dots$ of closed subsets, which is a contradiction to X being Noetherian.

(Uniqueness) Let $X = X_1 \cup \dots \cup X_r = Y_1 \cup \dots \cup Y_s$ be two such decompositions. Then $X_i = \bigcup_j (Y_j \cap X_i)$ so by the irreducibility of X_i we get $X_i \subset Y_{j(i)}$ for some $j(i)$. Similarly $Y_{j(i)} \subset X_k$ for some k. Thus $X_i \subset X_k$, which implies $i = k$ and $X_i = Y_{j(i)}$. 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. □

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

DEFINITION 1.32. Let $X \neq \emptyset$ be an irreducible topological space. The *dimension* $dim(X)$ of X is the largest integer n such that there is an ascending chain

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

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 1.33. (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 $\mathbb{A}^0 \subset \mathbb{A}^1 \subset \mathbb{A}^2 \dots$. Later when we have developed the theory further, we will study dimension carefully.

2. Projective varieties

Over the complex numbers and with the strong 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. So we want in some sense to compactify affine varieties. This is done by adding points at infinity and looking at projective space and projective varieties, which are zero sets of homogeneous polynomials on projective space. These are now compact in the strong topology. We shall see later that also as varieties they have a similar property.

2.1. Projective algebraic sets.

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 $\mathbb{P}^n$ is the space of lines in k^{n+1} through the origin.

We can view $\mathbb{P}^n$ as being obtained from $\mathbb{A}^n$ by adding points at infinity.

DEFINITION 2.2. Let

$$U_i := \{[a_0, \dots, a_n] \in \mathbb{P}^n \mid a_i \neq 0\}, \quad i = 0, \dots, n.$$

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

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

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. We identify $\mathbb{A}^n$ and U_0 by identifying $(a_1, \dots, a_n)$ with $[1, a_1, \dots, a_n]$. Thus $\mathbb{A}^n$ is 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 $H_\infty := \mathbb{P}^n \setminus U_0 = \{[a_0, a_1, \dots, a_n] \mid a_0 = 0\}$ the *hyperplane 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 $[1, 1] = [-1, -1]$. This problem is not there, if f is homogeneous.

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

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

So the question whether $g(a_0, \dots, a_n) = 0$ depends only on $[a_0, \dots, a_n]$. (The proof is an easy exercise).

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

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

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 of a set of polynomials, we write $Z_p(S)$ for the projective zero set and $Z_a(S)$ for the affine zero set.

EXAMPLE 2.5.
(1) $\emptyset = Z(1)$; $\mathbb{P}^n = Z(0)$ 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 $\mathbb{P}(V) := \{[a_0, \dots, a_n] \mid (a_0, \dots, a_n) \in V\}$ is called a *projective subspace* of $\mathbb{P}^n$ of dimension l. V can be written as the kernel of a matrix

$$V = ker \begin{pmatrix} c_{10} & \dots & c_{1n} \\ \dots & \dots & \dots \\ c_{r0} & \dots & c_{rn} \end{pmatrix} \quad (r = n - l).$$

Then we get

$$\mathbb{P}(V) = Z(c_{10}x_0 + \dots + c_{1n}x_n, \dots, c_{r0}x_0 + \dots + c_{rn}x_n).$$

Conversely every zero set $Z(f_1, \dots, f_r)$ of linear forms f_i is a projective subspace.

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.

Definition 2.6. Any polynomial $f \in k[x_0, \dots, x_n]$ can be written in a unique way as a sum $f = f^{(0)} + \dots + f^{(d)}$ 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). Thus we get $f^{(d)} = \sum_i a_i^{(d-deg(f_i))} f_i \in I$. □

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

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

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

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

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 $I_H(X)$.

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

Proposition 2.9.

1. *If $X \subset Y$, then $I(X) \supset I(Y)$.*
2. *If $Y \subset \mathbb{P}^n$ is closed, then $Z(I(Y)) = Y$.*
3. *For any homogeneous ideal $J \subset k[x_0, \dots, x_n]$ 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 $Z(ST) = Z(S) \cup Z(T)$.*

This proposition allows us to introduce a topology on $\mathbb{P}^n$ for which the closed subsets are the projective algebraic sets.

Definition 2.10. 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*.

Remark 2.11. As $k[x_0, \dots, x_n]$ is Noetherian, and every closed subset of $\mathbb{P}^n$ is the zero set of an ideal, we see that $\mathbb{P}^n$ and thus any subspace of $\mathbb{P}^n$ is a Noetherian topological space. In particular every open subset of a projective algebraic set has a decomposition into irreducible components.

Again we will mostly be interested in irreducible algebraic sets, the varieties.

Definition 2.12. A *projective variety* is an irreducible projective algebraic set. A *quasiprojective variety* is an open subset of a projective variety. A *variety* is a locally closed subvariety of $\mathbb{A}^n$ or $\mathbb{P}^n$.

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

2.3. Affine cones and the projective Nullstellensatz. Now we give a correspondence between the projective algebraic sets and the homogeneous ideals in $k[x_0, \dots, x_n]$, which is very similar to the affine case. In fact the proof can be reduced to the affine case by making use of cones.

Definition 2.13. 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

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

Obviously this is a cone.

The following is obvious from the definition.

Lemma 2.14. *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.

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

Theorem 2.15. *(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 $C(X) = Z_a(I)$ is either empty or $\{0\}$. By the Nullstellensatz, this is equivalent to $\sqrt{I} = I(C(X)) \supset \langle x_0, \ldots, x_n \rangle$. Therefore for each $i = 0, \ldots, n$ there exists j_i with $x_i^{j_i} \in I$. We can take $N := j_0 + \ldots + j_n$.

(2) $I_H(X) = I(C(X)) = I(Z_a(I)) = \sqrt{I}$, by the Nullstellensatz. □

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

COROLLARY 2.16. I_H *and* Z_p *are mutually inverse bijections between non-irrelevant homogeneous radical ideals* $I \subset k[x_0, \ldots x_n]$ *and projective algebraic sets* $X \subset \mathbb{P}^n$.

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

PROPOSITION 2.17. (1) *A projective algebraic set* $X \subset \mathbb{P}^n$ *is a projective variety if and only if* $I_H(X)$ *is a prime ideal, or equivalently if* $X = Z_p(I)$ *for* I *a prime ideal.*
(2) *A hypersurface* $Z_p(f) \subset \mathbb{P}^n$ *is irreducible, if and only if* $f \in k[x_0, \ldots, x_n]$ *is irreducible.*

PROOF. (1) We only need to prove the first statement. The second then follows from the projective Nullstellensatz, because prime ideals are radical. Thus if I is a prime ideal, then $I_H(Z_p(I)) = I$.

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 $I_P(X) = I(C(X))$ 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 $f^{(i)}g^{(j)} \in I$, and we can assume that f, g are homogeneous. Let $X_1 = Z_p(I \cup \{f\})$, $Y_2 = Z_p(I \cup \{g\})$. Then $X = X_1 \cup X_2$ is reducible. (2) follows in the same way as in the affine case. □

CHAPTER 2

Functions and Morphisms

The best way to study spaces with a structure (vector spaces, topological spaces, differentiable manifolds), is usually to look at the maps between them preserving the structure (linear maps, continuous maps, differentiable maps). An important special case is usually the functions, i.e. the maps to the ground field k (linear forms, continuous functions, differentiable functions). In this chapter we want to define and study these functions and maps for varieties.

1. Regular and rational functions

We will define regular functions on varieties, the analogues of differentiable functions in differential geometry. As algebraic varieties are zero sets of polynomials, one should expect that the functions are just polynomials. It turns out that these are not quite enough, we also need quotients of polynomials.

1.1. Regular functions on affine 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.

Definition 1.1. The *coordinate ring* of X is

$$A(X) := k[x_1, \dots, x_n]/I(X).$$

The class of $F \in k[x_1, \dots, x_n]$ in $A(X)$ is denoted by $[F]$. $A(X)$ is an integral domain because $I(X)$ is a prime ideal.

Example 1.2. If $X = Z(x_1 - x_2^2) \subset \mathbb{A}^2$, then $A(X) = k[x_1, x_2]/(x_1 - x_2^2) \simeq k[x]$.

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

Definition 1.3. Let $X \subset \mathbb{A}^n$ be a closed subvariety. A *polynomial function* $f : X \to k$ on X is the restriction $F|_X$ of a polynomial $F \in k[x_1, \dots, x_n]$, i.e. $f(p) = F(p)$ for all $p \in X$. Polynomial functions form a ring by pointwise addition and multiplication:

$$(f + g)(p) = f(p) + g(p), \quad (fg)(p) = f(p)g(p).$$

Polynomials $F, G \in k[x_1, \dots, x_n]$ define the same polynomial function if and only if $F - G \in I(X)$. Thus the ring of polynomial functions on X is canonically isomorphic to $A(X)$. In future we will identify the two.

Now we define regular functions on locally closed subvarieties of $\mathbb{A}^n$. These will be quotients of polynomial functions.

Reminder 1.4. 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 1.5. The quotient field $K(X)$ of $A(X)$ is called the *field of rational functions* on X. We put $K(V) := K(X)$ and call it the field of rational functions on V. Elements of $K(X)$ (resp. $K(V)$) are called *rational functions* on X (resp. on V).

Rational functions on V are functions on an open subset of V.

Definition 1.6. 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 1.7. (1) A regular function h on U 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 $\frac{f(p)}{g(p)} = \frac{f'(p)}{g'(p)}$.

(2) If $h \in K(V)$ is a rational function, then we can write $h = \frac{[F]}{[G]}$ with $F, G \in k[x_1, \dots, x_n]$ 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.

(3) If furthermore $h \in \mathcal{O}_{V,p}$, then we can choose G with $G(p) \neq 0$, i.e. an element of the local ring at p defines a regular function in a neighborhood of p.

The map $h \mapsto h(\ )$ identifies $\mathcal{O}_V(U)$ with the set of functions $U \to k$ which are locally the quotients of polynomials.

Lemma 1.8. *Denote by $O(U) \subset \{\text{functions } U \to k\}$ the subring of functions $h : U \to k$ with the following property: For each $p \in U$ there is an open neighborhood $W \subset U$ and $F, G \in k[x_1, \dots, x_n]$, such that for all $q \in W$, $G(q) \neq 0$ and $h(q) = \frac{F(q)}{G(q)}$.*

The map $\alpha : \mathcal{O}_V(U) \to O(U), h \mapsto h(\ )$ is an isomorphism.

PROOF. First we need to see that the image of α is in $O(U)$. Let $h \in \mathcal{O}_V(U)$, and let $p \in U$. Then we can write $h = \frac{[F]}{[G]}$ for $F, G \in k[x_1, \dots, x_n]$ with $G(p) \neq 0$. Thus on the neighborhood $W = U \setminus Z(G)$ of p we have $h(q) = \frac{F(q)}{G(q)}$.

Now we give the inverse map $\beta : O(U) \to \mathcal{O}_V(U)$. Let $m \in O(U)$. Let $p \in U$ and let W be an open neighborhood of p and $F, G \in k[x_1, \dots, x_n]$ with $m(q) = \frac{F(q)}{G(q)}$ and $G(q) \neq 0$ on W. Then we put $h := \frac{[F]}{[G]}$. We claim that $\beta(m) := h$ is the inverse map to α. This is trivial from the definitions, once we know it is well defined, i.e. independent of the choice of F, G.

If on an open neighborhood W' of a point p' we have $m(q) = \frac{F'(q)}{G'(q)}$, then, as V is irreducible $W'' := W \cap W'$ is open and dense in X. On W'' we have $\frac{F(q)}{G(q)} = \frac{F'(q)}{G'(q)}$, i.e. $FG' - G'F$ vanishes on W'', and thus on X. Thus $[F][G'] - [G'][F] = 0$ and therefore $\frac{[F]}{[G]} = \frac{[F']}{[G']}$. $\square$

We will therefore in future identify these two rings and view elements of $\mathcal{O}_V(U)$ as functions $U \to k$.

REMARK 1.9. 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 a closed subvariety of $\mathbb{A}^n$ the regular functions are just the polynomial functions:

PROPOSITION 1.10. *Let $X \subset \mathbb{A}^n$ be a closed subvariety. 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 $G(p) \neq 0$. Let

$$J := \left\{G \in k[x_1, \dots, x_n] \;\middle|\; h = \frac{[F]}{[G]}, \text{ for some } F \in k[x_1, \dots, x_n]\right\}$$

Then J is an ideal in $k[x_1, \dots, x_n]$, and by the assumption $h \in \mathcal{O}_X(X)$ we see $Z(J) = \emptyset$. By the Nullstellensatz $1 \in J$. Thus there exists an $F \in k[x_1, \dots, x_n]$ with $h = \frac{[F]}{1} \in A(X)$. $\square$

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.

DEFINITION 1.11. Let $I(X)$ be the homogeneous ideal of X. The *homogeneous coordinate ring* of X is $S(X) := k[x_0, \dots, x_n]/I(X)$. The class of $F \in k[x_1, \dots, x_n]$ in $S(X)$ is denoted by $[F]$. Again $S(X)$ is an integral domain.

REMARK 1.12. 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 1.13. 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

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

Elements of $K(V)$ are called *rational functions* on V.

DEFINITION 1.14. Let $p \in V$. The *local ring* of V at p is $\mathcal{O}_{V,p} := \left\{ \frac{f}{g} \in K(V) \mid g(p) \neq 0 \right\}$. For $U \subset V$ an open subset, the ring of regular functions on U is the subring

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

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

REMARK 1.15. 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 $q \in W$.

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

REMARK 1.16. By the above a rational 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 $U \to k$.

REMARK 1.17. Let $h \in \mathcal{O}_V(U)$. Then $h : U \to k$ is continuous ($k = \mathbb{A}^1$ is given the Zariski topology).

PROOF. 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 $h(q) = \frac{F(q)}{G(q)}$ with F, G polynomials (of the same degree in the quasiprojective case) for all $q \in U$. 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 $h^{-1}(a) = \{q \in U \mid F(q) = aG(q)\} = Z(F - aG) \cap U$. □

DEFINITION 1.18. 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.

2. Morphisms

2.1. Definition of a 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.

DEFINITION 2.1. 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 2.2. (1) The identity map $id_X : X \to X$ is regular, and $id_X^* = id_{\mathcal{O}_X(U)}$ for all U.
(2) If $\varphi : X \to Y$, $\psi : Y \to Z$ are morphisms of varieties, then the composition $\psi \circ \varphi$ is a morphism and $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.

DEFINITION 2.3. 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 2.4. (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 $\varphi^{-1}(W)$.

(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 $h \circ \varphi|_Z = H \circ \varphi|_{\varphi|_Z^{-1}(U)} \in \mathcal{O}(\varphi|_Z^{-1}(U))$. □

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

DEFINITION 2.5. A variety X is called *affine variety* if it is isomorphic to a an irreducible closed subset of some affine space $\mathbb{A}^n$.

2.2. 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 2.6. *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. So $\varphi^{-1}(W)$ is closed.

Now let $h \in \mathcal{O}_Y(U)$. Let $q \in U$. Then there exists an open neighborhood W of q such that $h(s) = \frac{F(s)}{G(s)}$ for polynomials F, G with $G(s) \neq 0$ for all $s \in W$. So for all $t \in V := \varphi^{-1}(W)$

$$\varphi^*(h)(t) = \frac{F(f_1(t), \dots, f_n(t))}{G(f_1(t), \dots, f_n(t))}.$$

As $\mathcal{O}_{X,t}$ is a k-algebra, $F(f_1, \dots, f_n), G(f_1, \dots, f_n) \in \mathcal{O}_{X,t}$ and as $G(f_1(t), \dots, f_n(t)) \neq 0$ we get that $G(f_1, \dots, f_n)$ is a unit in $\mathcal{O}_{X,t}$. Thus $\varphi^*(h) \in \mathcal{O}_{X,t}$ for all $t \in V$, i.e. it is regular on V. □

COROLLARY 2.7. *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 given by polynomials.

DEFINITION 2.8. Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be closed subvarieties. A map $\varphi : X \to Y$ is called a *polynomial map* if there exist $F_1, \dots, F_m \in k[x_1, \dots, x_n]$ such that $\varphi(p) = (F_1(p), \dots, F_n(p))$ for all $p \in X$. We then also write $\varphi = (F_1, \dots, F_n)$.

COROLLARY 2.9. *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 $\mathcal{O}_X(X) = A(X)$. □

EXAMPLE 2.10.
(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
$$\varphi^* : k[C] = k[x, y]/(x^2 - y^3) \to k[t]; x \mapsto t^3,\ y \mapsto t^2$$
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 2.11. 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 2.12. *X_F is an affine variety.*

PROOF. Let $Z := Z(\langle I(X), (Fx_{n+1} - 1)\rangle) \subset \mathbb{A}^{n+1}$. 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 injective 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. □

2.3. Morphisms to quasiprojective varieties. Before we had 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 the map $\varphi_i : U_i \to \mathbb{A}^n, [a_0, \dots, a_n] \mapsto (\frac{a_0}{a_i}, \dots, \widehat{\frac{a_i}{a_i}}, \dots, \frac{a_n}{a_i})$ 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 want to show that φ_i is an isomorphism. It follows in particular that every locally closed subvariety of $\mathbb{A}^n$ is isomorphic to a quasiprojective variety.

