SEMINAR ON FUNDAMENTALS OF ALGEBRAIC GEOMETRY I

HÔNG VÂN LÊ * AND PETR SOMBERG **

ABSTRACT. Algebraic geometry is one of the central subjects of mathematics. Mathematical physicists, homotopy theorists, complex analysts, symplectic geometers, representation theorists speak the language of algebraic geometry.

In this seminar we shall discuss some basic topics of algebraic geometry and their relation with current problems in mathematics.

Recommended textbook: J. Harris, Algebraic Geometry: A First Course, I. R. Shafarevich: Basic Algebraic Geometry 1,2, Dolgachev: Introduction to Algebraic Geometry (lecture notes)

CONTENTS

* Institute of Mathematics of ASCR, Zitna 25, 11567 Praha 1, email: hvle@math.cas.cz
** Mathematical Institute, Charles University, Sokolovska 83, 180 00 Praha 8, Czech Republic, email: somberg@karlin.mff.cuni.cz.

1. Overview and proposed topics

1.1. **Overview of our plan.** Algebraic geometry can be thought as an approach to solve *problems in (commutative) algebra and related fields* of computational complexity, representation theory, mathematical physics, number theory, etc. by systematical constructing necessary geometric objects, e.g. we associate to the solution of *a system of polynomial equations* with an *algebraic variety* in the corresponding affine space. The main philosophy is to associate appropriate geometric notions (points, sets, topology, mappings, etc.) with corresponding algebraic notions (ideals, rings, Zariski topology, morphisms, etc.) and conversely, appropriate algebraic notions with corresponding geometric notions. For example, a commutative algebra is considered as an algebra of functions on some set.

Our aims: understand the importance of the following notions and theorems concerning

(1) Algebraic sets and the Hilbert basis theorem
(2) Hilbert's Nullstellensatz and Zariski topology,
(3) Affine variety and projective variety,
(4) Algebraic varieties and their morphisms,
(5) Dimension and tangent spaces,
(6) Smoothness, singularity and resolution of singularity,
(7) Degree and Bezout's theorem,
(8) Riemann-Roch theorem

and able to apply them to various problems in mathematics.

These topics are fundamental in terms of concepts which arise from motivation of corresponding problems and they are important since the synthetic approaches to solve them are typical for algebraic geometry way of thinking. These topics appear in many fields. It is one of our aims to see their patterns in many other fields of mathematics, computer sciences and physics.

The first two books we recommended are classics. They are rich in examples, motivations and exercises with hint. There is one more modern lecture note by Dolgachev- Introduction to Algebraic Geometry (2013). It is modern since it quite short, simple and treats more general objects. Another good book is Undergraduate Algebraic Geometry (2013) by Reid based on his lecture course for 3rd year students in Warwick. It is very elementary and all statements in the book are explained in details. (Too much details without explaining the main idea/big picture is also not optimal.)

Our plan for seminar is as follows:

- Discuss exercises/ problems at the beginning of each meeting.

- Petr Somberg and I shall survey a chosen topic and one of you can explain some small part of chosen topics in detail.

We also make a very short notes of our seminars and place on website.

1.2. **A brief history.** (cf. [Dieudonne1972], see also [Shafarevich2013])

Algebraic geometry traces back to the Greek mathematics, where conics were used to solve quadratic equations. The true birth of algebraic geometry is marked by invention by Fermat and Descartes of "analytic geometry" around 1636 in their manuscripts. A new field of mathematics or sciences arises whenever we encounter a class of new problems or we discover new methods to solve them. Therefore history of algebraic geometry is also characterized by problems, the methods to solve them and related concepts. Since we have not adequate language to deal with concepts in algebraic geometry, the list of problems and methods below is very coarse.

(1) Classification, transformation and invariants (Italian schools in 19 century that leads to the modern notion of algebraic varieties and their morphisms)
(2) Definition and classification of singularities (The Serre varieties, Hironaka resolution of singularity)
(3) Commutative algebra and algebraic geometry (German algebraic school, notably Zariski topology, Hilbert's Nullstellensatz, Noetherian rings and the Hilbert basis theorem)
(4) Analysis and topology in algebraic geometry (The Riemann-Roch theorem)
(5) Grothendick program absorbing all previous developments and starting from the category of all commutative rings (French school)
(6) Applications in various fields of mathematics

1.3. **Tentative plan of our seminar.** Lecture 1: A quick review of the general concept (alg. var and their morphisms, Hilbert basic theorem, Hilbert Nullstellensatz) and discussion of chosen topics. (H. + S. + D.)

Lecture 2: Tangent spaces: motivation.
Lecture 3: Hensel's Lemma + Dimension.
Lecture 4: Dimension + Hilbert's polynomial.
Lecture 5: Smoothness and singularity.
Lecture 6: 27 lines on cubic surfaces.
Lecture 7: Characterization of smoothness via local rings.
Lecture 8: Birational geometry and resolution of singularity.
Lecture 9: Degree and Bezout's theorem.

Lecture 10: Bezout's theorem and resultant.
Lecture 11-12: Riemann-Roch theorem (D.)

2. Algebraic sets and the Hilbert basic theorem

Motivation. We want to translate algebraic language into geometric language. In our dictionary, a system of polynomial equations corresponds to the set of solutions which will be called *an algebraic set*. It is important to know that we can alway find a *finite* basic of the ideal defining an algebraic set. That is the content of the Hilbert basic theorem.

2.1. **Algebraic sets.** We denote by $\mathbb{C}^n$ the complex n-dimensional vector space. This space is also considered as a *complex affine space*, i.e. a set with a faithful freely transitive $\mathbb{C}^n$-action. We also denote this space by $A^n_{\mathbb{C}}$ or $\mathbb{C}^n$, or A^n, once the ground field $\mathbb{C}$ is specified.

The algebraic object associated to this affine space $\mathbb{C}^n$ is the ring $\mathbb{C}[z_1, \cdots, z_n]$ which is also called *the ring of regular functions* over $\mathbb{C}^n$:

$$\mathbb{C}^n \Longleftrightarrow \mathbb{C}[z_1, \cdots, z_n].$$

A set $X \subset \mathbb{C}^n$ is called *algebraic*, if there exists a subset $T \subset \mathbb{C}[z_1, \cdots, z_n]$ such that X is the zero set of T:

$$X = Z(T),$$

i.e. for any $f \in T$ and any $(z_1, \cdots, z_n) \in X$ we have $f(z_1, \cdots, z_n) = 0$. We regard T as a system of polynomial equations and X - its solution. Denote by $I(T)$ the ideal generated by T in $\mathbb{C}[z_1, \cdots, z_n]$. Then we have

$$Z(T) = Z(I(T)).$$

In this way we associate

$$\{I,\ I \text{ is an ideal in } \mathbb{C}[z_1, \cdots, z_n]\} \Longrightarrow \{\text{ algebraic sets in } \mathbb{C}^n\}.$$

It is not clear if the correspondence is injective. Hilbert's Nullstellensatz (Theorem 3.1) provides the full answer to this question.

Exercise 2.1. Show that the union of two algebraic sets is an algebraic set and the intersection of a family of algebraic sets is an algebraic set.

2.2. **The Hilbert basic theorem.**

Theorem 2.2. *Let k be a field. Every ideal in the ring $k[x_1, \cdots, x_n]$ is finitely generated. In other words $k[x_1, \cdots, x_n]$ is noetherian.*

Proof. Using the identity

$$k[x_1, \cdots, x_n] = k[x_1, \cdots, x_{n-1}][x_n]$$

it suffices to prove the following

Lemma 2.3. *Assume that R is a Noetherian ring. Then $R[x]$ is a Noetherian ring.*

Proof. The proof of Lemma 2.3 is very typical for arguments in commutative algebra, where in investigating a polynomial

$$f(x) = a_0x^r + a_x^{r-1} + \cdots$$

we look at its *leading coefficient* a_0, assuming $a_0 \neq 0$. The corresponding term a_0x^r is called *the leading term of f* and denoted by $LT(f)$, see also Subsection 5.1.

Now assume that $A \subset R[x]$ is a proper ideal. We need to show that A is finitely generated.

Denote by $R^i[x]$ the subset of polynomials of at most degree i in $R[x]$.

Let $A(i)$ denote the set of elements of R that occur ass the leading coefficient of a polynomial in $A \cap R^i[x]$. Clearly $A(i)$ is an ideal in R and we have

$$A(i) \subset A(i+1) \subset \cdots$$

since A is an ideal in $R[x]$.

Since R is Noetherian, there exists d such that

$$A(d) = A(d+1) = \cdots ....$$

Since $A(i)$ is ideal in R, it is finitely generated. say by $(a_{i1}, a_{i2}, \cdots, a_{in_i})$. By definition, a_{ij} is the leading coefficient of a polynomial $f_{ij} \in A$. We claim that the set (f_{ij}) generates the ideal A.

Let B denote the ideal generated by (f_{ij}). Clearly B is an ideal of A. By the construction $B(i) = A(i)$. We shall show that any $f \in A$ also belongs to B. Because $B(\deg(f)) = A(\deg(f))$ there exists a polynomial $g \in B$ such that $\deg(f - g) < \deg(f)$. Then

$$f = g + f_1$$

where $g \in B$ and $f_1 \in A$ with $\deg(f_1) < \deg(f)$. Continuing in this way we have

$$f = g + g_1 \cdots + \in B.$$

This completes the proof of Lemma 2.3 □

This completes the proof of Theorem 2.2 □

Remark 2.4. The Hilbert basic theorem is a basic theorem in commutative algebra and in computational algebra. One important tool of computational algebra is Gröbner basis whose idea stems from the proof of the Hilbert basis theorem. On the other hand, determining the lower bound for number of generators of a given ideal is an active area of research with application in computational complexity.

3. Hilbert's Nullstellensatz and Zariski topology

Motivation. In the previous lecture we establish a correspondence between algebraic sets in an affine space $\mathbb{C}^n$ and ideals of the polynomial ring $\mathbb{C}[x_1, \cdots, x_n]$. This correspondence is not 1-1. The Hilbert Nullstellensatz describes exactly the ideals in $\mathbb{C}[x_1, \cdots, x_n]$ which are ideal of algebraic sets. Then we move to geometry part of algebraic sets by introducing the notion of Zariski topology on algebraic sets, which also provides a translation of the notion of "close" or "far away" in the category of radical ideals.

3.1. **Hilbert's Nullstellensatz.** Let us study deeper the correspondence between algebraic sets Y_i in $\mathbb{C}^n$ and ideals $\mathfrak{a}_i$ in $\mathbb{C}[z_1, \cdots, z_n]$. The following properties are obvious

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \Longrightarrow Z(\mathfrak{a}_1) \supset Z(\mathfrak{a}_2),$$
$$Y_1 \subset Y_2 \Longrightarrow I(Y_1) \supset I(Y_2),$$
$$I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2).$$

We shall prove the following important theorem which says that the correspondence between algebraic sets in $\mathbb{C}^n$ and radical ideals in $\mathbb{C}[z_1, \cdots, z_n]$ are 1-1.

Theorem 3.1 (Hilbert's Nullstellensatz)**.** *Let $\mathfrak{a}$ be an ideal in $\mathbb{C}[z_1, \cdots, z_n]$. Then*

$$I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$

Proof. We produce the proof due to Rabinowitsch in his paper in 1929 for a short proof of Hilbert's Nullstellensatz. We reformulate Rabinowisch's trick as follows. Let A be a ring, $I \subset A$ an ideal and $f \in A$. Then it is not hard to see (cf. (3.1) and (3.2))

$$f \in \sqrt{I} \Longleftrightarrow 1 \in \tilde{I} := \langle I, 1 - z_0 f \rangle_{A[z_0]}.$$

Another ingredient is the following Lemma.

Lemma 3.2. *Any maximal ideal* $\mathfrak{m} \subset \mathbb{C}[z_1, \cdots, z_n]$ *is of the form*

$$\mathfrak{m} = (z_1 - a_1, \cdots, z_n - a_n),\ a_i \in \mathbb{C}.$$

Consequently for any ideal $\mathfrak{a} \neq \mathbb{C}[z_1, \cdots, z_n]$ *we have*

$$Z(\mathfrak{a}) \neq \emptyset.$$

Proof. Let $\mathfrak{m}$ be a maximal ideal in $\mathbb{C}[z_1, \cdots, z_n]$. Denote by K the residue class field $\mathbb{C}[z_1, \cdots, z_n]/\mathfrak{m}$. Clearly K contains $\mathbb{C}$ as its subfield, and K has a countable $\mathbb{C}$ -basis, since $\mathbb{C}[z_1, \cdots, z_n]$ has a countable $\mathbb{C}$-basis consisting of monomials $z_1^{k_1} \cdots z_n^{k_n}$.

If $K \neq \mathbb{C}$ then there is an element $p \in K \setminus \mathbb{C}$. Element p is transcendental over $\mathbb{C}$ because $\mathbb{C}$ is algebraic closed [1]. Hence the set

$$(\frac{1}{p - \lambda} |\ \lambda \in \mathbb{C})$$

is uncountable and their elements are linearly independent over $\mathbb{C}$, which is a contradiction, since K has a countable basis. Therefore $K = \mathbb{C}$. In particular we have

$$z_i + \mathfrak{m} = a_i + \mathfrak{m} \text{ for suitable } a_i \in \mathbb{C}.$$

This proves the first statement of Lemma 3.2.

The second assertion follows from the first one, taking into account that $\mathfrak{a}$ must belong to some maximal ideal. □

Continuation of the proof of Hilbert's Nullstellensatz. Let f be a polynomial which vanishes on the set $Z(\mathfrak{a})$. We shall find a finite number m such that $f^m \in \mathfrak{a}$.

We denote by R the ring $\mathbb{C}[z_0, z_1, \cdots, z_n]$. Let

$$\mathfrak{b} := (\mathfrak{a}, 1 - z_0 f) \subset R.$$

Clearly $Z(\mathfrak{b}) = 0$. By Lemma 3.2 we get

$$\mathfrak{b} = R.$$

In particular we can find solutions $h_i, h \in R$ and $f_i \in \mathfrak{a}$ to the following equation

$$\sum h_i f_i + h(1 - z_0 f) = 1. \tag{3.1}$$

Now let us substitute $\frac{1}{f}$ for z_0 as a formal variable in (3.1). We get

$$\sum_i h_i(\frac{1}{f}, z_1, \cdots, z_n) f_i = 1. \tag{3.2}$$

[1] that is why Lemma 3.2 does not hold for the ring $\mathbb{R}$

Let m be the maximal degree of z_0 of polynomials h_i in LHS of (3.2). Then multiplying the both sides of (3.2) with f^m we get

$$\sum_i \tilde{h}_i f_i = f^m,$$

where $\tilde{h}_i \in \mathfrak{a}$. This completes the proof of Hilbert's Nullstellensatz. $\square$

Remark 3.3. In all of its variants, Hilbert's Nullstellensatz asserts that some polynomial g belongs or not to an ideal generated, say, by $f_1, \cdots, f_k$ we have $g = f^r$ in the strong version, $g = 1$ in the weak form. This means the existence or the non existence of polynomials $g_1, \cdots, g_k$ such that $g = f_1 g_1 + \cdots + f_k g_k$. The usual proofs of the Nullstellensatz are not constructive, non effective, in the sense that they do not give any way to compute the g_i.

It is thus a rather natural question to ask if there is an effective way to compute the g_i (and the exponent r in the strong form) or to prove that they do not exist. To solve this problem, it suffices to provide an upper bound on the total degree of the g_i such a bound reduces the problem to a finite system of linear equations that may be solved by usual linear algebra techniques. Any such upper bound is called an —it effective Nullstellensatz.

Exercise 3.4. i) Prove that a system of polynomial equations

$$f_1(z_1, \cdots, z_n) = 0,$$
$$\cdots$$
$$f_m(z_1, \cdots z_n) = 0$$

has no solution in $\mathbb{C}^n$ iff 1 can be expressed as a linear combination

$$1 = \sum p_i f_i$$

with polynomial coefficients p_i.
ii)Show that any point x in an algebraic set $X \subset \mathbb{C}^n$ is a Zariski closed set.

Hint. Use the Nullstellensatz for the first statement and use Lemma 3.2 for the second statement.

3.2. **Zariski topology.** In this subsection we define Zariski topology on the set of ideals.

Definition 3.5. The Zariski topology on $\mathbb{C}^n$ is defined by specifying the closed sets in $\mathbb{C}^n$ to be precisely the algebraic sets. Equivalently a set is said to be *open in Zariski topology*, if it is a complement of an algebraic set.

Example 3.6. A closed set in $A^1_{\mathbb{C}}$ is either a finite set (the roots of a polynomial $P \in \mathbb{C}[z]$), or the whole affine line $A^1_{\mathbb{C}}$ (in this case $P = 0$). Thus this topology is not Haussdorf. (A topology is called Haussdorf if it satisfies the second separateness axiom which says that for any two different points we can find their neighborhoods which have no intersection.)

Exercise 3.7. If A and B are topological spaces, then we can define the product topology on the space $A \times B$ by specifying the base of this product topology to be the collection of the sets $U_\alpha \times V_\beta$, where U_α and V_β are open sets in A and B respectively. Show that the usual topology on $\mathbb{C}^n$ is the product topology of the usual topology on $\mathbb{C}$ but the Zariski topology on $\mathbb{C}^2$ is not the product of the Zariski topology on $\mathbb{C}$.

Hint Examine all closed subsets in the product of the Zariski topology on $\mathbb{C} \times \mathbb{C}$.

Let us define the closure $\bar{Y}$ of a set $Y \subset \mathbb{C}^n$ to be the smallest closed set which contains Y.

Exercise 3.8. Show that the closure of the set $S = \{(m, n), | \, m \ge n \ge 0, m \in \mathbb{Z}, n \in \mathbb{Z}\} \subset \mathbb{C}^2$ is equal to $\mathbb{C}^2$.

Hint. Let P be a polynomial on $\mathbb{C}^2$ such that S are roots of P. Examine the degree of P.

If Y is an algebraic set in $\mathbb{C}^n$ then we can define the induced Zariski topology on Y by specifying the open sets in Y to be the intersection of open sets in $\mathbb{C}^n$ with Y.

It is easy to see that the induced Zariski topology on $\mathbb{C}^1 = \{z_2 = 0\} \subset \mathbb{C}^2$ is the usual Zariski topology on $\mathbb{C}^1$.

4. Tangent space - a motivation + definition ...

In the analysis there is a well known notion of tangent space. In the case of the unit circle in the real plane $C : x^2 + y^2 - 1 = 0$, the tangent space T_pC of C at $p = (u, v)$ is given by the affine line

$$\begin{aligned}\frac{\partial}{\partial x}(x^2 + y^2 - 1)(u, v)(x - u) + \frac{\partial}{\partial y}(x^2 + y^2 - 1)(u, v)(y - v) \\ = 2u(x - u) + 2v(y - v) = 0. \qquad (4.1)\end{aligned}$$

As is customary in algebraic geometry, the tangent space is regarded as the vector subspace

$$\begin{aligned}&\frac{\partial}{\partial x}(x^2+y^2-1)(u,v)x+\frac{\partial}{\partial y}(x^2+y^2-1)(u,v)y\\ &=2ux+2vy=0\end{aligned} \tag{4.2}$$

in $\mathbb{R}^2$.

In order to define the notion of tangent space in algebraic geometry, we have to recall the basic concept of an algebraic variety as a functor of points. Let A be a unital commutative ring. The category of A-rings is given by objects (B,i) with B a ring and $i:A\to B$ a ring homomorphism, and morphisms $\mathrm{Hom}_{A-ring}((B,i),(B',i'))$ given by a ring homomorphism $f:B\to B'$ such that $f\circ i=i'$. In what follows, we shall simply write $\mathrm{Hom}_{A-ring}(B,B')$ for $\mathrm{Hom}_{A-ring}((B,i),(B',i'))$.

For two vector spaces V,W over a field k, an isomorphism $V\tilde{\to}k^n$ ($dim_k V=n$) producing basis vectors $e_1,\dots,e_n$ and a k-linear map $f:V\to W$, the evaluation map and its inverse

$$\begin{aligned}&\mathrm{Hom}_k(V,W)\to W^n, \quad f\mapsto (f(e_1),\dots,f(e_n)),\\ &W^n\to \mathrm{Hom}_k(V,W), \quad (w_1,\dots,w_n)\mapsto \{(a_1,\dots,a_n)\mapsto \sum_{i=1}^n a_iw_i\}\end{aligned}$$

($a_1,\dots,a_n$ are the coordinates in V with respect to $e_1,\dots,e_n$) are mutual inverses of each other. Consequently, $e_1,\dots,e_n$ freely generate k^n, i.e., there is no relation among them.

The non-linear variant of the previous linear algebra statement corresponds, in algebraic geometry, for any A-ring B, to the equivalence

$$\mathrm{Hom}_{A-ring}(A[x_1,\dots,x_n],B)\tilde{\to}B^n. \tag{4.3}$$

based on the evaluation map as well as in the linear algebra. This generalizes to the following situation: let A be a ring, $I\subset A[x_1,\dots,x_n]$ an ideal. For any A-ring B we define the B-points of an algebraic variety given by I (more precisely $i^*(I)\in B[x_1,\cdots,x_n]$)

$$Z(B):=\{b=(b_1,\dots,b_n)\in B^n\,|\,\forall f\in I\,:f(b)=0\} \tag{4.4}$$

and recall the notation $\mathcal{O}(Z)=A[x_1,\dots,x_n]/I$ for the ring of regular functions of $Z(:=Z(I))$. We use the notation $pr:A[x_1,\dots,x_n]\to A[x_1,\dots,x_n]/I$ for the projection, and the element in $A[x_1,\dots,x_n]$ when overlined denotes its image in $A[x_1,\dots,x_n]/I$ via pr. For any

A-ring B the two maps

$$\mathrm{Hom}_{A-ring}(\mathcal{O}(Z), B) \to Z(B), \quad \beta \mapsto (\beta(\bar{x}_1), \dots, \beta(\bar{x}_n)),$$
$$Z(B) \to \mathrm{Hom}_{A-ring}(\mathcal{O}(Z), B), \quad b = (b_1, \dots, b_n) \mapsto \bar{ev}_b$$

with $ev_b = \bar{ev}_b \circ pr$ are mutual inverses of each other and hence a bijection.

4.1. **Tangent space and the ring of dual numbers.** Let again B be an A-ring, the B-algebra $B[\epsilon] := B + B\epsilon = B[t]/t^2$ with $\epsilon = \bar{t}$ and $\epsilon^2 = 0$ is called the algebra of dual numbers. For $f \in A[x_1, \dots, x_n]$ and $b + b'\epsilon = (b_1 + b'_1\epsilon, \dots, b_1 + b'_1\epsilon) \in B[\epsilon]^n$, the Taylor expansion in the polynomial ring implies

$$f(b + b'\epsilon) = f(b) + \epsilon \sum_{j=1}^{n} \frac{\partial f}{\partial x_j}(b) b'_j. \tag{4.5}$$

We introduce

$$Z(B[\epsilon]) = \{b + b' \in B[\epsilon]^n \,|\, b \in Z(B)\,, b' \in (T_b Z)(B)\}, \tag{4.6}$$

where $T_b Z$ denotes the tangent space of Z (see (4.4)) at b:

$$(T_b Z)(B) := \{(x_1, \dots, x_n) \in B^n \,|\, \sum_{j=1}^{n} \frac{\partial f}{\partial x_j}(b) x_j = 0 \quad \forall\, f \in I\}. \tag{4.7}$$

The last condition is sufficient to verify on the generators of I only.

Example 4.1. In the case of $A[x, y]$ and the two algebraic varieties $Z : I = y$ and $Z' : I' = y^2$, respectively, describe the tangent spaces $T_{(0,0)} Z$ and $T_{(0,0)} Z'$, respectively.

4.2. **Tangent space and the Hensel's Lemma.** A well known application of the notion of the tangent space in number theoretical problems is the Hensel's Lemma, see Theorem 10.4. As an example we briefly consider the case $A = \mathbb{Z}/n\mathbb{Z}$ and

$$C :\; x^2 + y^2 - 1 = 0 \text{ mod n}. \tag{4.8}$$

The question is - can we characterize $C(\mathbb{Z}/n\mathbb{Z})$?

