A COURSE IN
ALGEBRAIC GEOMETRY

Eyal Z. Goren

Department of Mathematics and Statistics, McGill University

Preface

These notes are the notes for my course *Introduction to Algebraic Geometry*, taught at McGill University in the Fall term of 2001. The notes did not undergo a very serious proof reading, hence may contain typos or minor mistakes, for which I take no responsibility.

The format of this advanced graduate course was two (full) hours lectures a week and a seminar lecture of one hour, delivered every week by one of the students. The students also produced texts to accompany their lectures. I take even less responsibility as to the correctness of these texts.

I thank my class: Khanh Huynh, Neil Kennedy, Melisande Fortin-Boisvert, Dimitry Zuchowski, Pavel Dimitrov, Benoit Arbour, Dmitry Chtcherbine, Carlos Philips, Maxim Samsonov, Roman Tymkiv, Matthew Greenberg, Sebastien Loisel, Gabriel Chenevert, Vasilisa Chramtchenko and Alexandru Stanculescu, for a most enjoyable semester and for permitting me to include the text of their lectures.

Eyal Z. Goren
Department of Mathematics and Statistics,
McGill University

Montreal, Winter 2002.

Added on August 2012

It seemed a good idea to expand the notes and improve them on the occasion of teaching the course again in Fall 2012. For one, this term the course was given in the format of $3-4$ hours per week and that allowed covering additional material. Secondly, my own perspective and understanding had improved slightly over the last 10 years and so there were topics I wanted to discuss a bit differently. Nonetheless, the style of the text and the main syllabus stayed the same.

Contents

1. Orientation Meeting

Sophie Germain (1776-1831)[1]*:*

L'algèbre n'est qu'une géométrie écrite; la géométrie n'est qu'une algèbre figurée.

1.1. **Introducion.** Perhaps the first question is "what is algebraic geometry?" The answer is that algebraic geometry is essentially the study of solutions of polynomial equations. Here is the
Basic example. Let k be an algebraically closed field ($\mathbb{C}, \overline{\mathbb{F}}_p, \overline{\mathbb{Q}}, \ldots$). Let $x_1, \ldots, x_n$ be variables and let $f_1, \ldots, f_m$ be polynomials in $k[x_1, \ldots, x_n]$. Define

$$\mathcal{Z}(\{f_1, \ldots, f_m\}) = \{(a_1, \ldots, a_n) \in k^n : f_1(a_1, \ldots, a_n) = \cdots = f_m(a_1, \ldots, a_n) = 0\}.$$

The basic object of study in algebraic geometry is such sets. There is a question here that is both naive and very deep at the same time: what's to study here?! The deep aspect of this question relates to the problem of defining interesting properties of such sets. Here are some examples that you probably would have come up with yourself quite quickly:

(1) Is $\mathcal{Z}(\{f_1, \ldots, f_m\})$ empty or not and to what extent does it depend on $\{f_1, \ldots, f_m\}$?
(2) What is the dimension of $\mathcal{Z}(\{f_1, \ldots, f_m\})$? Is it connected? singular?
(3) When are two sets of the kind $\mathcal{Z}(\{f_1, \ldots, f_m\})$ to be considered "the same"? I.e., what is the correct notion of isomorphism? Which properties of $\mathcal{Z}(\{f_1, \ldots, f_m\})$ are then intrinsic and which depend on the particular representative for the isomorphism class?

Much more sophisticated invariants are

(4) Cohomology groups of $\mathcal{Z}(\{f_1, \ldots, f_m\})$. Here one can consider topological cohomology if we are working over $\mathbb{C}$, or sheaf cohomology in general. In the general case a challenge is posed by finding canonical sheaves on such sets.

    If you are arithmetically inclined you would have probably come up with questions like:

(5) Let R be a ring contained in the field k. What are the R points of $\mathcal{Z}(\{f_1, \ldots, f_m\})$? Namely, $\mathcal{Z}(\{f_1, \ldots, f_m\}) \cap R^n$. For example: what is $\mathcal{Z}(x^n + y^n - z^n) \cap \mathbb{Z}^3$ for $n = 2, 3, 4, \ldots$?
    Is there any relation between the geometric properties we defined above and this problem? Are the R points of $\mathcal{Z}$ distributed in a special fashion that can be defined in geometric terms?
    Gerd Faltings (1954-)[2]*: (Simplified) If (1) $\mathcal{Z}(\{f_1, \ldots, f_m\})$ is one dimensional, irreducible and smooth, (2) the coefficients of the polynomials $f_1, \ldots, f_m$ are rational numbers and (3) the genus of $\mathcal{Z}(\{f_1, \ldots, f_m\})$ is greater than 1, then $\mathcal{Z}(\{f_1, \ldots, f_m\}) \cap \mathbb{Q}^n$ is finite.*

(6) Is there a geometric theory connecting the geometry of the set of complex solutions $\mathcal{Z}(\{f_1, \ldots, f_m\})$ for polynomials f_i with integer coefficients, and the geometry of the set

[1] See http://www-groups.dcs.st-and.ac.uk/∼history/Mathematicians/Germain.html for more on this fascinating person.

[2] This theorem was conjectured by Mordell and is still often referred to as "Mordell's conjecture".

of $\overline{\mathbb{F}}_p$ solutions $\mathcal{Z}(\{\overline{f}_1, \ldots, \overline{f}_m\})$ for the polynomials $\{\overline{f}_i\}$, where $\overline{f}_i$ denotes the reduction of f_i modulo p?