DEFINITION 2.13. For $F \in k[x_0, \dots, x_n]$ the *dehomogenization* is

$$F_a := F(1, x_1, \dots, x_n) \in k[x_1, \dots, x_n].$$

THEOREM 2.14. (1) *$\varphi_i : U_i \to \mathbb{A}^n$ is an isomorphism.*
(2) *Every variety is isomorphic to a quasiprojective variety.*

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 $\frac{x_1}{x_0}$ 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

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

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. □

REMARK 2.15. (1) Above we said that we want to identify $(a_1, \dots, a_n) \in \mathbb{A}^n$ with $[1, a_1, \dots, a_n]$, 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 should 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.

Now we show that every variety has an open cover by affine varieties. This will allow us to reduce many proofs to the case of affine varieties.

THEOREM 2.16. *Every variety has an open cover by affine varieties.*

Proof. 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. $\square$

We have found a simple description of morphisms to affine varieties. Now we give a similar description of morphisms to quasiprojective varieties.

Theorem 2.17. *Let $X \subset \mathbb{P}^m$ and $Y \subset \mathbb{P}^n$ be quasiprojective varieties. A map $\varphi : X \to Y$ is a morphism, if and only if, for all $p \in X$ there exists an open neighbourhood $U \subset X$ and polynomials $F_0, \ldots, F_n \in k[x_0, \ldots, x_m]$ of the same degree, with no common zero on U such that*

$$\varphi(q) = [F_0(q), \ldots, F_n(q)] \quad \textit{for all } q \in U.$$

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

Proof. 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

$$\varphi|_U = (h_1, \ldots, h_n) = [1, h_1, \ldots, h_n], \quad h_i \in \mathcal{O}_X(U).$$

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 $G := G_1 \ldots G_n$, $L_i := F_i G_1 \ldots \widehat{G}_i \ldots G_n$. Then G and the L_i are homogeneous polynomials of the same degree, and

$$\varphi|_U = (h_1, \ldots, h_n) = [1, h_1, \ldots, h_n] = [G, L_1, \ldots, L_n].$$

On the other hand assume that in a neighborhood U of p, we have $\varphi|_U = [H_0, \ldots, H_n]$, 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 $\varphi|_U = (h_1, \ldots, h_n) : U \to \mathbb{A}^n$ is a morphism. Thus φ is a morphism in a neighborhood of every point, thus it is a morphism. $\square$

Example 2.18. Let $X = \mathbb{P}^1$, $Y = Z(y_0 y_2 - y_1^2) \subset \mathbb{P}^2$. $\varphi = [x_0^2, x_0 x_1, x_1^2] : X \to Y$ 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 $\varphi \circ \varphi^{-1} = [y_0^2, y_0 y_1, y_1^2] = [y_0^2, y_0 y_1, y_0 y_2] = [y_0, y_1, y_2]$.

Definition 2.19. (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 $H_1, \ldots, H_{n-k}$ such that $W = Z(H_1, \ldots, H_{n-k})$. The *projection from W* is the morphism $\pi_W = [H_1, \ldots, H_{n-k}] : X \to \mathbb{P}^{n-k-1}$. That $W \cap X = \emptyset$ means precisely that the H_i never vanish simultaneously on X. The most important case is the *projection from a point*. In particular the projection from $P = [0, \dots, 0, 1] \in \mathbb{P}^n$ is $\pi_P = [x_0, \dots, x_{n-1}]$.

REMARK 2.20. (1) We can identify $\mathbb{P}^{n-1}$ with $Z(x_n) \subset \mathbb{P}^n$, via $[a_0, \dots, a_{n-1}] \mapsto [a_0, \dots, a_{n-1}, 0]$. 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.

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

DEFINITION 2.21. 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, 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.

PROPOSITION 2.22. *(Fundamental theorem on projective transformations) Let $(p_0, \dots, p_{n+1})$, $(q_0, \dots, q_{n+1})$ be two $n+2$-tuples of points in $\mathbb{P}^n$ so that no $n+1$ of the p_i or of the q_i are linearly dependent (as vectors in k^{n+1}). Then there exists a unique projective linear transformation $[A] : \mathbb{P}^n \to \mathbb{P}^n$ with $[A](p_i) = q_i$ for all i.*

PROOF. We just show existence, uniqueness is an easy exercise. For $i = 0, \dots, n$ let $e_i \in \mathbb{P}^n$ be the point with i-th coordinate 1 and all other coordinates 0. Let $e_{n+1} := [1, \dots, 1]$. We can assume that $p_i = e_i$. Otherwise let $[P]$ be a projective linear transformation sending the e_i to p_i, and Q one sending the e_i to q_i, then we can put $[A] = [Q \circ P^{-1}]$.

For $i = 0, \dots, n$ let $q_i = [a_{i0}, \dots, a_{in}]$, let $q_{n+1} = [b_0, \dots, b_n]$. Choose $\lambda_0, \dots, \lambda_n$, so that $(b_0, \dots, b_n) = \sum_i \lambda_i (a_{i0}, \dots, a_{in})$. Note that the λ_i are all nonzero (if e.g. $\lambda_n = 0$, then $q_0, \dots, q_{n-1}, q_{n+1}$ are linearly dependent). Put $A := (\lambda_i a_{ij})_{ij}$. Then for $i = 0, \dots, n$ we get $[A](e_i) = [\lambda_i a_{ij}]_j = q_i$ and $[A](e_{n+1}) = [\sum_i \lambda_i a_{ij}]_j = q_{n+1}$. $\square$

3. Products

Some important properties of varieties and morphisms $\varphi : X \to Y$ of varieties are best understood in terms of the product $X \times Y$. Now we want to define and study these products.

3.1. Products of affine varieties. The definition of the product of affine varieties is very simple.

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_i, y_j 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. $\square$

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

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

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 $\mathbb{P}^N$:*

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

(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 $\mathbb{P}\big(\big\{[b_j a_i]_{ij} \mid a_0,\dots,a_n \in k\big\}\big)$.

(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 $i_q : \mathbb{P}^n \to \mathbb{P}^N$. $\square$

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.

EXAMPLE 3.9. 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 3.10. *(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 show this for p_1. We can assume that $X = \mathbb{P}^n$ and $Y = \mathbb{P}^m$, because in general p_1 is just the restriction $p_1|_X$. It is enough to show that $p_1|_{\Sigma^{ij}}$ is a morphism, because the Σ^{ij} form an open cover. We can assume $i = j = 0$. Then $p_1 = [z_{00}, z_{10}, \ldots, z_{n0}]$ 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 $Z^{ij} = (f, g)^{-1}(U_{ij}) = f^{-1}(U_i) \cap g^{-1}(U_j)$. Then Z^{ij} is open in Z and (f, g) is a morphism if and only if its restriction $(f, g)|_{Z_{ij}} : Z_{ij} \to \Sigma^{ij}$ is a morphism for all i, j, and this is equivalent to $(\sigma^{ij})^{-1} \circ (f, g) : Z_{ij} \to \varphi_i(X) \times \varphi_j(Y)$ being 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 3.11. 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 3.12. *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 $f^{-1} \times g^{-1}$. □

We want to describe the closed subsets of $\mathbb{P}^n \times \mathbb{P}^m$. They are the zero sets of bihomogeneous polynomials.

LEMMA 3.13. *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. By definition we need to show that $\sigma(W) \subset \mathbb{P}^N$ is closed if and only if W is the zero set of a set of bihomogeneous polynomials. Let $\sigma(W)$ 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 $W = Z(f_1(x_i y_j), \dots, f_r(x_i y_j))$ where the $f_k(x_i y_j)$ 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. Let f_k be homogeneous in the x_i of degree d and homogeneous in the y_j of degree $d+e$. Then we can replace f_k by $x_0^e f_k, \dots, x_n^e f_k$, which has the same zero set, similarly if the degree in the x_i is larger than that in the y_j. So we can assume that the f_k have the same degree in the x_i and in the y_j, but then they are polynomials $g_k(x_i y_j)$ in the $x_i y_j$, and by definition $Z(g_1(x_i y_j), \dots, g_r(x_i y_j)) = \sigma^{-1}(Z(g_1(z_{ij}), \dots, g_r(z_{ij}))$. □

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

DEFINITION 3.14. 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 3.15. *$\Delta_X \subset X \times X$ 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 3.16. The fact that Δ_X is closed in $X \times X$ is very important. It is what replaces the *Hausdorff* property in the strong 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.

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

DEFINITION 3.17. 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 3.18. *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 strong 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 strong 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 3.19. 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 3.20. $\mathbb{A}^1$ 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 3.21. *$p_1 : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^n$ is closed.*

PROOF. 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 as above one replaces f_j with a lower degree by $y_0^e f_j, \dots, y_n^e f_j$).

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). Then (1) is *false* if and only if there are polynomials $g_{ij}(y)$, such that

$$M_i(y) = \sum_j g_{ij}(y) f_j(P, y) \quad \text{for all i.}$$

As the $M_i(y)$ are homogeneous of degree s and the $f_j(P, y)$ are homogeneous of degree d, the relation then also holds if we replace the g_{ij} by their homogeneous components of degree $s-d$. So we can assume that the g_{ij} are homogeneous of degree $s-d$. Denote by $N_i(y)$ the homogeneous polynomials in the y_i of degree $s-d$ (in any order). Then (1) is false if and only if the set of polynomials

$$\left\{ N_i(y) f_j(P, y) \;\middle|\; 1 \leq s \leq \tbinom{m+s-d}{m},\ 1 \leq j \leq r \right\}$$

generates the vector space of all polynomial of degree s. We denote the $N_i(y) f_j(x, y)$ by $G_k(x, y)$ in any order. We write $G_j(x, y) = \sum_i A_{ij}(x) M_i(y)$ with $A_{ij}(x) \in k[x]$ homogeneous. Then (1) is not satisfied if and only if the matrix $(A_{ij}(P))_{ij}$ has the full rank $\binom{m+s-d}{m}$. Thus the set of points where (1) holds is the zero set of all the $\binom{m+s-d}{m}$-minors of $(A_{ij}(x))_{ij}$, which are homogeneous polynomials in the x_i. Thus it is closed. $\square$

It is now rather easy to deduce the general case.

THEOREM 3.22. *$\mathbb{P}^n$ and any projective variety are complete.*

PROOF. First we show it for $\mathbb{P}^n$. Let Y be a variety. If $Y \subset \mathbb{A}^m$, 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 $\mathbb{P}^n$, thus $p_2(Z)$ is closed in Y. $\square$

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

COROLLARY 3.23. *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. $\square$

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

COROLLARY 3.24. (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 3.25. (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 3.26. *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. □

CHAPTER 3

Dimension and Nonsingularity

1. Dimension

In the first chapter we briefly introduced the notion of dimension of a variety. 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

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

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 $B = Ab_1 + \dots + Ab_n$.

Proposition 1.2. (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*

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

(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

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

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. $\square$

Definition 1.3. 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 1.4.
(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 1.2. In particular if $\varphi : X \to Y$ be a finite morphism with $\varphi(X) \subset W$ for $W \subset Y$ closed, then $\varphi : X \to W$ is finite.
(4) On can show that finite morphisms are closed. We will not use this result, instead we will always prove directly that all finite morphisms $f : X \to \mathbb{A}^k$ that we use are closed: They are restrictions of morphisms $\overline{f} : \overline{X} \to \mathbb{P}^k$, where $\overline{X}$ is the projective closure of X and $\overline{f}^{-1}(\mathbb{A}^k) = X$. If $Z = \overline{Z} \cap X \subset X$ is closed, with $\overline{Z}$ closed in $\overline{X}$, then $f(Z) = \overline{f}(\overline{Z}) \cap \mathbb{A}^k$ is closed in $\mathbb{A}^k$.

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

Theorem 1.5. *(Noether Normalization Theorem)*
(1) *Let X be an affine variety. Then there exists a finite surjective morphism $\pi : X \to \mathbb{A}^k$ for some k.*
(2) *In case $X = Z(F) \subset \mathbb{A}^n$ for a nonconstant polynomial $F \in k[x_1, \dots, x_n]$ we have $k = n - 1$.*

Proof. (2) Let $X = Z(F)$, let $d := deg(F)$ and $F_H := x_0^d F(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0})$. Then $F_H \in k[x_0, \dots, x_n]$ is homogeneous of degree d and $Z(F_H) \cap \mathbb{A}^n = Z(F)$. By definition x_0 does not divide F_H, thus $F_H(0, x_1, \dots, x_n) \neq 0$. Therefore there is a point $p := [0, a_1, \dots, a_n] \in H_\infty$ with $F_H(p) \neq 0$. Applying a linear isomorphism $\varphi : \mathbb{A}^n \to \mathbb{A}^n$, we assume that $p = [0, \dots, 0, 1]$. Let $\pi = (x_1, \dots, x_{n-1}) : X \to \mathbb{A}^{n-1}$. Then $\pi = \overline{\pi}|_{Z(F)}$, where $\overline{\pi} = [x_0, \dots, x_n] : Z(F_H) \to \mathbb{P}^{n-1}$ is the projection form p. Note that $Z(F) = \overline{\pi}^{-1}(\mathbb{A}^{n-1})$. Thus π is closed.

Let $w_n \in A(X)$ be the class of x_n. Then $A(X) = \pi^*(k[x_1, \dots, x_{n-1}])[w_n]$. As $F_H(0, \dots, 0, 1) \neq 0$, we can assume that $F_H(0, \dots, 0, 1) = 1$, i.e. the coefficient of x_n^d of F_H and of F is 1, i.e. $F = x_n^d + \sum_{i=0}^{d-1} a_i x_n^i$ 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.

Finally 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

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

(1) 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 $F \in I(X) \backslash 0$. Then by part (2) there exist a finite closed morphism $\pi : Z(F) \to \mathbb{A}^{n-1}$. The inclusion $X \hookrightarrow Z(F)$ is a closed and finite morphism, thus the composition $\tilde{\pi} : X \to \mathbb{A}^{n-1}$ is closed and finite, let $Y \subset \mathbb{A}^{n-1}$ be its image. Then by induction there is a finite closed surjective morphism $\varphi : Y \to \mathbb{A}^k$. The composition $\varphi \circ \tilde{\pi} : X \to \mathbb{A}^k$ is a finite closed surjective morphism. □

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

LEMMA 1.6. *Let $\varphi : X \to Y$ be a finite closed 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 and closed. 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 $\varphi^*(a_0) = -g(g^{n-1} + \sum_{i=1}^{n-1} \varphi^*(a_i) g^{i-1}) \in \langle g \rangle$. Therefore $\varphi^*(a_0)|_Z = 0$ and thus $a_0|_{\varphi(Z)} = 0$, i.e. $\varphi(Z) \subsetneq Y$. □

COROLLARY 1.7. *Let $\varphi : X \to Y$ be a finite closed 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. Dimension. Now we want to use finite morphisms to study the dimension of varieties. The main point is that finite closed surjective morphisms preserve dimension. Then the Noether Normalization Theorem allows us to reduce questions about dimension to questions in $\mathbb{A}^k$.

DEFINITION 1.8. Let X be a variety. Let $\emptyset \neq X_0 \subsetneq X_1 \subsetneq \dots \subsetneq X_n = X$ be a chain of irreducible closed subsets of X. We call $X_0 \subsetneq X_1 \subsetneq \dots \subsetneq X_n$ *a chain in* X. We know that *dim*(X) is the maximal n such that such a chain exists. In this case we call $X_0 \subsetneq X_1 \subsetneq \dots \subsetneq X_n$ a *longest chain in* X.

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

LEMMA 1.9. (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. 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 1.10. *Let $f : X \to Y$ be a finite closed surjective morphism. Then $dim(X) = dim(Y)$.*

PROOF. $dim(X) \geq dim(Y)$ because f is surjective and closed. We show the opposite inequality. Let $X_0 \subsetneq \ldots \subsetneq X_n$ 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 $Y_0 \subsetneq \ldots \subsetneq Y_n$ is a chain in Y and $dim(Y) \leq dim(X)$. □

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

THEOREM 1.11. (1) *$dim(\mathbb{A}^n) = n$.*
(2) *Let $F \in k[x_1, \ldots, x_n]$ 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 $F \in k[x_1, \ldots, x_n]$ be a nonconstant polynomial. Then there is a finite closed 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 $Z_i := Z(x_{i+1}, \ldots, x_n) \subset \mathbb{A}^n$. Then $Z_i \simeq \mathbb{A}^i$, thus $Z_0 \subsetneq Z_1 \subsetneq \ldots \subsetneq Z_n$ 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 $X_0 \subsetneq X_1 \subsetneq \ldots \subsetneq X = X_{k-1} \subsetneq \mathbb{A}^n$ 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 1.9. □

Now we show that the intersection of a closed subvariety $X \subset \mathbb{A}^n$ with a hypersurface has dimension $dim(X) - 1$.

PROPOSITION 1.12. *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 1.13. 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 closed surjective morphism. We identify $k[x_1, \dots, x_{n-1}]$ with its image via π^* in $A(X)$. By finiteness there is a nonzero polynomial

$$H = x_n^d + \sum_{i=0}^{d-1} a_i x_n^i, \quad a_i \in k[x_1, \dots, x_{n-1}], \quad \text{with } H(x_1, \dots, x_{n-1}, f) = 0 \text{ in } A(X).$$

By replacing H by one of its irreducible factors we can assume that H is irreducible.