By the Chinese remainder theorem we can reduce n to a power of a prime number p^r, since for $n = p_1^{r_1} \dots p_k^{r_k}$ we have

$$C(\mathbb{Z}/n\mathbb{Z}) = C(\mathbb{Z}/p_1^{r_1}\mathbb{Z}) \times \dots \times C(\mathbb{Z}/p_k^{r_k}\mathbb{Z}). \tag{4.9}$$

From now on we assume $n = p^r$, $r \in \mathbb{N}$, and ask about the relationship between $C(\mathbb{Z}/p^r\mathbb{Z})$ and $C(\mathbb{Z}/p^{r+1}\mathbb{Z})$. Let $(u, v) \in \mathbb{Z}^2$ be a solution of

$$x^2 + y^2 - 1 = 0 \text{ mod } \mathrm{p}^{\mathrm{r}}, \tag{4.10}$$

and try to lift (u mod $\mathrm{p^r}$, v mod $\mathrm{p^r}$) in $C(\mathbb{Z}/p^r\mathbb{Z})$ to a solution mod $\mathrm{p^{r+1}}$. In other words, we ask for $(a,b) \in (\mathbb{Z}/p\mathbb{Z})^2$ such that

$$(u + p^r a)^2 + (v + p^r b)^2 - 1 = 0 \text{ mod } \mathrm{p^{r+1}}, \tag{4.11}$$

which is equivalent to

$$(u^2 + v^2 - 1)/p^r + (2ua + 2vb) = 0 \text{ mod p.} \tag{4.12}$$

In the case $p \neq 2$, at least one of the coefficients $2u, 2v$ is prime to p and hence the last congruence has a solution $(a_0, b_0) \in (\mathbb{Z}/p\mathbb{Z})^2$.

We observe that the linear equation $(2ux + 2vy) = 0$ mod p corresponds to the equation for $(\mathbb{Z}/p\mathbb{Z})$-valued points of (1-dimensional) tangent space $T_{(\bar{u},\bar{v})}C$ at $(\bar{u}, \bar{v}) = (u \text{ mod p}, v \text{ mod p})$ in $C(\mathbb{Z}/p\mathbb{Z})$. Hence the set of all solutions (4.12) is

$$(a_0, b_0) + T_{(\bar{u},\bar{v})}C(\mathbb{Z}/p\mathbb{Z}) \tag{4.13}$$

and we get the required comparison result $|C(\mathbb{Z}/p^{r+1}\mathbb{Z})| = p|C(\mathbb{Z}/p^r\mathbb{Z})|$.

Example 4.2. Does the same procedure work for $p = 2$? To conclude this question, prove and consequently apply the reduction of C to the double line,

$$x^2 + y^2 - 1 = (x + y - 1)^2 \text{ mod 2.} \tag{4.14}$$

4.3. **Hensel's lemma for algebraic varieties of dimension** 0**.** The content of classical version of Hensel's lemma is the characterization of zero dimensional algebraic varieties over compatible families of finite commutative unital rings.

As an example we consider the family of rings $A_n = \mathbb{Z}/7^n\mathbb{Z}$ for all $n \in \mathbb{N}$, and A_n-valued points of the algebraic variety

$$\tilde{C} : \, x^2 - 2 = 0 \text{ mod } 7^{\mathrm{n}}. \tag{4.15}$$

The A_1-valued points of $\tilde{C}$, i.e., the solutions of $x^2 - 2 = 0$ mod 7, are given by $x_1 = \pm 3$ mod 7.

Now assume we have an A_n-valued point of $\tilde{C}$, i.e., a solution of $x_n^2 - 2 = 0$ mod 7^{n}. We try to lift x_n to a A_{n+1}-valued point $x_{n+1} = x_n + 7^n y$ of $\tilde{C}$ for suitably chosen $y \in \mathbb{Z}$, i.e., to a solution $x_{n+1}^2 - 2 = 0$ mod $7^{\mathrm{n+1}}$. It is sufficient to consider y as an element of $A_1 = \mathbb{Z}/7\mathbb{Z}$, and we also observe that $x_{n+1} = x_n = \ldots = x_1 = \pm 3$ mod 7. The substitution for x_{n+1} yields

$$(x_n + 7^n y)^2 = x_n^2 + (2x_n y)7^n = 2 \text{ mod } 7^{\mathrm{n+1}}, \tag{4.16}$$

which is equivalent to

$$2x_n y = \frac{(2 - x_n^2)}{7^n} \text{ mod } 7 \tag{4.17}$$

(we notice that $2 - x_n^2$ is divisible by 7^n because $x_n^2 - 2 = 0 \bmod 7^{\rm n}$.) Due to $2x_n = \pm 6 \bmod 7^{\rm n} \neq 0 \bmod 7^{\rm n}$, there is a unique solution for $y \bmod 7$. This implies that for all $n \in \mathbb{N}$ there is a unique solution x_n once $x_1 = \pm 3 \bmod 7$ is chosen, which fulfills

$$x_{n+1} = x_n \bmod 7^{\rm n}. \tag{4.18}$$

The sequence $\{x_n\}_{n\in\mathbb{N}}$ represents a point on $\tilde{C}$ valued in the ring $\mathbb{Z}_7$ of 7-adic integers (there are just two solutions, distinguished by the value of x_1.) We remark that (4.17) can be interpreted as 7-adic Newton method for finding the solution space of $x^2 - 2 = 0$, because the series contains just the linear term of $f(x) = x^2 - 2$ in its Taylor expansion at 0. The previous considerations can be summarized as the formulation of the Hensel's lemma.

Lemma 4.3. *(Hensel's lemma in zero dimension) Let I be an ideal of a (commutative, unital) ring A, $f \in A[x]$ and $a \in A$ be such that $f(a) = 0 \bmod I^n$ (for some $n \geq 1$) and $f'(a) \bmod I$ is invertible in A/I. Then*

1. *there exists $b \in A$, which is unique* $\bmod I^{n+1}$, *such that $f(b) = 0 \bmod I^{n+1}$.*
2. *There exists unique $\tilde{a} \in \tilde{A} := \lim\limits_{\leftarrow n}(A/I^nA)$ (the I-adic completion of A) such that $f(\tilde{a}) = 0$ and the image of $\tilde{a}$ in A/I^nA is a.*

5. The Hilbert basis theorem and Groebner bases

Motivation. Theory of Groebner bases can be regarded as an algorithmic extension of the Hilbert basis theorem. As it is algorithmic, it gives algorithm for practical solving problems related to the existence of optimal basis of an ideal of the ring of polynomials, e.g. the Ideal membership problem (given an ideal $I \subset \mathbb{C}[x_1, \cdots, x_n]$ and a polynomial $f \in \mathbb{C}[x_1, \cdots, x_n]$ determine if $f \in I$), solving polynomial equation, the implicitization problem (find generators of the vanishing ideal of a *parametric algebraic variety* $f : \mathbb{C}^n \to \mathbb{C}^m$, where f is a polynomialmapping). Theory of Groebner bases demonstrates how a new theory arises when one digs deep in the proof of HBT.

5.1. **Groebner basis and Buchberger's algorithm.** A Groebner basis G of an ideal I in a polynomial ring R is a special generating set of I that has been motivated by the proof of Hilbert basis theorem.

Groebner bases were introduced in 1965, together with an algorithm to compute them (Buchberger's algorithm), by Bruno Buchberger in his Ph.D. thesis. He named them after his advisor Wolfgang Groebner. However, the Russian mathematician N. M. Gjunter had introduced a similar notion in 1913, published in various Russian mathematical journals. These papers were largely ignored by the mathematical community until their rediscovery in 1987 by Bodo Renschuch et al. An analogous concept for local rings was developed independently by Heisuke Hironaka in 1964, who named them standard bases. (https://en.wikipedia.org/wiki/Groebner_basis).

In the proof of the Hilbert basis theorem, the existence of grading of polynomial ring is very important. In the proof we have given above, the polynomial ring has only one variable. If we want to skip the induction step on the number of variables of the polynomial ring in the proof of HBT, we need to introduce a special grading, which is called *a monomial ordering*. In the given above proof of HBT this monomial ordering is implicitly given by choosing the induction step.

• To save notation we write $\mathbf{x}$ for $(x_1, \cdots, x_n)$ and for $\alpha := (\alpha_1, \cdots, \alpha_n)$ we denote by $\mathbf{x}^\alpha$ the monomial $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

Definition 5.1. A monomial ordering (or semigroup ordering) is a total ordering on the set of monomial $Mon_n := \{\mathbf{x}^\alpha | \, \alpha \in \mathbb{N}^n\}$ satisfying

$$\mathbf{x}^\alpha > \mathbf{x}^\beta \Longrightarrow \mathbf{x}^\gamma \mathbf{x}^\alpha > \mathbf{x}^\gamma \mathbf{x}^\beta$$

for all $\alpha, \beta, \gamma \in \mathbb{N}^n$.

The proof of the Hilbert basis theorem leads to notion of a Groebner basis and a leading ideal. First we need some notations related to monomial ordering.

For

$$f = a_\alpha \mathbf{x}^\alpha + a_\beta \mathbf{x}^\beta + \cdots \in K[\mathbf{x}]$$

where $\mathbf{x}^\alpha > \mathbf{x}^\beta > \cdots$ we set

(1) $LM(f) := \mathbf{x}^\alpha$ (leading monomial),
(2) $LE(f) := \alpha$ (leading exponent),
(3) $LC(f) := a_\alpha$ (leading coefficient),
(4) $LT(f) := LC(f) \cdot LM(f)$ (leading term)
(5) $tail(f) := f - LT(f)$.

For a subset $G \subset K[\mathbf{x}]$ we define *the leading ideal* of G by

$$L(G) := \langle LM(g) | \, g \in G \setminus \{0\}\rangle_{K[\mathbf{x}]}.$$

Definition 5.2. Let $I \subset K[\mathbf{x}]$ be an ideal. A finite set $G \subset I$ is called *Groebner basis* (or *standard basis*) if $L(I) = L(G)$.

It follows from the HBT that every ideal $I \subset K[\mathbf{x}]$ has a Groebner basis.

To construct a Groebner basis we apply Buchberger's algorithm. This algorithm arises from a detailed analysis of the proof of the HBT to understand how to recognize a basis is a Groebner basis. It follows immediately from the definition that a basis $(f_1, \cdots, f_s)$ is not a Groebner basis if there is a polynomial combinations of the f_i whose leading term is not in the ideal generated by $TL(f_i)$. This leads to the notion of a S-polynomial, which is such polynomial combination.

Definition 5.3. *The S-polynomial of f and g* is defined as follows

$$S(f,g) := \frac{\mathbf{x}^\gamma}{LT(f)} \cdot f - \frac{\mathbf{x}^\gamma}{LT(g)} \cdot g$$

where $\mathbf{x}^\gamma$ is the least common multiple of $LM(f)$ and $LM(g)$.

We also need the notion of division of a polynomial in $k[\mathbf{x}]$ by a (ordered) s-tuple $F = (f_1, \cdots, f_s)$ of s polynomials $f_i \in K[\mathbf{x}]$.

Proposition 5.4. *(*[CLO1996, Theorem 3, p. 61]*) Fix an monomial order in $\mathbb{Z}^n_{\geq 0}$ and let $F = (f_1, \cdot, f_s)$ be an ordered s-tuple of polynomials in $K[\mathbf{x}]$. Then for every $f \in K[\mathbf{x}]$ we have*

$$f = \sum a_i f_i + \overline{f}^F$$

where $a_i \in K[\mathbf{x}]$ and no term of $\overline{f}^F$ is divisible by any of $LT(f_1), \cdots, LT(f_s)$.

The division algorithm says that the remainder $\overline{f}^F$ does not belong the leading ideal $L(F)$.

Now we are ready to state an algorithmic criterion for a Groebner ([CLO1996, (p. 98)]).

Theorem 5.5. *Let I be a polynomial ideal. Then a basis $G = \{g_1, \cdots, g_s\}$ for I is a Groebner basis for I if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G is zero.*

Buchberger's algorithm for constructing a Groebner basis consists of the following. Take an arbitrary basis G. If $S(g_i, g_j) = 0$ for all $g_i, g_j \in G$, then we are done by Theorem 5.5. If not we add $\overline{S(g_i, g_j)}^G$ to obtain a new basis. After a finite step we obtain a Groebner basis.

5.2. **Some applications of Groebner bases.**

• *Ideal membership problem.* Let I be an ideal and G its Groebner basis. To verify if $f \in I$ we need only to check if $\overline{f}^G = 0$.

• *Solving polynomial equation.* Given $f_1, \cdots, f_s \in k[x_1, \cdots, x_n]$ we want to know whether the system of polynomial equations

$$f_1(x) = \cdots = f_k(x) = 0$$

has a solution in $\overline{k}^n$ where $\overline{k}$ is the algebraic closure of k. If there exists a solution can we find it?

To solve the first problem, applying the Hilbert Nullstellensatz, we reduce the existence problem to the ideal membership problem, namely, $V(I) = 0$ iff $1 \in I$, where $I = \langle f_1, \cdots, f_s \rangle_{k[x]}$.

There is an algorithm to solve the second problem in the case that the ideal I is zero dimensional. We refer to [GP2008, Section 1.8.5, p. 75].

• *The implicitization problem* is also called the problem of finding the Zariski closure of the image of a polynomial mapping. We need to find generators $p_1, \cdots, p_r$ of the vanishing ideal of the Zariski closure of the image of a polynomial mapping $f : \mathbb{C}^n \to \mathbb{C}^m$. The study of this problem lead to a new notion of elimination ordering and eliminate variables. We refer to two books [GP2008] and [CLO1996] for more details.

6. Affine varieties and projective varieties

Motivation. The decomposition of an algebraic set into its irreducible components leads to the notion of affine algebraic variety and quasi-affine variety. The study of projective varieties arises when we consider the action of the group $\mathbb{C}^*$ on $\mathbb{C}^n$. Factoring out the action of the non-compact group $\mathbb{C}^*$ we obtain the *compact* projective space $\mathbb{C}P^n$, which, in many topological and analytical problems, is easier to study than the analogous problems on the non-compact affine space $\mathbb{C}^n$. This also leads to useful technique of *projective closure* (Defintion 6.12).

6.1. **Affine algebraic varieties.** An algebraic set Y is called *irreducible*, if it cannot be represented as the union of two algebraic sets such that each of them is a proper subset in S. For example the affine line $\mathbb{C}^1 = \{(z_2 = 0)\} \subset \mathbb{C}^2$ is an irreducible algebraic set, because any closed set in $\mathbb{C}^1$ is either a finite set or the whole line $\mathbb{C}^1$.

Proposition 6.1. *An algebraic set is irreducible, if and only if, its ideal is prime.*

Proof. First we show that if a set Y is irreducible, then its ideal $I(Y)$ is prime. Indeed, if $fg \in I(Y)$ then $Y \subset Z(fg) = Z(f) \cup Z(g)$. Hence we get the decomposition

$$Y = (Y \cap Z(f)) \cup (Y \cap Z(g)),$$

so that $Z(f) \cap Y$ or $Z(g) \cap Y$ must be equal to Y. Consequently, $f \in I(Y)$ or $g \in I(Y)$ which implies that $I(Y)$ is prime.

Conversely, let $I(Y)$ be prime, we shall show that Y is irreducible. If $Y = Y_1 \cup Y_2$, then $I(Y) = I(Y_1) \cap I(Y_2)$. Assume that $I(Y) \neq I(Y_1)$ i.e. there is an element $g \in I(Y_1) \setminus I(Y)$. Since $I(Y)$ is prime, and $g \cdot I(Y_2) \subset I(Y)$ we get that $I(Y_2) \subset I(Y)$. Hence $I(Y_2) = I(Y)$, i.e. Y is irreducible. □

Definition 6.2. An *affine algebraic variety* (or simply affine variety) is an irreducible closed algebraic set with the induced Zariski topology of $\mathbb{C}^n$An open subset of an affine algebraic variety is called *a quasi-affine variety.*

Example 6.3. The twisted cubic curve $C = (t, t^2, t^3 | \, t \in \mathbb{C}) \subset \mathbb{C}^3$ is an affine algebraic variety. Clearly $I(C) = ((z_1^2 - z_2), (z_1 z_2 - z_3))$. To prove that $I(C)$ is prime, it suffices to show that the quotient $A(C) = \mathbb{C}[z_1, z_2, z_3]/I(C)$ is an integral domain. But it is easy to see that $A(C) = \mathbb{C}[z]$ is an integral domain.

Exercise 6.4. Prove that any closed subset Y in $\mathbb{C}^n$ has a decomposition of into irreducible closed subsets and this decomposition is unique.

Hint: Any chain of decompositions of closed subsets of Y must stop at irreducible closed subsets, since the ring $\mathbb{C}[z_1, \cdots, z_n]$ is Noetherian.

6.2. **Projective spaces.** We denote by $\mathbb{C}P^n$ the complex projective space whose points are complex lines in the vector space $\mathbb{C}^{n+1}$, i.e. 1-dimensional subspaces of the vector space $\mathbb{C}^n$. Equivalently

$$\mathbb{C}P^n = (\mathbb{C}^{n+1} \setminus \{0\})/\mathbb{C}^*$$

where $\mathbb{C}^*$ is the group of non-zero scalars acting on $\mathbb{C}^{n+1}$ by multiplication. This means that we consider a point of $\mathbb{C}P^n$ as an equivalence class of points in $\mathbb{C}^{n+1}$ under the action of $\mathbb{C}^*$ as follows. Two points $(z_0, \cdots, z_n)$ and $(z_0', \cdots, z_n')$ are equivalent, if there exists a number $\lambda \in \mathbb{C}^*$ such that

$$z_i = \lambda z_i', \text{ for all } 0 \leq i \leq n.$$

The equivalent class of $(z_0, z_1, \cdots, z_n)$ will be denoted by $[z_0 : z_1 : \cdots, : z_n]$.

6.3. **Homogeneous polynomials and graded rings.** We also define the dual action of $\mathbb{C}^*$ on the ring $\mathbb{C}[z_0, z_1, \cdots, z_n]$ by setting

$$(\lambda \circ P)(z_0, \cdots, z_n) := P(\lambda z_0, \cdots, \lambda z_n),$$

for any $\lambda \in \mathbb{C}^*$. Since $\mathbb{C}^*$ is abelian, the ring $\mathbb{C}[z_0, z_1, \cdots, z_n]$ considered as a vector space over $\mathbb{C}$ can be decomposed into eigen-spaces of the action of λ for all $\lambda \in \mathbb{C}$

$$\mathbb{C}[z_0, z_1, \cdots, z_n] = \oplus_k S_k. \tag{6.1}$$

Here S_k is an eigen-space w.r.t. weight $k \in Hom(\mathbb{C}^*, \mathbb{C}^*) : \lambda \mapsto \lambda^k$,

$$\lambda \circ P = \lambda^k \cdot P, \text{ if } P \in S_k,$$

for all $\lambda \in \mathbb{C}^*$. The splitting (6.1) is also called a *grading* of the ring $\mathbb{C}[z_0, \cdots, z_n]$, since we have

$$S_k \cdot S_l \subset S_{k+l}. \tag{6.2}$$

Elements of S_k are called *homogeneous polynomials of degree k*. The ring $\mathbb{C}[z_0, \cdots, z_n]$ provided with the splitting (6.1) which satisfies (6.2) is a *graded ring.*

An ideal $\mathfrak{a} \subset \mathbb{C}[z_0, \cdots, z_n]$ is called a *homogeneous ideal*, if

$$\mathfrak{a} = \oplus_k (\mathfrak{a} \cap S_k).$$

Example 6.5. A maximal ideal $\mathfrak{a} \subset \mathbb{C}[z_0, z_1, \cdots, z_n]$ is a homogeneous ideal, if and only if $Z(\mathfrak{a}) = \{0\} \in \mathbb{C}^{n+1}$.

Exercise 6.6. Prove that an ideal is homogeneous if and only if it can be generated by homogeneous elements. Prove that the sum, product, intersection and radical of homogeneous ideals are homogeneous.

6.4. **Projective varieties and homogeneous ideals.** We associate to any homogeneous polynomial $P \in V_k$ a function $\tilde{P} : \mathbb{C}P^n \to \{0, 1\}$ according to the following rule

$$\tilde{P}([z_0 : z_1, \cdots, : z_n]) = 0, \text{ if } P(z_0, z_1, \cdots, z_n) = 0,$$

$$\tilde{P}([z_0 : z_1, \cdots, : z_n]) = 1, \text{ if } P(z_0, z_1, \cdots, z_n) \neq 0.$$

Clearly the function $\tilde{P}$ is well-defined. So we can define for any set T of homogeneous polynomials in $\mathbb{C}[z_0, z_1, \cdots, z_n]$ its zero set $Z(T)$ in the projective space $\mathbb{C}P^n$ by setting

$$Z(T) := \{p \in \mathbb{C}P^n | \, \tilde{P}(p) = 0 \text{ for all } P \in T\}.$$

A subset $Y \subset \mathbb{C}P^n$ is called *algebraic*, if there exists a set T of homogeneous polynomials of $\mathbb{C}[z_0, \cdots, z_n]$ such that $Y = Z(T)$.

Exercise 6.7. Show that the union of two algebraic sets is an algebraic set. The intersection of any family of algebraic sets is an algebraic set.

For any subset $Y \subset \mathbb{C}P^n$ we denote by $I(Y)$ the *homogeneous ideals* of $Y \subset \mathbb{C}[z_0, \cdots, z_n]$ the ideal generated by homogeneous elements f in $\mathbb{C}[z_0, \cdots, z_n]$ such that f vanishes on Y. (This ideal is homogeneous according to Exercise 6.6.

The Zariski topology on $\mathbb{C}P^n$ is defined by specifying the open sets to be the complement of algebraic sets.

Once we have a topological space the notion of irreducible (not necessary algebraic) sets will apply. We say that a set Y is irreducible, if it cannot be represented as the union of two proper subsets which of them is closed in Y.

Definition 6.8. A *projective (algebraic) variety* is an irreducible algebraic set in $\mathbb{C}P^n$ with the induced topology. A *quasi projective variety* is an open subset in a projective variety.

Example 6.9. We denote by $H_i \subset \mathbb{C}P^n$ the zero set of the linear function z_i. Then H_i is called a hyper-plane. It is a projective variety, because $I(H_i) = (z_i)$ is a prime ideal. In fact an algebraic set $Y \subset \mathbb{C}P^n$ is irreducible, if and only if its homogeneous ideal is prime. To prove this we can repeat the proof of Proposition 6.1 or we observe that there is a correspondence between algebraic set $Y \subset \mathbb{C}P^n$ and its cone CY in $\mathbb{C}^{n+1}$ which is defined by

$$CY := \{(z_0, z_1, \cdots, z_n) | \, [z_0, z_1, \cdots, z_n] \in Y\}.$$

They have the same ideal. The property being reducible is also preserved by this correspondence. Thus our statement about the correspondence between homogeneous prime ideals and projective varieties is a consequence of the Proposition 6.1.

The following statement shows that the projective space $\mathbb{C}P^n$ is a compactification of the affine space $\mathbb{C}^n$.

Proposition 6.10. *The quasi-projective variety $U_i = \mathbb{C}P^n \setminus H_i$ with its induced topology is homeomorphic to the affine space $\mathbb{C}^n$ with its Zariski topology.*

Proof. We consider the map $\phi_i : U_i \to \mathbb{C}^n$

$$\phi_i([z_0 : \cdots : z_i]) = (\frac{z_0}{z_i}, \cdots_{\hat{i}}, \cdots, \frac{z_n}{z_i}).$$

Clearly ϕ_i is a bijection. We need to show that ϕ_i is a homeomorphism, i.e. ϕ_i and ϕ_i^{-1} send closed sets into closed sets.

Let Y be a closed set in U_i. Then there is a homogeneous ideal $T \subset \mathbb{C}[z_0, \cdots, z_n]$ such that $Y = Z(T) \cap U_i$. We want to find an ideal T' in $\mathbb{C}[z_0, \cdots,_{\hat{i}}, \cdot z_n]$ such that $\phi_i(Y) = Z(T')$. Let T' be the set of polynomials in $\mathbb{C}[z_0, \cdots, _{\hat{i}}, \cdots, z_n]$ obtained by restricting the set T^h of *homogeneous* elements in T to the hyper-plane $\{z_i = 1\}$ in $\mathbb{C}^{n+1}$. This map $T^h \to T'$ shall be denoted by r_i (restriction). Then we have for any homogeneous element t of degree d in T^h

$$r_i(t)(\phi_i(z)) = z_i^{-d} \cdot t(z), \text{ for all } z \in U_i. \tag{6.3}$$

Since ϕ_i is a bijection, it follows from (6.3) that $\phi_i(Y) = Z(T')$. So ϕ_i is a closed map.