(7) People which are more topologically inclined may ask: Are the sets $\mathcal{Z}(\{f_1, \ldots, f_m\})$ distinguished among all topological, or differentiable, manifolds? For example, for algebraic surfaces of general type one has the Bogomolov-Miyaoka-Yau inequality $c_1^2 \leq 3c_2$ (where c_1, c_2 are the Chern classes of the tangent bundle).

Algebraic geometry grew out of several motivations. The most ancient origin being perhaps the analytic and later the projective geometry created to serve engineering, architecture and art. This first led to the fundamental insight in which the set of solutions to equations is graphed as a geometric shape. It later led to the consideration of points at infinity, duality theorems and more.

On the other hand (much later) the insight of Riemann (1826-1866) as to the right domain of definition of naturally occurring multi-valued complex functions (e.g., the domain of definition for the function $\sqrt{x(x-1)(x-\lambda)}$ is the elliptic curve $y^2 = x(x-1)(x-\lambda)$) have led to the development of Riemann surfaces with strong connections to complex uniformization and function theory.

The work of Newton (1643-1727) and Bézout (1730 - 1783) on solutions to systems of polynomial equations lead to the development of intersection theory in projective spaces. The most renowned aspect of it is Bézouts theorem stating that two complex curves in $\mathbb{P}^2$ of degrees n and m, respectively, intersect in nm points.

2. Algebraic Sets and Affine Varieties

2.1. **Algebraic Sets.** We fix the following notation

k – a fixed algebraically closed field.

$\mathbb{A}^n$ $= \mathbb{A}^n(k) = \mathbb{A}^n_k = \{(a_1, \ldots, a_n) : a_i \in k\}$ – the affine n-space over k. We shall often write a for an element $(a_1, \ldots, a_n)$ of $\mathbb{A}^n$.

Definition 2.1. Given a non-empty subset $T \subseteq k[x_1, \ldots, x_n]$, define the **zero set of** T to be

$$\mathcal{Z}(T) = \{a \in \mathbb{A}^n : f(a) = 0, \ \forall f \in T\}.$$

It is the set of common solutions to all the polynomials $f \in T$.

Example 2.2. Here is an example (Figure 1) with $T = \{f_1, f_2\}$, where $f_1 = x^2 + y^2 - z^2$ (defining the cone) and $f_2 = x^2 + z + y^2 - 1$ (defining the "hill"). The figures are a bit misleading. In fact the

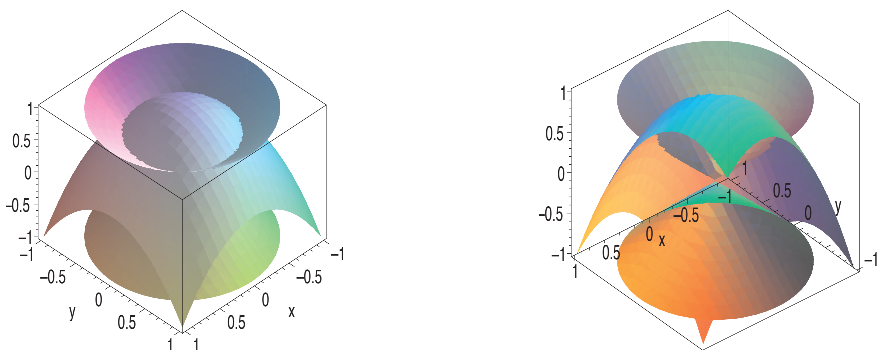


Figure 1. A cone and a regular surface

intersection has two components. Indeed, as $f_2 - f_1 = z^2 + z - 1$ vanishes on the intersection, we get that $z = (-1 \pm \sqrt{5})/2$ and the intersection consists of the two "circles" (in later terminology, rational curves)

$$\begin{cases} z = \frac{-1+\sqrt{5}}{2}, & x^2 + y^2 = \frac{3-\sqrt{5}}{2} \\ z = \frac{-1-\sqrt{5}}{2}, & x^2 + y^2 = \frac{3+\sqrt{5}}{2}. \end{cases}$$

See Figure 2

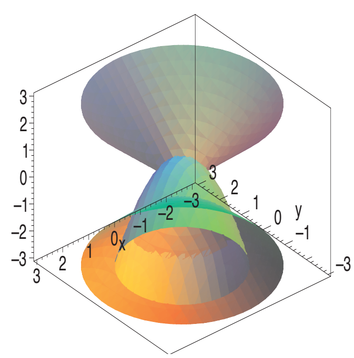


Figure 2. The other component

Example 2.3. Here is another example (Figure 3). This time, of a curve C defined by intersection of three surfaces S_1, S_2, S_3. Though the intersection of any two of these surfaces S_i, S_j yields a curve C_{ij}, this curve is reducible and C is one of its components. This is an example of a variety which is not a "complete intersection"; one needs more equations than the co-dimension to define the variety. Not only all the equations defining the surfaces S_i are needed, but, in fact, it is not possible to find *two* equations whose common solutions are precisely the curve C.