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. Let $\overline{X}$ be the projective closure of X, let $d = deg(f)$ and $F_H := x_0^d F(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0})$ and $\overline{\varphi} := [x_0^d, x_0^{d-1}x_1, \dots, x_0^{d-1}x_n, F_H] : \overline{X} \to \mathbb{P}^{n+1}$. Then $\varphi = \overline{\varphi}|_X$ and $X = \overline{\pi}^{-1}(\mathbb{A}^{n+1})$. Thus φ is closed.

By definition $\varphi(X) \subset Z(H)$. Thus $\varphi(X)$ is a closed subset of dimension n of $Z(H)$, which is irreducible of dimension n as a hypersurface in $\mathbb{A}^{n+1}$. Therefore $\varphi : X \to Z(H)$ is a finite closed 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 1.11, a_0 is constant and $Z(F) \cap X = Z(a_0) = \emptyset$. $\square$

A variety X and dense open subset $U \subset X$ have the same dimension.

THEOREM 1.14. *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 closed 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 1.15. (1) *$dim(\mathbb{P}^n) = n$.*

(2) *Let $F \in k[x_0, \dots, x_n]$ 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 $Z(F) \cap \mathbb{A}^n = Z(F(1, x_1, \dots, x_n))$ had 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 1.12: Every component of $Z(F) \cap X$ has dimension $dim(X) - 1$.

THEOREM 1.16. *Let $X \subset \mathbb{A}^n$ be an affine variety, and let $F \in k[x_1, \dots, x_n] \setminus I(X)$. Then every irreducible component of $X \cap Z(F)$ has dimension $dim(X) - 1$.*

REMARK 1.17. 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 1.14 and Theorem 1.16 are the main results about dimension that usually allow to compute the dimension of a variety. We give a number of consequences.

COROLLARY 1.18. *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 1.19. (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 1.20. (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 1.16 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 1.21. 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 1.22. *$\mathbb{P}^1 \times \mathbb{P}^1$ 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. □

2. Tangent space and nonsingularity

In this section we introduce tangent spaces of algebraic varieties and singular and 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. We first introduce the tangent cone which is instead the cone that best approximates X near p.

2.1. Tangent cone of an affine variety. Let $X \subset \mathbb{A}^n$ be an affine algebraic set. Note that we not not require X to be irreducible.

Definition 2.1. For $f \in k[x_1, \dots, x_n]$ let $f = \sum_i f^{(i)}$ be the decomposition into homogeneous parts. The *initial part* of f is $f^{in} := f^{(i)}$ for the smallest i such that $f^{(i)} \neq 0$. If $I \subset k[x_1, \dots, x_n]$ is an ideal, the *initial ideal* of I is $I^{in} := \left\langle f^{in} \mid f \in I \right\rangle$. By definition this is a homogeneous ideal.

Now let $X \subset \mathbb{A}^n$ be an affine algebraic set and assume $O = (0, \dots, 0) \in X$. The *tangent cone* of X at O is $C_O(X) := Z(I(X)^{in}) \subset \mathbb{A}^n$. As $I(X)^{in}$ is a homogeneous ideal, $C_O(X)$ is a cone. In fact let $C_O^p(X) := Z_H(I(X)) \subset \mathbb{P}^{n-1}$. $C_O^p(X)$ is called the *projective tangent cone* of X at O. Then by definition $C_O(X)$ is the affine cone $C(C_O^p(X))$ over $C_O^p(X))$. If $p = (p_1, \dots, p_n) \in X$, we put

$$X - p := \left\{(a_1 - p_1, \dots, a_n - p_n) \mid (a_1, \dots, a_n) \in X\right\},$$

and define $C_p(X) := C_O(X - p)$.

Usually we will assume that $p = O$. Then $C_O(X)$ is just the zero locus of the initial parts of all $f \in I(X)$.

Example 2.2. (1) $X = Z(y - x^2 + x) \subset \mathbb{A}^2$ be an irreducible conic. Then $C_0(X) = Z(y - x)$ is a line.

(2) $X = Z(y^2 - x^2 - x^3) \subset \mathbb{A}^2$ be a nodal cubic. Then $C_0(X) = Z(y^2 - x^2) = Z(y - x, y + x)$ is the union of two lines.

(3) Let $X = Z(y^2 - x^3) \subset \mathbb{A}^2$ be a cuspidal cubic, then $C_0(X) = Z(y^2)$ is a line.

REMARK 2.3. Let X be a variety. We will show that $C_p(X)$ has pure dimension $dim(X)$ for all $p \in X$, i.e. every irreducible component of $C_p(X)$ has dimension $dim(X)$.

2.2. The tangent space of an affine algebraic set. The tangent space of an affine algebraic set $X \subset \mathbb{A}^n$ 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 2.4. For $f \in k[x_1, \dots, x_n]$ let $f^{(1)}$ be the homogeneous part of degree 1. For an ideal $I \subset k[x_1, \dots, x_n]$ we put $I^{(1)} := \{f^{(1)} \mid f \in I\}$.

Now let $X \subset \mathbb{A}^n$ be an affine algebraic set and assume $O = (0, \dots, 0) \in X$. The *tangent space* of X at O is $T_O X := Z(I(X)^{(1)})$. As this is the zero set of linear functions it is a subvector space of k^n. The tangent space of X at $p \in X$ is $T_O(X - p)$. Usually we will assume $p = O$.

$p \in X$ is called a *nonsingular point*, if $dim(T_p X) = dim_p(X)$, i.e. the maximum of the dimensions of the components passing through p. Here we can take the dimension of $T_p X$ 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*.

EXAMPLE 2.5. (1) $X = Z(y - x^2 + x) \subset \mathbb{A}^2$ be an irreducible conic. Then $T_O X = Z(x + y)$. Thus O is a nonsingular point of X.

(2) Let $X = Z(y^2 - x^2 - x^3) \subset \mathbb{A}^2$, be a nodal cubic, then $T_O X = \mathbb{A}^2$. Thus O is a singular point of X.

(3) Let $X = Z(y^2 - x^3) \subset \mathbb{A}^2$ be a cuspidal cubic. $T_O X = \mathbb{A}^2$ and O is a singular point.

REMARK 2.6. (1) As $I(X)^{in} \supset I(X)^{(1)}$, we see that $C_p(X) \subset T_p(X)$. As $dim(C_p(X)) = dim_p(X)$, it follows that $dim(T_p(X)) \geq dim_p(X)$. Furthermore, as $T_p X$ is irreducible (as it is isomorphic to an affine space) we get that $dim(T_p(X)) = dim(X)$ if and only if $C_p(X) = T_p X$. In particular $p \in X$ is nonsingular if and only if $T_p X = C_p(X)$.

(2) If $X \subset \mathbb{C}^n$ is an affine variety over $\mathbb{C}$, then one can show that with the strong topology X_{reg} is a complex submanifold of $\mathbb{C}^n$ of dimension $dim(X)$.

REMARK 2.7. (1) One can make the definition a little bit more explicit. Let $f \in k[x_1, \dots, x_n]$ and $p = (p_1, \dots, p_n) \in \mathbb{A}^n$. The *differential* of f at p is

$$d_p f := \sum_{i=1}^n \frac{\partial f}{\partial x_i}(p) x_i.$$

This is a linear map $k^n \to k$. Note that $d_p(fg) = (d_p f)g(p) + f(p)d_p(g)$. By definition we see $d_O f = f^{(1)}$ and $d_p f = f(x + p)^{(1)}$. Thus we see $T_p X = Z\big(d_p f \bigm| f \in I(X)\big)$.

(2) Let $I(X) = \langle f_1, \dots, f_r \rangle$. Then

$$T_p X := Z(d_p f_1, \dots, d_p f_r) \subset k^n.$$

The inclusion $\supset$ is obvious. If $h = \sum_i h_i f_i \in I(X)$, then $f_i(p) = 0$ implies

$$d_p h = \sum_i h_i(p) d_p f_i + (d_p h_i) f_i(p) = \sum_i h_i(p) d_p f_i \in \langle d_p f_1, \dots, d_p f_r \rangle.$$

Like in differential geometry a morphism of affine varieties gives a linear map between tangent spaces.

DEFINITION 2.8. 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 $d_p \varphi := (d_p f_1, \dots, d_p f_m) : T_p X \to T_q Y$. In particular in case $p = O$ we have $d_O \varphi = (f_1^{(1)}, \dots, f_m^{(1)})$. Note that $d_p \varphi$ is linear, because it is given by linear polynomials. I leave it as an easy exercise to check that $d_p \varphi$ indeed maps $T_p X$ to $T_q Y$.

REMARK 2.9. Obviously we have $d_p id_X = id_{T_p X}$, 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 $d_p \varphi : T_p X \to T_{\varphi(p)} Y$ is an isomorphism for all $p \in X$.

EXAMPLE 2.10. (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. Tangent spaces for general varieties. Now we define the tangent space for general varieties X at a point $p \in X$. 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.

DEFINITION 2.11. Let X be a variety and let $p \in X$. Recall the local ring $\mathcal{O}_{X,p} := \{\frac{f}{g} \in K(X) \mid g(p) \neq 0\}$ and its maximal ideal

$$m_{X,p} := \{\frac{f}{g} \in K(X) \mid f(p) = 0,\ g(p) \neq 0\} = \{h \in \mathcal{O}_{X,p} \mid h(p) = 0\}.$$

By definition $m_{X,p}^2$ is the ideal $m_{X,p}^2 = \langle gh \mid g,h \in m_{X,p}\rangle$. Intuitively these are the rational functions vanishing at p to second order.

The *tangent space* of X at p is the dual vector space

$$\begin{aligned} T_pX &:= (m_{X,p}/m_{X,p}^2)^\vee = \{\text{linear maps } v : (m_{X,p}/m_{X,p}^2) \to k\} \\ &= \{\text{linear maps } v : m_{X,p} \to k \text{ with } v|_{m_{X,p}^2} = 0\}. \end{aligned}$$

$p \in X$ is called a *nonsingular point* or *regular point* of X if $dim(T_pX) = dim(X)$. 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 $X = X_{reg}$.

Again a morphism defines a linear map on tangent spaces.

DEFINITION 2.12. Let $\varphi : X \to Y$ be a morphism of varieties with $\varphi(p) = q$. For $g \in m_{X,p}$ (respectively $h \in m_{Y,q}$) The *differential* of φ at p is

$$d_p\varphi : T_pX \to T_qY, d_p\varphi(v)(h) := v(\varphi^*h), \quad v \in T_pX,\ h \in m_{Y,q}.$$

Obviously this is a linear map. Note that φ^* maps $m_{Y,q}$ to $m_{X,p}$ and $m_{Y,q}^2$ to $m_{X,p}^2$. Therefore $d_p\varphi$ is well-defined.

Now we want to see that for affine varieties the two different definitions agree. Let $X \subset \mathbb{A}^n$ be an affine variety, and let $p \in X$. We denote momentarily by $t_pX \subset \mathbb{A}^n$ our first definition of the tangent space for affine algebraic sets. We can assume $p = O$.

PROPOSITION 2.13. (1) *Write $M := m_{X,O}$. There is a canonical isomorphism $\alpha : k[x_1,\dots,x_n]^{(1)}/I(X)^{(1)} \to M/M^2$.*

(2) *There is a canonical isomorphism $\alpha^\vee : T_OX \to t_OX$*

(3) *$\alpha^\vee$ identifies the two definitions of $d_O\varphi$. Denote momentarily $D_O\varphi := d_O\varphi : T_OX \to T_OY$, then $D_O\varphi = (\alpha^\vee)^{-1} \circ d_O\varphi \circ \alpha^\vee$.*

PROOF. (1) For $F \in k[x_1, \dots, x_n]$ we denote by f the class in $A(X)$. Let $F \in k[x_1, \dots, x_n]^{(1)}$. We put $\widetilde{\alpha}(F) := f \in M$. Note that $x_i \in M$, thus for any $G \in k[x_1, \dots, x_n]^{(\geq k)}$, we have $g \in M^k$. If $F \in I(X)^{(1)}$, then $F = \widetilde{F} - H$ with $\widetilde{F} \in I(X)$ and $H \in k[x_1, \dots, x_n]^{(\geq 2)}$. Then $\widetilde{\alpha}(F) = -h \in M^2$. Thus we get an induced homomorphism $\alpha : k[x_1, \dots, x_n]^{(1)}/I(X)^{(1)} \to M/M^2, [F] \mapsto [f]$.

Injectivity: If $\alpha(F) = 0$, then $f \in M^2$, thus there is a $G \in I(X)$ with $H := F - G \in k[x_1, \dots, x_n]^{(\geq 2)}$. Thus $F = F^{(1)} = H^{(1)} + G^{(1)} = G^{(1)} \in I(X)^{(1)}$.

Surjectivity: Let $\frac{f}{g} \in M$. We can assume that $g(p) = 1$. Then $f - f^{(1)} \in M^2$ and $\frac{f}{g} - \widetilde{\alpha}(F^{(1)}) = \frac{f}{g} - f^{(1)} = \frac{f(1-g)}{g} + f - f^{(1)} \in M^2$, i.e. $[\frac{f}{g}] = \alpha([F^{(1)}])$.

(2) By definition $k[x_1, \dots, x_n]^{(1)}$ is the space of linear maps $k^n \to k$, i.e. $(k^n)^\vee$. Therefore we get

$$(t_O X)^\vee = k[x_1, \dots, x_n]^{(1)}/\{w \in k[x_1, \dots, x_n]^{(1)} \mid w|_{t_O X} = 0\} = k[x_1, \dots, x_n]^{(1)}/I(X)^{(1)}.$$

(3) is left as an exercise. □

Now we want to see that smoothness is easy to check.

DEFINITION 2.14. The *Jacobian* of $f_1, \dots, f_r \in k[x_1, \dots, x_n]$ is the $r \times n$ matrix

$$J(f_1, \dots, f_r) := det((\frac{\partial f_i}{\partial x_j})_{i,j}.$$

with coefficients in $k[x_1, \dots, x_n]$

PROPOSITION 2.15. *(Jacobi Criterion)*

(1) *Let $X \subset \mathbb{A}^n$ be an affine variety, with $I(X) = \langle f_1, \dots, f_r \rangle$. Then X is nonsingular at $p \in X$, if $J(f_1, \dots, f_r)(p)$ has rank at least $n - dim(X)$.*

(2) *Let $X \subset \mathbb{P}^n$ be a projective variety, with $I(X) = \langle F_1, \dots, F_r \rangle$, for $F_i \in k[x_0, \dots, x_n]$ homogeneous. Then X is nonsingular at $p \in X$, if $J(F_1, \dots, F_r)(p)$ has rank at least $n - dim(X)$ (this is now an $(n+1) \times r$ matrix).*

PROOF. (1) We know that

$$T_p(X) = Z(d_p f_1, \dots, d_p f_r) = ker(J(f_1, \dots, f_r)).$$

Thus X is smooth at p if and only if $rk(J(f_1, \dots, f_r)) = n - dim(X)$. We already know that $dim(T_p X) \geq dim(X)$. Thus it is enough to show $rk(J(f_1, \dots, f_r) \geq n - dim(X)$.
(2) We can assume $p = [1, 0, \dots 0]$. 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 $O = (0, \dots, 0)$ is a nonsingular point of $Z(f_1, \dots, f_r)$, if and only if $rk(J(f_1, \dots, f_r)(O)) \geq n - dim(X)$. By definition $\frac{\partial F_i}{\partial x_j}(p) = \frac{\partial f_i}{\partial x_j}(O)$ 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 by $x_j(p) = 0$ for $j \geq 1$ and $F_i(p) = 0$ we get $1 \frac{\partial F_i}{\partial x_0}(p) + \sum_{i=1}^n 0 = 0$. Thus $J(F_1, \dots, F_r)(p) = \begin{pmatrix} J(f_1, \dots, f_r)(O) & 0 \end{pmatrix}$ and $rk(J(F_1, \dots, F_r)(p)) = rk(J(f_1, \dots, f_r)(O))$. □

REMARK 2.16. In particular let $X \subset \mathbb{A}^n$ or $X \subset \mathbb{P}^n$ with $I(X) = \langle f_1, \dots, f_r \rangle$ (in the second case assume the f_i to be homogeneous) and assume $rk(J(f_1, \dots, f_r)) = r$. Then X is nonsingular of dimension $n - r$. Varieties of this form are called *complete intersections*. Complete intersections have particularly nice properties.

COROLLARY 2.17. *Let X be a variety. Then X_{sing} is a closed subset of X.*

PROOF. We can assume $X \subset \mathbb{A}^n$. Let $n - r = dim(X)$, and $I(X) = \langle f_1, \dots, f_s \rangle$. Let $\{J_I\}_I \in k[x_1, \dots, x_n]$ be the $r \times r$-minors of $J(f_1, \dots, f_s)$. Then $X_{sing} = Z(I(X), \{J_I\}_I)$. □

REMARK 2.18. It is not very difficult to show that for every variety $X_{reg} \neq \emptyset$. Thus X_{reg} is an open dense subset of X. This 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.

3. Rational maps and blowups

3.1. Rational maps. Let X, Y be varieties. Rational functions on X are functions that are only defined on an open dense subset. Similarly we also want to look at morphisms that are only defined on an open dense subset. These are called rational maps. The reason for looking at rational maps is that there are few morphisms, and a number of important properties of varieties are preserved by rational maps.