Now let W be a closed set in $\mathbb{C}^n$. Then $W = Z(T')$ for some ideal $T' \subset \mathbb{C}[z_0, \cdots _{\hat{i}}, \cdots z_n]$. We shall find a homogeneous ideal $T \subset \mathbb{C}[z_0, \cdots, z_n]$ such that $\phi_i^{-1}(W) = Z(T^h) = Z(T)$, where as before T^h denotes the set of homogeneous elements in T.

Let $t' \in T'$ be a polynomial of degree d. We set, cf. (6.3)

$$\beta(t')(z) := z_i^d \cdot t'(\phi_i(z)) \in \mathbb{C}[z_0, \cdots, z_n]. \tag{6.4}$$

Clearly $\beta(t')$ is a homogeneous polynomials of degree d. Let $T := \beta(T')$. Since ϕ_i is a bijection, (6.4) implies that $\phi_i^{-1}(W) = Z(T) \cap U_i$. Hence ϕ_i^{-1} is also a closed map. □

Remark 6.11. The map $\beta : T' \to T$ is not a ring homomorphism. Thus if $\{l_i\}$ generate some ideal $\mathfrak{a}$, the set $\{\beta(l_i)\}$ may not generate the ideal $\beta(\mathfrak{a})$, see Example 6.13 below.

Definition 6.12. If $Y \subset \mathbb{C}^n$ is an affine variety then we shall say $\bar{Y} \subset \mathbb{C}P^n$ is *the projective closure of* Y, if Y is the closure of $\phi_0(Y)$ in $\mathbb{C}P^n$, or equivalently $I(\bar{Y}) = \beta(I(Y))$.

So $\bar{Y}$ is a projective closure of Y iff $\bar{Y} = Y(\beta(I(Y))$.

Example 6.13. Now let us consider for example the projective closure of the twisted cubic curve $C = (t, t^2, t^3)$. The closure $\bar{C}$ has an ideal $I(\bar{C})$ generated by $\{(z_1^2 - z_0z_2), (z_1z_3 - z_2^2), (z_1z_2 - z_0z_3)\}$ but not by $\{\beta(z_2 - z_1^2) = z_0z_2 - z_1^2, \beta(z_1z_2 - z_3) = z_1z_2 - z_0z_3\}$ (see [**?**, Example 1.10] for a proof of the last statement).

Exercise 6.14 (Homogeneous Nullstellensatz)**.** If $\mathfrak{a} \subset S$ is a homogeneous ideal, and if f is a homogeneous polynomial such that $f(P) = 0$ for all $P \in Z(\mathfrak{a}) \subset \mathbb{C}P^n$, then $f^q \in \mathfrak{a}$ for some $q > 0$.

Hint. We use the correspondence between $Z(\mathfrak{a})$ and $CZ(\mathfrak{a}) \subset \mathbb{C}^{n+1}$ to deduce this Proposition from the Hilbert's Nullstellensatz.

Exercise 6.15. We define the Serge embedding $\psi : \mathbb{C}P^r \times \mathbb{C}P^s \to \mathbb{C}P^N$ as follows. Set $N = rs + r + s$ and

$$\psi([x_0, \cdots, x_r] \times [y_0, \cdots, y_s]) = [\cdots, x_iy_j, \cdot]$$

Prove that ψ is injective and the image of ψ is a subvariety in $\mathbb{C}P^N$.

Hint. Show that $\psi(\mathbb{C}P^r \times \mathbb{C}P^s) = Z(\ker\theta)$ where $\theta : \mathbb{C}[z_{ij}, i = \overline{0,r}, j = \overline{0,s}] \to \mathbb{C}[x_i, y_j, i = \overline{0,r}, j = \overline{0,s}]$: $\theta(z_{ij}) = x_i y_j$.

7. Coordinate ring and the dimension of an algebraic set

Motivation. Functions on a topological space S are observables (or features) of the space. The space of functions on S has a ring structure, since $\mathbb{R}$ is a ring. When S is an algebraic set, it suffices to consider a smaller class functions, called the coordinate ring of S. We shall show in this section that the coordinate ring provides most basic topological characterization of a space: its topological (also called Krull) dimension, which is defined strictly in topological terms, is equal to it algebraic dimension, which is defined in terms of field extension (Theorem 7.9).

7.1. **Affine coordinate ring.** We have already introduced the notion of an affine coordinate ring in Example 6.3 for the affine twisted curve. In general case, *the affine coordinate ring of an affine algebraic set* $Y \subset \mathbb{C}^n$ is defined to be the quotient

$$A(Y) := \mathbb{C}[z_1, \cdots, z_n]/I(Y).$$

$A(Y)$ is called the coordinate ring, since any element $f \in A(Y)$ is the restriction of some polynomial $\tilde{f} \in \mathbb{C}[Z_1, \cdots, z_n]$ to Y, and moreover, as we shall see in Corollary 7.3, the values $f(x) \in \mathbb{C}, f \in A(Y)$, can distinguish different points in Y.

Remark 7.1. (cf. Exercise 7.4) Since $\mathbb{C}[z_1, \cdots, z_n]$ is a finitely generated $\mathbb{C}$-algebra, the quotient $A(Y)$ is a finitely generated algebra. We have seen in Example 6.3 that the affine coordinate ring $A(Y)$ is an integral domain, if Y is irreducible. Conversely, if B is a finitely generated $\mathbb{C}$-algebra which is an integral domain, then $B = \mathbb{C}[z_1, \cdots, z_n]/\mathfrak{a}$, where $\mathfrak{a}$ is prime. So B is the affine coordinate ring of the algebraic set $Z(\mathfrak{a})$. Summarizing we have the following correspondence between algebra and geometry

$$\{ \text{ finitely generated } \mathbb{C}\text{-algebras which are domains}\} \Longleftrightarrow \{ \text{ affine varieties } \}.$$

For $y \in Y$ we set $\mathfrak{m}_y := \{f \in A |\, f(y) = 0\}$. Then $\mathfrak{m}_y$ is a maximal ideal in $A(Y)$.

Proposition 7.2. *(i) The correspondence $y \mapsto \mathfrak{m}_y$ is a 1-1 correspondence between points $y \in Y$ and the maximal ideals in $A(Y)$.*
(ii) There is a 1-1 correspondence between closed sets in Y and perfect (radical) ideals $\mathfrak{m}$ in $A(Y)$.

Proposition 7.2 says that Y as a topological space can be defined by the structure of the ring $A(Y)$.

Proof. (i) Denote by p the projection $\mathbb{C}[z_1, \cdots, z_n] \to A(Y)$. Let $\mathfrak{m}$ be a maximal ideal in $A(Y)$. Then $p^{-1}(\mathfrak{m})$ is a maximal ideal in $\mathbb{C}[z_1, \cdots, z_n]$. By Hilbert's Nullstellensatz $p^{-1}(\mathfrak{m}) = (z_1 - a_1, \cdots, z_n - a_n) = \{f \in \mathbb{C}[z_1, \cdots, z_n] \,|\, f(a_1, \cdots, a_n) = 0\}$. Since $I(Y) \subset p^{-1}(\mathfrak{m})$ the point $(a_1, \cdots, a_n)$ belongs to Y. Hence $\mathfrak{m} = \{f \in A(Y)|f(a_1, \cdots, a_n) = 0\}$. Thus the correspondence $y \mapsto \mathfrak{m}_y$ is surjective. In fact this correspondence is 1-1 because there is a 1-1 correspondence between maximal ideals in $\mathbb{C}[z_1, \cdots, z_n]$ which contain $I(Y)$ and maximal ideals in $A(Y)$.

To prove the second assertion it suffices to show that $I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$ for any $\mathfrak{a} \subset A$. From Hilbert's Nullstellensatz we get

$$p^{-1}(I(Z(\mathfrak{a}))) = \sqrt{p^{-1}(\mathfrak{a})}.$$

Hence

$$I(Y(\mathfrak{a})) = p(\sqrt{p^{-1}(\mathfrak{a})}) = \sqrt{p \circ p^{-1}(\mathfrak{a})} = \sqrt{\mathfrak{a}}.$$

□

From the proof of Proposition 7.2

Corollary 7.3. *For any $y \neq y' \in Y$ there exists $f \in A(Y)$ such that $f(y) = 0$ and $f(y') = 1$.*

Exercise 7.4. Show that a $\mathbb{C}$-algebra A is an affine coordinate ring $A(Y)$ for some algebraic set Y iff A is reduced (i.e. its only nilpotent element is 0) and finitely generated as $\mathbb{C}$-algebra.

Hint. Write $A = \mathbb{C}[z_1, \cdots, z_n]/I$ and use the Hilbert Nullstellensatz.

7.2. **Dimension of a topological space.** Let X be a topological space. Then we define the *(Krull) dimension* of X to be the supremum of all integers n such that there exists a chain $Z_0 \subset Z_1 \subset \cdots \subset Z_n$ of distinct irreducible closed subsets of X. This definition depends on the structure of all closed subsets of X but we shall see that dimension is a local property.

Proposition 7.5. *a) If Y is any subset of a topological space X, then* $\dim Y \le \dim X$.
b) If X is topological space which is covered by a family of open subsets $\{U_i\}$, then $\dim X = \sup \dim U_i$.
c) If Y is a closed subset of an irreducible finite-dimensional topological space X, and if $\dim Y = \dim X$*, then $X = Y$.*

Proof. The first and last statements follow directly from the definition.

Let us prove the second assertion. Let $Z_0 \subset \cdots \subset Z_n$ be distinct closed irreducible subsets of X and U an open set from the covering $\{U_j\}$ such that $Z_n \cap U \neq \emptyset$. Then $\{Z_j \cap U | \, j = \overline{0,n}\}$ are closed subsets of U. They are all irreducible, since U is open: if we have a decomposition $Z = (\bar{Z}_A \cap U) \cup (\bar{Z}_B \cap U)$, then

$$Z = [(Z \cap (X \setminus U)) \cup (Z \cap \bar{Z}_A)] \cup (Z \cap \bar{Z}_B)$$

is not irreducible. Finally they all are distinct, since if $(Z_j \cap U) = (Z_{j+1} \cap U)$ then $Z_{j+1} = Z_j \cup (Z_{j+1} \cap (X \setminus U))$ is irreducible. This proves that $\dim X \leq \sup \dim U_i$. Combining with the first statement we get the second statement. □

Exercise 7.6. (i) Prove that $\dim \mathbb{C}^1 = 1$.
(ii) Prove that if X is an affine variety in $\mathbb{C}^n$ and $Y \subset X$ is a proper closed subset then we have $\dim Y < \dim X$.

Now we translate the notion of Krull dimension in the category of rings.

In a ring A the *height* of a prime ideal $\mathfrak{p}$ is the supremum of all integers n such that there exists a chain $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$ of distinct prime ideals. The *Krull dimension* of A is defined as the supremum of the height of all prime ideals.

Proposition 7.7. *If Y is an affine algebraic set, then the dimension of Y is equal to the dimension of its affine coordinate ring $A(Y)$.*

Proof. By definition the dimension of Y equals the length of the longest chain of closed irreducible subsets in Y which correspond to the chain of prime ideals of $A(Y)$. □

There is also another natural notion of dimension in the category of modules and rings, which we shall compare with the notion of Krull dimension in most important cases.

Definition 7.8. The *algebraic dimension* of a commutative ring A over a field k is the maximal number of algebraically independent elements over k in A if it is defined and ∞ otherwise. We will denote it by $alg.\dim_k A$.

This notion of algebraic dimension is *natural*, since we want to have the dimension of the algebra of functions equal to the dimension of the underlying topological space, see also Corollary 7.16 below. The following theorem shows that the two notions agree in the case of algebras equal to coordinate rings of affine varieties (see Remark 7.1).

Theorem 7.9. *(*[Dolgachev2013, Theorem 11.8, p. 95]*) Let A be a finitely generated k-algebra without zero divisors and F(A) be the field of fractions of A. Then*

$$alg.\dim_k F(A) = alg.\dim_k A = \dim A.$$

Proof. The proof of Theorem 7.9 uses the Noether normalization theorem that describes the structure of finitely generated k-algebra without zero divisor. Noether's normalization theorem together with HBT and Hilbert's Nullstellensatz are three basic techniques in algebraic geometry, since finitely generated k-algebra without zero divisor are coordinate rings of affine varieties.

Theorem 7.10 (Noether's normalization theorem)**.** *Let A be a finitely generated algebra over a field k. Then A is isomorphic to an integral extension of the polynomial algebra $k[Z_1, \cdots, Z_n]$.*

Digression: Noether's normalization theorem. Noether's normalization theorem is also a basic theorem in commutative algebra, see e.g. [Lang2005, Theorem 2.1, p. 357] and a sketch of a proof at the end of Subsection 8.2. In [Shafarevich2013, §5.4, p. 65] Shafarevich provided a simple geometric proof of the Noether's normalization theorem. For this purpose, we introduce the notion of a finite map, extending the correspondence between finitely generated algebras and affine varieties in Remark 7.1.

Definition 7.11. Let X and Y be affine varieties. A regular map $f : X \to Y$ is called *a finite map* if $k[X]$ is integral over $k[Y]$.

Now we translate the Noether's normalization theorem as follows.

Theorem 7.12. *For an irreducible affine variety X there exists a finite map $\varphi : X \to k^n$ to an affine space k^n.* [2]

Using the projective closure, we reduce Theorem 7.12 to the following projective version.

Theorem 7.13. *For an irreducible projective variety X there exists a finite map $\varphi : X \to P^n$ to an affine space P^n.*

---

[2]Geometric Noether normalization theorem (Theorem 7.12) is a generalization of Riemann's theorem which say that every algebraic curve is a covering of the sphere $\mathbb{C}P^1$. Geometric Noerther normalization theorem is slightly weaker than the algebraic Noerther normalization theorem, which does not require the zero divisor condition, but it suffices for the proof of Theorem 7.9.

To prove Theorem 7.13 we find a point $x \in P^n \setminus X$, and the map φ is obtained by projecting X away from x will be regular. The image $\varphi(X) \subset P^{n-1}$ is projective, and the map $\varphi : X \to \varphi(X)$ is finite. Repeating this procedure, if $\varphi(X) \neq P^{n-1}$, we obtain Theorem 7.13.

Continuation of Theorem 7.9. By Noether's normalization A is integral over its subalgebra isomorphic to $k[Z_1, \cdots, Z_N]$. We shall relate the dimension of A with that of its subalgebra $k[Z_1, \cdots, Z_N]$. The later ring is simple and we can compute it by proving Theorem 7.9 for this coordinate ring in Exercise 7.14 below.

Exercise 7.14. $\dim k[Z_1, \cdots, Z_n] = alg. \dim_k [Z_1, \cdots, Z_N]$.

Hint. First we assume the validity of the following haft of of Theorem 7.9.

Lemma 7.15. *(*[Dolgachev2013, Lemma 11.5, p. 95]*) Let A be a k-algebra without zero divisors and $F(A)$ be the field of fractions of A. Then*

$$alg. \dim_k A = alg. \dim_k F(A) \geq \dim A.$$

(The proof of Lemma 7.15 will be outlined later.)

We derive Exercise 7.14 from the following corollary of Lemma 7.15

Corollary 7.16.

$$alg.dim_k k[Z_1, \cdots, Z_n] = alg.dim_k k(Z_1, \cdots, Z_n) = n$$

$$\geq \dim k[Z_1, \cdots, Z_n] \geq n.$$

(The last inequality in Corollary 7.16 is obtained by considering the following sequence of proper prime ideals:

$$(0) \subset (Z_1) \subset (Z_1, Z_2) \subset \cdots \subset (Z_1, \cdots, Z_n).)$$

Now we relate the Krull dimension of A with the Krull dimension of its polynomial subalgebra.

Lemma 7.17. *(*[Dolgachev2013, Lemma 11.7]*)*

$$\dim A = \dim k[Z_1, \cdots, Z_N].$$

(We note that the algebraic dimension does not change with an algebraic extension so Lemma 7.17 says that the Krull dimension behaves in the same way.)

Proof. First we prove

$$\dim A \leq \dim k[Z_1, \cdots, Z_N] \tag{7.1}$$

Let $0 \subset P_1 \subset \cdots ...$ be a chain of proper prime ideals in the bigger ring A. Then $0 \subset P_1 \cap A \subset \cdots ...$ be a proper prime ideals in the smaller ring F. This proves (7.1). To complete the proof of Lemma 7.17 it suffices to prove the following

$$\dim A \geq \dim k[Z_1, \cdots, Z_N] \tag{7.2}$$

Fact F. ([Dolgachev2013, Lemma 10.3. (vi), p. 85]) *For every prime ideal P in the smaller ring $F := k[Z_1, \cdots, Z_N]$ there exists a prime ideal P' in the bigger ring A such that $P' \cap F = P$.*

Fact F implies immediately (7.2), since any chain of proper prime ideals in F implies the existence of a chain of prime ideals in A. More precisely, let $0 \subset P_1 \subset P_2 \subset \cdots$ be a chain proper prime ideals in the smaller ring F. The fact F implies the existence of a prime ideal $Q_0 \subset A$ such that $Q \cap F = P_0$. Set

$$\bar{F} := F/P_0 \text{ and } \bar{A} := A/Q_0.$$

Then $\bar{A}$ is an integral extension of $\bar{F}$ via the canonical injective homomorphism $\bar{F} \to \bar{A}$. Applying the fact F again, we find a prime ideal $\bar{Q}_1$ in $\bar{A}$ such that $\bar{Q}_1 \cap F = \bar{P}_1$. Lifting $\bar{Q}_1$ to $Q_1 \subset A$ we have

$$Q_1 \cap F = P_1.$$

In this way we find a chain of proper prime ideals in the bigger ring A of the same length. This proves (7.2) and completes the proof of Lemma 7.17. $\square$

Summarizing, we have

$$alg.\dim_k A \overset{Lemma\, 7.15}{\geq} \dim A \overset{Lemma\, 7.17}{=} \dim k[Z_1, \cdots, Z_n]$$

$$\overset{Corollary\, 7.16}{=} alg.dim_k k(Z_1, \cdots, Z_n) \overset{Noether\, Theorem\, 7.10}{=} alg.\dim_k F(A)$$

$$\overset{Lemma\, 7.15}{=} alg.\dim_k A.$$

This completes the proof of Theorem 7.9 modulo the proofs of Lemma 7.15 and Lemma 7.17.

Completion of the proof of Theorem 7.9 It remains to give a *Proof of Lemma 7.15.* It suffices to prove the following three inequalities

$$alg.\dim F(A) \geq alg.\dim A, \tag{7.3}$$

$$alg.\dim A \geq alg.\dim F(A), \tag{7.4}$$

$$alg.\dim_k A \geq \dim A. \tag{7.5}$$

Since $A \subset F(A)$, the inequality (7.3) is obvious.

Let us prove (7.4). It suffices to show that for any r algebraically independent elements $x_1, \cdots, x_r$ in $F(A)$ we find also r algebraically independent elements $y_1, \cdots, y_r$ in A. Write $x_i = a_i/r$, where $a_i, r \in A$. Let Q_0 be the subfield of $F(A)$ generated by $a_1, \cdots, a_r, s$. Since $Q_0 \ni x_1, \cdots x_r, s$ we have

$$alg.\dim_k Q_0 \geq r.$$

If $a_1, \cdots a_r$ are algebraically dependent, then Q_0 is an algebraic extension of the subfield Q_1 generated by s and $a_1, \cdots, a_r$ with some a_i, say a_r, omitted. Since $alg.\dim_k Q_0 = alg.\dim_k Q_1$, we find r algebraically independent elements $a_1, \cdots, a_{r-1}, s \in A$. This proves (7.4).

It remains to prove (7.5). Let $0 \subset P_1 \subset \cdots P_n$ be a chain of proper prime ideals in A. We need to find n algebraically independent elements in A. It suffices to prove $alg.\dim_k A > alg.\dim_k A/P_0$. Let $\bar{x}_1, \cdots, \bar{x}_n \in A/P_0$ be algebraic independent. Take their representative x_i in A. We claim that for any $x \in P$, $(n+1)$-elements $(x_1, \cdots, x_n, x)$ are algebraically independent. Suppose the opposite. Then there is a polynomial in x with coefficient in the polynomial ring of $(x_1, \cdots, x_n)$ which vanishes. We can assume that the zero order coefficient of this polynomial is not zero. Passing to the factor ring A/P, since $x \in P$, the vanishing of F implies the zero order coefficient of F is zero, or equivalently $(\bar{x}_1, \cdots, \bar{x}_n)$ are algebraically dependent. This contradicts to our assumption and hence completes the proof of (7.5). □

Remark 7.18. In the proof of Theorem 7.9 we requires A to be an integral domain in order to have the field of fractions $F(A)$. In general, the equality $alg.\dim k[Z_1, \cdots, Z_n] = alg.\dim_k A$ is valid without the condition that A is an integral domain.

Exercise 7.19. (cf. [Shafarevich2013, Theorem 1.21, p.69]) A variety $Y \subset \mathbb{C}^n$ has dimension $n-1$ if and only if its ideal $I(Y)$ is generated by a single non-constant irreducible polynomial f in $\mathbb{C}[z_1, \cdots, z_n]$.

Hint. To prove that $\dim Z(f) = n-1$ we use the identity $\dim Z(f) = alg.\dim_{\mathbb{C}} Z(f)$. ($alg.\dim_{\mathbb{C}} Z(f) \leq n-1$, since $x_1, \cdots, x_n$ are algebraically dependent. Next, $alg.\dim Z(f) \geq n-1$, since $I(Z(f)) =$

$\sqrt{(f)}$.) For the statement that $\dim Y = n-1$ implies $Y = Z(f)$ use Hilbert's Nullstellensatz.

Exercise 7.19 is a particular case of the Geometric Krull's Hauptidealsatz, which says that the co-dimension of the (irreducible component of) the zero set of a non-invertible and non-zero regular functions on an affine variety is one (see [Dolgachev2013, Theorem 11.10] for a proof.)

7.3. **Homogeneous coordinate ring and dimension.** Let Y be an algebraic set in $\mathbb{C}P^n$ and $I(Y)$ its homogeneous ideal. Then we define the *homogeneous coordinate ring of* Y to be $S(Y) = C[z_0, \cdots, z_n]/I(Y)$. For any $y \in Y$ denote by $\mathfrak{m}_y$ the set $\{f \in S(Y) | \, f(y) = 0\}$. It is easy to see that $\mathfrak{m}_y$ is a homogeneous maximal ideal of $S(Y)$.

Unlike the affine case (see Proposition 7.2(i)), not every homogeneous maximal ideal $\mathfrak{a}$ in $S(Y)$ is of the form $\mathfrak{m}_y$ for some $y \in Y$, as the following example shows. Let us consider the homogeneous ideal $S_+ = \oplus_{d>0} S_d$. Then $I(Y) \subset S_+$. The ideal $S_+/I(Y)$ is a homogeneous maximal ideal in $S(Y)$ but it does not correspond to any point $y \in Y$. In fact by using the correspondence $Y \mapsto CY$ we conclude that $S_+/I(Y)$ is the only homogeneous maximal ideal in $S(Y)$ which does not have the form $\mathfrak{m}_y$.

Proposition 7.20. *(i) There is a 1-1 correspondence between points y in an algebraic set* $Y \subset \mathbb{C}P^n$ *and homogeneous maximal ideals* $\mathfrak{m}_y$ *in* $S(Y)$.
(ii) $\dim S(Y) = \dim Y + 1$.

Proof. (i) This statement follows from Proposition 7.2.(i) and our observation about $\mathfrak{m}_y$ above.