The curve is given in parametric form by (t^3, t^4, t^5) and the surfaces are given by the equations $x^4 - y^3 = 0$, $y^5 - z^4 = 0$ and $x^5 - z^3 = 0$. In fact, consider the intersection of the surfaces S_1 and

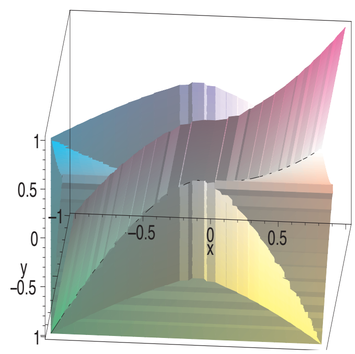


Figure 3. Non complete intersection

S_2, given by $y^3 = x^4$ and $y^5 = z^4$, respectively. Putting $u = x^5, v = z^3$ we find that the equation $u^4 - v^4 = (u - v)(u + v)(u + iv)(u - iv) = 0$ is satisfied on the intersection $S_1 \cap S_2$ of the surfaces. We get that the intersection of these two surfaces is a union of 4 curves: $u = v$, $y^3 = x^4$ and $y^5 = z^4$ is one curve - the intersection of S_1, S_2, S_3. But other curves are $u = -v$, $y^3 = x^4$ and $y^5 = z^4$, etc. Each of these curves admits a uniformisation. The first, by (t^3, t^4, t^5); the second, by $(t^3, t^4, -t^5)$, and so on. This shows that each of these components is irreducible - although at this point we don't have yet a precise notion of irreducible.

Definition 2.4. A subset $Y \subseteq \mathbb{A}^n$ is called an **algebraic set** if there exists a set $T \subseteq k[x_1, \ldots, x_n]$ such that $Y = \mathcal{Z}(T)$.

Proposition 2.5. (The Zariski Topology) *There is a unique topology on $\mathbb{A}^n$ whose closed sets are the algebraic sets.*

Proof. We verify the axioms for closed sets:

(1) The empty set $\emptyset$ is closed: $\emptyset = \mathcal{Z}(\{1\})$ (the zero set of the constant polynomial 1). The total space $\mathbb{A}^n$ is also closed: $\mathbb{A}^n = \mathcal{Z}(\{0\})$ (the zero set of the zero polynomial).
(2) A finite union of closed sets is closed. In fact, we prove a more precise formula

$$\mathcal{Z}(T_1) \cup \mathcal{Z}(T_2) = \mathcal{Z}(T_1 T_2),$$

where by $T_1 T_2$ we mean the set of all products fg with $f \in T_1$ and $g \in T_2$. We verify this formula: Let $x \in \mathcal{Z}(T_1)$ then $f(x) = 0$ for all $f \in T_1$ and hence $(fg)(x) = f(x)g(x) = 0$ for all products fg in $T_1 T_2$. Thus, $x \in \mathcal{Z}(T_1 T_2)$. We have established the inclusion $\mathcal{Z}(T_1) \cup \mathcal{Z}(T_2) \subseteq \mathcal{Z}(T_1 T_2)$.

Conversely, let $x \in \mathcal{Z}(T_1T_2)$. Either $x \in \mathcal{Z}(T_1)$ or there exists a $f_0 \in T_1$ such that $f_0(x) \neq 0$. In the latter case, since $f_0 g(x) = 0$ for all $g \in T_2$, we get that $g(x) = 0$ for all $g \in T_2$ and therefore $x \in \mathcal{Z}(T_2)$.

(3) An arbitrary intersection of closed sets is closed. Indeed, let $\{\mathcal{Z}(T_\alpha) : \alpha \in \mathcal{J}\}$ be a collection of closed sets; we prove that

$$\bigcap_{\alpha\in\mathcal{J}} \mathcal{Z}(T_\alpha) = \mathcal{Z}(\bigcup_{\alpha\in\mathcal{J}} T_\alpha).$$

This is straightforward: x solves all polynomials in T_α, for each α (l.h.s.) if an only if x solves all the polynomials in $\bigcup_{\alpha\in\mathcal{J}} T_\alpha$ (r.h.s.).

□

Given a set $T \subset k[x_1, \dots, x_n]$ we denote by $\langle T \rangle$ the ideal generated by it. Given an ideal $\mathfrak{a} \lhd k[x_1, \dots, x_n]$ we denote by $\sqrt{\mathfrak{a}}$ its **radical**. Recall that

$$\sqrt{\mathfrak{a}} = \{f \in k[x_1, \dots, x_n] : f^n \in \mathfrak{a} \text{ for some } n \in \mathbb{N}\}.$$

It is an ideal containing $\mathfrak{a}$ that is equal to its own radical. In general, an ideal equal to its radical is called a **radical ideal**. Every prime ideal is a radical ideal. The ideal $\langle xy \rangle$ is a radical ideal that is not prime.

Remark 2.6. One easily verifies the following important assertions:

- $\mathcal{Z}(T) = \mathcal{Z}(\langle T \rangle) = \mathcal{Z}(\sqrt{\langle T \rangle})$.
- For ideals $\mathfrak{a}, \mathfrak{b} \lhd k[x_1, \dots, x_n]$ we have

$$\mathcal{Z}(\mathfrak{a}) \cup \mathcal{Z}(\mathfrak{b}) = \mathcal{Z}(\mathfrak{a}\mathfrak{b}), \qquad \mathcal{Z}(\mathfrak{a}) \cap \mathcal{Z}(\mathfrak{b}) = \mathcal{Z}(\mathfrak{a} + \mathfrak{b}).$$

Important conclusion: By Hilbert's basis theorem, every ideal in $k[x_1, \dots, x_n]$ is finitely generated (equivalently, $k[x_1, \dots, x_n]$ is a noetherian ring). Therefore, in particular, since $\mathcal{Z}(T) = \mathcal{Z}(\langle T \rangle)$ it follows that we can find finitely many polynomials $f_1, \dots, f_m$ such that $\mathcal{Z}(T) = \mathcal{Z}(\{f_1, \dots, f_m\})$. Indeed, all we need to do is to take generators for the ideal $\langle T \rangle$.