LEMMA 3.1. *Let $\psi_1, \psi_2 : X \to Y$ be morphism between varieties. If $\varphi|_U = \psi|_U$ for a nonempty open subset $U \subset X$, then $\varphi = \psi$.*

PROOF. Let $p \in X$. We need to show $\psi_1(p) = \psi_2(p)$. We can assume that $Y \subset \mathbb{A}^n$. Otherwise $Y \subset \mathbb{P}^n$. There is a hyperplane $H \subset \mathbb{P}^n$ which contains neither $\psi_1(p)$ nor $\psi_2(p)$. By applying a projective linear transformation we can assume $\psi_1(p), \psi_2(p) \in U_0 \simeq \mathbb{A}^n$. Let $V = \psi_1^{-1}(U_0) \cap \psi_2^{-1}(U_0)$. Now we can write $\varphi_0 \circ \psi_i = (f_1^i, \dots, f_n^i) : V \to \mathbb{A}^n$ with $f_j^i \in \mathcal{O}_X(V)$. We have $f_i^1|_{U \cap V} = f_i^2|_{U \cap V}$, so $f_i^1 = f_i^2$. Therefore $\varphi(p) = \psi(p)$. □

DEFINITION 3.2. 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 3.1 implies the transitivity. It is easy to see that the rational functions on X are the same as the rational maps $f : X \dashrightarrow \mathbb{A}^1$. We can also view rational maps $\varphi : X \dashrightarrow Y$ as regular maps $\varphi : dom(\varphi) \to Y$, where $dom(\varphi) = \bigcup_{\langle V, \psi \rangle \sim \langle U, \varphi \rangle} V$. We say that φ is *defined at p* if $p \in dom(\varphi)$. We call $\varphi(dom(\varphi))$ the *image* of φ.

REMARK 3.3.

(1) Let X be a variety, let $f_1, \dots, f_n \in K(X)$. Then $(f_1, \dots, f_n) : X \dashrightarrow \mathbb{A}^n$ is a rational map defined on $\bigcap_{i=1}^n dom(f_i)$.

(2) Let $X \subset \mathbb{P}^n$ be a quasiprojective variety. 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 $X \setminus \bigcap_{i=0}^n Z(F_i)$.

Example 3.4. Let $W \subset \mathbb{P}^n$ be a linear subspace of dimension k given by $W = Z(H_1, \dots, H_{n-k})$ for H_i linear forms. Then the linear projection $\pi_W = [H_1, \dots, H_{n-k}] : \mathbb{P}^n \dashrightarrow \mathbb{P}^{n-k-1}$ 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 $\varphi(X) \cap dom(\psi) = \emptyset$. To remedy this, we make the following definition.

Definition 3.5. A rational map $\varphi : X \to Y$ of varieties is called *dominant* if its image contains a nonempty open (and therefore dense) subset of Y. 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 $\langle U \cap \varphi^{-1}(V), \psi \circ \varphi \rangle$ is a representative of the composition.

Example 3.6. 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 3.7. 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 $\varphi \circ \varphi^{-1} = id_Y$, $\varphi^{-1} \circ \varphi = id_X$. If φ is in addition a morphism, it is called a *birational morphism*. X and Y are called *birational* if there exists birational map $\varphi : X \dashrightarrow Y$.

Remark 3.8. (1) X and Y are birational, if and only if there are open subsets $U \subset X$, $V \subset Y$ with $U \simeq V$.

Proof. "$\Longleftarrow$" If $\varphi : U \to V$ is an isomorphism, then $\varphi : X \dashrightarrow Y$ is a rational map, whose inverse is φ^{-1}. "$\Longrightarrow$" Let $\varphi : X \dashrightarrow Y$ be a birational map, defined on $W_1 \subset X$. The inverse is defined on an open set $W_2 \subset Y$. $U := W_1 \cap \varphi^{-1}(W_2)$ is open in X and $V := \varphi(W_1) \cap W_2$ is open in Y and the restriction of φ is an isomorphism $\varphi : U \to V$. $\square$

Corollary 3.9. *If X and Y are birational, then $dim(X) = dim(Y)$.*

Example 3.10. The cuspidal cubic $C = Z(x^3 - y^2) \subset \mathbb{A}^2$. We have seen that C 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 3.11. A variety X is called *rational* if it is birational to $\mathbb{A}^n$.

Example 3.12. (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 $\mathbb{A}^{n+m}$.

3.2. Blowups of affine varieties. We now come to the most important examples of birational morphisms: the blowups. One can define the blowup of a variety along any ideal. We will restrict ourselves to the blowup of a variety X in a point. We start by blowing up $\mathbb{A}^{n+1}$ in the point $O = (0, \dots, 0)$.

DEFINITION 3.13. On $\mathbb{A}^{n+1}$ let the coordinates be $x_0, \dots, x_n$ and on $\mathbb{P}^n$ let the homogeneous coordinates be $y_0, \dots, y_n$. The *blowup* of $\mathbb{A}^{n+1}$ at O is the closed subset

$$\widehat{\mathbb{A}}^{n+1} := Z\big(x_i y_j - x_j y_i \bigm| i, j = 0, \dots, n\big) \subset \mathbb{A}^{n+1} \times \mathbb{P}^n.$$

We will often just write x for $(x_0, \dots, x_n)$ and $[y]$ for $[y_0, \dots, y_n]$. Let $\pi : \widehat{\mathbb{A}}^{n+1} \to \mathbb{A}^{n+1}$ be the projection. We call $E = E_{\mathbb{A}^{n+1}} := \pi^{-1}(O)$ the *exceptional divisor* of π.

We shall see that blowing up O leaves $\mathbb{A}^{n+1} \setminus O$ unchanged, but O is replaced by $\mathbb{P}^n$, which we can identify with the space of lines through O. In particular π is a birational morphism.

PROPOSITION 3.14. (1) *$\widehat{\mathbb{A}}^{n+1} \setminus E$ is the graph of the morphism*

$$s : \mathbb{A}^{n+1} \setminus O \to \mathbb{P}^n, (a_0, \dots, a_n) \mapsto [a_0, \dots, a_n],$$

which sends a point p to the line through p and O. In particular the restriction of π to $\widehat{\mathbb{A}}^{n+1} \setminus E$ is an isomorphism to $\mathbb{A}^{n+1} \setminus O$.
(2) *$\widehat{\mathbb{A}}^{n+1}$ has an open cover by affine spaces: For $j = 0, \dots, n$ let $V_j := \big\{(x, [y]) \in \widehat{\mathbb{A}}^{n+1} \bigm| y_j \neq 0\big\}$. Then there is an isomorphism*

$$\psi_j := (x_j, \frac{y_0}{y_j}, \dots, \widehat{\frac{y_j}{y_j}}, \dots, \frac{y_n}{y_j}) : V_j \to \mathbb{A}^{n+1}.$$

(3) *$\widehat{\mathbb{A}}^{n+1}$ is irreducible and nonsingular. It is the closure of the graph of s.*
(4) *$\psi_j(E) = Z(x_j)$.*
(5) *$E = O \times \mathbb{P}^n$.*

PROOF. (1) Let $q = (x, [y]) \in \pi^{-1}(\mathbb{A}^{n+1} \setminus O)$. We can assume $x_0 \neq 0$. Then $x_0 y_i = x_i y_0$, i.e $y_i = x_i \frac{y_0}{x_0}$ for all i. Thus $[y] = [x]$. Thus $q = (x, s(x))$.

(2) We can assume $j = 0$. Write $z = (z_1, \dots, z_n)$. For

$$v_0 : \mathbb{A}^{n+1} \to V_0, (t, z) \mapsto ((t, tz), [1, z]), \quad \psi_0 = (x_0, y_1/y_0, \dots, y_n/y_0) : V_0 \to \mathbb{A}^{n+1}.$$

We see that

$$\psi_0 \circ v_0((t, z)) = \psi_0(((t, tz), [1, z])) = (t, z),$$
$$v_0 \circ \psi_0(x, [y]) = v_0((x_0, y_1/y_0, \dots, y_n/y_0)) = (x, [y]).$$

(3) $\widehat{\mathbb{A}}^{n+1}$ has an open cover by affine spaces V_i, thus it is nonsingular. Any two of the V_i have a nonempty intersection, thus $\widehat{\mathbb{A}}^{n+1}$ is irreducible. As by (1) it contains the graph of s as an open subset, it is its closure.

(4) We can assume $j = 0$. By definition $\pi(v_0(x_0, t_1, \dots, t_n)) = (x_0, x_0 t_1, \dots, x_0 t_n)$, which is O if and only if $x_0 = 0$.

(5) By definition $\pi^{-1}(O) = \big\{(O, [y]) \bigm| 0 y_i = 0 y_i \text{ for all } i, j\big\} = O \times \mathbb{P}^n$. $\square$

Remark 3.15. Part (2) of this proposition is very important for working with $\widehat{\mathbb{A}}^{n+1}$. It means that the open set V_0 is an affine space with coordinates $x_0, \frac{y_1}{y_0} \dots, \frac{y_n}{y_0}$. Then (4) says that in these coordinates E is given by $x_0 = 0$. We also see that in these coordinates $\pi \circ v_0$ is given by $(x_0, t_1, \dots, t_n) \mapsto (x_0, x_0 t_1, \dots, x_0 t_n)$.

Now we define the blowup of an affine variety $X \subset \mathbb{A}^{n+1}$ in a point of X. We can assume that this point is O.

Definition 3.16. Let $X \subset \mathbb{A}^{n+1}$ be a closed subvariety and assume $O \in X$ and $X \neq \{O\}$. The *blowup* $\widehat{X}$ of X in O is the closure of $\pi^{-1}(X \setminus O)$ in $\widehat{\mathbb{A}}^{n+1}$. We will denote by $\pi = \pi_X$ the restriction of π to $\widehat{X}$. $E = E_X := \pi_X^{-1}(O)$ is called the *exceptional divisor* of $\widehat{X}$. By definition $\widehat{X}$ is irreducible and $\pi|_{\widehat{X} \setminus E}$ is an isomorphism onto $X \setminus O$. If $Y \subset X$ is a subvariety with $O \in Y$, the *strict transform* $\widehat{Y} \subset \widehat{X}$ is the closure of $\pi^{-1}(Y \setminus O)$ in $\widehat{X}$. Note that this is just the blowup of Y in O.

If $p \in X$ is another point, the blowup of X in p is $\widehat{X - p}$.

Remark 3.17. By definition $\widehat{X} \setminus E$ is the graph of the map $s : X \to \mathbb{P}^n$, sending $p \in X$ to the secant line $[p]$ through O and p. Thus $\widehat{X}$ is the closure of the graph of s. So the exceptional divisor $\widehat{X}$ should be the limits of the secant lines as p approaches O, i.e. they should be tangent lines at O.

Now we describe $\widehat{X}$. It is best understood in terms of the coordinates on the V_j.

Notation 3.18. For a polynomial $f \in k[x_0, \dots, x_n]$ the *initial degree* $i(f)$ of f is the minimal i with $f^{(i)} \neq 0$.

Remark 3.19. Let $f \in k[x_0, \dots, x_n]$. Then we can write

$$f(x_0, t_1 x_0, \dots, t_n x_0) = x_0^{i(f)} \Big(f^{(i(f))}(1, t_1, \dots, t_n) + \sum_{j \geq 1} x_0^j f^{(j + i(f))}(1, t_1, \dots, t_n) \Big).$$

Thus $i(f)$ is the maximal integer r such that $f(x_0, t_1 x_0, \dots, t_n x_0)$ is divisible by x_0^r.

In the next lemma we denote $x_0, t_1, \dots, t_n$ the coordinates on $\mathbb{A}^{n+1}$.

PROPOSITION 3.20. (1) *E has pure dimension $dim(X) - 1$ in $\widehat{X}$.*

(2) *$I(\psi_0(\widehat{X})) = \{f(x_0, x_0t_1, \dots, x_0t_n)/x_0^j \mid f \in I(X),\ j \le i(f)\}$, and similarly for the other ψ_j.*

(3) *$E = O \times C_O^p(X)$, where $C_O^p(X)$ is the projective tangent cone of X at O.*

PROOF. (1) It is enough to show that $\psi_j(E)$ has pure codimension 1 in $\psi_j(\widehat{X})$ for all j. We can assume $j = 0$. Then we know that

$$\psi_0(E) = \psi_0(E_{\mathbb{A}^{n+1}} \cap \widehat{X}) = Z(x_0) \cap \psi_0(\widehat{X}).$$

As $E \neq \widehat{X}$ it follows that $\psi_0(E)$ has pure codimension 1 in $\psi_0(\widehat{X})$.

(2) Put $Y := \psi_0(\widehat{X})$ and $Y_0 := Y \setminus Z(x_0) = \psi_0(\widehat{X} \setminus E)$. Let $f \in I(X)$, then $I(Y) \ni v_0^*(f) = f(x_0, t_1x_0, \dots, t_nx_0)$. We write $f(x_0, t_1x_0, \dots, t_nx_0) = x_0^{i(f)}g$ with $g \in k[x_0, t_1, \dots, t_n]$. Then, as x_0 is nowhere 0 on Y_0, we see that $g(x_0, t_0, \dots, t_n)$ vanishes on Y_0. As Y_0 is dense in Y it follows that $g \in I(Y)$.

Conversely let $g(x_0, t_1, \dots, t_n) \in I(Y)$. Choose an r such that $f := x_0^r g(x_0, \frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}) \in k[x_0, \dots, x_n]$. Then $g = f(x_0, t_1x_0, \dots, t_nx_0)/x_0^r$. Then f is zero on $X \setminus Z(x_0)$. Thus $f \in I(X)$. By the remark above we have $r \le i(f)$.

(3) We again look at the chart V_0. We know by (1), (2) that

$$\psi_0(E) = Z\big(x_0, \{f(x_0, x_0t_1, \dots, x_0t_n)/x_0^j \mid f \in I(X),\ j \le i(f)\}\big).$$

We know that

$$f(x_0, x_0t_1, \dots, x_0t_n)/x_0^j = x_0^{i(f)-j}\big(f^{in}(1, t_1, \dots, t_n) + x_0 g(x_0, t_1, \dots, t_n)\big).$$

This is zero on $Z(x_0)$ unless $j = i(f)$, when it is $f^{in}(1, t_1, \dots, t_n)$. Thus $\psi_0(E) = Z\big(x_0, \{f^{in}(1, t_1, \dots, t_n) \mid f \in I(X)\}\big)$. Thus

$$E \cap V_0 = O \times \{[1, t_1, \dots, t_n] \mid f^{in}(1, t_1, \dots, t_n) = 0\ \forall_{f \in I(X)}\} = (O \times C_O^p(X)) \cap V_0.$$

On the other V_i one argues in the same way. □

COROLLARY 3.21. *Let X be a variety. $C_p(X)$ has pure dimension $dim(X)$.*

PROOF. We can assume that $p = O$. Let Z a component of $C_O^p(X)$ and $C(Z)$ the corresponding component of $C_O(X)$. The morphism $C(Z) \to Z; a \to [a]$ is surjective and all fibres are $\mathbb{A}^1 \setminus 0$. Thus $dim(C(Z)) = dim(Z) + 1 = dim(X)$. □

EXAMPLE 3.22. In all examples below we consider curves in $\mathbb{A}^2$. On $\mathbb{A}^2$ let the coordinates be x, y and on $\mathbb{P}^1$ let the coordinates be u, t, so that $\widehat{\mathbb{A}}^2 = \{((x, y)[u, t]) \in \mathbb{A}^2 \times \mathbb{P}^1 \mid xu = yt\}$.

(1) For $a \in k$ let $L_a := Z(y - ax) \subset \mathbb{A}^2$ be lines through O. In the chart $t \neq 0$ the strict transforms $\widehat{L}_a = Z((ux - ax)/x) = Z(u - a)$ are parallel lines.

(2) Let $C = Z(y(y - ax))$ the union of two lines intersecting in 0. Then in the same chart we have $\widehat{C} = Z(ux(ux - ax)/x^2) = Z(u(u - a))$, the union of two parallel lines in $\mathbb{A}^2$.

(3) Let $C = Z(y^2 - x^2(x + 1))$ be a nodal cubic. On the chart $t \neq 0$ we have $\widehat{C} = Z((x^2u^2 - x^3 - x^2)/x^2) = Z(u^2 - x - 1)$, which is nonsingular. Thus $\widehat{C} \cap V_0$ is nonsingular, and similarly one checks that $\widehat{C} \cap V_1$ is nonsingular. Thus $\widehat{C}$ is nonsingular. We see that in this chart the exceptional divisor E_C is given by $u^2 = 1$, i.e. it contains of the two points $(0, 1)$, $(0, -1)$, corresponding to the fact that the tangent cone $C_O(X)$ consists of two lines.

(4) Let $C = Z(x^3 - y^2) \subset \mathbb{A}^2$ be the cuspidal cubic. On the chart $t \neq 0$ we have $\widehat{C} = Z((x^3 - x^2t)/x^2) = Z(x - t^2)$, which is nonsingular. Thus $\widehat{C} \cap V_0$ is nonsingular, and similarly one checks that $\widehat{C} \cap V_1$ is nonsingular. Thus $\widehat{C}$ is nonsingular.

DEFINITION 3.23. Let X be a variety. Then a *resolution of singularities* of X is a birational morphism $\varphi : \widetilde{X} \to X$, such that $\widetilde{X}$ is nonsingular and $\varphi|_{\varphi^{-1}(X_{reg})}$ is an isomorphism.

So in the example above $\widehat{C} \to C$ is a resolution of singularities. One can show that any curve has a resolution of singularities by a composition of blowups at points.

In general a very deep theorem of Hironaka says that in characteristic 0 every variety has a resolution of singularities by a composition of blowups along subvarieties. This is a very important result, because one can work much better on nonsingular varieties, so usually one will study even singular varieties by using their resolution.