(ii) Using the correspondence between an algebraic set Y in $\mathbb{C}P^n$ and its cone $CY \subset \mathbb{C}^{n+1}$ (see Example 6.9) we conclude that $\dim S(Y) = \dim A(CY) = \dim CY$. Clearly $\dim Y = \dim(CY \cap \{z_i \neq 0\})$ for some i by Proposition 7.5.b. Hence $\dim Y = \dim[A(CY)/z_i = 1] \geq \dim CY - 1$. Now to prove that $\dim CY > \dim Y$ we use Exercise 7.6.(ii) and Proposition 7.5.b which says that $\dim Y = \dim Y \cap U_i$. Alternatively use the hint for exercise 7.19. □

Exercise 7.21. i) Prove that a projective variety $Y \subset \mathbb{C}P^n$ has dimension $(n-1)$, if and only if it is the zero set of a single irreducible homogeneous polynomial f of a positive degree.
ii) Prove that if a projective variety $Y \subset \mathbb{C}P^n$ is not a hypersurface H_i then $\dim(Y \cap H_i) = \dim Y - 1$.

8. Regular functions and morphisms

Motivations. Continuing our translation between algebra and geometry, in this section we define the notion of morphisms between algebraic varieties in terms of morphism between their coordinate rings, or more general, the ring of regular functions on an algebraic variety (Proposition 8.11). The later one is defined *locally*, but it is related to the concept of regular functions (coordinate functions) on *affine varieties*, which is defined *globally* (Theorem 8.7, Remark 8.8). In contrast, since any polynomial function on a projective variety is constant (see e.g. Theorem 8.9 (i), Exercise 8.15), the concept of a regular function that is defined only in an open set is a logical necessity in the category of projective varieties. We also study topological and algebraical properties of regular functions (Lemma 8.3, Theorems 8.7, 8.9).

8.1. **Regularity of a function at a point.**

Definition 8.1. Let Y be a quasi-affine variety in $\mathbb{C}^n$. A function $f : Y \to \mathbb{C}$ is *regular at a point* $P \in Y$, if there is an open neighborhood U with $P \in U \subset Y$ and polynomials $g, h \in \mathbb{C}[z_1, \cdots, z_n]$ such that h is nowhere zero on U, and $f = g/h$ on U. We say that f is *regular on* Y if it is regular at every point of Y.

This definition includes the set of rational functions (g/h) as regular functions, since we want to include the notion of a (local) inverse of a function for a polynomial function.

Definition 8.2. Let Y be a quasi-projective variety in $\mathbb{C}P^n$. A function $f : Y \to \mathbb{C}$ is *regular at a point* $P \in Y$, if there is an open neighborhood U with $P \in U \subset Y$ and a homogeneous polynomials $g, h \in \mathbb{C}[z_1, \cdots, z_n]$ of the same degree, such that h is nowhere zero on U and $f = g/h$ on U. We say that f is *regular on* Y if it is regular at every point of Y.

The condition of "the same degree" ensures that g/h is well-defined as a function on U.

Lemma 8.3. *A regular function is continuous with respect to the Zariski topology.*

Proof. It suffices to prove that for each closed subset $Z \subset \mathbb{C}$ the pre-image $f^{-1}(Z)$ is a closed set in Y. Any closed subset Z of $\mathbb{C}$ is a finite set of points. Thus it suffices to prove that the pre-image of any point $z \in \mathbb{C}$ is a closed subset of Y. Let us consider the intersection $f^{-1}(z) \cap U$. For $f = g/h$ this set consists of all $y \in U$ such that

$g(y) - z \cdot h(y) = 0$, so it is a closed subset of U. Hence $f^{-1}(z)$ is a closed subset in Y. $\square$

8.2. **Local rings and rational functions.**

Definition 8.4. Let Y be a variety (i.e. any affine, quasi-affine, projective or quasi-projective variety). We denote by $\mathcal{O}(Y)$ the ring of all regular functions on Y. For any point $P \in Y$ we define the *local ring* of P on Y, $\mathcal{O}_{P,Y}$ (or simply $\mathcal{O}_P$) to be the ring of germs of regular functions on Y near P:

$$\mathcal{O}_P = \lim_{U \to p} \{(U, f),\ f \text{ is a regular function on } U\}.$$

Exercise 8.5. Prove that $\mathcal{O}_P$ is a local ring.

Hint. Show that the only maximal ideal in $\mathcal{O}_P$ is the set of germs of regular functions vanishing at P, because any other ideal contains invertible elements $f, 1/f$ for a somewhere non-vanishing f.

To any variety X we have associated a coordinate ring $A(X)$. Now we shall associate to X a field $K(X)$ which is called *the function field* of X as follows.

Any element of $K(X)$ is an equivalence class of pairs $\langle U, f\rangle$ where U is a nonempty open subset of Y and f is a regular function on U. Two pairs $\langle U, f\rangle$ and $\langle V, g\rangle$ are equivalent, if $f = g$ on the intersection $U \cap V$. The elements of $K(X)$ is called *rational functions* on Y.

Remark 8.6. i) There exists a natural addition and multiplication on $K(X)$, so $K(X)$ is a ring. For any element $\langle U, f\rangle \in K(X)$ with $f \neq 0$, the element $\langle U \setminus U \cap Z(f), 1/f\rangle$ is an inverse for $\langle U, f\rangle$. Hence $K(X)$ is a field.

ii) There exists natural maps $\mathcal{O}(X) \stackrel{i_p}{\to} \mathcal{O}_P \stackrel{j_p}{\to} K(X)$, whre i_p is the restriction and j_p is the projection (i.e. j_p associates (U, f) to the equivalence class of (U, f) in $K(X)$. Clearly j_p is injective. It is also not hard to see that i_p is injective, since any polynomial that vanishes on an open subset vanishes on the whole domain of its definition. So we consider $\mathcal{O}(X)$ and $\mathcal{O}_P$ as sub-rings of $K(X)$.

Theorem 8.7. *Let $Y \subset \mathbb{C}^n$ be an affine variety with affine coordinate ring $A(Y)$. Then*
i) $\mathcal{O}(Y) \cong A(Y)$.
ii) for each P the local field $\mathcal{O}_P$ is isomorphic to the localization $A(Y)_{\mathfrak{m}_P}$, where $\mathfrak{m}_P$ is the maximal ideal of functions vanishing at P (see Proposition 7.2), moreover $\dim \mathcal{O}_P = \dim Y$.
iii) $K(Y)$ is isomorphic to the field of fractions $F(A(Y))$ of $A(Y)$ and hence the dimension of $K(Y)$ is equal to the dimension of $A(Y)$.

Proof. ii) Let us first prove the second statement. Let α be the natural inclusion $A(Y) \to \mathcal{O}(Y)$. This map i descends to a map

$$\bar{\alpha} : A(Y)_{\mathfrak{m}_P} \to \mathcal{O}_P,\ (f, s) \mapsto (f/s).$$

Then $\bar{\alpha}$ is injective since α is injective. Clearly $\bar{\alpha}$ is surjective by definition of $\mathcal{O}_P$. So $\mathcal{O}_P \cong A(Y)_{\mathfrak{m}_P}$. Hence

$$\dim \mathcal{O}_P = \dim A(Y)_{\mathfrak{m}} \overset{7.15}{=} \dim A(Y) \overset{Prop. 7.7}{=} \dim Y.$$

This proves the second assertion of Theorem 8.7.

iii) Using Remark 8.6 ii) we conclude that the field of fractions $F(\mathcal{O}_P)$ of $\mathcal{O}_P$ is a subfield of $K(Y)$, so by the second assertion of Theorem 8.7, which is just proved, $F(A(Y)) \subset K(Y)$. But any rational function is in some $\mathcal{O}_P$, so $K(Y) \subset \cup_{P\in Y} F(\mathcal{O}_P) = F(A(Y))$. This proves the third assertion of Theorem 8.7.

i) Clearly

$$\mathcal{O}(Y) \subset \cap_{P\in Y}\mathcal{O}_P \overset{Theorem 8.7.ii}{=} \cap_{\mathfrak{m}_P} A(Y)_{\mathfrak{m}_P} \subset F(A(Y)),$$

where $\mathfrak{m}_P$ are maximal ideals. We shall show that

$$\cap_{\mathfrak{m}_P} A(Y)_{\mathfrak{m}_P} = A(Y). \tag{8.1}$$

It suffices to show that if $(a, x) \in A(Y)_{\mathfrak{m}}$ for all maximal ideal $\mathfrak{m}$, then $(a, x) = (\bar{a}, 1)$ for some $\bar{a} \in A(Y)$. Let

$$x \in \cap_{P\in Y}(A(Y) \setminus \mathfrak{m}_P).$$

Then $x(P) \neq 0$ for all $P \in Y$. Hence x must be $c + I(Y)$ for some constant $c \neq 0$. Hence $(a, x) = (a/c, 1)$, what is required to prove.

□

Remark 8.8. We cannot mimic the definition of a regular function of an affine variety for the case of a quasi-affine variety, since a quasi-affine variety cannot defined via vanishing ideal. The later one always defines a *closed* subset.

Before stating a structure theorem for projective varieties let us introduce a new notation. For a homogeneous prime ideal $\mathfrak{p}$ in a graded ring S we denote by $S_{(\mathfrak{p})}$ the subring of elements of degree 0 in the localization of S w.r.t. the multiplicative subset T consisting of the homogeneous elements of S not in $\mathfrak{p}$. Here the degree of an element (f/g) in $T^{-1}S$ is given by $\deg f - \deg g$. Clearly $S_{(\mathfrak{p})}$ is a local ring with maximal ideal $(\mathfrak{p} \cdot T^{-1}S) \cap S_{(\mathfrak{p})}$, since any $y \in S_{(\mathfrak{p})} \setminus \{\mathfrak{p} \cdot T^{-1}S) \cap S_{(\mathfrak{p})}\}$ is invertible. In particular the localization $S_{((0))}$ is a field, if S is a domain.

Theorem 8.9. *Let Y be a projective variety. Then:*
i) $\mathcal{O}(Y) = \mathbb{C}$,
ii) $\mathcal{O}_P = S(Y)_{(\mathfrak{m}_P)}$, where $\mathfrak{m}_P \subset S(Y)$ is ideal generated by homogeneous elements f vanishing at P,
iii) $K(Y) \cong S(Y)_{((0))}$.

Except statement (i), which is an analog of the Louiville theorem, the other statements (ii) and (iii) of Theorem 8.9 are similar to that ones in Theorem 8.7.

Proof of Theorem 8.9. ii) As in the proof of Theorem 8.7 we begin with the second statement. This is a local statement, so we shall apply Theorem 8.7.ii to this situation. We cover $\mathbb{C}P^n$ by open sets $U_i = \mathbb{C}P^n \setminus H_i$ (see Proposition 6.10) and let $\phi : U_i \to \mathbb{C}^n$ be the homeomorphism defined in Proposition 6.10. Now we define $\phi^* : \mathcal{O}(\mathbb{C}^n) \to \mathcal{O}(U_0)$ by

$$\phi^*(f)(z) = f(\phi(z)). \tag{8.2}$$

We shall show that this definition is correct, i.e. if locally $f = g/h$, where $g, h \in \mathbb{C}[z_1, \cdots z_n]$, then $\phi^*(f) = \tilde{g}/\tilde{h}$ where $\tilde{f}, \tilde{g}$ are homogeneous polynomials of the same degree in $\mathbb{C}[z_0, \cdots, z_n]$. Using (6.4) and substituting t' in (6.4) by g and h resp. we have

$$\frac{g(\phi(z))}{h(\phi(z))} = \frac{z_0^{-deg(g)}\beta(g)(z)}{z_0^{-deg(h)}\beta(h)(z)},$$

where $\beta(g)$ (resp. $\beta(h)$) is a homogeneous polynomial of degree $deg(g)$ (resp. $deg(h)$). Hence homogeneous polynomials $\tilde{g} = \beta(g)z_0^{deg(h)}$ and $\tilde{f} = z_0^{deg(g)}\beta(f)$ satisfy the required conditions.

Lemma 8.10. *The map $\phi^* : \mathcal{O}(\mathbb{C}^n) \to \mathcal{O}(U_i)$ is a ring isomorphism.*

Proof. Clearly ϕ^* is a ring homomorphism and ϕ is injective, since $f \in \ker \phi^*$ iff $f = 0$. To see that ϕ is surjective, we observe that if $f = (\tilde{g}/\tilde{h}) \in \mathcal{O}(U_0)$, where $\tilde{g}$ and $\tilde{h}$ are homogeneous of the same degree then

$$f(z) = \frac{r(\tilde{g})(\phi(z))}{r(\tilde{h})(\phi(z))},$$

where r is defined in (6.3) and we replace t in (6.3) by $\tilde{g}$ (resp. $\tilde{h}$). So

$$f = \phi^*(\frac{r(\tilde{g})}{r(\tilde{h})}).$$

□

Now let us continue the proof of Theorem 8.9.ii. Let $Y_i = Y \cap U_i$. We can consider Y_i as an affine variety in $U_i = \mathbb{C}^n$. Using Lemma 8.10 and Theorem 8.7.ii we get $\mathcal{O}_P \cong A(Y_i)_{\mathfrak{m}'_P}$ where $Y_i \ni P$ and $\mathfrak{m}'_P$ is the maximal ideal of $A(Y_i)$ corresponding to P. Since $z_i \notin \mathfrak{m}_P$ and $\beta^{-1}(\mathfrak{m}_P) \subset \mathfrak{m}'_P$ we can construct a map $\phi^* : A(Y_i)_{\mathfrak{m}'_p} \to S(Y)_{(\mathfrak{m}_P)}$ as follows

$$(g, h) \overset{\phi^*}{\mapsto} (z_i^{deg(h)}\beta(g), z_i^{deg(g)}\beta(h)) \tag{8.3}$$

(cf. (8.2)). Clearly ϕ^* is a ring homomorphism whose kernel is empty because $\beta^{-1}(\mathfrak{m}_P) \subset \mathfrak{m}'_P$. It is easy to check that ϕ^* is surjective, so ϕ^* is an isomorphism which proves (ii).

iii) First we note that $K(Y) = K(Y_i)$ since any pair (U, f) representing an element in $K(Y)$ is equivalent to an element $(U \cap Y_i, f_{|(U\cap Y_i)})$. By Theorem 8.7.iii we get that $K(Y) = K(Y_i)$ is the quotient field $K(A(Y_i))$ of $A(Y_i)$. Using the natural isomorphism ϕ^* in (8.3) which extends to an isomorphism between the quotient field $K(A(Y_i))$ and $S(Y)_{((0))}$ we prove the statement (iii).

i) Let $f \in \mathcal{O}(Y)$ be a global function. Then f is regular on Y_i and therefore, by Theorem 8.7.i we have $f \in A(Y_i)$. Using the isomorphism $\phi^* : A(Y_i) = S(Y)_{(z_i)}$ (see the proof of (ii) above, here we consider $A(Y_i)$ as a subring of $A(Y_i)_{\mathfrak{m}'_P}$) we conclude that $\phi^*(f)$ has the form $g_i/x_i^{N_i}$ where $g_i \in S(Y)$ is a homogeneous polynomial of degree N_i. Recall that $S(Y)_N$ denotes the subspace of $S(Y)$ with grading N. Choose a number $N \geq \sum N_i$ and note that $S(Y)_N \cdot (\phi^*(f)) \subset S(Y)_N$. Hence we get $S(Y)_N \cdot \phi^*(f)^q \subset S(Y)_N$. In particular $x_0^N \cdot \phi^*(f)^q \in S(Y)_N \subset S(Y)$ for all q.

Thus the subring $S(Y)[\phi^*(f)] \subset K(S(Y))$ is contained in $x_0^{-N}S(Y)$. Since $S(Y)$ is a noetherian ring, $S(Y)[\phi^*(f)]$ is finitely generated $S(Y)$-module. By Noether normalization theorem (Theorem 7.10), $\phi^*(f)$ is integral over $S(Y)$, or equivalently there are $a_1, \cdots, a_m \in S(Y)$ such that

$$\phi^*(f)^m + a_1\phi^*(f)^{m-1} + \cdots + a_m = 0. \tag{8.4}$$

($\phi^*(f)$ is a root of the characteristic polynomial).

Now we observe that $deg\, \phi^*(f) = 0$, so (8.4) still valid if we replace a_i by their homogeneous component of degree 0, i.e. we can assume that $a_i \in \mathbb{C}$. Thus $\phi^*(f)$ is algebraic over $\mathbb{C}$, so $\phi^*(f) \in \mathbb{C}$, hence $f \in \mathbb{C}$. □

Digression. Outline of the proof of Noether's normalization theorem. For the sake of convenience of the reader we shall reproduce another proof of Theorem 7.10 from [AM1969].

Let $x_1, \cdots, x_k$ be a system of generators of $S(Y)[f]$. Denote by M_f the endomorphism of $S(Y)[f]$ defined by the multiplication with f. Then

$$M_f(x_i) = \sum a_{ij} x_{ij}, \, \forall i$$

$$\Longleftrightarrow \sum_j (\delta_{ij} M_f - a_{ij}) x_j = 0, \, \forall i. \tag{8.5}$$

Multiplying the LHS of (8.5) with the adjoint matrix of $(\delta_{ij} M_f - a_{ij})$, we note that $\det(\delta_{ij} M_f - a_{ij})$ annihilates all x_i, so $\det(\delta_{ij} M_f - a_{ij}) = 0$. Decompose this polynomial and substituting f by $\phi^*(f)$ we conclude that $\phi^*(f)$ is integral over $S(Y)$.

8.3. **Morphisms between varieties.** We have met and used the notion of isomorphism between two particular varieties in Lemma 8.10. In general, a *morphism* $\phi : X \to Y$ is a continuous map such that for every open set $V \subset Y$ we have $\phi^*(\mathcal{O}(V)) \subset \mathcal{O}(\phi^{-1}(V))$, i.e. ϕ preserves the structure sheaf. We denote by $Mor(X, Y)$ the set of all morphisms from X to Y.

Proposition 8.11. *Let X be a variety and let Y be an affine variety. Then there is a natural bijective map of sets*

$$\alpha : Mor(X, Y) \to Hom(A(Y), \mathcal{O}(X)).$$

Proof. A morphism $\phi \in Mor(X, Y)$ defines a homomorphism $\phi^* : \mathcal{O}(Y) \to \mathcal{O}(X)$. Since Y is affine, by Theorem 8.7.i this natural transformation defines a map α. We first show that map α is injective, i.e. if ϕ_1 and ϕ_2 are two different morphisms, then ϕ_1^* and ϕ_2^* are different homomorphisms.

Any map $\phi : X \to Y \subset \mathbb{C}^n$ can be written in the following form

$$\phi(P) = (\xi_1(P), \cdots, \xi_n(P)) \in Y \subset \mathbb{C}^n. \tag{8.6}$$

Clearly $\mathcal{O}(X) \ni \xi_i = \phi^*(\bar{z}_i)$ where $\bar{z}_i$ the image of z_i in $A(Y) = \mathbb{C}[z_1, \cdots, z_n]/I(Y)$.

From (8.6) we see immediately that α is injective.

Now we shall show that α is surjective. Let $\bar{\phi}$ be a homomorphism from $A(Y)$ to $\mathcal{O}(X)$. Let $\xi_i = \bar{\phi}(\bar{z}_i) \in \mathcal{O}(X)$. We shall define a continuous map $\phi : X \to \mathbb{C}^n$ by (8.6). To complete the proof it suffices to show that $\phi(P) \in Y$ and $\phi^* = \bar{\phi}$. First we shall show that for any $f \in I(Y)$ we have $f(\phi(P)) = 0$ which shall imply that $\phi(P) \in Y$. Since $\bar{\phi}$ is a homomorphism of $\mathbb{C}$-algebras we have

$$\begin{aligned} f(\phi(P)) = f(\xi_1(P), \cdots, \xi_n(P)) &= f(\bar{\phi}(\bar{z}_1(P)), \cdots, \bar{\phi}(\bar{z}_n(P))) \\ &= \bar{\phi}(f(\bar{z}_1, \cdots \bar{z}_n))(P) = 0. \end{aligned}$$

The second statement $\phi^* = \bar{\phi}$ follows by checking

$$\phi^*(\bar{z}_i)(P) \stackrel{def}{=} \bar{z}_i(\phi(P)) = \bar{z}_i(\xi_1(P), \cdots, \xi_n(P)) = \bar{\phi}(\bar{z}_i)(P).$$

□

Now we shall say that a morphism $(\phi, \phi^*) : X \to Y$ is an *isomorphism*, if ϕ and ϕ^* admit inverse. In the category of differentiable manifolds with structure sheaf consisting of differentiable functions we can replace the global condition of invertibility of ϕ^* by the local invertibility of the tangent map $D\phi$. Analogously in the category of (complex algebraic) varieties we can replace the condition of global invertibility of ϕ^* by invertibility of the induced homomorphism $\phi^*_P : \mathcal{O}_{\phi(P),Y} \to \mathcal{O}_{P,X}$ for all $P \in X$.

Example 8.12. Let $H_d \subset \mathbb{C}P^n$ be a hyper-surface defined by a homogeneous polynomial P^d of degree d. We shall show that $\mathbb{C}P^n \setminus H_d$ is isomorphic to an affine variety. First we shall find an embedding $\phi_d : \mathbb{C}P^n \to \mathbb{C}P^N$ such that $\phi_d(H_d)$ lies in some hyper-plane $\{z_j = 0\}$ in $\mathbb{C}P^N$. Then we shall show that ϕ^*_d induces an isomorphism of local rings $\mathcal{O}_{\phi(P),\phi(\mathbb{C}P^n)}$ and $\mathcal{O}_{P,\mathbb{C}P^n}$ for all $P \in \mathbb{C}P^d$. This shall imply that $(\mathbb{C}P^n \setminus H_d)$ is isomorphic to the affine variety $\phi_d(\mathbb{C}P^n \setminus H_d) \subset \mathbb{C}^N = \mathbb{C}P^N \setminus \{z_j = 0\}$ with the induced ring of regular functions. In particular $\mathcal{O}_{\phi(P),\phi(\mathbb{C}P^n)} = j^*\mathcal{O}_{P,\mathbb{C}P^N}$, where $j : \phi_d(\mathbb{C}P^n \setminus H) \to \mathbb{C}P^N$ is the inclusion map.

The map ϕ_d can be chosen as a Veronese map of degree d

$$\phi_d : \mathbb{C}P^n \to \mathbb{C}P^N$$

$$[z_0, \cdots z_N] \mapsto [\cdots X^I \cdots]$$

where z^I ranges over all monomials of degree d in $z_0, \cdots, z_n$. Clearly ϕ_d is an embedding. Since P^d can be written as a linear combination of z^I, this proves the first statement. To show that ϕ^*_d induces a local isomorphism for all P it suffices to do it for any $P \in U_0 \subset \mathbb{C}P^n$. In this case $\mathcal{O}_{P,\mathbb{C}P^n} = \mathbb{C}[z_1, \cdots, z_n]_{\mathfrak{m}_P}$ and it is easy to check that $\phi^*_d(\mathcal{O}_{\phi(P),\mathbb{C}P^N}) = \mathcal{O}_{P,\mathbb{C}P^n}$, so $\phi^*_d : \mathcal{O}_{\phi(P),\phi(\mathbb{C}P^n)} \to \mathcal{O}_{P,\mathbb{C}P^n}$ is surjective. The kernel of ϕ^*_d at P consists of regular functions $g/h \in \mathcal{O}_{P,\mathbb{C}P^N}$ such that $(g/h)(\phi(U_P)) = 0$ for some neighborhood $P \in U_P \subset \mathbb{C}P^n$, hence $g \in I(\phi(U_P))$, so ϕ^*_d is injective.

Exercise 8.13. (i) Let $X \subset \mathbb{C}^n$ be an affine variety and $f \in \mathcal{O}(X)$. Define the open set $X_f \subset X$ by

$$X_f := X \setminus Z(f) = \{x \in X | \, f(x) \neq 0\}.$$

Prove that $\mathcal{O}(X_f) = \mathcal{O}(X)_{|X_f}[1/f]$. Using this show that $(X_f, \mathcal{O}(X_f))$ is an affine variety.

(ii) Prove that on any variety Y there is a base for the topology consisting of open affine subsets.