Example 2.7. Let $Z \subsetneqq \mathbb{A}^1$ be a non-empty proper closed set. Then $Z = \mathcal{Z}(\mathfrak{a})$ for some radical ideal $\mathfrak{a} \lhd k[x]$. Since $k[x]$ is a principal ideal domain, $\mathfrak{a} = (f)$ for some polynomial $f \in k[x]$ and $Z = \mathcal{Z}(f)$. Since k is algebraically closed, our assumption that $Z \neq \emptyset$ is equivalent to $\deg(f) > 0$. Write $f(x) = (x - a_1) \cdots (x - a_n)$ and f has no repeated roots because $\mathfrak{a}$ is radical. Then $Z = \{a_1, \dots, a_n\}$. In particular, the Zariski topology on $\mathbb{A}^1$ is the co-finite topology, which is not Hausdorff (k is infinite), but it is T_1.

END OF LECTURE 1 (September 5).

2.2. **Some Topological Concepts.** The results of this section will later be applied to the space $\mathbb{A}^n$ with its Zariski topology.

Definition 2.8. A non-empty topological space X is called **irreducible** if $X = Y_1 \cup Y_2$, where Y_1, Y_2 are closed sets, implies that either $X = Y_1$ or $X = Y_2$. Note that if X is irreducible and $X = Y_1 \cup \cdots \cup Y_n$, a finite union of closed sets, then $X = Y_i$ for some i.

Lemma 2.9. *The following properties are equivalent.*

(1) *X is irreducible;*
(2) *Every non-empty open set is dense in X;*
(3) *Every two non-empty open sets intersect.*

Proof. We first prove (1) $\Rightarrow$ (2). Let U be a non-empty open set. Let $Y_1 = X \setminus U$ and let $Y_2 = \overline{U}$. Then $X = Y_1 \cup Y_2$, a union of closed sets. Since U is non-empty $Y_1 \neq X$ and hence $Y_2 = X$, that is, U is dense.

Suppose now that (2) holds. If U, V are disjoint non-empty open sets then $\overline{U} \subset X \setminus V \neq X$, and, in particular, U is not dense in X. Contradiction.

Suppose that (3) holds. Let $X = Y_1 \cup Y_2$, a union of closed sets. Let $U_i = X \setminus Y_i$. Then, either some $U_i = \emptyset$ and hence $X = Y_i$, or $U_1 \cap U_2 \neq \emptyset$. But $U_1 \cap U_2 = X \setminus (Y_1 \cup Y_2)$, so $U_1 \cap U_2 \neq \emptyset$ does not occur. □

The Lemma shows that such topological spaces are very far from our experience. Note that an irreducible space with more than one point is not Hausdorff.

If U is an open subset of X and $V \subset U$ is open in the induced topology then V is open in X. Using (3) we thus deduce:

Corollary 2.10. *Let U be a non-empty open subset of an irreducible topological space, then U is irreducible in the induced topology.*

Definition 2.11. A topological space X is called **noetherian** if any decreasing sequence of closed sets stabilizes: If

$$Y_0 \supset Y_1 \supset Y_2 \supset \dots,$$

are closed sets, there exists an integer $N \in \mathbb{N}$ such that $n \geq N \Rightarrow Y_n = Y_N$.

Proposition 2.12. *Let X be a noetherian topological space. Every closed subset Z of X can be written as a finite union*

$$Z = \bigcup_{i=1}^{m} Z_i$$

of irreducible closed sets such that $Z_i \not\supset Z_j$ for $i \neq j$. Furthermore, such an expression is unique up to reordering the terms.

Proof. Let Σ be the collection of closed subsets of X that cannot be written as a union of irreducible closed sets. Suppose that Σ is non-empty. Since descending chains are finite, there is an element $Z_0 \in \Sigma$ which is minimal with respect to inclusion. In particular, Z_0 is reducible and hence has a non-trivial decomposition of the form $Z_0 = Z_1 \cup Z_2$, where Z_1, Z_2 are closed sets.

The minimality of Z_0 implies that each Z_i is a union of irreducible closed sets hence so is Z_0. Contradiction. Thus, $\Sigma = \emptyset$. Note that if a closed subset Z is a finite union of irreducible closed sets $Z = \cup Z_i$ then, by omitting some of the Z_i, we may assume that $Z_i \not\supset Z_j$ for $i \neq j$.