In the blowup of $\mathbb{A}^{n+1}$ is that O is replaced by the space $\mathbb{P}^n$ of tangent lines to $\mathbb{A}^{n+1}$ at O. Thus O is stretched out to a $\mathbb{P}^n$ in $\widehat{\mathbb{A}}^{n+1}$ and to $C^p_O(X)$ in $\widehat{X}$. Intuitively O is enlarged, like under a microscope with infinite magnification. If $X \subset \mathbb{A}^{n+1}$ is singular at O, this often makes $\widehat{X}$ a resolution of singularities of X. If X is already nonsingular, then also $\widehat{X}$ is nonsingular.

PROPOSITION 3.24. *Let $X \subset \mathbb{A}^{n+1}$ be a variety of dimension d and assume O is a nonsingular point of X.*

(1) $E = O \times \mathbb{P}(T_O X) \simeq \mathbb{P}^{d-1}$.
(2) *All points of E are nonsingular points of $\widehat{X}$.*

PROOF. (1) is clear, because $C_O(X) = T_O X$ for O a nonsingular point.

(2) Let $Q := (O, [v]) \in E$. We need to show that Q is a nonsingular point of $\widehat{X}$. We know that $[v]$ is the class in $\mathbb{P}^n$ of $v \in T_O X$. By a change of coordinates we can assume that $v = [1, 0, \dots, 0]$ and that $T_O X = Z(x_d, \dots, x_n)$. Let $Y := \psi_0(\widehat{X})$. By assumption there are $f_d, \dots, f_n \in I(X)$ such that $f_i = x_i + g_i$ with $g_i \in k[x_0, \dots, x_n]^{(\geq 2)}$. Thus $I(Y)^{(1)} \ni f_i(x_0, x_0 t_1, \dots, x_0 t_n)/x_0 = t_i + a_i x_0$, where a_i is the coefficient of x_0^2 of f_i. Thus the dimension of $T_Q Y = Z(I(Y)^{(1)})$ is at most d. $\square$

3.3. Blowup of projective varieties. The blowup of a projective variety in a point is very similar to the blowup of a an affine variety in a point. In this section we use u_{n+1} to identify $\mathbb{A}^{n+1}$ with $U_{n+1} \subset \mathbb{P}^{n+1}$, i.e. we identify $(a_0, \dots, a_n) \in \mathbb{A}^{n+1}$ with $[a_0, \dots, a_n, 1] \in \mathbb{P}^{n+1}$. In particular $O = [0, \dots, 0, 1] \in \mathbb{P}^{n+1}$.

DEFINITION 3.25. The *blowup* of $\mathbb{P}^{n+1}$ in O is

$$\widehat{\mathbb{P}}^{n+1} := \big\{([x_0, \dots, x_{n+1}], [y_0, \dots, y_n]) \in \mathbb{P}^{n+1} \times \mathbb{P}^n \ \big|\ x_i y_j = x_j y_i \text{ for } 0 \leq i, j \leq n\big\}.$$

Let $\pi : \widehat{\mathbb{P}}^{n+1} \to \mathbb{P}^{n+1}$ and $p : \widehat{\mathbb{P}}^{n+1} \to \mathbb{P}^n$ be the projections. The *exceptional divisor* is $E = E_{\mathbb{P}^{n+1}} := \pi^{-1}(O)$.

Let $X \subset \mathbb{P}^{n+1}$ and assume $O \in X$. The blowup $\widehat{X}$ of X in O is the closure of $\pi^{-1}(X \setminus O)$ in $\widehat{\mathbb{P}}^{n+1}$. We denote by $\pi = \pi_X$ and $p = p_X$ also the restrictions of π and p to $\widehat{X}$. The *exceptional divisor* is $E = E_X := \pi_X^{-1}(O)$.

We define the blowup of X in a point $p \in X$ by first applying a projective change of coordinates, so that p becomes O and then blowing up in O.

REMARK 3.26. By definition $\widehat{X}$ is the closure of the graph of the projection $\pi_O = [x_0, \dots, x_n] : X \setminus \{O\} \to \mathbb{P}^n$ which is just the projection from O. We then have $p : \widehat{X} \to \mathbb{P}^n$ with $p \circ \pi^{-1}|_{X\setminus\{O\}} = \pi_O$. Thus the projection from O now becomes defined on the whole of $\widehat{X}$. One says that we have *resolved the indeterminacy* of the rational map π_O.

REMARK 3.27. The blowup of $X \subset \mathbb{P}^{n+1}$ is very closely related to the blowup of $X \cap \mathbb{A}^{n+1}$ in $\mathbb{A}^{n+1}$. With our identification $(a_0, \dots, a_n) = [a_0, \dots, a_n, 1]$ we get $\widehat{X \cap \mathbb{A}^{n+1}} = \pi^{-1}(X \cap \mathbb{A}^{n+1}) \subset \widehat{X}$, where on the left hand side the blowup is in $\mathbb{A}^{n+1}$ and on the left hand side in $\mathbb{P}^n$. $\pi : \widehat{X} \to X \subset \mathbb{P}^{n+1}$ is the projection. Thus locally the blowup of a projective variety is just the blowup of an affine variety.

We finish by mentioning two interesting results about blowups of surfaces. We cannot give a complete proof of the results, but we try to explain why they are true.

THEOREM 3.28. *The blowup of $\mathbb{P}^1 \times \mathbb{P}^1$ in a point is isomorphic to the blowup of $\mathbb{P}^2$ in 2 points.*

PROOF. (Idea) We have $\mathbb{P}^1 \times \mathbb{P}^1 = Z(x_0x_3 - x_1x_2) \subset \mathbb{P}^3$, and we see that $O = [0,0,0,1] \in \mathbb{P}^1 \times \mathbb{P}^1$. With a suitable choice of coordinates $O = ([1,0],[1,0]) \in \mathbb{P}^1 \times \mathbb{P}^1$. The blowup $\widehat{\mathbb{P}^1 \times \mathbb{P}^1}$ of $\mathbb{P}^1 \times \mathbb{P}^1$ at O is the closure of the graph of $\pi_O : \mathbb{P}^1 \times \mathbb{P}^1 \setminus \{O\} \to \mathbb{P}^2$. Thus $p : \widehat{\mathbb{P}^1 \times \mathbb{P}^1} \to \mathbb{P}^2$ is a morphism. We know that $l_1 := [1,0] \times \mathbb{P}^1$ and $l_2 := \mathbb{P}^1 \times [1,0]$ are lines in $\mathbb{P}^3$ through O. Thus π_O maps $l_1 \setminus \{O\}$ to a point $p_1 \in \mathbb{P}_2$ and $l_2 \setminus \{O\}$ to a point $p_2 \in \mathbb{P}^2$. Thus p maps the strict transform of the l_i to the points p_i. Furthermore we see that $\pi_O|_{\mathbb{P}^1 \times \mathbb{P}^1 \setminus (l_1 \cup l_2)}$ is injective because any line through O and $p \in \mathbb{P}^1 \times \mathbb{P}^1 \setminus (l_1 \cup l_2)$ intersects $\mathbb{P}^1 \times \mathbb{P}^1$ only in O and p. Thus is conceivable that we get an inverse rational map, $\mathbb{P}^2 \dashrightarrow \widehat{\mathbb{P}^1 \times \mathbb{P}^1}$, which is not defined at p_1 and p_2 and becomes a morphism after blowup of p_1 and p_2. $\square$

REMARK 3.29. It is *not* true that $\mathbb{P}^1 \times \mathbb{P}^1$ is isomorphic to the blowup of $\mathbb{P}^2$ in one point.

THEOREM 3.30. *A nonsingular cubic $Z(F) \subset \mathbb{P}^3$ is isomorphic to the blowup of $\mathbb{P}^2$ in 6 points.*

PROOF. (Idea) We assume $F = x_0^2x_3 + f(x_0, x_1, x_2)$. Let $\nu_3 : \mathbb{P}^2 \to \mathbb{P}^9$ be the Veronese embedding of order 3. Recall that it sends $[x_0, x_1, x_2]$ to $[M_0, \ldots, M_9]$ where the M_i are the monomials in x_0, x_1, x_2 of order 3. As before we denote by $\{M_i\}$ the coordinate on $\mathbb{P}^9$ corresponding to the monomial M_i on $\mathbb{P}^2$, and we write $\{\sum a_iM_i\} = \sum a_i\{M_i\}$. Now we project successively from $\nu_3(p_i)$ for 6 different points $p_i \in \mathbb{P}^2$. We can choose the points in such a way that the composition of the projections is $[\{x_0^3\}, \{x_0^2x_1\}, \{x_0^2x_2\}, \{f\}]$. Let Y be the blowup of $\mathbb{P}^2$ in the p_i, (which is isomorphic to the blowup of $\nu_3(\mathbb{P}^2)$ at the $\nu_3(p_i)$), and let Y_0 be $\mathbb{P}^2$ the complement of the p_i in $\mathbb{P}^2$, which we can identify with the complement of the exceptional divisors in Y. Thus the composition of ν_3 and the composition of the projections gives a morphism $s : Y \to \mathbb{P}^3$. Let $(a_0, a_1, a_2) \in Y_0$. Then

$$s(a_0, a_1, a_2) = (a_0^3, a_0^2a_1, a_0^2a_2, f(a_0, a_1, a_2)) =: (b_0, b_1, b_2, b_3).$$

Then we see $f(b_0, b_1, b_2) = a_0^6f(a_0, a_1, a_2) = b_0^2b_3$, i.e $F(b_0, b_1, b_2, b_3) = 0$. Thus the image of Y_0 is contained in $Z(F)$. As Y is irreducible, $s(Y) \subset Z(F)$. One can show: $s : Y \to Z(F)$ is an isomorphism. □

REMARK 3.31. In particular we see that a nonsingular cubic in $\mathbb{P}^3$ is rational. One can show that a nonsingular hypersurface in $\mathbb{P}^n$ of degree $\geq n+1$ is not rational. Similarly if X is a complete intersection in $\mathbb{P}^n$ of hypersurfaces of degree $n_1, \ldots, n_k$ with $\sum n_i > n$, then X is not rational. On the other hand it is not known whether all nonsingular cubics in $\mathbb{P}^5$ are rational.

CHAPTER 4

Plane curves

In this chapter we study plane curves, i.e. curves in $\mathbb{P}^2$. A curve in $\mathbb{P}^2$ is just the zero locus $Z(F)$ of a nonconstant homogeneous polynomial $F \in k[x, y, z]$. Let $F = F_1^{n_1} \dots F_r^{n_r}$ be the decomposition of F into irreducible factors. Then $Z(F) = Z(F_1) \cup \dots \cup Z(F_r)$ is the decomposition of $Z(F)$ into irreducible components. In particular $Z(F)$ "forgets" the multiplicities $n_1, \dots, n_r$. We will however want to remember these multiplicities. Strictly speaking, this means that we are taking the zero locus of F not just as an algebraic set, but as a subscheme. Practically it just means the following: Any nonconstant homogeneous polynomial F determines a curve $Z(F)$, together with the multiplicities n_i of the irreducible components $Z(F_i)$. Conversely $Z(F)$ and the multiplicities n_i determine F up to multiplication by a nonzero constant $\lambda \in k$. So we are just talking about homogeneous polynomials $F \in k[x, y, z]$ modulo multiplication by constants.

We will mostly study the intersection behavior of two such curves. We have compactified $\mathbb{A}^2$ to $\mathbb{P}^2$, so that any two lines (i.e. zero loci of linear polynomials) intersect in $\mathbb{P}^2$. From the chapter on dimension it follows that now any two curves $Z(F)$, $Z(G)$ in $\mathbb{P}^2$ intersect. The main result of this chapter is the famous Theorem of Bézout. It says that $Z(F)$ and $Z(G)$ (with no common components) intersect in precisely $deg(F)deg(G)$ points, if we count the points with the correct (scheme theoretic) multiplicities. The Theorem of Bézout can be viewed as the starting point of Intersection Theory, an important field of algebraic geometry, which deals with the intersection of subvarieties of a given variety. In particular it computes the number of intersection points when it is finite.

We then give a number of applications of the Theorem of Bézout to the geometry of plane curves. The most important application is that a nonsingular cubic in $\mathbb{P}^2$ is in a natural way an abelian group. This can be viewed as the beginning of the theory of elliptic curves and abelian varieties.

1. Plane curves

1.1. Definitions of plane curves. We now want to define plane curves in $\mathbb{A}^2$ and in $\mathbb{P}^2$. As said above, we want to allow them also to be defined by polynomials with multiple factors.

DEFINITION 1.1. Let $F \in k[x, y]$ be a nonconstant polynomial. Let $[F]$ be the class of F modulo multiplication by nonzero constants. We call $[F]$ an *affine plane curve*. Similarly let $F \in k[x, y, z]$ be a nonconstant homogeneous polynomial. Let again $[F]$ the class of F modulo multiplication by nonzero constants. Then we call $[F]$ a *projective plane curve.* Most of the time we will just write F instead of $[F]$.

Now let either $F \in k[x, y]$ be a nonconstant polynomial or $F \in k[x, y, z]$ a nonconstant homogeneous polynomial. We say that $p \in F$, if $p \in Z(F)$ (or equivalently if $F(p) = 0$). We call $Z(F)$ the *support* of F. Let $F = F_1^{n_1} \ldots F_r^{n_r}$ the decomposition of F into irreducible factors. Then we know that $Z(F) = Z(F_1) \cup \ldots \cup Z(F_r)$ is the decomposition of $Z(F)$ into irreducible components. We call n_i the *multiplicity* of $Z(F_i)$. If $n_i > 1$, then $Z(F_i)$ is called a *multiple component.* We call the plane curve F *irreducible*, if F is irreducible as a polynomial, i.e. if $Z(F)$ is irreducible and not multiple. Otherwise F is called reducible. The *degree* $deg(F)$ of the plane curve F is just the degree of F as a polynomial.

REMARK 1.2. It is evident that giving $[F]$ is equivalent to giving $Z(F)$ and the multiplicities n_i of the irreducible components $Z(F_i)$.

Now we concentrate on local properties of plane curves. If $F \subset \mathbb{P}^2$ is a projective plane curve, we can look at $F_a = F(x, y, 1)$. This defines a plane curve $[F_a] \subset \mathbb{A}^2$. Let $F = F_1^{n_1} \ldots F_r^{n_r}$ be the decomposition of F into irreducible factors. Then $Z(F) \cap \mathbb{A}^n = Z(F_a)$ and $F_a = (F_1)_a^{n_1} \ldots (F_r)_a^{n_r}$ is the decomposition of F_a into irreducible factors. To study the local properties of the curve F near a point $(a, b) = [a, b, 1] \in \mathbb{A}^2$, we can study F_a. We extend the definitions of some local properties of affine varieties to plane curves (which no longer are varieties).

DEFINITION 1.3. Let $F \subset \mathbb{A}^2$ be an affine plane curve. We can assume that $p = (0, 0) \in F$. The *tangent space* of F at p is $T_pF := Z(F^{(1)})$. p is called a *nonsingular point* of F if $T_pF \neq \mathbb{A}^2$, or equivalently if $F^{(1)} \neq 0$. Otherwise p is called a *singular point.* The *tangent cone* of F at p is $C_pF := Z(F^{in})$. This is a cone in $\mathbb{A}^2$, i.e. a union on lines through $p = (0, 0)$. Let us briefly see this directly: F^{in} is a homogeneous polynomial in x, y. Thus $F^{in}(x, 1)$ is a polynomial in one variable, that splits into linear factors $F^{in}(x, 1) = (x - a_1)^{r_1} \ldots (x - a_k)^{r_k}$. Then $F^{in} = y^l (x - a_1 y)^{r_1} \ldots (x - a_k y)^{r_k}$ for some $l \geq 0$.

We have to see that for irreducible curves in $\mathbb{A}^2$ these definition coincide with our previous ones.

REMARK 1.4.
1. By definition, if F is irreducible and $C = Z(F)$, then $T_pC = T_pF$ and $C_pC = C_pF$, in particular p is a nonsingular point of C if and only if it is a nonsingular point of $[F]$.
2. More generally, let $C = C_1 \cup \ldots \cup C_r$ be the decomposition of $C = Z(F)$ into irreducible components, and assume that C_1 is not a multiple component and $p \in C_1 \setminus (C_2 \cup \ldots \cup C_r)$. Then $T_p[F] = T_pC_1$ and $C_pF = C_pC_1$ in particular p is a nonsingular point of C if and only if it is a nonsingular point of $[F]$.
3. Now let $p \in F$ lie on the intersection of two components or on a multiple component of F. Then p is a singular point of F.

PROOF. (1) is clear. (2) We can assume $p = (0, 0)$. Let $F = F_1 G$, where F_1 is the irreducible factor corresponding to C_1 and G is the product of all other irreducible factors. Then $G(0,0) = a \neq 0$ and $F^{(1)} = F_1^{(1)} \cdot a$. Thus $T_pC_1 = T_p[F]$ and $C_pC_1 = C_p[F]$.

(3) We can assume $p = (0,0)$. Assume $F = F_1F_2$ (with possibly $F_1 = F_2$ and $F_1(p) = F_2(p) = 0$. Then $F^{(1)} = F_1^{(1)}F_2(p) + F_1(p)F_2^{(1)} = 0$. Thus p is a singular point of F. □

1.2. Moduli spaces of plane curves. Now we restrict our attention to projective plane curves. We introduce the *moduli space* of all curves of degree d, i.e. a space that parametrizes all curves of degree d in $\mathbb{P}^2$. This will allow us to study all curves of degree d at the same time. This is very simple, because as we have just said, $[F]$ is just the equivalence class of the polynomial F modulo multiplication by nonzero constants.