Hint. (i) Let $\tilde{X} := Z(I(X), f \cdot z_{n+1} - 1) \subset \mathbb{C}^{n+1}$. Show that the projection $p : \mathbb{C}^{n+1} \to \mathbb{C}^n$ that forgets the last coordinate z_{n+1} maps $\tilde{X}$ bijectively onto X_f. Denote by $\tilde{p}$ the restriction of p to $\tilde{X}$. Show that $(\tilde{p}^{-1})^*((z_{n+1})_{|\tilde{X}}) = f^{-1}_{|X_f}$.

(ii) If Y is an affine variety or quasi-affine variety, then reduce (ii) to (i). If Y is projective or quasi-projective, use the fact that Y can be covered by quasi-affine varieties (see Proposition 6.10 and consider the intersection $(U_i \cap Y)$).

Exercise 8.14. Let $f : X \to Y$ be a morphism between affine varieties. Prove that the image $\phi(X)$ is also an affine variety.

Hint. Extend ϕ to a morphism $e \circ \phi : X \to \mathbb{C}^n$ where $e : Y \to \mathbb{C}^n$ is the canonical embedding. Show that $I(e \circ \phi(X)) = \ker(e \circ \phi)^* : \mathbb{C}[z_1, \cdots, z_n] \to A(X)$.

Exercise 8.15. Let X be a projective variety. Show that any regular function f on X is constant.

Hint. We extend f to a function, also denoted by f from X to $\mathbb{C}P^1$. The graph $\Gamma_f : \{(x, f(x)) \in X \times \mathbb{C}P^1\}$ of f is a closed subset in $X \times \mathbb{C}P^1$. Show that the image $\pi_1(\Gamma_f)$ of the projection of Γ_f to $\mathbb{C}P^1$ is a closed subset and hence consists of finite point. Clearly $X = f^{-1}(\pi_1(\Gamma_f))$. Since X is irreducible, the image $\pi_1(\Gamma_f)$ consists of one point, i.e. f is constant.

9. Smoothness and tangent spaces

9.1. **Zariski tangent spaces.** We shall start with the affine case. Suppose that $X \subset \mathbb{C}^n$ is an affine variety. *A tangent vector* δ_{x_0} at a point $x_0 \in X$ is a "rule" to differentiate regular functions in x_0, i.e. it is a $\mathbb{C}$-linear map $\delta : \mathcal{O}(X) \to \mathbb{C}$ satisfying the Leibniz rule

$$\delta_{x_0}(f \cdot g) = f(x_0)\delta_{x_0}(g) + g(x_0)\delta_{x_0}(f),$$

for all $f, g \in \mathcal{O}(X)$. Such a map is called *derivation of* $\mathcal{O}(X)$ *in* x_0. It follows that $\delta_{x_0}(f^n) = nf^{n-1}(x_0)\delta_{x_0}(f)$ and so, for any polynomial $F = F(y_1, \cdots, y_m)$ we get

$$\delta_{x_0}(F(f_1, \cdots, f_m)) = \sum_{j=1}^{m} \frac{\partial F}{\partial y_j}(f_1(x_0), \cdots, f_m(x_0))\delta(f_j).$$

This implies that a derivation at x_0 is completely determined by its values on a generating set of the algebra $\mathcal{O}(X)$. As a consequence the set of all derivations in x_0 is a finite dimensional subspace of $Hom(\mathcal{O}(X), \mathbb{C})$.

Definition 9.1. The *Zariski tangent space* T_{x_0} of a variety X at a point x_0 is defined to be the set of all tangent vectors at x_0: $T_{x_0}X := Der_{x_0}(\mathcal{O}(X))$.

Note that $T_{x_0}X$ is a finite dimensional linear subspace of $Hom(\mathcal{O}(X), \mathbb{C})$.

Exercise 9.2. Let δ be a tangent vector in x. Prove that
(i) $\delta(c) = 0$ for every constant $c \in \mathcal{O}(X)$.
(ii) If $f \in \mathcal{O}(X)$ is invertible, then $\delta(f^{-1}) = -\frac{\delta f}{f(x)^2}$.

Since $\mathcal{O}(X) = \mathbb{C} \oplus \mathfrak{m}_x$ for all $x \in X$ we see that any element $\delta \in T_xX$ is determined by its restriction to $\mathfrak{m}_x$. The Leibniz formula shows that the restriction to $\mathfrak{m}_x^2$ vanishes. Hence δ induces a linear map $\bar{\delta} : \mathfrak{m}_x/\mathfrak{m}_x^2 \to \mathbb{C}$.

Lemma 9.3. *Given an affine variety X and a point $x \in X$ there is a canonical isomorphism*

$$T_xX \to Hom(\mathfrak{m}_x/\mathfrak{m}_x^2, \mathbb{C}),$$

given by $\delta \mapsto \bar{\delta} := \delta_{|\mathfrak{m}_x}$.

Proof. We have seen that $\delta \mapsto \bar{\delta}$ is injective. Let $\lambda \in Hom(\mathfrak{m}_x/\mathfrak{m}_x^2, \mathbb{C})$. Let C be a complement of $\mathfrak{m}_x^2$ in $\mathfrak{m}_x$, so $\lambda : C \to \mathbb{C}$ is a linear map. Now we extend λ to a linear map $\delta : \mathcal{O}(X) = \mathbb{C} \oplus C \oplus \mathfrak{m}_x^2 \to \mathbb{C}$ by putting $\delta_{|\mathbb{C}\oplus\mathfrak{m}_x^2} = 0$. □

Lemma 9.4. *For all $z \in \mathbb{C}^n$ we have $T_z\mathbb{C}^n = \{\frac{\partial}{\partial z_i}_{|z}\}, i = 1, n$.*

Proof. Let $z = (a_1, \cdots, a_n)$. The maximal ideal in $\mathbb{C}[z_1, \cdots, z_n]$ corresponding to z is $\mathfrak{m}_z = (z_1 - a_1, \cdots z_n - a_n)$. We define the derivation map

$$D : \mathfrak{m}_z/(\mathfrak{m}_z)^2 \to \mathbb{C}^n : f \mapsto (\frac{\partial f}{\partial z_i}_{|z}, i = 1, n).$$

Clearly $\{D(z_i - a_i),\ i = 1, n\}$ form a basis of $\mathbb{C}^n$, hence D is an isomorphism . Now Lemma 9.4 follows immediately from Lemma 9.3. □

Exercise 9.5. If $Y \subset X$ are affine varieties in $\mathbb{C}^n$ and $x \in Y$ then $\dim T_xY \leq \dim T_xX$.

Hint. The surjective map $A(X) = \mathcal{O}(X) \to \mathcal{O}(Y) = A(Y)$ induces a surjective map $\mathfrak{m}_{x,X}/\mathfrak{m}_{x,X}^2 \to \mathfrak{m}_{x,Y}/\mathfrak{m}_{x,Y}^2$.

The space $(\mathfrak{m}_x/\mathfrak{m}_x^2)$ is called the *cotangent space* of X at x.

Definition 9.6. Let A be a noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field $k = A/\mathfrak{m}$. We say that A is a *regular local ring*, if $\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim A$.

9.2. **Smoothness in algebraic geometry.** To motivate the notion of smoothness in algebraic geometry, we first remind it in the real and complex analytic category. Let $f_1, \dots, f_k \in C^\infty(U)$ be smooth functions (or $f_1, \dots, f_k \in \mathcal{O}(U)$ holomorphic functions in the complex case), $U \subset \mathbb{R}^n$ (or $U \subset \mathbb{C}^n$) and $k \in \mathbb{N}$. We assume $b = (b_1, \dots, b_n) \in U$ is a point such that $f_1(b) = \dots = f_k(b) = 0$ and

$$\det\Big(\frac{\partial f_i}{\partial x_j}\Big)_{1\le i,j\le k}(b) \neq 0. \tag{9.1}$$

Then there exists an open $U' \subset U$, $b \in U'$, such that the projection

$$\begin{aligned} \mathrm{pr} : Z = \{x \in U |\, f_1(x) = \dots = f_k(x) = 0\} &\to \mathbb{R}^{n-k} \quad (\text{or } \mathbb{C}^{n-k}) \\ (x_1, \dots, x_n) &\mapsto (x_{r+1}, \dots, x_n) \end{aligned} \tag{9.2}$$

is a diffeomorphism (or a biholomorphic map) between $Z \cap U'$ and the open neighborhood $\mathrm{pr}(Z \cap U')$ of $(b_{r+1}, \dots, b_n) \in \mathbb{R}^{n-k}$ (or $\mathbb{C}^{n-k}$). In other words, the implicit function theorem based on (9.1) implies that b is a smooth point of a manifold Z given by the zero locus of $f_1, \dots, f_k$ and $(x_{r+1} - b_{r+1}, \dots, x_n - b_n)$ gives the local chart on Z around b.

We now turn to an analogous construction in the category algebraic varieties. To that aim, we consider the free algebra $K[x_1, \dots, x_n]$ over a field K, the ring of regular functions $\mathcal{O}(Z) := K[x_1, \dots, x_n]/I$ of an algebraic variety Z given by an ideal I generated by polynomials $f_1, \dots, f_k$ and Q a maximal ideal $K[x_1, \dots, x_n]$ resp. P the maximal ideal in $\mathcal{O}(Z)$ of the form $P = Q/I$ ($I \subset Q$), see Definition 8.2 and Theorem 8.7. We denote $K[x_1, \dots, x_n]_Q$ the localization along Q and $\mathcal{O}(Z)_P$ the localization along P, we have

$$\mathcal{O}(Z)_P = K[x_1, \dots, x_n]_Q / I K[x_1, \dots, x_n]_Q \tag{9.3}$$

because localization commutes with quotients. To be specific, for a K-rational point $b = (b_1, \dots, b_n) \in Z(K) \subset K^n$ we have $Q = (x_1 - b_1, \dots, x_n - b_n)$, $P = (\bar{x}_1 - b_1, \dots, \bar{x}_n - b_n)$ and

$$\mathcal{O}(Z)_P = K[x_1, \dots, x_n]_{(x_1 - b_1, \dots, x_n - b_n)} / \langle f_1, \dots, f_k \rangle. \tag{9.4}$$

We shall examine the concept of smoothness on the simplest motivating example of an affine algebraic curve (smoothness is a local notion and so it suffices to restrict to the affine case.) We assume $n = 2$, $k = 1$, $I :\ f \in K[x, y] \setminus K$, $Z :\ f(x, y) = 0$, $\mathcal{O}(Z) = K[x, y]/\langle f \rangle$ with

$Z(K) \hookrightarrow \mathbb{A}^2_K$. For $b = (b_1, b_2) \in Z(K)$,

$$P = \mathrm{K}er(\overline{ev}_b) = Q/\langle f\rangle = \mathrm{K}er(ev_b)/\langle f\rangle \tag{9.5}$$

for the evaluation homomorphisms $\overline{ev}$ and ev on $\mathcal{O}(Z)$ and $K[x,y]$, respectively. A working definition of smoothness for affine algebraic curves is

$$Z \text{ is smooth at } P \Longleftrightarrow \frac{\partial f}{\partial x}(b) \neq 0 \text{ or } \frac{\partial f}{\partial y}(b) \neq 0. \tag{9.6}$$

By applying an automorphism of $\mathbb{A}^2_K$, we can and in what follows we shall assume $b = (0,0)$ so that $Q = (x,y)$, $P = (x,y)/\langle f\rangle$. If Z is smooth at P defined by b, we can assume (perhaps after permuting x for y) $\frac{\partial f}{\partial x}(0,0) \neq 0$, which is equivalent to the property that $T_{(0,0)}Z$ is not horizontal. Perhaps after multiplying by a non-zero element of K, the polynomial f is of the form

$$f(x,y) = x + cy + \sum_{i+j\geq 2} c_{i,j}x^i y^j, \quad c, c_{i,j} \in K. \tag{9.7}$$

Polynomials can be inverted in the ring of formal power series and in fact, there is an elementary division algorithm for formal power series: for any $g \in K[[x,y]]$ there exists a unique $h \in K[[x,y]]$ such that $g - fh \in K[[y]]$. This means that the composition

$$K[[y]] \hookrightarrow K[[x,y]] \to K[[x,y]]/\langle f\rangle \tag{9.8}$$

is an isomorphism of K-algebras. This statement is a formal power series analogue of (9.2).

In the next Lemma we retain the notation of the previous paragraphs.

Lemma 9.7. (1) *Assume* $\frac{\partial f}{\partial x}(0,0) \neq 0$. *Then*

$$A_P = A_{(x,y)} = K[x,y]_{(x,y)}/\langle f\rangle \tag{9.9}$$

is domain and its maximal ideal $(x,y)A_{(x,y)}$ *is equal to* $\bar{y}A_{(x,y)}$. *We recall*

$$K[x,y]_{(x,y)} = \{\frac{g}{h} |\, g,h \in K[x,y],\, h(0,0) \neq 0\} \subset K(x,y). \tag{9.10}$$

(2) *Assume* A_P *is domain (in particular, a local ring). If its maximal ideal* $PA_P = tA_P$ *is principal for some* $t \in A_P$, *then* Z *is smooth algebraic variety at* P.

9.3. **Nonsingular varieties.** The smoothness definition in (9.6) is formalized in the general case as follows.

Definition 9.8. Let $Y \subset \mathbb{C}^n$ be an affine variety and let $f_1, \cdots, f_l \in \mathbb{C}[z_1, \cdots, z_n]$ be a set of generators for the ideal of Y. We say that Y is *nonsingular at a point* $P \in Y$ if the rank of the matrix $[(\partial f_i/\partial x_j)]_P$ at P is $n-r$ where r is the dimension of Y. We say that Y is *nonsingular*, if it is nonsingular at every point. The following theorem explains that the notion of nonsingularity does not depend on the choice of $(f_1, \cdots, f_n)$, i.e. on the choice of embedding $Y \to \mathbb{C}^n$.

Theorem 9.9. *Let $Y \subset \mathbb{C}^n$ be an affine variety. Let $P \in Y$ be a point. Then Y is nonsingular at P, if and only if the local ring $\mathcal{O}_{P,Y}$ is a regular local ring.*

Proof. Let $I(Y) \subset \mathbb{C}[z_1, \cdots, z_n]$ be the ideal of Y and let $f_1, \cdots f_l$ be a set of generators of $I(Y)$. Denote by $I(Y)_P$ the image of $I(Y)$ in the local ring $\mathfrak{m}_{P,\mathbb{C}^n}$. Then the rank of the Jacobian matrix $J_P = ||(\partial f_i/\partial x_j)||_P$ is the dimension of the space $D(I(Y)_P) \subset \mathbb{C}^n$, where $D : \mathfrak{m}_{P,\mathbb{C}^n} \to \mathbb{C}^n$ is defined in Lemma 9.4. Since D is an isomorphism we have

$$(9.11) \qquad rank\ J = \dim D(I(Y)_P) = \dim((I(Y)_P + \mathfrak{m}^2_{P,\mathbb{C}^n})/\mathfrak{m}^2_{P,\mathbb{C}^n}).$$

Denote by j the surjection $\mathbb{C}^n[z_1, \cdots, z_n] \to \mathcal{O}(Y) = A(Y)$ and by j_P the induced surjective map from $\mathfrak{m}_{P,\mathbb{C}^n} \to \mathfrak{m}_{P,Y}$ (see also Exercise 9.5). The kernel of j is $I(Y)$ and the kernel of j_P is $I(Y)_P$. Thus

$$(9.12) \qquad \frac{\mathfrak{m}_{P,Y}}{\mathfrak{m}^2_{P,Y}} = \frac{\mathfrak{m}_{P,\mathbb{C}^n}/(\ker j_P)}{(\mathfrak{m}_{P,\mathbb{C}^n}/\ker j_P)^2} = \frac{\mathfrak{m}_{P,\mathbb{C}^n}}{I(Y)_P + \mathfrak{m}^2_{P,\mathbb{C}^n}}.$$

Now since $\dim(\mathfrak{m}_{P,\mathbb{C}^n}/\mathfrak{m}^2_{P,\mathbb{C}^n}) = n$, taking into account (9.11) and (9.12) we get

$$(9.13) \qquad \dim(\mathfrak{m}_{P,Y}/\mathfrak{m}^2_{P,Y}) + rank\ J = n.$$

Let $\dim Y = r$. Then according to Theorem 8.7(ii) $\mathcal{O}_P$ is a local ring of dimension r. By definition $\mathcal{O}_p$ is *regular* if $\dim \mathfrak{m}/\mathfrak{m}^2 = r$. From (9.13) we get that this relation is equivalent to the relation $rank\ J = n - r$. □

Exercise 9.10. Let $X \subset \mathbb{C}^n$ be an affine subvariety. Prove that

$$T_{x_0}X = \{\delta \in T_{x_0}\mathbb{C}^n |\ \delta(f) = 0 \text{ for all } f \in I(X)\} \subset T_{x_0}\mathbb{C}^n = \mathbb{C}^n.$$

Hint Compare with Exercise 9.5.

Theorem 9.9 motivates us to give the following definition of (non)singularity of a variety. Let Y be a variety (not necessary affine). Then a point

$P \in Y$ is *nonsingular* if the local ring $\mathcal{O}_{P,Y}$ is a regular local ring. Y is *nonsingular* if it is nonsingular at every point. Y is singular, if it is not nonsingular.

Example 9.11. Let $H := Z(f) \subset \mathbb{C}^n$ be a hypersurface where $f \in \mathbb{C}[z_1, \cdots, z_n]$ is an irreducible polynomial, hence $I(H) = (f)$. Then the tangent space in a point $x_0 \in H$ is given by (see Exercise 9.10)

$$T_{x_0} := \{a = (a_1, \cdots, a_n)| \sum a_i \frac{\partial f}{\partial x_i}(x_0) = 0\}. \tag{9.14}$$

Let Y be a singular point of H. Then by definition the ring $\mathcal{O}_{P,H}$ is not regular, i.e. $\dim(\mathfrak{m}_{Y,H}/(\mathfrak{m}_{Y,H})^2) \neq \dim \mathcal{O}_{P,H}$. But $\mathcal{O}_{P,H} = A(H)_{\mathfrak{m}_{P,H}}$ and then using Theorem 7.9 we get

$$\dim \mathcal{O}_{P,H} = \dim A(H) = n - 1.$$

Thus Y is singular, iff $\dim T_{x_0} H \neq n - 1$. Using (9.14) we see that the set H_{sing} of singular points of H is given by

$$H_{sing} = Z(f, \frac{\partial f}{\partial z_1}, \cdots, \frac{\partial f}{\partial z_n}) \subset H.$$

Proposition 9.12. *Let X be an irreducible affine variety. Then the set X_{sing} of singular points is a proper closed subset of X whose complement is dense.*

Proof. We can assume that X is an irreducible closed subvariety in $\mathbb{C}^n$ of dimension d. Let $f_1, \cdots, f_l$ be a set of generators of $I(X)$. By Theorem 9.9

$$X_{sing} = \{x \in X| \, rk[\frac{\partial f_j}{\partial z_i}(x)] < n - d\}$$

is a closed subset defined by vanishing of all $(n - d) \times (n - d)$ minors of the Jacobian matrix J.

To show that X_{sing} is a proper subset of X we apply Exercise 13.7 to get X birational to a hypersurface $H \subset \mathbb{C}P^n$. Since birational maps preserve the dimension of variety and they map singular points/nonsingular points to singular points/nonsingular points, applying Example 9.11 we get Proposition 9.12. □

9.4. **Projective tangent spaces.** Consider now a projective variety $X \subset \mathbb{C}P^n$. We may also associate to it a projective tangent space at each point $p \in X$, denoted T_pX which is a projective subspace of $\mathbb{C}P^n$. One way to do this is to choose an affine open subset $U \cong \mathbb{C}^n \subset \mathbb{C}P^n$ containing p and define the projective tangent space to X to be the closure in $\mathbb{C}P^n$ of the tangent space at p of the affine variety $X \cap U \subset U = \mathbb{C}^n$.

There is another way to describe the projective tangent space to a variety $X \subset \mathbb{C}P^n$ at a point $p \in X$. Let $\tilde{X} \subset \mathbb{C}^{n+1}$ be the cone over X and $\tilde{p} \in \tilde{X}$ be a point lying over p. Then the projective tangent space T_pX is the subspace of $\mathbb{C}P^n$ corresponding to the Zariski tangent space $T_{\tilde{p}}\tilde{X} \subset T_{\tilde{p}}\mathbb{C}^{n+1} = \mathbb{C}^{n+1}$.

9.5. **Tangent cones and singular points.** In definition of the Zariski tangent space T_xY at a point x of an affine variety $Y \subset \mathbb{C}^n$ we take into account only the first order expansion $\mathfrak{m}_x/\mathfrak{m}_x^2$ of the local ring $\mathcal{O}_{x,Y}$, or equivalently the zero set of the first order of the image of $I(Y)$ in the local ring $\mathcal{O}_{x,\mathbb{C}^n}$ (Lemma 9.3, Exercise 9.10). If we take into account higher order expansion of $\mathfrak{m}_x \subset \mathcal{O}_{x,\mathbb{C}^n}$, we shall get a finer invariant, namely the tangent cone TC_pX at a point x of Y. There are a geometric method and an algebraic method to define the tangent cone TC_xY at $x \in Y$ (Definition 9.13, Lemma 9.14).

A geometric method to define the tangent cone TC_xY at $x \in Y$. By affine transformation, we assume that $x \in Y \subset \mathbb{C}^n$ with $x = (0, ..., 0)$. We now look at all the lines that are limiting position of secants

$$\tilde{Y} := \{(a,t) \in \mathbb{C}^n |\ a \in \mathbb{C}^n \text{ and } t \in \mathbb{C}\}.$$

Clearly $\tilde{Y}$ is an algebraic set. Furthermore, $\tilde{Y}$ has two irreducible components $\tilde{Y}_1$ and $\tilde{Y}_2$. Denote by $pr_1 : \tilde{Y} \to \mathbb{C}$ and by $pr_n : \tilde{Y} \to \mathbb{C}^n$ the natural projections. Then

$$\tilde{Y}_2 = \{(a,0)|a \in \mathbb{C}^n\} \text{ and } \tilde{Y}_1 = \overline{pr_1^{-1}(\mathbb{C} \setminus 0)},$$

where $\overline{X}$ denotes the Zariski closure of X.

Definition 9.13. The set $TC_0Y := pr_n(pr_1^{-1}(0) \cap \tilde{Y}_1)$ is called *the tangent cone* of Y at $0 \in \mathbb{C}^n$.

Lemma 9.14. *The tangent cone TC_0Y is the zero set of the leading ideal $L(\mathfrak{m}_{0,Y})$. So it is the cone in the tangent space T_xY whose ideal is generated by the leading monomials of degree at least 2 in $\mathfrak{m}_{0,Y}$.*

Proof. Note that

$$I(\tilde{Y}) = \{\tilde{f}|\tilde{f}(a,t) = f(at) \text{ for } f \in \mathfrak{m}_{0,Y}\}.$$

Expanding

$$\tilde{f}(at) = \sum_{i=k}^{l} t^i \tilde{f}_i(a),$$

it is not hard to see that $\tilde{Y}_1 = Z(LM(f)|\, f \in L(\mathfrak{m}_{0,Y})$. This proves the first assertion. The second assertion follows from the first one, noting that the leading monomials of degree 1 in $\mathfrak{m})0, Y$ defines the tangent spce T_0Y. □

10. Completion

10.1. **What is the completion of a ring?** Let R be an abelian group and let $R = \mathfrak{m}_0 \supset \mathfrak{m}_1 \cdots$ be a sequence of subgroups (a descending filtration). We define *the completion* $\hat{R}$ *of* R *w.r.t. the* $\mathfrak{m}_i$ to be the inverse limit of the factor groups $R/\mathfrak{m}_i$ which is by definition a subgroup of the direct product

$$\hat{R} := \lim_{\leftarrow} R/\mathfrak{m}_i$$

$$:= \{g = (g_1, g_2, \cdots) \in \prod_i R/\mathfrak{m}_i | g_j \cong g_i (\mod \mathfrak{m}_i) \text{ for all } j > i\}.$$

If R is a ring and all $\mathfrak{m}_i$ are ideals then each of $R/\mathfrak{m}_i$ is a ring. Hence $\hat{R}$ is also a ring.