We now prove uniqueness. If $Z = \cup_{i \in I} Z_i = \cup_{j \in J} \widetilde{Z}_j$ (union of closed irreducible closed sets such that $Z_i \not\subset Z_j$ for $i \neq j$ and $\widetilde{Z}_i \not\subset \widetilde{Z}_j$ for $i \neq j$) then $Z_i = \cup_j (Z_i \cap \widetilde{Z}_j)$, a union of closed sets, and therefore for every i there exists some $j(i)$ such that $Z_i \subseteq \widetilde{Z}_{j(i)}$. By symmetry, we get a function $j \mapsto i(j)$ such that $\widetilde{Z}_j \subseteq Z_{i(j)}$. Because $Z_i \subseteq Z_{i(j(i))}$, we have $i(j(i)) = i$ and, similarly, $j(i(j)) = j$ and also $Z_i = \widetilde{Z}_{j(i)}$. This gives the permutation of the index set. □

2.3. **The Fundamental Theorem of Algebraic Geometry.** The main tool here is

THEOREM **1.** [3]**(Hilbert's Nullstellensatz)** *Let k be an algebraically closed field and let $\mathfrak{a}$ be an ideal of $k[x_1, \dots, x_n]$. Let $f \in k[x_1, \dots, x_n]$ be a polynomial such that $f(x) = 0$ for all $x \in \mathcal{Z}(\mathfrak{a})$, i.e., f vanishes on every point of the zero set of $\mathfrak{a}$. Then $f \in \sqrt{\mathfrak{a}}$.*

Definition 2.13. Given a subset $Y \subseteq \mathbb{A}^n$ define the ideal of functions vanishing identically on Y by

$$\mathcal{I}(Y) = \{f \in k[x_1, \dots, x_n] : f(y) = 0, \ \forall y \in Y\}.$$

Proposition 2.14.

(1) *For any two subsets $T_1 \subset T_2 \subset k[x_1, \dots, x_n]$ we have $\mathcal{Z}(T_1) \supset \mathcal{Z}(T_2)$.*
(2) *For any two subsets $Y_1 \subset Y_2 \subset \mathbb{A}^n$ we have $\mathcal{I}(Y_1) \supset \mathcal{I}(Y_2)$.*
(3) *For any two subsets $\mathcal{I}(Y_1 \cup Y_2) = \mathcal{I}(Y_1) \cap \mathcal{I}(Y_2)$.*
(4) *For any ideal $\mathfrak{a} \lhd k[x_1, \dots, x_n]$ we have $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.*
(5) *For any subset $Y \subset \mathbb{A}^n$ we have $\mathcal{Z}(\mathcal{I}(Y)) = \overline{Y}$.*

Proof. In (1) we only say that a common zero of the elements of T_2 is a common zero of the elements of T_1. This is clear. Similarly, (2) just says that a polynomial vanishing identically on Y_2 vanishes identically on Y_1, which is also clear. Also (3) has a simple content: a polynomial vanishes identically on both Y_1 and Y_2 if and only if it vanishes identically on Y_1 <u>and</u> on Y_2.

Part (4) is far from having a trivial content, but is just a reformulation of Hilbert's Nullstellensatz. It remains to prove (5).

By definition, there exists an ideal $\mathfrak{a} \lhd k[x_1, \dots, x_n]$ such that $\overline{Y} = \mathcal{Z}(\mathfrak{a})$. We may assume that $\mathfrak{a}$ is a radical ideal. We have $\mathcal{Z}(\mathfrak{a}) \supseteq Y$, hence $\mathfrak{a} = \mathcal{I}(\mathcal{Z}(\mathfrak{a})) \subseteq \mathcal{I}(Y)$. This gives $\overline{Y} = \mathcal{Z}(\mathfrak{a}) \supset \mathcal{Z}(\mathcal{I}(Y))$.

On the other hand, if $y \in Y$ then $f(y) = 0$ for any $f \in \mathcal{I}(Y)$. That is, $Y \subset \mathcal{Z}(\mathcal{I}(Y))$. Because $\mathcal{Z}(\mathcal{I}(Y))$ is a closed set also $\overline{Y} \subset \mathcal{Z}(\mathcal{I}(Y))$. □

Theorem 2.15. (The Fundamental Theorem) *There is $1:1$ inclusion-reversing correspondence between radical ideals of $k[x_1, \dots, x_n]$ and closed (i.e., algebraic) sets in $\mathbb{A}^n$ given by*

$$\mathfrak{a} \mapsto \mathcal{Z}(\mathfrak{a}), \qquad Y \mapsto \mathcal{I}(Y).$$

Under this correspondence we have[4]

$$\mathcal{I}(Y_1 \cup Y_2) = \mathcal{I}(Y_1) \cap \mathcal{I}(Y_2), \qquad \mathcal{I}(Y_1 \cap Y_2) = \sqrt{\mathcal{I}(Y_1) + \mathcal{I}(Y_2)};$$

equivalently,

$$\mathcal{Z}(\mathfrak{a}) \cup \mathcal{Z}(\mathfrak{b}) = \mathcal{Z}(\mathfrak{a} \cap \mathfrak{b}), \qquad \mathcal{Z}(\mathfrak{a}) \cap \mathcal{Z}(\mathfrak{b}) = \mathcal{Z}(\mathfrak{a} + \mathfrak{b}) = \mathcal{Z}(\sqrt{\mathfrak{a} + \mathfrak{b}}).$$

Under this correspondence prime ideals correspond to irreducible closed sets.

Proof. We have $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \sqrt{\mathfrak{a}} = \mathfrak{a}$ and $\mathcal{Z}(\mathcal{I}(Y)) = \overline{Y} = Y$ for a radical ideal $\mathfrak{a}$ and a closed set Y.