DEFINITION 1.5. Fix $d > 0$. Let $N(d) := \binom{d+2}{2} - 1$. Let $M_0, \ldots, M_{N(d)}$ be a fixed ordering of all monomials of degree d in x, y, z. Giving $[F]$ for $F = \sum_{i=0}^{N(d)} a_iM_i$ is equivalent to giving the point $[a_0, \ldots, a_{N(d)}] \in \mathbb{P}^{N(d)}$. Thus we call $\mathbb{P}^{N(d)}$ the *space of curves of degree* d in $\mathbb{P}^2$. When there is no risk of confusion we will also just write $[F]$ for $[a_0, \ldots, a_{N(d)}]$, if $F = \sum_{i=0}^{N(d)} a_iM_i$.

REMARK 1.6. $\mathbb{P}^{N(d)}$ is the simplest example of a *moduli space*, i.e. a variety that parametrizes in a natural way other objects of algebraic geometry – in this case plane curves of degree d. The study of moduli spaces is an important field of algebraic geometry.

EXAMPLE 1.7.
(1) ($d = 1$) A line $ax + by + cz$ in $\mathbb{P}^2$ corresponds to $[a, b, c] \in \mathbb{P}^2$. Thus the lines in $\mathbb{P}^2$ form a $\mathbb{P}^2$.
(2) ($d = 2$) The conic $ax^2+bxy+cy^2+dxz+eyz+fz^2$ corresponds to $[a, b, c, d, e, f] \in \mathbb{P}^5$, so the conics in $\mathbb{P}^2$ form a $\mathbb{P}^5$. Similarly the cubics (curves of degree 3) in $\mathbb{P}^2$ form a $\mathbb{P}^9$.

If we put conditions on curves of degree d, the curves satisfying these conditions will form a subset of $\mathbb{P}^{N(d)}$. In nice cases it will be a closed subset of $\mathbb{P}^{N(d)}$, or even a linear subspace. Then we can intersect several such subspaces to find curves which fulfill several conditions simultaneously.

LEMMA 1.8.
(1) *Let $p \in \mathbb{P}^2$. The set of curves of degree d passing through p is a hyperplane in $\mathbb{P}^{N(d)}$.*
(2) *Let $T : \mathbb{P}^2 \to \mathbb{P}^2$ be a projective change of coordinates. The map $[F] \mapsto [F \circ T]$ is a projective change of coordinates on $\mathbb{P}^{N(d)}$.*

PROOF. (1) The curve corresponding to $[a_0, \ldots, a_{N(d)}]$ passes through $p = [a, b, c]$, if and only if $\sum_{i=0}^{N(d)} a_iM_i(a, b, c) = 0$. This defines a hyperplane.

(2) If $F = \sum_{i=0}^{N(d)} a_iM_i$, then $F \circ T = \sum_{i=0}^{N(d)} a_i(M_i \circ T)$ and each $M_i \circ T$ is a linear combination of the M_j. Thus the map $[F] \mapsto [F \circ T]$ is linear. It is invertible, because its inverse is $[F] \mapsto [F \circ T^{-1}]$. □

Corollary 1.9. *Given a set of $N(d)$ points in $\mathbb{P}^2$ there is a curve of degree d containing all points in the set.*

Proof. This is clear because the intersection of $N(d)$ hyperplanes in $\mathbb{P}^{N(d)}$ is nonempty. $\square$

Example 1.10. Through any two points $p \neq q$ in $\mathbb{P}^2$ there is a unique line.

Given $N(d)$ *general* points in $\mathbb{P}^2$, one could hope that there is a unique curve of degree d passing through all of them. We show that for conics this is indeed the case. The point is to show that the hyperplanes in $\mathbb{P}^{N(d)}$ corresponding to the points are linearly independent.

Corollary 1.11. *Let p, q, r, s, t be 5 different points in $\mathbb{P}^2$ and assume that no 3 of them lie on a line. Then there is a unique conic C through p, q, r, s, t. Furthermore C is irreducible.*

Proof. By a projective change of coordinates we can assume that

$$p = [u, v, 1],\ q = [1, 1, 1],\ s = [1, 0, 0],\ t = [0, 1, 0],\ r = [0, 0, 1].$$

Let $F = ax^2 + bxy + cy^2 + dxz + eyz + fz^2$ be a conic. Then $s \in F$ means $a = 0$, $t \in F$ means $c = 0$, $r \in F$ means $f = 0$. $q \in F$ means $b + d + e = 0$, i.e. $e = -b - d$. Thus $F = bxy + dxz - (b + d)yz$. Then $p \in F$ means $b(uv - v) + d(u - v) = 0$. Thus

$$[F] = [(u - v)xy + (v - uv)xz + (uv - u)yz].$$

Note that F has to be irreducible, because no 3 of p, q, r, s, t lie on a line, thus no union of two lines can contain them all. $\square$

This is a very simple example of how to use moduli spaces and intersection theory to solve problems of enumerative geometry. Assume our task was to determine the number of *irreducible* conics through 5 general points in $\mathbb{P}^2$. First we introduced the *projective* moduli space $\mathbb{P}^5$ of all conics, on which intersection theory works well (in this case that just means that the intersection of 5 hyperplanes is nonempty). We used this to show that there is a unique conic through 5 general points. Finally we showed that it has to be irreducible.

1.3. Closed subschemes of $\mathbb{A}^2$. We will want to count the intersection points $Z(F, G)$ of two curves F, G in $\mathbb{A}^2$ or $\mathbb{P}^2$ with their natural multiplicities. The best way of understanding these multiplicities is by viewing the intersection as a scheme. Therefore we will introduce in an ad hoc way closed subschemes of $\mathbb{A}^2$. The idea is that giving a closed subscheme of $\mathbb{A}^2$ is equivalent to giving an ideal in $k[x, y]$.

Definition 1.12. A *closed subscheme* $X \subset \mathbb{A}^2$ is a pair $X = (X_{red}, I(X))$, where $I(X) \subset k[x, y]$ is an ideal and $X_{red} = Z(I(X))$ is a closed subset of $\mathbb{A}^2$. $I(X)$ is called the *ideal* of X and X_{red} the *support* of X. We put $A(X) := k[x, y]/I(X)$.

We can extend some of the local properties of varieties to closed subschemes of $\mathbb{A}^2$. We say $p \in X$ if $p \in X_{red}$. Let $p \in X$. We can assume that $p = (0, 0)$. Then $T_pX := Z(I^{(1)})$ is called the *tangent space* of X at p.

REMARK 1.13. (1) $X = (X_{red}, I(X))$ is determined by $I(X)$. Thus a closed subscheme of $\mathbb{A}^2$ is essentially just an ideal in $k[x, y]$.
(2) Giving a plane curve $[F] \subset \mathbb{A}^2$ is equivalent to giving the closed subscheme $(Z(F), \langle F \rangle)$. Thus plane curves in $\mathbb{A}^2$ are subschemes of $\mathbb{A}^2$.
(3) A closed subset $Y \subset \mathbb{A}^2$ can be identified with the closed subscheme $(Y, I(Y))$. Thus the closed subsets of $\mathbb{A}^2$ form a subset of the closed subschemes of $\mathbb{A}^2$.
(4) Obviously everything works in the same way in $\mathbb{A}^n$.

How is $X = (X_{red}, I(X))$ different from the just the algebraic set X_{red}? The difference is that $A(X)$ is larger than $A(X_{red})$. Let $\pi : k[x, y] \to A(X)$ be the natural projection. If $X \subset \mathbb{A}^2$ is a closed subset, π is just the restriction to X. Intuitively, also for $X \subset \mathbb{A}^2$ a closed subscheme we want to view π as the restriction to X. Then there are $F \in k[x, y]$ with $F|_{X_{red}} = 0$, but $F|_X \neq 0$. Intuitively this means that X is (infinitesimally) larger than X_{red}.

EXAMPLE 1.14. (1) Let $X = Z_S(y^2) \subset \mathbb{A}^2$. Then $X_{red} = Z(y)$ and $A(X) = k[x, y]/\langle y^2 \rangle$. Thus $F = \sum_i a_i(x)y^i$ (with $a_i(x) \in k[x]$) vanishes on X if and only if $a_0(x) = a_1(x) = 0$. One says that X is a first order neighbourhood of $Z(y)$.
(2) Now we want to see what this has to do with intersecting curves in $\mathbb{A}^2$. For $a \in k$ let $F_a = y - x^2 + a^2$. Then the intersection scheme of $Y_2 := Z(F_a)$ and $Y_1 := Z(y)$ is $X_a = (Z(F_a, y), \langle F_a, y \rangle)$. For $a \neq 0$ we see that X_a is the closed subset $Z(x^2 + a^2, y) = \{(a, 0), (-a, 0)\}$ and $X_0 = (\{(0, 0)\}, \langle x^2, y \rangle)$, i.e. when the two intersection points come together, they become a subscheme. In both cases we get $dim_k(A(X_a)) = 2$. So this dimension gives us the number of intersection points with multiplicities. Note also that $T_{(0,0)}X_0 = Z(x)$, thus X_0 "remembers" that the two points $(a, 0)$, $(-a, 0)$ came together on the line $x = 0$.

2. Bézout's Theorem and applications

2.1. Intersection numbers and intersection multiplicities. Let $F, G \subset \mathbb{P}^2$ be two plane projective curves without a common component. Then $Z(F, G)$ is a finite set $\{p_1, \dots, p_r\}$. Thus there is a line $L \subset \mathbb{P}^2$ passing through none of the p_i. We can assume (by a change of coordinates) that $L = Z(z)$ is the line at infinity. Let $F_a = F(x, y, 1)$ and $G_a = G(x, y, 1)$ then (identifying as usual $(a, b) = [a, b, 1]$) we have $Z(F, G) = Z(F_a, G_a)$.

In the example above we have seen that $dim_k(k[x,y]/\langle F_a, G_a\rangle)$ should count the number of intersection points of F and G with the correct multiplicities. How do we get the multiplicities for the p_i? We have to see that as a vector space $k[x,y]/\langle F_a, G_a\rangle$ is the direct sum of $k[x,y]/I_j$ where I_j is an ideal with $Z(I_j) = \{p_i\}$.

DEFINITION 2.1. Let R, S be rings. Then the *product ring* is $R\times S$ with componentwise addition $(r_1, s_1)+(r_2, s_2) = (r_1+r_2, s_1+s_2)$ and multiplication $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2)$.

THEOREM 2.2. *Let $F, G \in k[x,y]$ and assume $Z(F,G) \subset \mathbb{A}^2$ is a finite set of points $\{p_1, \dots, p_r\}$. Let $M_i := I(p_i)$. Then for any d sufficiently large, there is a natural isomorphism*

$$\varphi : k[x,y]/\langle F, G\rangle \to \times_{i=1}^r k[x,y]/(\langle F, G\rangle + M_i^d).$$

Furthermore $k[x,y]/(\langle F, G\rangle + M_i^d)$ is independent of d as long as d is large enough.

PROOF. By the Nullstellensatz we get that

$$\sqrt{I} = I(\{p_1, \dots, p_r\}) = \bigcap_{i=1}^r M_i.$$

Thus $(\bigcap_i M_i)^d \subset I$ for some $d > 0$. (If $f_1, \dots, f_l$ are generators of $\bigcap_i M_i$, then $f_i^s \in I$ for some $s > 0$. Take $d \geq rs$.) It is not difficult to show (exercise) that $\bigcap_i M_i^d = (\bigcap_i M_i)^d \subset I$.

We write $R := k[x,y]/\langle F, G\rangle$ and $R_i := R/M_i^d$. Thus we have the (surjective) canonical projections $\varphi_i : R \to R_i$. This give a canonical homomorphism $\varphi = (\varphi_1, \dots, \varphi_r) : R \to \times_{i=1}^r R_i$.

φ is injective. Let $h \in R$ be the class of $H \in k[x,y]$, with $\varphi_i(h) = 0$ for all i. Then $H \in \langle F, G\rangle + M_i^d$ for all i, as $\langle F, G\rangle \supset \bigcap_i M_i^d$, this implies $H \in \langle F, G\rangle$ and $h = 0$.

φ is surjective. Choose $F_i \in k[x,y]$ with $F_i(p_j) = 1$ if $i = j$ and 0 otherwise. Let $E_i = 1 - (1 - F_i^d)^d$ and let e_i be its class in R. Note that $E_i = F_i^d D_i$ for some $D_i \in k[x,y]$. Thus $E_i \in \bigcap_{j\neq i} M_j^d$ and $1-E_i = (1-F_i^d)^d \in M_i^d$. Therefore $\varphi_i(e_j) = 1$ if $i = j$ and 0 otherwise. Let $(b_1, \dots, b_r) \in \times_{i=1}^r R_i$. As the φ_i are surjective, $b_i = \varphi_i(a_i)$ for some $a_i \in R$, and $\varphi(e_1 a_1 + \ldots + e_r a_r) = (\varphi_1(a_1), \dots, \varphi_r(a_r)) = (b_1, \dots, b_r)$.

The last statement is easy: Assume $d_1 > d$. Let $\varphi_i' : R \to R/M_i^{d_1} := R_i'$ and $\psi_i : R/M_i^{d_1} \to R/M_i^d$ be the natural projections and let $\varphi' = (\varphi_1', \dots, \varphi_r')$. Then φ and φ' are isomorphisms and $\varphi = (\psi_1 \times \ldots \times \psi_r)\circ\varphi'$, thus all ψ_i are isomorphisms. $\square$

REMARK 2.3. It is easy to show that $k[x,y]/(\langle F, G\rangle + M_i^d) \simeq \mathcal{O}_{\mathbb{A}^2, p_i}/\langle F, G\rangle$.

DEFINITION 2.4. The *intersection number* of F and G is

$$deg(F.G) := dim_k(k[x,y]/\langle F_a, G_a\rangle).$$

Let $p \in \mathbb{P}^2$. We write $M_p := I(p)$. The *intersection multiplicity* of F and G at p

$$I_p(F.G) := \begin{cases} dim_k(k[x,y]/(\langle F_a, G_a\rangle + M_p^d) & p \in F \cap G,\ d \text{ sufficiently large}, \\ 0 & \text{otherwise}. \end{cases}$$

A *zero cycle* on $\mathbb{P}^2$ is a formal sum

$$\sum_{p\in\mathbb{P}^2} n(p)p, \quad n(p)\in\mathbb{Z}, \quad \text{only finitely many } n(p)\neq 0.$$

We write $\sum_{p\in\mathbb{P}^2} n(p)p \geq \sum_{p\in\mathbb{P}^2} m(p)$ if $n(p)\geq m(p)$ for all p. In particular we write $\sum_{p\in\mathbb{P}^2} n(p)p \geq 0$ and call it a *positive zero cycle* if all $n(p)\geq 0$. The *degree* of a zero cycle is $deg(\sum_p n(p)p) = \sum_p n(p)$.

The *intersection cycle* of F and G is

$$F.G := \sum_{p\in\mathbb{P}^2} I_p(F.G)p.$$

Note that $F.G$ is a positive 0 cycle of degree $deg(F.G)$ the intersection number of F and G.

We now want to see how to compute the intersection numbers $I_p(F.G)$. This works best if p is a nonsingular point on one of the curves (say on F).

Remark 2.5. (1) Fix $d>0$. Let $M := \langle x,y\rangle$. Note that in $k[x,y]/M^d$ the class of every $H\in k[x,y]$ with $H(0)\neq 0$ is invertible: We can assume $H(0)=1$ and write $H=1-L$ with $L\in M$. Then $H(1+L+\ldots+L^{d-1}) = 1-L^d\equiv 1$ modulo M^d.

(2) In complex analysis, if we have an equation $y=f(x,y)$ with $f(x,y)\in M^2$, we can use the implicit function theorem to solve for y, i.e in a neighbourhood of $(0,0)$ we can write $y=g(x)$ for g a holomorphic function. In algebraic geometry this is impossible, but we can do it modulo M^d:

Let $F := y - F_2(x,y)$ with $F_2\in M^2$. For all $i=3,\ldots,d$ put $F_i = F_{i-1}(x,F_2(x,y))$. Finally put $\overline{F} := F_d(x,0)\in k[x]$, and for $G\in k[x,y]$ we put $\overline{G} = G(x,\overline{F})$. Then

$$\langle y-\overline{F}\rangle + M^d = \langle F\rangle + M^d, \quad G\equiv \overline{G} \bmod \langle F\rangle + M^d, \quad \langle y-\overline{F},\overline{G}\rangle + M^d = \langle F,G\rangle + M^d.$$

Proof. We have polynomials $F=H_0,\ldots,H_s = y-F_d$ where each H_{i+1} is obtained from H_i by replacing a monomial $a_{ij}x^iy^j$ in H_i with $j>0$ and $i+j\geq 2$ by $a_{ij}x^iy^{j-1}F_2$, i.e. $H_{i+1} = H_i - a_{ij}x^iy^{j-1}F$. Thus finally $y-F_d = F-LF = F(1-L)$ for $L\in M$. As $(1-L)$ is invertible modulo M^d it follows that $\langle F\rangle + M^d = \langle y-F_d\rangle + M^d$.