If moreover $\mathfrak{m}_i = \mathfrak{m}^i$ for some ideal $\mathfrak{m} \subset R$ then

$$\hat{\mathfrak{m}}_i := \{g = (g_1, g_2, \cdots) \in \hat{R} | \, g_j = 0 \text{ for all } j \le i\},$$

is called *the* $\mathfrak{m}$*-adic filtration of* R. The corresponding completion $\hat{R}$ is denoted by $\hat{R}_{\mathfrak{m}}$. We write $\hat{\mathfrak{m}} = \mathfrak{m}_1$.

Exercise 10.1. If $\mathfrak{m}$ is a maximal ideal, then $\hat{R}_{\mathfrak{m}}$ is a local ring with maximal ideal $\hat{\mathfrak{m}}$.

Hint. Show that $\hat{R}/\hat{R}_{\mathfrak{m}} = R/\mathfrak{m}$ which is a field.

Example 10.2. If $R = \mathbb{C}[z_1, ..., z_n]$ and $\mathfrak{m} = (z_1, ..., z_n)$, then the completion with respect to $\mathfrak{m}$ is the formal power series ring $\hat{R}_{\mathfrak{m}} = \mathbb{C}[[z_1, ..., z_n]]$. Indeed, from the map $\mathbb{C}[[z_1, ..., z_n]] \to R/\mathfrak{m}_i$ sending f to $f + \mathfrak{m}_i$ we get a map $\mathbb{C}[[z_1, ..., z_n]] \to \hat{R}_{\mathfrak{m}}$ sending

$$f \mapsto (f + \mathfrak{m}, f + \mathfrak{m}^2, \cdots) \in \hat{R}_{\mathfrak{m}} \subset \prod R/\mathfrak{m}_i.$$

The inverse map is given as follows

$$\hat{R}_{\mathfrak{m}} \ni (f_1 + \mathfrak{m}, f_2 + \mathfrak{m}^2, \cdots) \mapsto (f_1 + (f_2 - f_1) + (f_3 - f_2) + \cdots . \tag{10.1}$$

Here the condition $f_j \cong f_i (\mod \mathfrak{m}^i)$ for $j > i$ implies that $deg\,(f_{i+1} - f_i) \ge i + 1$. Thus the RHS of (6.1.3) is a well-defined formal power series.

Definition 10.3. If the natural map $R \to \hat{R}_{\mathfrak{m}}$ is an isomorphism we call R *complete w.r.t.* $\mathfrak{m}$. When $\mathfrak{m}$ is a maximal ideal, we say that R is a *complete local ring.*

10.2. **Why to use the completion of a ring?** In the algebraic geometry we don't have a version of the implicit function theorem, since the inverse of a polynomial map is not a polynomial map. But the inverse can be represented by a formal power series which is a case of complete rings. The analog of the implicit function theorem for complete rings is the following Hensel's Lemma.

Theorem 10.4 (Hensel's Theorem)**.** *Let R be a ring that is complete w.r.t. the ideal $\mathfrak{m}$, and let $f(x) \in R[x]$ be a polynomial. If a is an approximate root of f in the sense that*

$$f(a) \cong 0(\mod f'(a)^2\mathfrak{m})$$

then there is a root b of f near a in the sense that

$$f(b) = 0 \text{ and } b \cong a(\mod f'(a)\mathfrak{m}).$$

If $f'(a)$ is a nonzero-divisor in R, then b is unique.

11. 27 lines on cubic surfaces

A cubic surface $V \subset \mathbb{C}P^3$ is the zero set of a homogeneous cubic polynomial

$$F([T_0 : T_1 : T_2 : T_3]) = \sum_{i_0,\cdots,i_3} a_{i_0,\cdots i_3} T_0^{i_0} \cdots T_3^{i_3} \text{ where } \sum_{j=0}^{3} i_j = 3.$$

We also write $V(F)$ instead of V. In 1849 Cayley and Salmon proved the following

Theorem 11.1. *On each smooth cubic surface there is exactly 27 lines.*

That event has been called the beginning of modern algebraic geometry. We shall give a proof of an weaker version of this theorem, replacing "each" by "almost every", following [Dolgachev2013, Lecture 12, p. 105]. The argument of this proof is very typical in algebraic geometry.

Proof of Theorem 11.1. Instead to consider an isolated cubic surface and investigate lines on it we consider *all* smooth cubic surfaces and lines on each of them. This requires a parametrization of cubic surfaces, a parametrization of lines in the projective space $\mathbb{C}P^3$. We shall single out a "generic condition" for a cubic surface to contain exactly 27 lines. (With some more work, this generic condition can be shown to be equivalent to the smoothness of the surface in consideration).

• *Parametrization of cubic surfaces.* Note that two homogeneous cubic polynomials F and F' define the same zero set, if and and only if $F = \lambda \cdot F'$ for some $\lambda \in \mathbb{C}^*$. Hence the set of cubic surfaces is in a 1-1 correspondence with the set of coefficients of a homogeneous polynomial F of degree 3 in 4 variables modulo the action of $\mathbb{C}^*$. This set is exactly parametrized by projective space $\mathbb{C}P^{\binom{3+3}{3}-1} = \mathbb{C}P^{19}$.

- *Parametrization of lines in* $\mathbb{C}P^3$. Every line in $\mathbb{C}P^3$ corresponds to a plane in $\mathbb{C}^4$, and this correspondence is 1-1. The set of all planes in $\mathbb{C}^4$ is called the Grassmannian $Gr_2(\mathbb{C}^4)$. The Grassmanian $Gr_2(\mathbb{C}^4)$ is an algebraic subset of the projective space $\mathbb{C}P^{\binom{4}{2}-1} = \mathbb{C}P^5$ of all 2-vectors in $\mathbb{C}^4$ modulo $\mathbb{C}^*$-action. Once we fix a basis (e_1, e_2, e_3, e_4) for $\mathbb{C}^4$ and a basis (f_1, f_2) of a plane $E^2 \subset \mathbb{C}^4$ we can express E^2 via the *Plücker coordinates of* $Gr_2(\mathbb{C}^4)$, that is the (projective) coordinates of $f_1 \wedge f_2$ in basis of $\{e_i \wedge e_j | \, i < j\}$.

Lemma 11.2. *The Grassmannian $Gr_2(\mathbb{C}^4)$ is an irreducible projective set of dimension 4.*

Proof. We note that the algebraic group $Gl(4, \mathbb{C})$ acts transitively on $Gr_2(\mathbb{C}^4)$ with stabilizer of codimension 4. The group $GL(4, \mathbb{C})$ is an irreducible algebraic set in the affine space $gl(5, \mathbb{C}) = \mathbb{C}^{25}$ via the embedding $e : GL(4, \mathbb{C}) \to SL(5, \mathbb{C}), g \mapsto T_0 \oplus g$ with $T_0 = \det(g)^{-1}$. It has dimension 16. It is not hard to see that the projection $GL(4, \mathbb{C}) \to Gr_2(\mathbb{C}^4)$ is a regular map whose fibers are of the same dimension 12 and irreducible. By Proposition 11.3 below the dimension of $Gr_2(\mathbb{C}^4) = 4$ and $Gr_2(4, \mathbb{C})$ is irreducible.

Proposition 11.3. *(*[Dolgachev2013, Lemma 12.7]*) Let $f : X \to Y$ be a surjective regular map of projective algebraic sets. Assume that Y is irreducible and all the fiber are irreducible and of the same dimension. Then X is irreducible and* $\dim X = \dim Y + \dim f^{-1}(y)$ *for any $y \in Y$.*

□

Continuation of the proof of Theorem 11.1. Set

$$I := \{(V, l) \in \mathbb{C}P^{19} \times Gr_2(\mathbb{C}^4) | l \subset V\}.$$

Lemma 11.4. *The set I is an irreducible algebraic set of dimension 19. The projection $q : I \to \mathbb{C}P^{19}$ is surjective.*

Proof. We consider the projection $p : I \to Gr_2(\mathbb{C}^4)$. For each $E \subset Gr_2(\mathbb{C}^4)$ the fiber $p^{-1}(E)$ consists of all hypersurface $V(F)$ that contains E. Wlog we assume that E is given by the equation $T_1 = T_2 = 0$. Thus the fiber $p^{-1}(E)$ consists of homogeneous cubic form F whose coefficients at monomials containing any variables T_1, T_2 vanishes. Hence $\dim p^{-1}(E) = \binom{6}{3} - \binom{4}{1} - 1 = 15$. Taking into account $\dim Gr_2(\mathbb{C}^4) = 4$, we obtain the first assertion of Lemma 11.4.

Now let us prove the second assertion of Lemma 11.4. Suppose that the image $q(I)$ is a proper closed subset of $\mathbb{C}P^{19}$. Then $\dim q(I) < 19$ and hence $\dim q^{-1}(y) \geq 1$. Then every cubic surface containing a line contains infinitely many of them. The argument at the end of the proof of Theorem 11.1 given below shows that is not the case. In fact we show that there are at most 27 lines at stated in the theorem to be proved. This completes the proof of Lemma 11.4.

□

Completion of the proof of the weak version of Theorem 11.1 It follows from Lemma 11.4 that every cubic surface $V(F)$ hat at least one line. Let us pick such a line $l \subset V(F)$. Change coordinates if necessary, we assume that l is defined by the equation $T_2 = T_3 = 0$. Then F is written as

$$F = T_2(Q_0(T_0, T_1, T_2, T_3) + T_3 Q_2(T_0, T_1, T_2, T_2), \tag{11.1}$$

where Q_0 and Q_1 are quadratic polynomials.

To find more lines on $V(F)$ we look at the intersection of a plan $\pi \subset \mathbb{C}P^3$ with $V(F)$. Wlog, we assume that π contains the given l. Such a plan $\pi = \pi(\lambda, \mu) = \mathbb{C}P^2 \subset \mathbb{C}P^3$ is given by the equation

$$\lambda T_2 - \mu T_3 = 0 \text{ for } \lambda, \mu \in \mathbb{C}.$$

Choosing coordinates $[t_0 : t_1 : t_2]$ on π such that

$$T_0 = t_0,\ T_1 = t_1,\ T_2 = \mu t_2,\ T_3 = \lambda t_2.$$

Then, using (11.1), we rewrite the equation $F = 0$ as follows

$$\mu t_2 Q_0(t_0, t_1, \mu t_2, \lambda t_2) + \lambda t_2 Q_1(t_0, t_1, \mu t_2, \lambda t_2) = 0. \tag{11.2}$$

It follows that $\pi \cap V(F)$ contains a line l with equation $t_2 = 0$ and a conic

$$C(\lambda, \mu) := \{\mu Q_0(t_0, t_1, \mu t_2, \lambda t_2) + \lambda Q_1(t_0, t_1, \mu t_2, \lambda t_2) = 0\}.$$

Let

$$Q_0 = \sum a_{ij} T_i T_j \text{ and } Q_1 = \sum b_{ij} T_i T_j.$$

Then

$$\begin{aligned} C(\lambda, \mu) = \{ &(\mu a_{00} + \lambda b_{00}) t_0^2 + (\mu a_{11} + \lambda b_{11}) t_1^2 + (\mu^2(\mu a_{22} + \lambda b_{22}) + \lambda^2(\mu a_{33} + \lambda b_{33})) t_2^2 \\ &+ (\mu a_{01} + \lambda b_{01}) t_0 t_1 + (\mu(\mu a_{02} + \lambda b_{02}) + \lambda(\mu a_{03} + \lambda b_{03})) t_0 t_2 \\ &+ (\mu^2 a_{12} + \lambda \mu b_{12} + \mu \lambda a_{13} + \lambda^2 b_{13}) t_1 t_2 = 0 \}. \end{aligned}$$

Not that $\pi \cap l$ has more lines iff $Q(\lambda, \mu)$ is reducible, that is equivalent to the vanishing of the discriminant of $Q(\lambda, \mu)$. The later has degree 5 in λ, μ. Thus there exists an open set $U \subset \mathbb{C}P^{19}$ such that if $V \in U$

then the discriminant of $C(\lambda,\mu)$ that depends on V has 5 distinct roots (λ_i,μ_i). Each such a solution defines a plane π_i which cut out $V(F)$ at line l and the union of two lines or a double line. Choosing the genericity, we assume that the later does not occur. Then we have all together 11 lines. Now we want to know if we count all line on $V(F)$.

Pick some π_i, say $i=1$. Repeating the procedure but for the new lines l' and l'' from the reducible conic $C(\mu,\lambda)$, we get 4 other planes through l' and 4 other planes through l'' which of them contain a new pair of lines. Altogether we have $11+4\cdot 2+4\times 2=27$ lines.

It remains to show that there is no more line on $V(F)$. Assume that $L\subset V(F)$. Let π be a plan through L that contain L, L', L'' on $V(F)$. This plane π intersects the lines l, l', l'' at some points p, p', p'' respectively. We can assume that U is generic, so all points p, p', p'' are distint. Since neither L nor L' can pass through two of these points, it follows that one of these points lies in L. Hence L is coplanar with one of l, l', l''. It implies that L has been accounted for. This completes the proof of Theorem 11.1. □

Exercise 11.5. Prove that a 2-vector $e\in\Lambda^2(\mathbb{C}^4)$ is decomposable (i.e. e corresponds to a 2-plane) iff $e\wedge e=0$. Derive from here that $\dim Fr_2(\mathbb{C}^4)=4$. Give an alternative proof of Lemma 11.2.

12. Characterization of smoothness via local rings

Let C be an affine algebraic curve in $\mathbb{A}^2$ over a field K of characteristic zero given by zero locus of polynomial equation $F(x,y)=0$, $F\in K[x,y]$. Let $P\in C$ be a point and $\mathfrak{m}_P\subset\mathcal{O}(C)$ its maximal ideal in the ring of regular functions $\mathcal{O}(C)$. An important local characterization of smoothness of $P\in C$ is the following one:

Lemma 12.1. *Denoting $Frac(\mathcal{O}(C))$ the fraction field of $\mathcal{O}(C)$, let us consider the localization of $\mathcal{O}(C)$ along the maximal ideal $\mathfrak{m}_P\subset\mathcal{O}(C)$:*

$$\mathcal{O}(C)_{\mathfrak{m}_P}=\{f\in Frac(\mathcal{O}(C))\,|\,f=\frac{a}{b}\quad for\quad b\notin\mathfrak{m}_P\}. \tag{12.1}$$

Then $P=(p_1,p_2)$ is a smooth (non-singular) point (i.e., either $\frac{\partial F}{\partial x}(p_1,p_2)\neq 0$ or $\frac{\partial F}{\partial y}(p_1,p_2)\neq 0$) if and only if $\mathcal{O}(C)_{\mathfrak{m}_P}$ is a discrete valuation ring.

Proof: We note $b\notin\mathfrak{m}_P$ is equivalent to $b(P)\neq 0$, and apply a well known assertion in commutative algebra that localization commutes with quotients:

$$\big(K[x,y]/\langle F\rangle\big)_{(x-p_1,y-p_2)}\simeq\big(K[x,y]_{(x-p_1,y-p_2)}\big)/\langle F\rangle. \tag{12.2}$$

By composing with an automorphism of $\mathbb{A}^2$,

$$x \to x - p_1, \quad y \to y - p_2, \tag{12.3}$$

we may assume $P = (0,0)$. Without lost of generality we may suppose $\frac{\partial F}{\partial y}(0,0) \neq 0$, and set $R = \big(K[x,y]_{(x,y)}\big)/\langle F\rangle$. By (12.2), R is a local ring and hence has a unique maximal ideal. We claim that it is generated by $\bar{x}$, the residue class of x modulo $\langle F\rangle$ (this implies that the ideal is principal and as it follows from our proof, all other ideals are powers of this maximal ideal, hence R is a discrete valuation ring.)

All we have to prove is $y \in \langle x\rangle$, i.e., $y \in \langle x, F\rangle K[x,y]_{(x,y)}$. We write $F(x,y) = yF_0(x,y) + xF_1(x,y)$ for some (not unique) $F_0, F_1 \in K[x,y]$. Since $\frac{\partial F}{\partial y}(0,0) \neq 0$, we get

(12.4)
$$0 \neq \frac{\partial F}{\partial y}(0,0) = F_0(0,0) + (y\frac{\partial F_0}{\partial y})(0,0) + (x\frac{\partial F_1}{\partial y})(0,0) = F_0(0,0).$$

Consequently, $F_0(x,y)$ is invertible in the local ring $\mathcal{O}(C)_{\mathfrak{m}_{(0,0)}}$ and hence $F(x,y) = yF_0(x,y) + xF_1(x,y)$ implies

$$\langle x, F\rangle K[x,y]_{(x,y)} = \langle x, y\rangle K[x,y]_{(x,y)}. \tag{12.5}$$

The proof is complete.
□

In the case of singular point $P \in C$, a useful way in algebraic geometry which allows to analyze the local structure of singularity is the notion of local analytic neighborhood of P.

Let us fix the base field $K = \mathbb{C}$ and $P \in C$ to be $P = (0,0)$. The notion of analytic neighborhood of P is based on the ring of formal power series $\mathbb{C}[[x,y]]$. The following properties hold for $\mathbb{C}[[x,y]]$ (they are true in any finite number of variables, not only x, y):

(1) $\mathbb{C}[x,y]$ is a $\mathbb{C}$-subalgebra of $\mathbb{C}[[x,y]]$.
(2) Any formal power series with non-zero constant term admits multiplicative inverse and has N-th root for all $N \in \mathbb{N}$: $g \in \mathbb{C}[[x,y]]$ such that $g_{00} \neq 0$, $g(x,y) = \sum_{i,j\in\mathbb{N}_0} g_{ij}x^iy^j$, then $\frac{1}{g}$ and $g^{\frac{1}{N}}$ are in $\mathbb{C}[[x,y]]$.
(3) $\mathbb{C}[[x,y]]$ is a unique factorization domain (similarly to $\mathbb{C}[x,y]$ or the ring of analytic functions).
(4) A $\mathbb{C}$-linear homomorphism

$$\varphi : \mathbb{C}[[x,y]] \to \mathbb{C}[[x',y']] \tag{12.6}$$

is an isomorphism if and only if

$$(d\varphi)(0,0) = \begin{pmatrix} \frac{\partial}{\partial x}\varphi_{x'} & \frac{\partial}{\partial y}\varphi_{x'} \\ \frac{\partial}{\partial x}\varphi_{y'} & \frac{\partial}{\partial y}\varphi_{y'} \end{pmatrix} \tag{12.7}$$

is invertible.

We shall demonstrate all basic considerations in the case of two affine algebraic curves

$$C:\, F(x,y) = y^2 - x^2 - x^3, \quad \tilde{C}:\, \tilde{F}(\tilde{x},\tilde{y}) = \tilde{y}^2 - \tilde{x}^2. \tag{12.8}$$

We observe $\tilde{F}$ is reducible in $\mathbb{C}[x,y]$, while F is irreducible in $\mathbb{C}[x,y]$. However, F is reducible in $\mathbb{C}[[x,y]]$:

$$F(x,y) = (y - x\sqrt{x+1})(y + x\sqrt{x+1}) \tag{12.9}$$

with

$$\sqrt{x+1} = 1 + \sum_{n=1}^{\infty} \frac{(-1)\dots(1-2n)}{2^n} x^n \in \mathbb{C}[[x,y]]. \tag{12.10}$$

Moreover, we have an isomorphism of local rings

$$\begin{aligned} &\mathcal{O}(C)_{(0,0)} \to \mathcal{O}(\tilde{C})_{(0,0)}, \\ &\qquad (\bar{\tilde{y}}, \bar{\tilde{x}}) \mapsto (\bar{y}, \bar{x} + \sum_{n=1}^{\infty} \frac{(-1)\dots(1-2n)}{2^n} \bar{x}^{n+1}) \end{aligned} \tag{12.11}$$

over $\mathbb{C}[[x,y]]$. This means that the type of singular points of $C, \tilde{C}$ at $(0,0)$ is the same - the node singularity of the elliptic curve C locally analytically looks like the transversal intersection of two lines.

Definition 12.2. The two formal power series $g, h \in \mathbb{C}[[x,y]]$ are formally equivalent if there exists an automorphism $\varphi : \mathbb{C}[[x,y]] \to \mathbb{C}[[x,y]]$ such that $g \mapsto h = \varphi(g)$. We say that $h \in \mathbb{C}[[x,y]]$ with $h(0,0) = 0$ is singular if

$$g_{1,0} = \frac{\partial g}{\partial x}(0,0) = 0 = g_{0,1} = \frac{\partial g}{\partial y}(0,0). \tag{12.12}$$

Exercise 12.3. Prove that each non-singular formal power series is formally equivalent to $x \in \mathbb{C}[[x,y]]$.

Exercise 12.4. Prove that the two formal power series

$$C:\, F(x,y) = y^4 - x^4, \quad C':\, F'(x,y) = (y^2 - x^2)(y^2 - 2x^2) \tag{12.13}$$

are not formally equivalent in $\mathbb{C}[[x,y]]$.

One of the basic invariants of equivalence classes of formal power series is the Milnor invariant, encoding the geometry/topology of fibers in the deformation family $g(x,y) = t$, $t \in \mathbb{C}$.

13. Birational geometry and resolution of singularities

Motivation. We have seen in Lecture 11 that to study a particular object it is useful to to consider it as an element in a family. To study a family, or more general, a class of objects, it is an important problem of mathematics to classify objects up to an equivalence/isomorphism that characterize most important properties of objects we are interested in. In mathematics, birational geometry is a field of algebraic geometry the goal of which is to determine when two algebraic varieties are isomorphic outside lower dimensional subsets. This amounts to studying mappings that are given by rational functions rather than polynomials the map may fail to be defined where the rational functions have poles. The classification up to birational equivalence is very satisfactory in view of Hironaka's theorem, which states that over a field of characteristic 0 (such as the complex numbers), every variety is birational to a *smooth* projective variety. In other words we can resolute a singularity with help of a dominant rational map. Other consequence of Hironaka's theorem is the reduction of birational classification of algebraic varieties to the subset of smooth projective varieties. We shall consider important examples of resolution of singularity: a blow-up of a point and of a submanifold which can be extended to category of symplectic geometry.

13.1. **Rational maps.**

The notion of a rational map is an extension of the notion of a rational function. A rational map is a morphism which is only defined on some open subset of a variety.

Definition 13.1. Let X, Y be varieties. *A rational map* $\phi : X \to Y$ is an equivalence class of pairs $\langle U, \phi_U\rangle$ where U is a nonempty open subset of X, ϕ_U is a morphism of U to Y, and $\langle U, \phi_U\rangle$ is said to be equivalent to $\langle V, \phi_V\rangle$ if ϕ_U and ϕ_V agree on $U \cap V$.

The rational map ϕ is *dominant*, if for some pair $\langle U, \phi_U\rangle$ the image of ϕ_U is dense in Y.

Example 13.2. Let $Y = \{(z_1, z_2) \in \mathbb{C}^2 |\, z_1 z_2 = 1\}$. Define a map $\phi : Y \to \mathbb{C}$ by setting : $\phi(z_1, z_2) = z_1$. Then ϕ is a dominant rational map.

Exercise 13.3. Let X be an irreducible affine variety and $\langle U, \Phi_U\rangle$ a rational dominant map such that the image of ϕ_U is dense in Y. Show that the image of $\Phi_V : V \to Y$ is dense, if $\langle U, \Phi_U\rangle$ is equivalent to $\langle V, \Phi_V\rangle$.

Hint. Use that fact that $U \cap V$ is dense in X and hence $Y = f(\overline{U \cap V}^{U\cup V})$.

A *birational map* $\phi : X \to Y$ is a rational map which admits an inverse, i.e. there is a rational map $\psi : Y \to X$ such that $\psi \circ \phi = Id_X$ and $\phi \circ \psi = Id_Y$. If there is a birational map from X to Y, we say that X and Y are *birational equivalent*, or simply *birational*.

The equivalence notion of rational maps is very strong, since any open set is dense in Zariski topology.

Lemma 13.4. *Let X and Y be varieties and let ϕ and ψ be two morphisms from X to Y such that there is a nonempty open subset $U \subset X$ with $\phi_{|U} = \psi_{|U}$. Then $\phi = \psi$.*

Proof. Morphisms ϕ and ψ can be composed further with any morphism χ from Y to another variety Z leaving U unchanged. Therefore we can assume that $Z = \mathbb{C}P^n = Y$. We consider the map

$$(\phi \times \psi) : X \to \mathbb{C}P^n \times \mathbb{C}P^n.$$

Using the Serge embedding (Exercise 6.15) we can provide $\mathbb{C}P^n \times \mathbb{C}P^n$ with a structure of a projective variety. Denote by $\triangle$ the diagonal in $\mathbb{C}P^n \times \mathbb{C}P^n$. Then $\triangle$ is a closed subset of $\mathbb{C}P^n \times \mathbb{C}P^n$. By assumption we have $(\phi \times \psi)(U) \subset \triangle$. But any open set U is dense, hence $(\phi \times \psi)(X) \subset \triangle$. □

Denote by $Mor_d(X, Y)$ the subset of dominant rational maps from X to Y.