The formulas $\mathcal{I}(Y_1 \cup Y_2) = \mathcal{I}(Y_1) \cap \mathcal{I}(Y_2)$ and $\mathcal{I}(Y_1 \cap Y_2) = \sqrt{\mathcal{I}(Y_1) + \mathcal{I}(Y_2)}$ now follow from Remark 2.6. It remains to prove that a closed set is irreducible iff it is the zero locus of a prime ideal.

[3] For the proof see [Mum] pp. 8-10.

[4] We remark that for radical ideals $\mathfrak{a}$, $\mathfrak{b}$, the ideal $\mathfrak{a} \cap \mathfrak{b}$ is radical and $\mathfrak{a} \cap \mathfrak{b} = \sqrt{\mathfrak{a}\mathfrak{b}}$. On the other hand, $\mathfrak{a} + \mathfrak{b}$ need not be radical. For example, take $\mathfrak{a} = \langle y - x^2 \rangle$, $\mathfrak{b} = \langle y \rangle$ - both are prime ideals - and $\mathfrak{a} + \mathfrak{b} = \langle y, x^2 \rangle$, which is not a radical ideal.

Let $\mathfrak{a}$ be a prime ideal. If $\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\mathfrak{c}) \cup \mathcal{Z}(\mathfrak{d})$ then $\mathfrak{a} = \mathfrak{c} \cap \mathfrak{d}$. Suppose that there exists an element $c \in \mathfrak{c} \setminus \mathfrak{a}$. Let $d \in \mathfrak{d}$. We have $cd \in \mathfrak{a}$ and therefore $d \in \mathfrak{a}$ ($\mathfrak{a}$ prime implies either c or d belong to $\mathfrak{a}$). That is $\mathfrak{d} = \mathfrak{a}$ and hence $\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\mathfrak{d})$.

Suppose now that $\mathfrak{a}$ is a radical ideal and $\mathcal{Z}(\mathfrak{a})$ is irreducible. Let $fg \in \mathfrak{a}$ then $\mathcal{Z}(fg) = \mathcal{Z}(f) \cup \mathcal{Z}(g) \supset \mathcal{Z}(\mathfrak{a})$ and hence $\mathcal{Z}(\mathfrak{a}) = (\mathcal{Z}(\mathfrak{a}) \cap \mathcal{Z}(f)) \cup (\mathcal{Z}(\mathfrak{a}) \cap \mathcal{Z}(g))$. It follows, without loss of generality, that $\mathcal{Z}(\mathfrak{a}) \subset \mathcal{Z}(f)$. Therefore, $\mathfrak{a} = \mathcal{I}\mathcal{Z}(\mathfrak{a}) \supset \mathcal{I}\mathcal{Z}(f) = \sqrt{(f)} \supset (f)$ and, in particular, $f \in \mathfrak{a}$. $\square$

It is important to notice that some information is lost in passing to radical ideals. For example, let $a \in k$ and consider the intersection of the two sets in $\mathbb{A}^2$

$$Y_1 = \mathcal{Z}(y - x^2), \qquad Y_2 = \mathcal{Z}(y - a).$$

This intersection is equal to the zero set of the ideal

$$(y - a, x^2 - a).$$

For $a \neq 0$ this is a radical ideal, equal to $(y - a, x - \sqrt{a}) \cap (y - a, x + \sqrt{a})$, while for $a = 0$ this is not a radical ideal; it is equal to (y, x^2) whose radical is (y, x). By passing to the radical we are loosing the information that the point $(0, 0)$ should receive multiplicity two if it is derived as intersection of Y_1 and Y_2. See Figure 4.

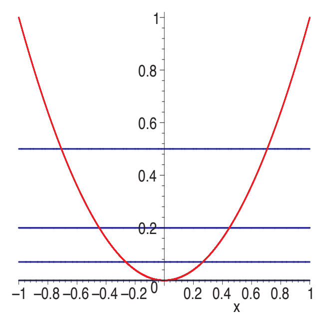


Figure 4. A double point

Corollary 2.16. *The set $\mathbb{A}^n$ with its Zariski topology is a noetherian irreducible topological space.*

Proof. Since the ideal (0) is a prime ideal of $k[x_1, \ldots, x_n]$ the space $\mathbb{A}^n$ is irreducible. Let $Y_1 \supset Y_2 \supset Y_3 \supset \ldots$ be a decreasing sequence of closed sets in $\mathbb{A}^n$. Let $\mathcal{I}(Y_1) \subset \mathcal{I}(Y_2) \subset \mathcal{I}(Y_3) \ldots$ be the corresponding sequence of radical ideals of $k[x_1, \ldots, x_n]$. Since $k[x_1, \ldots, x_n]$ is a noetherian ring[5] this sequence stabilizes: for some N we have $\mathcal{I}(Y_N) = \mathcal{I}(Y_{N+1}) = \mathcal{I}(Y_{N+2}) = \ldots$. Therefore, $Y_N = Y_{N+1} = Y_{N+2} = \ldots$, which proves that $\mathbb{A}^n$ is noetherian (and explains the terminology!). $\square$

Corollary 2.17. [6] *Every maximal ideal of $k[x_1, \ldots, x_n]$ is of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for suitable $a_i \in k$.*

Proof. Indeed, the minimal closed sets are points $(a_1, \ldots, a_n)$. $\square$

[5] Recall that this means that any ascending sequence of ideals stabilizes. A theorem of Hilbert states that if a commutative unital ring R is noetherian then so is $R[x]$. By induction, one concludes that $k[x_1, \ldots, x_n]$ is noetherian.