Finally y occurs in F_i only in monomials of degree at least i, thus $\overline{F}\equiv y-F_d$ modulo M^d. For each monomial $N := a_{ij}x^iy^j$ we get $N-\overline{N}=0$ if $j=0$ and otherwise

$$N-\overline{N} = a_{ij}x^i(y^j - \overline{F}^j) = a_{ij}x^i(y-\overline{F})(y^{j-1}+\ldots+\overline{F}^{j-1}) \in \langle y-\overline{F}\rangle.$$

Thus $G-\overline{G}\in\langle y-\overline{F}\rangle \subset \langle F\rangle + M^d$. □

Definition 2.6. Let $p\in F$ be a nonsingular point. We make an affine coordinate change so that $p=(0,0)$ and $F^{(1)} = y$, i.e. $F = y - F_2(x,y)$, with $F\in M^2$. Choose d as in the Theorem, so that $k[x,y]/(\langle F,G\rangle + M^d) = k[x,y]/(\langle F,G\rangle + M^e)$ for all $e>d$. Then $\overline{G} = x^kG'$ with $G'(0)\neq 0$. We put $ord_p^F(G) := k$, i.e. it is the multiplicity of 0 as a root of $\overline{G}$.

LEMMA 2.7. *$I_p(F.G) = ord_p^F(G)$.*

PROOF. By the above we have

$$\begin{aligned} k[x,y]/(\langle F,G\rangle + M^d) &= k[x,y]/(\langle y-\overline{F},\overline{G}\rangle + M^d) \\ &\simeq k[x]/\langle \overline{G}, x^d\rangle = k[x]/\langle x^k, x^d\rangle = k[x]/\langle x^k\rangle, \end{aligned}$$

because G' is invertible and $d \geq k$. □

EXAMPLE 2.8. $ord_p^F(G)$ is rather easy to compute. Let $F := y - x^2 - xy$, $G := y^2 - x^3$ and $p = (0,0)$. Then $\overline{F} = x^3 + x^4 + \ldots + x^d$. Thus $\overline{G} = x^3 + O(x^4)$, i.e. $ord_p^F(G) = 3$. Note that we don't usually need to determine $\overline{F}$ to a high order but just enough to determine the lowest nonvanishing term of $\overline{G}$.

COROLLARY 2.9. *Let $F, G \in k[x,y]$ and let $p \in F \cap G$.*

1. *If p is a nonsingular point of F and G, and $T_pF \neq T_pG$ (we say F and G intersect* transversally *at p), then $I_p(F.G) = 1$.*
2. *If p is a nonsingular point of F and G, and $T_pF = T_pG$ then $I_p(F.G) \geq 2$.*
3. *If p is a nonsingular point of F, but singular on G, then $I_p(F.G) \geq 2$.*
4. *If p is a singular point of F and G, then $I_p(F.G) \geq 3$.*
5. *If p is a nonsingular point of F and $G, H \in k[x,y]$ have no common component with F, then $I_p(F,GH) = I_p(F,G) + I_p(F,H)$.*
6. *If all points of $F \cap G$ are nonsingular points of F, then $F.GH = F.G + F.H$.*
7. *Let $A \in k[x,y]$. Then $F.(G + AF) = F.G$.*

PROOF. We can assume that $p = (0,0)$. (1),(2),(3) We can assume $F = y + F_2$ and $G = ax + by + G_2$ with $F_2, G_2 \in M^2$. Then $\overline{F} = x^2F'$ with $F' \in k[x]$ and $\overline{G} = ax + O(x^2)$. Thus $I_p(F,G) \geq 2$ if and only if $a = 0$. G is nonsingular at p and not tangent to F at p if and only if $a \neq 0$, if and only if $I_p(F,G) = 1$.

(4) Let F, G be singular at $p = (0,0)$. Then $F, G \in M^2$. Thus by the canonical surjection $k[x,y]/(\langle F,G\rangle + M^d) \to k[x,y]/(\langle F,G\rangle + M^2) = k[x,y]/M^2$, we get $dim_k(k[x,y]/(\langle F,G\rangle + M^d) \geq dim_k(k[x,y]/M^2) = 3$.

(5) We can assume $F = y + F_2$ with $F_2 \in M^2$. Write $\overline{G} = x^kG'$, $\overline{H} = x^lH'$) with $G'(0) \neq 0$, $H'(0) \neq 0$. Then by definition $\overline{GH} = \overline{G}\,\overline{H} = x^{k+l}G'H'$. Thus $ord_p^F(GH) = ord_p^F(G) + ord_p^F(H)$.

(6) Let $p \in F \cap GH$. We have to show $I_p(F,GH) = I_p(F,G) + I_p(F,H)$. If $p \in F \cap G$ this is (5). Thus assume $p \notin F \cap G$. Then $I_p(F,G) = 0$ and $G(p) \neq 0$, thus G is a unit in $k[x,y]/M^d$. Therefore $\langle F, GH\rangle + M^d = \langle F,H\rangle + M^d$, i.e. $I_p(F,GH) = I_p(F,H) = I_p(F,G) + I_p(F,H)$.

(7) This is because $\langle F, G + AF\rangle = \langle F,G\rangle$. □

2.2. Exact sequences. We need a tool for the proof of Bézout's Theorem: exact sequences. They play an important role in algebra and algebraic topology.

DEFINITION 2.10. A sequence

$$A_0 \xrightarrow{\varphi_1} A_1 \xrightarrow{\varphi_2} \ldots \xrightarrow{\varphi_n} A_n$$

of vector spaces A_i and linear maps φ_i is called an *exact sequence*, if $ker(\varphi_i) = im(\varphi_{i-1})$ for all i.

EXAMPLE 2.11. (1) The sequence $0 \to A \xrightarrow{\varphi} B \to 0$ is exact if and only if φ is an isomorphism.
(2) The sequence $0 \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to 0$ is exact if and only if φ is injective, ψ is surjective and $im(\varphi) = ker(\psi)$.

We will want to use the following.

LEMMA 2.12. *Let $0 \to A_0 \to A_1 \to \ldots \to A_n \to 0$ be an exact sequence of finite-dimensional vector spaces. Then $\sum_{i=0}^{n}(-1)^i dim(A_i) = 0$.*

PROOF. We prove this by induction on $n \geq 1$. The case $n = 1$ is trivial. If $0 \to A_0 \to A_1 \to A_2 \to 0$ is an exact sequence, then $A_2 \simeq A_1/A_0$. Thus $dim(A_2) = dim(A_1) - dim(A_0)$. Now let $0 \to A_0 \to A_1 \to \ldots \to A_n \to 0$ be an exact sequence. Put $B_{n-1} = ker(A_{n-1} \to A_n)$. Then we have an exact sequences

$$0 \to A_0 \to A_1 \to \ldots \to B_{n-1} \to 0, \quad 0 \to B_{n-1} \to A_{n-1} \to A_n \to 0.$$

Thus

$$0 = \sum_{i=0}^{n-2}(-1)^i dim(A_i) + (-1)^{n-1} dim(B_{n-1}) = \sum_{i=0}^{n}(-1)^i dim(A_i).$$

□

2.3. Bézout's Theorem. Now we can finally state and prove the Theorem of Bézout.

THEOREM 2.13. *Let C, D be projective plane curves of degrees m and n respectively, without a common component. Then $deg(C.D) = nm$.*

PROOF. Since $C \cap D$ is finite, we can assume that none of the intersection points lies on the line at infinity $z = 0$. Let $C = [F]$, $D = [G]$ with $F, G \in k[x, y, z]$. Let $F_a = F(x, y, 1), G_a = G(x, y, 1) \in k[x, y]$. Then we know that

$$\sum_{p \in \mathbb{P}^2} I_p(C.D) = \sum_{p \in \mathbb{A}^2} I_p(C.D) = dim_k(k[x, y]/\langle F_a, G_a \rangle).$$

We put

$$\begin{aligned} R &:= k[x, y, z], \quad R^d := k[x, y, z]^{(d)} \\ \Gamma &:= R/\langle F, G \rangle, \quad \Gamma^d = k[x, y, z]^{(d)}/\langle F, G \rangle^{(d)} \text{ (image of } R^d \text{ in } \Gamma), \\ \Gamma_a &:= k[x, y]/\langle F_a, G_a \rangle \end{aligned}$$

The theorem is proved, once we show that

$$dim_k(\Gamma_a) = dim_k(\Gamma^d) = nm, \text{ for } d \geq n + m.$$

(1) Let $d \geq n + m$. We show that $dim_k(\Gamma^d) = nm$. Let $\pi : R^d \to \Gamma^d$ be the natural projection. By definition π is surjective. Let

$$\varphi : R^{d-m} \times R^{d-n} \to R^d; (A, B) \mapsto AF + BG.$$

Then

$$Im(\varphi) = \{AF + BG \mid A \in R^{d-m},\ B \in R^{d-n}\} = \langle F, G\rangle^{(d)} = ker(\varphi).$$

Let $\psi : R^{d-m-n} \to R^{d-m} \times R^{d-n}, C \mapsto (GC, -FC)$. Then obviously ψ is injective and $\varphi \circ \psi = 0$. If $(A, B) \in ker(\varphi)$ then $AF = -BG$. As F and G have no common factors, it follows that $F|B$ and $G|F$, i.e. there exists a $C \in k[x, y, z]^{(d-n-m)}$ with $(A, B) = (GC, -FC) = \psi(C)$. Thus we have shown that the sequence

$$0 \to R^{d-n-m} \xrightarrow{\psi} R^{d-m} \times R^{d-n} \xrightarrow{\varphi} R^d \xrightarrow{\pi} \Gamma^d \to 0$$

is exact. Thus we get

$$\begin{aligned} dim_k(\Gamma^d) &= dim_k(R^d) - dim_k(R^{d-m}) - dim_k(R^{d-n}) + dim_k(R^{d-n-m}) \\ &= \binom{d+2}{2} - \binom{d-m+2}{2} - \binom{d-n+2}{2} + \binom{d-n-m+2}{2} = nm. \end{aligned}$$

(2) For H in R let $[H]$ be its class in Γ. Now we show that $\alpha : \Gamma^d \to \Gamma^{d+1}, [H] \mapsto [zH]$ is injective.

Thus assume $zH = AF + BG$, then we have to show that $H = A'F + B'G$ for some $A', B' \in k[x, y, z]$. For $L \in k[x, y, z]$ let $L_0 := L(x, y, 0) \in k[x, y]$. Since F, G, z have no common zeros, F_0 and G_0 are relatively prime. By $zH = AF + BG$ we have $A_0F_0 = -B_0G_0$. Thus $B_0 = F_0C$, $A_0 = -G_0C$ for some $C \in k[x, y]$. Let $A_1 = A + CG$, $B_1 = B - CF$. Since $(A_1)_0 = (B_1)_0 = 0$, we get $A_1 = zA'$, $B_1 = zB'$ for $A', B' \in k[x, y, z]$. By

$$zH = AF + BG = A_1F + B_1G$$

it follows $H = A'F + B'G$.

(3) Let $d \geq n + m$. Let $A_1, \ldots, A_{nm} \in R^d$ such that their classes $[A_i]$ form a basis of Γ^d. Let $(A_i)_a = A_i(x, y, 1)$ and let a_i be the class of $(A_i)_a$ in Γ_a. We claim that the a_i form a basis of Γ_a. Note that $\alpha : \Gamma^d \to \Gamma^{d+1}$ is an isomorphism as an injective homomorphism of vector spaces of the same dimension. Thus the $[z^rA_i]$ form a basis of Γ^{d+r} for all $r \geq 0$.

The a_i generate Γ_a: Let h be the class of $H \in \Gamma_a$. Then $z^lH(\frac{x}{z}, \frac{y}{z}) \in k[x, y, z]^{(d+r)}$ for some $l, r \geq 0$. Thus

$$z^lH(\tfrac{x}{z}, \tfrac{y}{z}) = \sum_i \lambda_i z^r A_i + BF + CG, \quad \text{for } \lambda_i \in k,\ B, C \in k[x, y, z].$$

Then

$$H = (z^lH(\tfrac{x}{z}, \tfrac{y}{z}))_a = \sum_i \lambda_i (A_i)_a + B_aF_a + C_aG_a, \quad \text{i.e. } h = \sum_i \lambda_i a_i.$$

The a_i are linearly independent: If $\sum_i \lambda_i a_i = 0$, then

$$\sum_i \lambda_i (A_i)_a = BF_a + CG_a, \quad \text{for } B, C \in k[x, y].$$

For $H \in k[x, y, z]$ we have $H = z^k H_a(x/z, y/z)$ for some $k \geq 0$. Thus we get

$$\sum_i \lambda_i z^r A_i = z^s B(\tfrac{x}{z}, \tfrac{y}{z})F + z^t C(\tfrac{x}{z}, \tfrac{y}{z})G,$$

with $r, s, t \geq 0$ s.th. $z^s B(\frac{x}{z}, \frac{y}{z}), z^t C(\frac{x}{z}, \frac{y}{z}) \in k[x, y, z]$. Thus $\sum_i \lambda_i [z^r A_i] = 0$ in Γ^{d+r}. As the $[z^r A_i]$ form a basis of Γ^{d+r}, we get $\lambda_i = 0$ for all i. □

So we know that $[F]$ and $[G]$ intersect in nm points counted with multiplicities. So they intersect in at least one point and at most in nm points.

COROLLARY 2.14. *Let $[F], [G]$ be projective plane curves of degrees n and m respectively. If they have more than nm points in common, then they have a common component.*

2.4. Singular points. We can apply Bézout's Theorem to get a sharp bound on the number of singular points that an irreducible curve of degree d in $\mathbb{P}^2$ can have. A line in $\mathbb{P}^2$ has no singular point. If a conic Q in $\mathbb{P}^2$ has a singular point p, then it is reducible: By a change of coordinates we can assume $p = (0, 0) \in \mathbb{A}^2$. Then $Q^{(0)} = Q^{(1)} = 0$, thus $Q = Q^{(2)}$, therefore $Z(Q)$ is equal to its tangent cone, i.e. a union of lines.

THEOREM 2.15. *Let $C \subset \mathbb{P}^2$ be an irreducible curve of degree d. Then C has at most $\binom{d-1}{2}$ singular points.*

PROOF. Let C be a curve with more than $\binom{d-1}{2}$ singular points. We have to show that C is reducible. Choose $\binom{d-1}{2} + 1$ singular points q_i of C and $2d - 3$ other points on p_i on C, so that all the p_i and all the q_i are distinct. These are $\binom{d+1}{2} - 1$ points in $\mathbb{P}^2$, thus there is a curve D of degree $(d - 1)$ through the p_i and the q_i. Assume C and D do not have a common component. Then $I_{q_i}(C.D) \geq 2$ and $I_{p_i}(C.D) \geq 1$. Thus $deg(C.D) \geq 2\binom{d-1}{2} + 2 + (2d - 3) = d(d - 1) + 1$ a contradiction to Bézout's Theorem. Thus C and D have a common component and C is reducible. □

A question that is natural to ask is what happens when the inequality becomes an equality: How many irreducible curves of degree d are there in $\mathbb{P}^2$ with precisely $\binom{d-1}{2}$ singularities? One can show that the curves with 1 singularity form a hypersurface in the moduli space $\mathbb{P}^{N(d)}$ of all curves of degree d in $\mathbb{P}^2$. Thus we expect a finite number N_d of irreducible curves of degree d through $\binom{d+2}{2} - 1 - \binom{d-1}{2} = 3d - 1$ general points in $\mathbb{P}^2$.

EXAMPLE 2.16. $N_1 = 1$, there is one line through 2 points. We have shown $N_2 = 1$, there is one irreducible conic through 5 general points. It is not difficult to show $N_3 = 12$, there are 12 irreducible singular cubics through 8 general points. Zeuthen showed in 1873 that $N_4 = 620$.

The general formula is a famous result of Kontsevich proved in 1993.

THEOREM 2.17. *(Kontsevich) For $d \geq 2$*

$$N_d = \sum_{e=1}^{d-1} N_e N_{d-e} \Big(e^2(d-e)^2 \binom{3d-4}{3e-2} - e^3(d-e)\binom{3d-4}{3e-1} \Big).$$

This formula determines all the N_d starting from $N_1 = 1$. The methods of proof are motivated by theoretical physics. The result stands at the beginning of the very active research topic of quantum cohomology. Kontsevich uses a new moduli space of curves in $\mathbb{P}^2$ (or rather morphisms of curves into $\mathbb{P}^2$). A somewhat elementary introduction to this result can be found in: J. Kock, I. Vainsencher, *Kontsevich's formula for rational plane curves*,

`http://www.mat.ufmg.br/~israel/kontsevich.html`

2.5. Max Noether's Theorem. Let $F, G, H \subset \mathbb{P}^2$ be plane curves. Assume $H.F \geq G.F$, i.e. H intersects F in a bigger 0-cycle than G. Can we find a curve B that accounts for the difference, i.e. $B.F = H.F - G.F$? Note that we do not claim that B has to be a component of H. Note also that automatically $deg(B) = deg(H) - deg(G)$. Max Noether's theorem ensures that this is at least the case if all points of $G \cap F$ are nonsingular points of F. In fact the original theorem is more general, but this is the most important special case.