Theorem 13.5. *For any variety X and Y there is a bijection B between sets*

$$Mor_d(X, Y) \cong Hom(K(Y), K(X)),$$

where $K(X), K(Y)$ are regarded as $\mathbb{C}$-algebras.

Proof. Let us make a point why dominant rational map appear in Theorem 13.5. Note that a rational map $\phi \in Mor(X, Y)$, represented by $\langle U, \phi_U \rangle$, defines a homomorphism $\phi^* : K(Y) \to K(X)$ iff the pull back of a rational function $\langle V, f \rangle$ is defined an *open* domain $\phi_U^{-1}(V)$. The later holds if $\phi_U(U)$ is dense in Y. The other assertion of Theorem 13.5 will be proved by reducing it to the case where Y is an affine variety.

Let $\phi \in Mor_d(X, Y)$ be a dominant rational map represented by $\langle U, \phi_U \rangle$. Let $f \in K(Y)$ be a rational function, represented by $\langle V, f \rangle$, where V is an open set in Y and f is a regular function on V. We define B by

$$B(\phi)\langle V, f \rangle := \langle \phi^{-1}(V), \phi^*(f) \rangle.$$

Clearly $B(\phi)$ is a homomorphism from $K(Y)$ to $K(X)$, since a composition of rational functions is a rational function.

Now we shall construct an inverse B^{-1}. Let $\theta : K(Y) \to K(X)$ be a homomorphism of $\mathbb{C}$-algebras. We shall reduce the construction $B^{-1}\theta$ in $Mor_d(X, Y)$ to the case that Y is an affine variety and then use Proposition 8.11 where such case has been treated.

To define an element ϕ in $Mor_d(X, Y)$ it suffices to define a dominant rational map ϕ from X onto an open set U_Y of Y. By Exercise 8.13 (ii) Y can be covered by affine varieties, so we shall choose U_Y being one of them. We have $A(U_Y) \subset K(Y)$ so we shall use the restriction of θ to $A(U_Y)$ to construct $B^{-1}(\theta) \in Mor_d(X_Y)$ and prove that it is a dominant rational map.

Let $y_1, \cdots, y_k$ be generators of $A(U_Y)$. Then $\theta(y_i)$ are rational functions on X. Let U_X be an open set in X where all $\theta(y_i)$ are regular functions on U_X. This implies that θ defines a homomorphism from $A(U_Y)$ to $\mathcal{O}(U_X)$ whose kernel is empty since θ is a homomorphism of the quotient field. Since U_Y is an affine variety, Proposition 8.11 yields that θ gives rise to an element $\tilde{B}(\theta) \in Mor(U_X, U_Y)$. Since θ is injective on $A(U_Y)$ the image $\tilde{B}(U_X)$ cannot be contained in an algebraic set in U_Y, hence $\tilde{B}(\theta)$ is a dominant rational map from X to Y. The proof of Proposition 8.11 yields that $\tilde{B}$ is inverse of B restricted to $A(U_Y)$, and hence $\tilde{B} = B^{-1}$. □

Corollary 13.6. *Two varieties X and Y are birationally equivalent, if and only if $K(X)$ is isomorphic to $K(Y)$ as $\mathbb{C}$-algebras.*

Proof. Suppose that X and Y are birational equivalent, i.e. there are rational map $\phi : X \supset U \to Y$ and $\psi : Y \supset V \to X$ which are inverse to each other. We shall find two open dense sets $U_1 \subset X$ and $V_1 \subset Y$ such that U_1 isomorphic to U_1. Then $\psi \circ \phi$ is represented by $\langle \phi^{-1}(V), \psi \circ \phi \rangle$. By assumption the composition $\phi \circ \psi$ is the identity on $\psi^{-1}(U)$. Now let $U_1 = \phi^{-1}(\psi^{-1}(U))$ and $V_1 = \psi^{-1}(\phi^{-1}((V))$. It is easy to see that U_1 and V_1 isomorphic via ϕ and ψ. Hence $K(X) = K(U_1) = K(V_1) = K(Y)$.

The second statement follows from Theorem 13.5 directly. □

Exercise 13.7. Prove that the quadratic surface $Q : xy = zw$ in $\mathbb{C}P^3$ is birational to $\mathbb{C}P^2$ but not isomorphic to $\mathbb{C}P^2$.

Hint. Show that Q is isomorphic to the Serge embedding of $\mathbb{C}P^1 \times \mathbb{C}P^1$ into $\mathbb{C}P^3$ (see Exercise 6.15) so it is birational equivalent to $\mathbb{C}P^2$ (cf. Remark 13.8 below).

Remark 13.8. We should mention here a well known fact that every irreducible variety X is birational to a hypersurface in $\mathbb{C}P^n$ (see e.g.

[Hartshorne1997, Proposition 4.9, p. 27]). To prove this fact one relies on the statement that if X is a projective variety in $\mathbb{C}P^n$, a general projection $\pi_p : X \to \mathbb{C}P^{n-1}$ gives a birational isomorphism from X to its image $\bar{X}$, if X is not hypersurface. In this case a general line meeting X meets it only in one point, or in other words, there exists an open set of X where the projection to its image in $\mathbb{C}P^k$ is 1-1. (This is a slightly different from the proof of geometric Noether's theorem 7.13, where we have a finite map from X to $\mathbb{C}P^k$). We can also use the algebraic Noether normalization theorem to prove the mentioned above fact. It suffices to prove for irreducible affine variety X. In this case the Noether normalization theorem says that $A(X)$ is integral extension of $\mathbb{C}[x_1, \cdots, x_k]$. Since $K(X) = F(A(X))$ there is is a transcendence base $x_1, \cdots, x_k$ for the function field of $K(X)$, and $K(X)$ is generated over $k(x_1, \cdots, x_k)$ by a single element x_{k+1} satisfying an irreducible polynomial relation

$$F(x_{k+1}) = a_d(x_1, \cdots x_k) \cdot x_{k+1}^d + \cdots + a_0(x_1, \cdots, x_k)$$

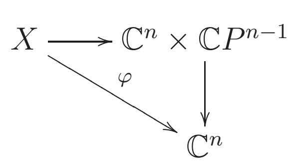
with coefficients $a_i \in K(x_1, \cdots, x_k)$. Clearing denominators we may take F to be an irreducible polynomial in $(k+1)$ variables. So by Corollary 13.6 X is birational to the hypersurface in $\mathbb{C}^{n+1}$ given by this polynomial.

13.2. **Blow up of a point.** In this subsection we study a particular example of a dominant rational map - a blow up of a point of $\mathbb{C}^n$ at the origin 0, which is the main tool in the resolution of singularities of an algebraic variety. Let x_i, $i = \overline{1, n}$ be coordinates on $\mathbb{C}^n$. The blow-up of $\mathbb{C}^n$ at 0, denoted by X, is an *algebraic set* $X \subset \mathbb{C}^n \times \mathbb{C}P^{n-1}$ that is defined by the following equation

$$x_i y_j = x_j y_i \text{ for all } i, j = \overline{1, n}$$

where y_i are homogeneous coordinates of $\mathbb{C}P^{n-1}$. Geometrically speaking, coordinate (y_i) is the coordinate of the line through points 0 and x on $\mathbb{C}^n$ regarded as an element in $\mathbb{C}P^n$.

Now we consider the following commutative diagram



where φ is obtained by restricting the projection $\mathbb{C}^n \times \mathbb{C}P^{n-1} \to \mathbb{C}^n$ to X.

- The projection $pr : X \times \mathbb{C}P^n$ is a universal line bundle over $\mathbb{C}P^{n-1}$.

• For $P \neq 0 \in \mathbb{C}^n$ we have $\#(\varphi^{-1}(P)) = 1$. To see this we assume that $x_1(P) \neq 0$. Let $\tilde{P} \in \varphi^{-1}(P)$. Then $y_j(\tilde{P}) = y_1(\tilde{P}) \cdot (x_j(P)/x_1(P))$, which defines $\tilde{P}$ uniquely. Geometrically, it is obvious, since if $X \neq 0$ there is only a unique point $y \in \mathbb{C}P^n$ defined by the line through 0 and x.

• It is easy to see that $\varphi^{-1}(0) = \mathbb{C}P^{n-1}$.

• We claim that X is irreducible. We consider the projection $q : X \to \mathbb{C}P^{n-1}$. The preimage $q^{-1}([t_1 : \cdots t_n])$ is a linear subspace in $\mathbb{C}^n$ defined by

$$x_i t_j = x_j t_i \text{ for all } i, j = \overline{1, n}.$$

By Proposition 11.3 X is irreducible.

Definition 13.9. Assume that Y is a closed subvariety of $\mathbb{C}^n$ passing through 0. We define *the blowing-up of Y at the point* 0 to be the closure $\tilde{Y}$ of $\varphi^{-1}(Y \setminus \{0\})$.

Example 13.10. ([Hartshorne1997, Example 4.9.1, p. 29]) Let Y be the plane cubic curve $y^2 = x^2(x+1)$ in $\mathbb{C}^2$. Let (t, u) be coordinates of $\mathbb{C}P^1$. Then the blow-up of $\mathbb{C}^2$ at 0 is (cf. Exercise 13.7).

$$X = \{xu = ty\} \subset \mathbb{C}^2 \times \mathbb{C}P^1.$$

The set $E := \varphi^{-1}(0) = \mathbb{C}P^1$ is called *the exceptional curve.* The equation of $\tilde{Y}$ in coordinates with $t \neq 0$ (and hence $t = 1$) is

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

$$y = xu.$$

Substituting we get $x^2u^2 - x^2(x+1) = 0$. Thus we have two irreducible components. The one consists of $E = \{x = 0 = y, u \in \mathbb{C}\}$. The second one is $\tilde{Y} = \{u^2 = x+1,\ y = xu\}$. Note that $\tilde{Y}$ meets E at $u = \pm 1$.

We also blow-up a variety at a subvariety in the same way, see [Harris1992, Example 7.18, p. 82].

14. Degree and Bezout's theorem

In this section we shall study an important invariant of a projective variety - its degree, which has both algebraic and topological interpretation (Theorem 14.2). We prove Bezout's theorem which is an important tool for computing the degree of a projective variety (Theorem 14.6).

14.1. **Degree of a projective variety.** If an irreducible projective variety $X \subset \mathbb{C}P^n$ is a hypersurface, then its vanishing ideal is defined uniquely by a homogeneous polynomial f_X. The degree of f_X is called *the degree of* X.

Definition 14.1. Let X be an irreducible projective variety. *The degree of* X is defined to be the degree of of hypersurface that is birational equivalent to X.

We denote the degree of X by $deg(X)$. The following theorem asserts that the degree of a variety is well-defined, i.e. any hypersurface that is birational equivalent to X has the same degree. Equivalently we can define the degree in an invariant manner.

Theorem 14.2. *Let X be an irreducible k-dimensional projective variety in $\mathbb{C}P^n$. Let Ω be a general $(n-k)$-plane in $\mathbb{C}P^n$. Then Ω intersects at X at $deg(X)$ points.*

Proof. If X is a hypersurface i.e. $k = n-1$, the assertion of Theorem 14.2 follows from the fundamental theorem of algebra that every polynomial of degree d has d roots. Geometrically, d is the number of points in the fiber $\pi^{-1}(y)$ of the projection $\pi : X \to \mathbb{C}P^{n-1}$.

Now assume that $k \le n-2$. Denote by π_Λ the projection from X^k to $\mathbb{C}P^k$ which is obtained by iteration of the projection $X^k \to \mathbb{C}P^{n-1}$. Its is not hard to see that the fiber of this projection is the intersection $\Omega \cap X^k$. As we have noted, the projection of X^k to $\mathbb{C}P^{n-1}$ is 1-1 on its image, if $k < n-1$. Hence the pre-image $\pi_\Lambda^{-1}(y)$ for $y \in \mathbb{C}P^k$ contains the same number of points as the pre-image of the projection of the hypersurface $\bar{X}^k$ in $\mathbb{C}P^{k+1}$ that is obtained from the iteration projection. The later one is equal to the degree of X^k as we just proved above. This completes the proof of Theorem 14.2. □

The degree of a projective variety can be encoded in its Hilbert polynomial. *A Hilbert polynomial of an projective variety* X is defined as follows. Let $S(X) := \mathbb{C}[z_0, \cdots, z_n]/I(X)$ be the homogeneous coordinate ring of X. Then we define *the Hilbert function of* X as follows

$$h_X : \mathbb{N} \to \mathbb{N}$$
$$h_X(m) = \dim(S(X)_m).$$

Exercise 14.3. There is a unique polynomial p_X such that for *all* sufficiently large m we have $h_X(m) = p_X(m)$. Moreover $deg(p_X) = \dim X$.

Hint. The uniqueness of p_X follows from the fact that a polynomial of degree d has at most d (finite) roots. To prove the existence of p_X

we use induction argument on the dimension of X by considering the intersection $\bar{X} := X \cap \mathbb{C}P^{n-1}$, where $\mathbb{C}P^n$ intersects X transversally. Then $\dim \bar{X} = \dim X - 1$. Since $I(\bar{X}) = \langle I(X), L\rangle$, where L is the linear function defining $\mathbb{C}P^{n-1}$ we have

$$h_{\bar{X}}(m) = h_X(m) - h_X(m-1).$$

By induction $h_{\bar{X}}(m)$ is a polynomial $p_{\bar{X}}(m)$ of degree $\dim \bar{X}$. (The induction statement for X being set of d points says that $h_X(m) = d$ for $m \geq d$, see Lemma 14.5 below). Hence $h_X(m)$ is the sum polynomials of degree $\dim \bar{X}$. Now using a known Faulhaber's formula that expresses the sum $\sum_{k=1}^n k^p$ as a polynomial of degree $(p+1)$ in n we prove the existence of p_X.

Proposition 14.4. *Assume that* $\dim X = k$. *Then the degree of* X *is equal to* $k!LC(p_X)$.

Proof. Denote by Ω the general $(n-k)$-plane in $\mathbb{C}P^n$ that intersects X transversally.

Lemma 14.5. *We have* $p_{X\cap\Omega}(m) = deg(X)$.

Proof. By Theorem 14.2 $\#(X\cap\Omega) = deg(X)$. Recall that $S_k[x_0, \cdots, x_n]$ denotes the subspace of homogeneous polynomials of degree k in $\mathbb{C}[x_0, \cdots, x_n]$. To prove Lemma 14.5 it suffices to show that the evaluation mapping $ev : S_k[x_0, \cdots, x_n] \times (X \cap \Omega) \to \mathbb{C}^d$ is surjective (and therefore its fiber at 0 - the vanishing ideal $I(X \cap \Omega)$ is of codimension d) if k is sufficiently large. This follows from the known interpolation formula due to Lagrange: given d points there exists a polynomial of degree $d-1$ that vanishes at the given d point. Multiplying the interpolating polynomial of degree d with an arbitrary non-vanishing polynomial of degree $k-d$ we obtain Lemma 14.5 □

Now let us complete the proof of Proposition 14.4. By induction, using Lemma 14.5 it is easy to see that the leading term of $p_X(m)$ is $d \cdot m^k/k!$ which proves Proposition 14.4. □

14.2. **Bezout's theorem.** To compute degree of a projective variety we use the Bezout theorem. We say that X has pure dimension k if each irreducible component of X has dimension d. Furthermore, we say that two projective varieties X, Y of $\mathbb{C}P^n$ intersect *generically transversely*, if each irreducible components X_i, Y_j intersect at smooth point p_{ij} such that $T_{p_{ij}}X_i \oplus T_{p_{ij}}Y_j = T_{p_{ij}}\mathbb{C}P^n$.

Theorem 14.6. *Let* X *and* Y *are projective subvarieties of pure dimensions* k *and* l *respectively of a projective space* $\mathbb{C}P^n$. *Suppose that*

X and Y intersect generically transversely. Then

$$deg(X \cap Y) = deg(X) \cdot deg(Y).$$

Proof. First we note that Theorem 14.6 holds for Y being a generic hyperplane by Theorem 14.2. Using this observation we shall reduce the proof of Theorem 14.6 to the case that X, Y intersect generically transversely by intersecting X, Y with a plan of dimension $n - k - l$.

Next we embed X and Y into $\mathbb{C}P^{2n+1}$ by

$$i(X) = [X, 0] \subset \mathbb{C}P^{2n+1},$$
$$j(Y) = [0, Y] \subset \mathbb{C}P^{2n+1}.$$

Now we set

$$J(i(X), j(Y)) := \cup_{x \in i(X), y \in j(Y)} \overline{x, y},$$

where $\overline{x, y}$ denotes the line joining x and y.

Lemma 14.7. $\dim J(i(X), j(Y)) = \dim X + \dim Y + 1$.

Proof. Since $i(X)$ and $j(Y)$ lie on non-intersecting linear subspaces every point in $J(i(X), j(Y))$ lies in a unique line $\overline{i(x), j(y)}$. hence follows Lemma 14.7. □

Now let us consider the linear subspace $L \subset \mathbb{C}P^{2n+1}$ defined by the following linear equation

$$z_i - z_{n+i} = 0 \text{ for } i \in [0, n].$$

Note that

$$\#(L \cap J(i(X), j(Y))) = \#(X \cap Y). \tag{14.1}$$

By Theorem 14.2 we have

$$\#(L \cap J(i(X), j(Y))) = deg(J(i(X), j(Y)). \tag{14.2}$$

To complete the proof of Theorem 14.6 we shall show

Lemma 14.8.

$$deg(J(i(X), j(Y)) = deg(X) \cdot deg(Y).$$

Proof. To prove Lemma 14.8, using Proposition 14.4 we compute the leading coefficient of the Hilbert polynomial of $J(i(X), j(Y))$. Since $i(X)$ and $j(Y)$ lie in disjoint linear subspaces we have

$$S(J(i(X), j(Y)) = S(X) \otimes S(Y).$$

Hence

$$S(J(i(X), j(Y))_m = \oplus(S(X)_j \otimes S(Y)_{m-j}).$$

So

$$h_{J(i(X),j(Y))}(m) = \sum h_x(j) \cdot h_Y(m - j)$$

$$= \sum_{j=0}^{m}(deg(X)\cdot\binom{j+k}{k}+O(j^{k-1})\cdot(deg(Y)\binom{m-j+l}{l}+O((m-j)^{l-1}))$$

(since $j^k/k! = (j+k)!/(j!k!) + O(j^{k-1})$)

$$= deg(X)\cdot deg(Y)\cdot \sum_{j=0}^{m}\binom{j+k}{k}\cdot\binom{m-j+l}{l} + O(m^{k+l}$$

$$= deg(X)deg(Y)\cdot\binom{m+k+l+1}{k+l+1} + O(m^{k+l})$$

$$= \frac{deg(X)\cdot deg(Y)}{(k+l+1)!}m^{k+l+1} + O(m^{k+l}.$$

The last identity yields Lemma 14.8 by Proposition 14.4. □

As we note Lemma 14.8 completes the proof of Theorem 14.6. □

15. Bezout's theorem and resultants

The common solution space of finite number of polynomial equations geometrically corresponds to the intersection of algebraic varieties in affine or projective spaces. A few phenomena are captured in the following examples ($\mathbb{R}$ and $\mathbb{C}$ denote the field of real and complex numbers, respectively.)

Example 15.1. In $\mathbb{A}^2(\mathbb{R})$, we consider two lines $ax + by + c = 0$, $dx + ey + f = 0$ as elements of $\mathbb{R}[x, y]$, $a, b, c, d \in \mathbb{R}$. Their intersection is either line, or point or the empty set.

In the projective space $\mathbb{P}^2(\mathbb{R})$, parallel lines always intersect: two lines $ax+by+cz = 0$ and $ax+by+fz = 0$, $c \neq f$, (regarded as elements in the ring of homogeneous polynomials in $\mathbb{R}[x, y, z]$) intersect in the point at infinity $[b, -a, 0]$.

Example 15.2. In $\mathbb{A}^2(\mathbb{R})$, the intersection of the line $x + y = 0$ and conic $x^2 + y^2 - 2 = 0$ is given by two points, while the intersection of the line $x + y - 4 = 0$ and conic $x^2 + y^2 - 2 = 0$ is empty (although the intersection in $\mathbb{A}^2(\mathbb{C})$ consists of two points.)

The notion of resultant leads to the proof of the (weak form of) Bezout's theorem.

Definition 15.3. Let k be a field, $P(x) = a_0 + a_1x + \ldots + a_nx^n$ and $Q(x) = b_0 + a_1x + \ldots + b_mx^m$ with $a_nb_m \neq 0$ elements of $k[x]$. The resultant of P, Q, $R(P,Q)$, is an element of k given by the determinant of $(m+n)\times(m+n)$ matrix

$$(15.1)\quad R(P,Q) := \det\begin{pmatrix} a_0 & a_1 & \dots & a_n & 0 & \dots & 0 & 0\\ 0 & a_0 & \dots & a_{n-1} & a_n & 0 & \dots & 0\\ & & \dots & & & & \dots & \\ 0 & \dots & 0 & 0 & a_0 & a_1 & \dots & a_n\\ b_0 & b_1 & \dots & b_m & 0 & \dots & 0 & 0\\ 0 & b_0 & \dots & b_{m-1} & b_m & 0 & \dots & 0\\ & & \dots & & & & \dots & \\ 0 & \dots & 0 & 0 & b_0 & b_1 & \dots & b_m \end{pmatrix}$$

Analogously, $R(P,Q)$ is defined as an element of $k[y,z]$ for two polynomials $P(x,y,z) = a_0(y,z)+a_1(y,z)x+\ldots+a_n(y,z)x^n$ and $Q(x,y,z) = b_0(y,z) + a_1(y,z)x + \ldots + b_m(y,z)x^m$ with $P(1,0,0)Q(1,0,0) \neq 0$ in $k[x,y,z] \simeq (k[y,z])[x]$.

Proposition 15.4. (1) *For $P(x), Q(x) \in k[x]$, we have $R(P,Q) = 0$ if and only if P and Q have a (non-constant) common factor in $k[x]$.*
(2) *For $P(x,y,z), Q(x,y,z) \in k[x,y,z]$ with $P(1,0,0)Q(1,0,0) \neq 0$, we have $R(P,Q) = 0$ if and only if P and Q have a (non-constant) common homogeneous factor in $k[x,y,z]$.*

Proof. We prove the claim for $k[x]$, the second assertion is analogous. As for the first implication, suppose $P(x) = R(x)\varphi(x)$ and $Q(x) = R(x)\psi(x)$ with $R(x) \in k[x]$ of positive degree. Assume $\varphi(x) = c_0 + \ldots + c_{m-1}x^{m-1}$ and $\psi(x) = d_0 + \ldots + d_{n-1}x^{n-1}$ have no common factor; c_{m-1} or d_{n-1} can be zero, but $\varphi(x), \psi(x)$ are not identically zero. Comparing the coefficients of monomials in x in the expansion of $P(x)\psi(x) = Q(x)\varphi(x)$ corresponds to the triviality of a non-trivial linear combination of the rows in $R(P,Q)$:

$$(15.2)\quad \sum_{j=1}^{m} d_{j-1}(j\text{-th row}) + \sum_{i=1}^{n} c_{i-1}((i+m)\text{-th row}) = 0,$$

which implies $R(P,Q) = 0$.

The opposite implication is also clear: suppose $R(P,Q) = 0$. The linear dependence of the rows in the matrix computing the resultant implies the existence of polynomials $\varphi(x), \psi(x)$ in $k[x]$ such that $P\psi = Q\varphi$, $deg(\varphi) \leq n-1$ and $deg(\psi) \leq m-1$. Therefore, P and Q have a common (non-constant) factor in $k[x]$ (recall that $k[x]$ is the unique factorization domain.) □

An elementary consequence of Theorem [?] is that when $P(x,y,z)$ and $Q(x,y,z)$ are homogeneous polynomials of degree n and m, respectively, $R(P,Q)$ is homogeneous of degree mn.