[6] However, in practice, one first proves the Corollary and deduces from it the Theorem.

Corollary 2.18. *Every radical ideal $\mathfrak{a} \lhd k[x_1, \dots, x_n]$ can be written uniquely as the product of prime ideals, $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_m$, with $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ for $i \neq j$. Moreover, the ideals $\mathfrak{p}_i$ are the minimal prime ideals of the ring $k[x_1, \dots, x_n]$ that contain $\mathfrak{a}$.*

Proof. Given that $\mathbb{A}^n$ is a noetherian irreducible topological space, the corollary follows from Proposition 2.12. $\square$

Example 2.19. Let $\mathfrak{a}$ be the ideal $\langle xz - x, x^2 - yz \rangle$. Consider the three ideals

$$\mathfrak{p}_1 = \langle x, y \rangle, \quad \mathfrak{p}_2 = \langle x, z \rangle, \quad \mathfrak{p}_3 = \langle z - 1, x^2 - yz \rangle.$$

These are three prime ideals defining three varieties $Y_i = \mathcal{Z}(\mathfrak{p}_i)$. In fact,

$$k[x, y, z]/\mathfrak{p}_1 \cong k[z], \quad k[x, y, z]/\mathfrak{p}_2 \cong k[y], \quad k[x, y, z]/\mathfrak{p}_3 \cong k[x].$$

Each ideal $\mathfrak{p}_i$ contains $\mathfrak{a}$. I claim that the ideals $\mathfrak{p}_i$ actually define the irreducible components of $\mathcal{Z}(\mathfrak{a})$ (see Figure 5). Namely, that each $\mathfrak{p}_i$ is a minimal prime ideal containing $\mathfrak{a}$, that they are all distinct and every minimal prime ideal containing $\mathfrak{a}$ is equal to some $\mathfrak{p}_i$. It is clear that the $\mathfrak{p}_i$ are distinct, and so we need to check that if a prime ideal $\mathfrak{q}$ contains $\mathfrak{a}$ then such that $\mathfrak{q} \supseteq \mathfrak{p}_i$ for some i. The element $xz - x$ belongs to the prime ideal $\mathfrak{q}$, hence either x or $z - 1$ belongs to $\mathfrak{q}$. Say $x \in \mathfrak{q}$. Then also $x^2 - (x^2 - yz) \in \mathfrak{q}$ so $yz \in \mathfrak{q}$ and hence either $y \in \mathfrak{q}$ or $z \in \mathfrak{q}$. That is, $\mathfrak{q} \supset \mathfrak{p}_1$ or $\mathfrak{q} \supset \mathfrak{p}_2$. If $z - 1 \in \mathfrak{q}$ then $\mathfrak{q} \supset \mathfrak{p}_3$.

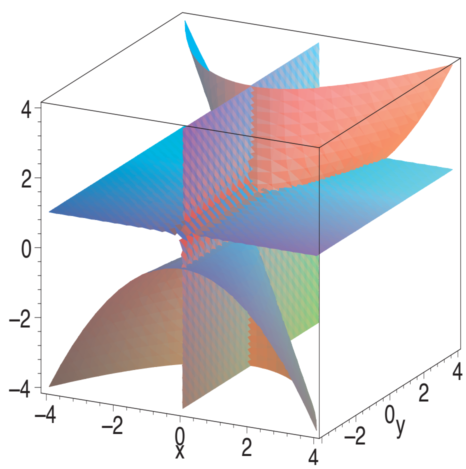


Figure 5.

END OF LECTURE 2 (September 10)

2.4. **Affine and Quasi-Affine Varieties, and Coordinate Rings.** A little bit of terminology. An irreducible algebraic set is called an **affine variety**. It is the zero set of a prime ideal. A non-empty open subset of an affine variety is called a **quasi-affine variety**. We remark that a quasi-affine may, or may not, be isomorphic to an affine variety. For example, the quasi affine variety $\mathbb{A}^1 - \{0\}$ is isomorphic to the affine variety $\mathcal{Z}(xy - 1) \subset \mathbb{A}^2$ (the notion of isomorphism will be defined later on, but for now let's take that to mean that in every sense considered in algebraic geometry they are to be considered the same). On the other hand, one can prove that the quasi-affine variety $\mathbb{A}^2 - \{0\}$ is not isomorphic to any affine variety.

Let $\mathfrak{a} \lhd k[x_1, \dots, x_n]$ be a radical ideal and $Y = \mathcal{Z}(\mathfrak{a})$ its zero set. The **coordinate ring** $A(Y)$ of Y is, by definition, the quotient ring $k[x_1, \dots, x_n]/\mathfrak{a}$. Otherwise said, it is the ring of polynomial functions on Y modulo those polynomials vanishing identically on Y. If we think of $k[x_1, \dots, x_n]$ as the ring of functions of $\mathbb{A}^n$ then the coordinate ring of Y is obtained by restriction of functions.

We remark that the coordinate ring of $\mathcal{Z}(\mathfrak{a})$ ($\mathfrak{a}$ a radical ideal) is a finitely generated k-algebra with no nilpotent elements and that it has zero divisors if and only if $\mathfrak{a}$ is not prime. Conversely, any finitely generated k-algebra with no nilpotent elements arises as a coordinate ring.