THEOREM 2.18. *(M. Noether's $AF + BG$ Theorem) Let $F, G, H \subset \mathbb{P}^2$ be plane curves without common components. Assume $H.F \geq G.F$. Assume furthermore that all points of $G \cap F$ are nonsingular points of F. Then there exists a curve B of degree $deg(H) - deg(G)$ with $H.F = B.F + G.F$.*

PROOF. It is enough to find forms $A, B \in k[x, y, z]$ with $H = AF + BG$, because then $H.F = BG.F = B.F + G.F$. We can assume that $F \cap G \subset \mathbb{A}^2$. Let $p \in F \cap G$, we can assume $p = (0, 0)$ and $F = y + F_2$ with $F_2 \in M^2$. For $E \in k[x, y, z]$ let $E_a := E(x, y, 1)$. We use the notations of Remark 2.5. We write $\overline{E}$ for $\overline{E}_a$. We have $\overline{H} = x^l H'$, $\overline{G} = x^k G'$, with $H'(0) = G'(0) \neq 0$ and $l = I_p(H.F) \geq I_p(G.F) = k$. As G' is invertible in $k[x, y]/M^d$, we get

$$\overline{H} = x^{l-k}\overline{G}H'/G' \in \langle \overline{G} \rangle + M^d,$$

As $H_a \equiv \overline{H} \bmod \langle F \rangle + M^d$, we get that $H_a \in \langle F, \overline{G} \rangle + M^d = \langle F, G \rangle + M^d$. Thus the class of H_a in $R_p := k[x, y]/(\langle F_a, G_a \rangle + M_p^d)$ is zero for all $p \in F \cap G$. As the canonical map $k[x, y]/\langle F_a, G_a \rangle \to \times_{p \in F \cap G} R_p$ is an isomorphism, the class of H_a in $k[x, y]/\langle F_a, G_a \rangle$ is zero. In other words we have $H_a = aF_a + bG_a$ with $a, b \in k[x, y]$. Let $A_1 := z^{deg(a)} a(\frac{x}{z}, \frac{y}{z})$, $B_1 := z^{deg(b)} b(\frac{x}{z}, \frac{y}{z})$. Thus $z^r H = z^t A_1 F + z^s B_1 G$ for some $r, s, t \geq 0$, i.e. $z^r H \in \langle F, G \rangle$. In the proof of Bézout's theorem we showed that the multiplication by z on $k[x, y, z]/\langle F, G \rangle$ is injective. Thus we get $H = AF + BG$ with $A, B \in k[x, y, z]$. Replacing A by its part of degree $deg(H) - deg(F)$ and B by its part of degree $deg(H) - deg(G)$, we get A and B homogeneous. $\square$

As a first application of Noether's theorem we prove the Theorem of Pascal: If a Hexagon is inscribed in a nonsingular conic, then the 3 intersection points of the opposite sides lie on a line. This is to be interpreted as follows. Let Q be a conic and let $p_1, p_2, p_3, p_4, p_5, p_6$ be 6 distinct nonsingular points on Q. Let L_i be the line joining p_i and p_{i+1} (where we compute the indices modulo 6).

THEOREM 2.19. *(Pascal) The points* $q_1 := L_1 \cap L_4$, $q_2 := L_2 \cap L_5$ *and* $q_3 := L_3 \cap L_6$ *lie on a line.*

The theorem of Pappus is the special case where Q is the union $H_1 \cup H_2$ of two lines and $p_1, p_3, p_5 \in H_1$ and $p_2, p_4, p_6 \in H_2$.

PROOF. Let $C = L_2 L_4 L_6$, $D = Q$ and $E = L_1 L_3 L_5$ in Noether's theorem. Then $C.D = \sum_{i=1}^{6} p_i$ and these are nonsingular points on C. We have $C.E = (\sum_{i=1}^{6} p_i) + q_1 + q_2 + q_3$, thus by Noether's theorem q_1, q_2, q_3 lie on a line. $\square$

3. Elliptic curves

Let $C \subset \mathbb{P}^2$ be a nonsingular cubic. Fix a point $\mathbf{0}$ in C. The most important application of Bézout's theorem and Noether's theorem is to show that C has in a natural way the structure of an abelian group with $\mathbf{0}$ as neutral element. The pair $(C, \mathbf{0})$ is also called an elliptic curve. The theory of elliptic curves is an important field of algebraic geometry and number theory.

3.1. Group law on a cubic. We first need a result about the intersection of cubics in $\mathbb{P}^2$, which is also interesting in its own right. If a cubic passes through 8 of the 9 intersection points of a cubic with a nonsingular cubic, then it also has to pass through the last.

PROPOSITION 3.1. *Let C, C', C'' be cubics. Suppose $C'.C = \sum_{i=1}^{9} p_i$ for p_i (non necessarily distinct) nonsingular points of C and $C''.C = \sum_{i=1}^{8} p_i + q$. Then $q = p_9$.*

PROOF. Assume $q \neq p_9$. Let L be a line through p_9 not passing through q. Then $L.C = p_9 + r + s$ and $(LC'').C = C'.C + q + r + s$. Thus by Noether's Theorem there is a line L' with $L'.C = q + r + s$. But then $L = L'$ because they have two points in common. Thus $p_9 = q$. □

LEMMA 3.2. *Let C be an irreducible curve of degree $d \geq 2$ and let L be a line. Given $p, q \in C$ nonsingular points (possibly equal), there is a unique line L with $L.C \geq p + q$.*

PROOF. If $p \neq q$ this is obvious. Otherwise L is the tangent line to C at p. □

DEFINITION 3.3. A pair $(C, \mathbf{0})$ of a nonsingular cubic $C \subset \mathbb{P}^2$ and a point $\mathbf{0} \in C$ is called an *elliptic curve*.

We want to see that every elliptic curve has a natural structure of an abelian group. Note that for any two points $p, q \in C$ there is a unique line L such that $L.C = p + q + r$ for some $r \in C$ (if $p = q$, then L is the tangent line to L at p). Define $\varphi : C \times C \to C, (p, q) \mapsto r$. We define an addition $\oplus$ on C by $p \oplus q = \varphi(\mathbf{0}, \varphi(p, q))$.

THEOREM 3.4. *$(C, \oplus)$ is an abelian group, with neutral element $\mathbf{0}$. The inverse of p is $\ominus p := \varphi(p, \varphi(\mathbf{0}, \mathbf{0}))$.*

PROOF. Obviously $\varphi(p, q)$ is symmetric in p and q, therefore $\oplus$ is commutative. $\mathbf{0}$ *is the neutral element:* Let L, L' be lines with

$$L.C = p + \mathbf{0} + r, \quad L'.C = r + \mathbf{0} + p \oplus \mathbf{0}.$$

Then $L = L'$ and $p = p \oplus \mathbf{0}$.

$\ominus p$ is the inverse of p: Choose lines M, M' with

$$M.C = 2\mathbf{0} + \varphi(\mathbf{0},\mathbf{0}), \quad M'.C = p + \varphi(\mathbf{0},\mathbf{0}) + \ominus p.$$

Then $\varphi(p, \ominus p) = \varphi(\mathbf{0},\mathbf{0})$, thus $p \oplus (\ominus p) = \varphi(\mathbf{0}, \varphi(\mathbf{0},\mathbf{0})) = \mathbf{0} \oplus \mathbf{0} = \mathbf{0}$.

The only more difficult part is the associativity. Let $p, q, r \in C$. Let

$$L_1.C = p + q + s, \quad M_1.C = \mathbf{0} + s + p \oplus q, \quad L_2.C = p \oplus q + r + t$$
$$M_2.C = q + r + s', \quad L_3.C = \mathbf{0} + s' + q \oplus r, \quad M_3.C = q \oplus r + p + t'.$$

Then $(p \oplus q) \oplus r = \varphi(\mathbf{0}, t)$, $p \oplus (q \oplus r) = \varphi(\mathbf{0}, t')$, thus we need to show $t = t'$. Let $C' := L_1L_2L_3$, $C'' := M_1M_2M_3$ in the proposition above. Then

$$C'.C = p + q + s + p \oplus q + r + t + \mathbf{0} + s' + q \oplus r$$
$$C''.C = \mathbf{0} + s + p \oplus q + q + r + s' + q \oplus r + p + t'$$

Thus $t = t'$. □

REMARK 3.5. (1) It is not difficult to show that $\ominus : C \to C$ and $\oplus : C \times C \to C$ are morphisms. An algebraic variety X which is also a group such that the group operations are given by morphisms is called an *algebraic group*. If X is projective and the group structure is abelian, then X is called an *abelian variety*. Thus an elliptic curve is an abelian variety. But there are abelian varieties of any dimension.

(2) Let $(C, \mathbf{0})$ be a pair of an irreducible cubic in $\mathbb{P}^2$ and a nonsingular point of C. Then the above definition defines a group structure on C_{reg} with neutral element $\mathbf{0}$.

If $C = Z(zy^2 - x^3)$ is the cuspidal cubic, then $(C_{reg}, \oplus) \simeq (k, +)$.

If $C = Z(zy^2 - (x^2(x+1))$ is a cubic with a node, then $(C_{reg}, \oplus) \simeq (k^*, \cdot)$.

3.2. Weierstrass normal form. The group structure on a cubic C becomes simpler and more geometric if we assume that C has a special form.

DEFINITION 3.6. A plane elliptic curve $(C, \mathbf{0})$ is in *Weierstrass normal form (WNF)* if $C = Z(y^2z - (x^3 + axz^2 + bz^3))$, for $a, b \in k$, and $\mathbf{0} = [0, 1, 0]$.

We write $n \odot p := \underbrace{p \oplus \ldots \oplus p}_{n \text{ times}}$, and call $\{p \in C \mid n \odot p = \mathbf{0}\}$ the group of *n-division points* of C. Evidently this is a subgroup of $(C, \oplus)$.

The special fact about the Weierstrass normal form is that $\mathbf{0}$ is a flex of C.

DEFINITION 3.7. Let $D \subset \mathbb{P}^2$ be an irreducible curve of degree $d \geq 2$. A nonsingular point $p \in D$ is called a *flex* of D if the tangent line L at p fulfills $I_p(L, D) \geq 3$ (i.e. L has a higher order contact).

REMARK 3.8. Let $(C, \mathbf{0})$ be a plane elliptic curve in Weierstrass normal form. We assume $char(k) \neq 2, 3$.

(1) It is easy to check that the nonsingularity of C is equivalent to $x^3 + ax + b$ having only simple roots and this is equivalent to $4a^3 \neq 27b^2$.
(2) $\mathbf{0}$ is a flex of C, and the line $z = 0$ is the tangent line at $\mathbf{0}$.

(3) One can show that every cubic curve D is projectively equivalent to an elliptic curve in Weierstrass normal form, but we will not prove this here. The point is to show that D has a flex.

PROOF. (2) $C_a := C(x, 1, z) = z - (x^3 + axz^2 + bz^3)$ and thus $\overline{C}_a = C_a(x, 0) = x^3$, thus $ord_p^z(C) = 3$. $\square$

THEOREM 3.9. *Let* $(C = Z(zy^2 - (x^3 + ax + b)), \mathbf{0})$ *be an elliptic curve in (WNF).*

(1) *The group structure on* C *is defined by* $p \oplus q \oplus r = \mathbf{0}$*, whenever there is a line with* $L.C = p + q + r$*.*
(2) *For* $(u, v) \in \mathbb{A}^2 \cap C = C \setminus \mathbf{0}$ *we get* $\ominus(u, v) = (u, -v)$*.*
(3) *In particular the* 2*-division points of* C *are* $\mathbf{0}$*,* $e_1 := (\epsilon_1, 0)$*,* $e_2 := (\epsilon_2, 0)$*,* $e_3 := (\epsilon_3, 0)$*, where* $x^3 + ax + b = (x - \epsilon_1)(x - \epsilon_2)(x - \epsilon_3)$*. The group of* 2*-division points is isomorphic to* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$*.*
(4) *A point* $p \in C$ *is a* 3*-division point if and only if it is a flex. (One can show that there are precisely* 9 *flexes and that the group of* 3 *division points is isomorphic to* $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$*).*

PROOF. (2) $\varphi(\mathbf{0}, \mathbf{0}) = \mathbf{0}$ because $\mathbf{0}$ is a flex. Thus by definition $\ominus p = \varphi(p, \varphi(\mathbf{0}, \mathbf{0})) = \varphi(p, \mathbf{0})$. Let $p = (u, v) = [u, v, 1] \in C \setminus \{\mathbf{0}\}$. The line joining p and $\mathbf{0}$ is

$$L_u := Z(x - uz) = \{(u, t) \mid t \in k\} \cup \{\mathbf{0}\}.$$

The two roots of $y^2 = u^3 + au + b$ are $v, -v$. Thus $L_u.C = (u, v) + (u, -v) + \mathbf{0}$ (if $u^3 + au + b = 0$, L_u is tangent to C in $(u, 0)$). Thus $\ominus(u, v) = \varphi((u, v), \mathbf{0}) = (u, -v)$.

(1) Let L be a line with $L.C = p + q + r$. Then $r = \varphi(p, q)$ and $p \oplus q = \varphi(\mathbf{0}, r) = \ominus r$, i.e. $p \oplus q \oplus r = \mathbf{0}$.

(3) p is a 2-division point if and only if $p = \ominus p$. By (2) this is equivalent to $p = \mathbf{0}$ or $p = (u, 0)$ for u a root of $x^3 + ax + b$. We define

$$\mu : \{\mathbf{0}, e_1, e_2, e_3\} \to \mathbb{Z}/2 \oplus \mathbb{Z}/2; \mathbf{0} \mapsto (0, 0), e_1 \mapsto (1, 0), e_2 \mapsto (0, 1), e_3 \mapsto (1, 1).$$

Then $e_i \oplus e_i = \mathbf{0}$ and $Z(y) \cap C = e_1 + e_2 + e_3$, i.e. $e_i + e_j = e_k$ for $\{i, j, k\} = \{1, 2, 3\}$. Thus μ is an isomorphism.

(4) p is a flex if and only if there is a line with $L.C = 3p$. This is equivalent to $p \oplus p \oplus p = 0$. $\square$

So the group law becomes very geometric: Let $p, q \in C \cap \mathbb{A}^2$. Then $p + q$ is obtained as follows. Let L be the line through p and q. Let $r = (u, v)$ be the third intersection point of L with C. Then $p \oplus q$ is the reflection $(u, -v)$ of r at the $y = 0$-axis.

3.3. Elliptic curves over the complex numbers. We will very briefly sketch without proofs how elliptic curves arise in complex analysis. This also gives one 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.

Let $U \subset \mathbb{C}$ be open in the strong 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 3.10. 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 3.11. *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 3.12.

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3, \qquad g_2 = 60 \sum_{\omega\in\Lambda'} \frac{1}{\omega^4}, \quad g_3 = 140 \sum_{\omega\in\Lambda'} \frac{1}{\omega^6}.$$

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 3.13. φ *is a continuous and holomorphic map. Let* C *be the elliptic curve* $Z(y^2z - 4x^3 + g_2xz^2 + g_3z^3) \subset \mathbb{P}^2_{\mathbb{C}}$ *(in WNF) (with the strong topology). Then* φ *induces a homeomorphism* $\overline{\varphi} : \mathbb{C}/\Lambda \to C$.

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 3.14. $\overline{\varphi}$ *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* $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.

3.4. Elliptic curves in number theory. Let $(C, \mathbf{0})$ be an elliptic curve over $\mathbb{Q}$. This means that $C = Z(F)$ where the coefficients of F are rational numbers. If C is in WNF, this means: $C = Z(y^2z - (x^3 + axz^2 + bz^3))$ with $a, b \in \mathbb{Q}$. In number theory one studies the set

$$C(\mathbb{Q}) := \{[a,b,c] \in C \mid a, b, c \in \mathbb{Q}\}$$

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 3.15. (1) The Fermat cubic $C = Z(x^3+y^3-z^3)$. Fermats last theorem (which is easy for $n = 3$), says that $C(\mathbb{Q}) = \{[1,-1,0],[1,0,1],[0,1,1]\}$. Choosing one of these points as $\mathbf{0}$ we get $C(\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$.
(2) Let $C := Z(y^2z + yz^2 - (x^3 - xz^2))$, which is essentially in WNF. Let $\mathbf{0} := [0,1,0]$, which is a flex. Then it has been shown by Tate (1974) that for $P := [0,0,1]$ the map $\mathbb{Z} \to C(\mathbb{Q}), n \mapsto n \odot P$ is an isomorphism of groups, in particular C has rank 1.

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.

Appendix: Proof of 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. We will use Definition 1.1 and Proposition 1.2 from Chapter 3.

REMARK 3.16. Let $f \in k[x_1, \dots, x_n]$ with $f(p) = 0$ for all $p \in \mathbb{A}^n$, then $f = 0$.

PROOF. If $n = 0$, the result is clear. Assume $f \neq 0$. Write $f = \sum_i f_i x_n^i$ with $f_i \in k[x_1, \dots, x_{n-1}]$. 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 $g(x) := f(a_1, \dots, a_{n-1}, x) \neq 0$. This is a polynomial in one variable, so it splits $g(x) = (x - b_1)^{n_1} \cdot \ldots \cdot (x - b_l)^{n_l}$. Choose $b \in k$ with $b \notin \{b_1, \dots, b_l\}$ (this is possible because k is algebraically closed and therefore infinite). Then $f(a_1, \dots, a_{n-1}, b) \neq 0$. $\square$

THEOREM 3.17. *(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 $F^{(d)}(b_1 x, \dots, b_{n-1} x, 1) = F^{(d)}(b_1, \dots, b_{n-1}, 1) x^d$. 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 $im(\varphi)$. $\square$

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 $k = L$. $\square$