Proposition 15.5. *Suppose k is the splitting field for $P(x), Q(x) \in k[x]$, i.e., $P(x) = \prod_{i=1}^{n}(x-\lambda_i)$ and $Q(x) = \prod_{j=1}^{m}(x-\mu_j)$. Then*

$$R(P,Q) = \prod_{i,j}(\mu_j - \lambda_i) = \prod_j P(\mu_i) = (-1)^{mn}\prod_i Q(\lambda_i). \tag{15.3}$$

Proof. We have $P(x) \in k[x,\lambda_1,\dots,\lambda_n]$ and $Q(x) \in k[x,\mu_1,\dots,\mu_m]$, so that $R(P,Q) \in k[x,\lambda,\dots,\lambda_n,\mu_1,\dots,\mu_m]$ is of degree mn. By Proposition [?], $R(P,Q) = 0$ if and only if $\lambda_i = \mu_j$ for some i,j. Therefore, $\prod_{i,j}(\mu_j - \lambda_i)$ divides $R(P,Q)$ in $k[x,\lambda,\dots,\lambda_n,\mu_1,\dots,\mu_m]$, hence by degree of $R(P,Q)$ we have $R(P,Q) = C\prod_{i,j}(\mu_j - \lambda_i)$ for some $C \in k$. Taking $Q(x) = x^m$ and P as above, we get

$$C\prod_{i,j}(\mu_j - \lambda_i)|_{\mu_j=0 \text{ for all } j} = R(P,Q) \tag{15.4}$$

$$= \begin{pmatrix} a_0 & a_1 & \dots & a_n & 0 & \dots & 0 & 0 \\ 0 & a_0 & \dots & a_{n-1} & a_n & 0 & \dots & 0 \\ & & \dots & & & & \dots & \\ 0 & \dots & 0 & 0 & a_0 & a_1 & \dots & a_n \\ 0 & & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & & \dots & & 0 & 1 & \dots & 0 \\ & & \dots & & & & \dots & \\ 0 & \dots & & 0 & \dots & 0 & \dots & 1 \end{pmatrix} \tag{15.5}$$

$$= a_0^m = \prod_i (-\lambda_i)^m, \tag{15.6}$$

which implies $C = 1$. The rest is elementary, hence the proof is complete. □

An easy consequence of the previous theorem is that for all $P, Q, S \in k[x]$ split over k, we have $R(P,QS) = R(P,Q)R(P,S)$.

Theorem 15.6. *(weak Bezout's theorem) Let k be algebraically closed, $C, D \subset \mathbb{P}^2(k)$ projective curves defined by homogeneous polynomials $P(x,y,z)$ and $Q(x,y,z)$. Suppose P and Q of degree m and n, respectively, have no common component. Then they have at most mn points of intersection.*

Proof. Suppose the claim is not true. We denote by M the set of $mn+1$ distinct points of the intersection $C \cap D$. We choose the coordinate system such that $[1,0,0]$ does not belong to $C \cap D$ and at the same time does not lie on any line passing through couple of distinct points in M. For any $[a,b,c] \in M$, we have $P(a,b,c) = 0 = Q(a,b,c)$. The resultant of $P(x) := P(x,b,c)$ and $Q(x) := Q(x,b,c)$ is zero, because $P(x)$ and $Q(x)$ have common root (namely, $x = a$). Therefore, $bz - cy$ divides the resultant $R(P,Q)$ regarded as a polynomial in y, z. If $[a', b', c']$ is another (intersection) point in M, then $b'z - c'y$ is not a constant multiple of $bz - cy$ (if so, $[1,0,0], [a,b,c]$ and $[a',b',c']$ are collinear, a contradiction.) So $mn+1$ are distinct linear factors dividing $R(P,Q)$. On the other hand, $R(P,Q)$ is of degree mn and over the algebraically closed field k splits into the product of mn linear factors of the form $b_i z - c_i y$ $(i = 1, \ldots, mn)$. This is the required contradiction and hence the assumption of the proof does not apply. □

The weak Bezout's theorem can be improved by introducing intersection multiplicity $I_p(C,D)$ for $p \in \mathbb{P}^2(k)$. We write $I_p(P,Q)$ for $I_p(C,D)$ and define $I_p(C,D)$ recursively:

(1) $I_p(P,Q) = I_p(Q,P)$,
(2) $I_p(P,Q)$ is equal to ∞ if p is in a common component of C and D, $I_p(P,Q)$ is in $\mathbb{N}_+$ if p is not in a common component of C and D and $p \in C \cap D$, and $I_p(P,Q)$ is equal to zero if $p \notin C \cap D$,
(3) If C, D are lines (i.e., $deg(P) = deg(Q) = 1$) and $\{p\} = C \cap D$, then $I_p(P,Q) = 1$,
(4) I_p is multiplicative: $I_p(P_1 P_2, Q) = I_p(P_1, Q) + I_p(P_2, Q)$,
(5) $I_p(P,Q) = I_p(P, Q + PS)$ if $deg(S) = deg(Q) - deg(P)$.

There exists the unique multiplicity function $I_p(C,D)$, satisfying and characterized by five points above. The following theorem is left without proof.

Theorem 15.7. *(Bezout's theorem) Suppose two projective curves $C, D \subset \mathbb{P}^2(k)$ of degree m and n, respectively, have no common component. Then there are precisely mn points of intersection counting multiplicities, i.e.,*

$$\sum_{p \in C \cap D} I_p(C,D) = mn. \tag{15.7}$$

16. Riemann-Roch theorem

The Riemann-Roch theorem is an important theorem in mathematics, specifically in complex analysis and algebraic geometry, for the computation of the dimension of the space of meromorphic (rational) functions with prescribed zeroes and allowed poles. It relates the complex analysis of a connected compact Riemann surface with the surface's purely topological genus g, in a way that can be carried over into purely algebraic settings.

Initially proved as Riemann's inequality by Riemann (1857), the theorem reached its definitive form for Riemann surfaces after work of Riemann's short-lived student Gustav Roch (1865). It was later generalized to algebraic curves, to higher-dimensional varieties and beyond.

16.1. **Divisors and meromorphic functions.** We consider a meromorphic function on a Riemannian surface S as a holomorphic function $\bar{f}$ from S to a Riemannian sphere S^1. The zero point of f is the preimage of $0 \in \mathbb{C}P^1$ and the pole of f is the preimage of $\infty \in \mathbb{C}P^1$. In order to understand the zero and poles of a meromorphic function we introduce the notion of divisor.

Definition 16.1. A divisor is an element of a free abelian group generated by the points p_i of a Riemannian surface. A *degree* of a divisor $D = \sum_i n_i p_i$ is the sum $deg(D) := \sum n_i$. We say $D \geq 0$ if all the coefficients n_i of $D = \sum n_i p_i$ are non-negative. We say $D_1 \geq D_2$ if $D_1 - D_2 \geq 0$.

For a meromorphic function f on a Riemannian surface S we define a divisor (f) as follows. For a point $p \in S$ we define

$$ord_p(f) := k \text{ if } f \text{ has a zero of multiplicity } k \text{ at } p,$$

$$ord_p(f) := -k \text{ if } f \text{ has a pole of multiplicity } k \text{ at } p,$$

$$(f) := \sum_{p \in S} ord_p(f) \cdot p.$$

Lemma 16.2. *$Deg((f)) = 0$.*

Proof. Any holomorphic function $f : S \to \mathbb{C}$ corresponds to a holomorphic map $\bar{f} : S \to \mathbb{C}P^1$. Clearly we have

$$Deg((f)) = deg_0(\bar{f}) - deg_\infty(\bar{f}),$$

where $deg\bar{f}$ is the degree of the covering map $\bar{f}$. Since the degree is the constant number, we obtain Lemma 16.2 immediately. □

Example 16.3. *A meromorphic 1-form* ω on a Riemann surface is a section of the complex cotangent bundle T^*S which can be written locally written as $f(z)dz$ where $f(z)$ is a meromorphic function. For example, if f is a meromorphic function then df is a meromorphic 1-form. Then we assign *the canonical divisor* (ω) *of* ω as follows

$$(\omega) := \sum_{p\in S} ord_p(f_\omega)\cdot p \text{ where } f_\omega dz \text{ is a local representation of } \omega\ .$$

This definition does not depend on the choice of local coordinates z n a neighborhood of p since transition functions are holomorphic.

Exercise 16.4. Let f, g be meromorphic functions. Then

$$(f\cdot g) = (f) + (g)\,\&(f/g) = (f) - (g).$$

All canonical divisors have the same degree.

Hint. The first assertion is trivial. The second assertion follows from the first assertion and Lemma 16.2 taking into account the fact that a meromorphic 1-form van be obtained from any meromorphic 1-form by multiplying with a meromorphic function.

Lemma 16.5. *The degree of a canonical divisor* ω *on a compact Riemannian surface is equal* $-\chi$*, where* χ *is the Euler characteristic of the Riemann surface.*

Proof. It suffices to prove Lemma 16.5 for the 1-form df, where f is some non-constant meromorphic 1-form on S whose pole and zero are related with the genus of S via the Riemann-Hurwitz formula. We consider f as a holomorphic map $\bar{f} : S \to \mathbb{C}P^1$. Using the change of coordinate if necessary, we assume that there are no ramification points among preimages of f at $-\infty$ i.e. all poles are simple and at the other zero f has ramification index $e_1, \cdots e_m$. (The ramification index of a holomorphic map $f : S_1 \to S_2$ at $z_1 \in S_1$ is the winding number of f at z_1 and equal k, where locally $f = h(z - z_1)^k$, $h \neq 0$.) Let degree of $\bar{f}$ be equal n. Then at each of them the 1-form df has order 2 and m zero of order $e_1 - 1, \cdots, e_m - 1$. Summing up we have

$$deg(df) = \sum_{i=1}^{m}(e_i - 1) - 2n. \tag{16.1}$$

By The Riemann-Hruwitz formula the RHS of (16.1) is $-\chi = 2g - 2$. This completes the proof of Lemma 16.5. □

Digression. Riemann-Hurwitz formula. Let $f : X \to Y$ be a non-constant holomorphic map of one compact Riemannian surface into another. Let $deg(f) = n$, the genus of X equal $g(X)$, the genus of Y equal $g(Y)$ and f ramified at m points with ramification index

$e_1, \cdots, e_m$. Then

$$2 - g(X) = n(2 - 2g(Y)) - \sum_{i=1}^{m}(e_i - 1).$$

16.2. **Riemann-Roch theorem.**

Definition 16.6. For a given divisor D we set

$$l(D) : \dim_{\mathbb{C}}\{ \text{ meromorphic functions } f |\, (f) + D \geq 0\},$$
$$i(D) := \dim_{\mathbb{C}}\{ \text{ meromorphic 1-form } \omega |\, (\omega) - D \geq 0\}.$$

Theorem 16.7 (Riemann-Roch Theorem)**.** *If D is a divisor on a compact Riemannian surface of genus g then $l(D) - i(D) - deg(D) + 1 - g$.*

Proof. We break the proof of Theorem 16.7 into three Lemmas.

Lemma 16.8. *Theorem 16.7 holds if $D \geq 0$.*

Proof. If $D \geq 0$ then

$$D = \sum_{i=1}^{m} m_i p_i \text{ where } m_i > 0.$$

Set

$$V(D) := \{(f_1, \cdots, f_n) \in [\mathcal{M}(\mathbb{C})]^n | f_i = \frac{c_{m_i}}{z^{m_i}} + \cdots + \frac{c_1}{z},\ c_k \in \mathbb{C}\}.$$

It is not hard to see that $\dim V(D) = deg(D)$.

Now let $\Phi : L(D) \to V(D)$ be the map that sends a meromorphic function $f \in L(D)$ to its principal part of f (the portion of the Laurent series of f) at p_i.

The kernel of Φ consists of meromorphic functions with no pole. Hence thery are holomorphic funcions and

$$\dim \ker \Phi = 1.$$

Clearly

$$l(D) = \dim \ker \Phi + \dim \mathrm{Im}\Phi = 1 + \dim \mathrm{Im}\Phi. \tag{16.2}$$

Now let us compute the dimension of $\mathrm{Im}\Phi$. To find out elements in $\mathrm{Im}\Phi$ we use the following

Proposition 16.9 (Reverse Residue Theorem)**.** *If we have a set of points $\{a_1, \cdots, a_n\}$ on a compact Riemann surface S and also a set of principal parts $\{f_1, \cdots, f_n\}$, then the following are equivalent:*
(1) There exists a meromorphic function f that has principal part f_i at each point a_i and has no other poles.
(2) $\sum_{i=1}^{n} Res_{a_i} f_i \omega = 0$ for all holomorphic 1-form ω on S.

The Reverse Residue Theorem is the main new tool in the proof of Rimann-Roch theorem, namely the proof of Lemmas 16.8, 16.10 exposed by Valeriya Talovikova, which we follow. (Talovikova's exposition follows closely [Mirand1995] and is a variation of the proof of the Rimann-Roch Theorem in [Griffiths1985]. The Reverse Residue Theorem addresses the Mitaag-Leffler problem that asks under which condition there exists a $f \in K(\Sigma_g)$ such that in a neighborhood of a_i function f has f_i as its principal parts). The $\Longrightarrow$ in the Reverse Residue Theorem is simple, it can be proved by using Stock formula, see e.g. [Shafarevich2013, Theorem 3.27, p. 224]. The other part of Theorem is less known, and it is proved in [Mirand1995].

Recall that *the residue of a meromorphic 1-form* ω with pole at p is the integral

$$\int_\gamma \omega$$

where γ is a small circle around p such that the closed disk centered at p and boundary equal γ has no pole of ω. This integral does not depend on γ by the Stock formula.

By Reverse Residue Theorem the image of Φ consists of meromorphic functions f such that for all holomorphic 1-forms ω on S we have

$$\sum_{i=1}^{n} Res_{p_i} f_i \omega = 0.$$

Denote by $\Omega^1_{hol}(S)$ the linear space generated by holomorphic 1-forms on S. Then there is a map

$$R : \Omega^1_{hol}(S) \times V \to \mathbb{C},\ (\omega, [f_i]) \mapsto \sum_i Res_{p_i} f_i \omega.$$

The Reserve Residue Theorem implies that $R(\cdot, f) = 0$ iff $[f_i] \in \Phi(L(D))$. Hence setting

$$W := \Omega^1_{hol}(S)/\ker R(\cdot, V)$$

we have

$$\dim \mathrm{Im}\Phi = \dim V - \dim W. \tag{16.3}$$

Note that $\ker R(\cdot, V)$ consists of those holomorphic 1-form ω (since ω must have no pole) such that $ord_{p_i}\omega \geq m_i$. Hence $\omega \in I(D)$ and

$$\dim \ker R(\cdot, V) = i(D),$$

and since $\dim \Omega^1_{hol}(S) = g$ [3] taking into account (16.3) we have

$$\dim \mathrm{Im}\Phi = \dim V - g + i(D).$$

Taking into account (16.2) we obtain

$$l(D) = 1 + \dim V - g + i(D)$$

which proves Lemma 16.8. □

Lemma 16.10. *For all D we have*

$$l(D) - i(D) \geq 1 + deg(D) - g.$$

Proof. Lemma 16.8 implies that Lemma 16.10 holds for any positive divisor. Note that the RHS in Lemma 16.10 is additive w.r.t. D. Thus it suffices to prove the following inequality for any divisor D and any point $a \in S$

$$l(D-a) - i(D-a) \geq (l(D) - i(D)) - 1. \tag{16.4}$$

Indeed, if (16.4) holds then from Lemma 16.10 for D we obtain

$$l(D-a) - i(D-a) \geq (l(D) - i(D)) - 1 = deg(D-a) - g$$

which is Lemma 16.10 for $D - a$.

Note that

$$l(D) \geq l(D-a) \geq l(D) - 1. \tag{16.5}$$

The first inequality is obvious, since $(f)+(D-a) \geq 0$ implies $(f)+D \geq 0$. To see the second inequality we multiply with some member in $L(D-a)$ to obtain a member in $L(D)$, using Exercise 16.4. Using the same argument we have

$$i(D) + 1 \geq i(D-a) \geq i(D). \tag{16.6}$$

From (16.5) and (16.6), assuming Lemma 16.10) holds for D, we conclude that Lemma 16.10) violates for $D - a$, only if

$$l(D-a) = l(D) - 1 \text{ and } i(D-a) = i(D) + 1. \tag{16.7}$$

We shall show that (16.7) is impossible. Assume the opposite. Then there exists

$$f \in L(D) \setminus L(D-a) \text{ and } \omega \in i(D-a) \setminus I(D). \tag{16.8}$$

Now assume that

$$D = na + n_i a_i$$

[3]This formula is a special case of the Riemann-Roch theorem for the case $D = 0$. Its proof occupies p. 102-109 in [Griffiths1985].

Then (16.8) implies that $n-1 < ord_a f \le n$ and $n-1 \le ord_a\omega < n$ and hence

$$ord_a f = n \text{ and } ord_a(\omega) = n-1. \tag{16.9}$$

Moreover for any $p \neq a$ we have

$$ord_p(f\cdot\omega) \ge 0 \tag{16.10}$$

since $(f) \ge -D$ and $(f\omega) = (f) + (\omega) \ge -a$ which implies that $f\omega$ has only pole in a of order 1. On the other hand by Reserve Residue Theorem we have $\sum_i Res_{a_i}(f\omega) = 0$. This is contradiction. This completes the proof of Lemma 16.10. □

Let K denote a canonical divisor. K plays the role of the volume form in the following Brill-Noether reciprocity.

Lemma 16.11. *We have*

$$I(D) \cong L(K-D) \text{ and } I(K-D) \cong L(D)$$

Proof. We shall prove that $I(K-D)$ is isomorphic to $L(D)$ first. We assume that $K = (\omega)$ for some meromorphic 1-form ω. If f is a meromorphic function, then

$$(f) + D = (f\omega) - (\omega) + D = (f\omega) - (K-D).$$

Hence we have

$$f \in L(D) = \{g|(g)+D \ge 0\} \Longleftrightarrow f\omega \in I(K-D) = \{\beta|(\beta) \ge K-D\}. \tag{16.11}$$

Thus, we have a map:

$$L(D) \to I(K-D),\ f \mapsto f\omega.$$

Since every meromorphic 1-form in $I(K-D)$ can be presented as $f\omega$ for some meromorphic function, we similarly have an inverse function $I(K-D) \to L(D)$. By (16.11), it is not hard to see that these linear map are inverse to each other. □

Completion of the proof of Theorem 16.7 By Lemma 16.11 we have

$$l(K-D) = i(D).$$

Hence Lemma 16.10 for $K-D$ implies

$$(K-D) - i(K-D) \ge deg(K-D) + 1 - g,$$
$$i(D) - l(D) \ge deg(K-D) + 1 - g,$$
$$i(D) - l(D) \ge deg(K) - deg(D) + 1 - g.$$

By Lemma 16.5, $deg(K) = 2-2g$. Hence

$$i(D) - l(D) \ge 2g - 2 - deg(D) + 1 - g = g - 1 - deg(D)$$

$$l(D) - i(D) \leq deg(D) + 1 - g.$$

Combining with Lemma 16.10 and Lemma 16.8 we complete the proof of Theorem 16.7. □

17. Complementary materials

17.1. **Hanack's Theorem.** (written by Martin Cech based on his talk given at the seminar.)

Harnack's Theorem gives an upper bound to the number of connected components of a curve of degree d in the real projective plane. The number given by Harnack's theorem is the best possible and moreover, each lower count can be attained.

Let us begin by stating some facts about curves in the real projective plane.

If γ is a nonsingular algebraic curve in $\mathbb{RP}^2$, it can be decomposed into connected components. Each of this component is homeomorphic to a circle. We will call these components *ovals*. The circle S^1 can be embedded into $\mathbb{RP}^2$ in two different ways (by an embedding p):

- $\mathbb{RP}^2 \setminus p(S^1)$ consists of two connected components, one of them homeomorphic to an open disc (the interior) and the other homeomorphic to a Mbius band (the exterior).
- $\mathbb{RP}^2 \setminus p(S^1)$ is connected and homeomorphic to an open disc.

We will call the ovals of the first type *even* and the oval of the second type *odd*.

The two types of ovals can be distinguished using the fundamental group of $\mathbb{RP}^2$. Since $\pi_1(\mathbb{RP}^2) = \mathbb{Z}/2\mathbb{Z}$, the odd ovals are exactly those whose homotopy class is nontrivial. Hence the even ovals are null-homotopic and it follows that the number of intersections of any curve with on even oval is even - this is because the parity of the number of intersections does not change when we "continuously" deform the curve. For a similar reason, any two odd ovals intersect and therefore a curve can have at most one odd oval.

We are now ready to proof Harnack's theorem.

Theorem 17.1 (**Harnack**)**.** *Any nonsingular algebraic curve of degree d in $\mathbb{RP}^2$ has at most $\frac{(d-1)(d-2)}{2} + 1$ connected components.*

Proof. If $d = 2$, the theorem holds so we may assume $d > 2$. It also suffices to consider irreducible curves because if we let $p(d) = \frac{(d-1)(d-2)}{2} + 1$, then $p(d_1) + p(d_2) \leq p(d_1 + d_2)$.

Suppose for contradiction that there exists an irreducible nonsingular curve γ of degree d which has more than $\frac{(d-1)(d-2)}{2}+1$ connected components. Since at most one of the connected components is odd, we can choose some $p=\frac{(d-1)(d-2)}{2}+1$ even ovals of γ, denote them $\omega_1,\dots,\omega_p$. Then γ has at least one more oval ω. Note that for $d>2$ it holds that $\frac{1}{2}d(d-1)-1\geq p$. Hence we can choose $\frac{1}{2}d(d-1)-1$ distinct points on γ so that each of the first p points lies on a different even oval from $\omega_1,\dots,\omega_p$ and the other points lie on ω. Because the dimension of the space of homogeneous polynomials of degree $d-2$ has dimension $\binom{d}{2}$ and we have chosen $\binom{d}{2}-1$ points, there exists a nonsingular curve δ of degree $d-2$ passing through all the chosen points. Because γ was irreducible and δ has degree $d-2$, they don't have an irreducible component in common and hence by Bzout's theorem, they have at most $d(d-2)$ intersections. Let's count the number of intersections in a different way:

- The curve δ contains one point from each oval $\omega_1,\dots,\omega_p$ and since these ovals are even, it intersects each of them in at least one more point. This gives us at least $2p$ intersections.
- There are at least $\frac{1}{2}d(d-1)-1-p$ intersections of δ with the oval ω.

Hence we get at least $\frac{1}{2}d(d-1)-1+p=\frac{1}{2}d(d-1)-1+\frac{1}{2}(d-1)(d-2)+1=d^2-2d+1=d(d-1)+1$, which is a contradiction with Bzout's theorem. $\square$

References

[AM1969] M. F. Atyah and I. G. Macdonald, Introduction to commutative algebra, Addison-Westley Publishing Company, 1969.
[CLO1996] D. Cox, J. Little and Donal O'Shea, Ideals, Varieties and Algorithms, Springer, 1996.
[Dolgachev2013] I. V. Dolgachev, Introduction to Algebraic Geometry, 2013.
[Dieudonne1972] J. Dieudonne, The Historical Development of Algebraic Geometry, The American Mathematical Monthly, Vol. 79, No. 8 (Oct., 1972), pp. 827-866.
[GP2008] G.M. Greuel and G. Pfister, A singular introduction to commutative algebra, Springer, 2008.
[Griffiths1985] , Introduction to Algebric curves, Translation of Math. Monographs vol. 76, AMS, 1985.
[Harris1992] J. Harris, Algebraic Geometry, A First Course, Springer, 1992.
[Hartshorne1997] R. Hartshone, Algebraic Geometry, Springer, 1997.
[Lang2005] S. Lang, Algebra, Springer, 2005.
[Mirand1995] , Algebraic curves and Riemanian surfaces, AMS, 1995.
[Reid2013] M. Reid, Undergraduate Algbraic Geometry, C.U.P. 2013.

[Shafarevich2013] I. R. Shafarevich, Basic Algebraic Geometry 1, Varieties in Projective Space, Springer, 2013.