2.5. **Dimension and Height.** The following definition of dimension is completely flawed for any reasonable topological space, e.g., a manifold. It is designed to work specifically for the Zariski topology.

Definition 2.20. Let X be a topological space. We define the **dimension** of X to be the maximal integer n such that there exists a chain

$$Z_0 \subsetneqq Z_1 \subsetneqq \cdots \subsetneqq Z_n$$

of distinct irreducible closed subsets of X. (Recall that, by definition, Z_0 is not empty.)

We define the dimension of an affine variety, or a quasi-affine variety, to be its dimension as a topological space.

The next definition gives the counterpart of the definition above in the setting of rings.

Definition 2.21. Let R be a commutative ring with 1 and let $\mathfrak{p} \lhd R$ be a prime ideal. We define the **codimension** (also called **height**) of $\mathfrak{p}$ to be the maximal integer n such that there exists a chain

$$\mathfrak{p}_n \subsetneqq \cdots \subsetneqq \mathfrak{p}_0 = \mathfrak{p}$$

of distinct prime ideals. The **dimension** of R is the supremum of the codimensions of its maximal ideals, i.e., either ∞ or the maximal integer n such that there exists a chain of distinct prime ideals of length $n+1$.

Proposition 2.22. *Let $Y \subset \mathbb{A}^n$ be an algebraic set. Then*

$$\dim(Y) = \dim(A(Y)).$$

Proof. Indeed, chains of irreducible closed sets contained in Y correspond to chains of prime ideals of $k[x_1, \dots, x_n]$ containing $\mathcal{I}(Y)$. $\square$

THEOREM **2.** ([Eis, p. 290]) *Let k be a field and let B be a finitely generated k-algebra which is an integral domain. Let K be the quotient field of B. Then*[7]

(1) $\dim(B) = \text{tr.deg.}(K/k)$.
(2) *For any prime ideal $\mathfrak{p} \lhd B$ we have* $\dim(B/\mathfrak{p}) = \dim(B) - \text{codim}(\mathfrak{p})$.

---

[7] Let K/L be a field extension. Recall that an element $r \in K$ is called algebraic over L if it is a zero of a polynomial in $L[x]$. There exists a maximal integer $n \geq 0$ for which there is an embedding $L(x_1, \dots, x_n) \hookrightarrow K$ over L. The extension $L(x_1, \dots, x_n)/L$ is purely transcendental (which means that no element in $L(x_1, \dots, x_n) \setminus L$ is algebraic over L) and the extension $K/L(x_1, \dots, x_n)$ is algebraic. The elements $x_1, \dots, x_n$ are called a transcendence basis for $L(x_1, \dots, x_n)/L$.

The number n is called the transcendence degree of K over L and is canonical in the following sense. If for some m there is an embedding $L(y_1, \dots, y_m) \hookrightarrow K$ and the extension $K/L(y_1, \dots, y_m)$ is algebraic then $n = m$. On the other hand the image of $L(x_1, \dots, x_n) \hookrightarrow K$ is not canonical in any way (e.g., look at the subfield $L(x_1^2, x_2 \dots, x_n)$). See [Lang, Ch. X] for more.

Corollary 2.23. *We have* $\dim(\mathbb{A}^n) = n$*.*

Proof. We have $\dim(\mathbb{A}^n) = \dim(k[x_1, \ldots, x_n]) = \text{tr.deg.}(k(x_1, \ldots, x_n)/k) = n$. □

Remark 2.24. Let $\mathfrak{a}$ be a prime ideal of $k[x_1, \ldots, x_n]$. The coordinate ring $A(\mathcal{Z}(\mathfrak{a})) = k[x_1, \ldots, x_n]/\mathfrak{a}$ is **catenary**. Namely, if it has dimension r then every chain of distinct prime ideals of $A(\mathcal{Z}(\mathfrak{a}))$ can be refined to a chain of $r+1$ distinct prime ideals. This is very convenient in applications, since one only needs to find a single chain of prime ideals that cannot be refined to calculate the dimension. For example, the dimension of $\mathbb{A}^n$ is n (as we have already seen), but also, we have the chain of prime ideals

$$\langle 0 \rangle \subset \langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \cdots \subset \langle x_1, \ldots, x_n \rangle.$$

This is a chain with $n+1$ elements which cannot be refined. Namely, there is no prime ideal lying strictly between $\langle x_1, \ldots, x_i \rangle$ and $\langle x_1, \ldots, x_{i+1} \rangle$. We leave that as an exercise. Probably the easiest way to do it is to use Krull's hauptidealsatz (Theorem 3).

Proposition 2.25. *Let* $Y \subseteq \mathbb{A}^n$ *be a quasi-affine variety. Then* $\dim(Y) = \dim(\overline{Y})$*.*

Remark 2.26. This is not a general property of topological spaces. For example, let $X = \{1, 2\}$ with topology $\{\emptyset, \{1\}, X\}$. Then $\dim(X) = 1$ because $Z_0 := \{2\} \subset Z_1 := X$ is the unique maximal chain of irreducible closed sets. The subset $\{1\}$ is open in X and of dimension 0.

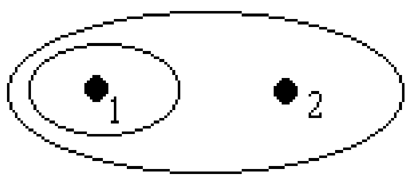


Figure 6. The space X

Proof. Let $Z_0 \subsetneqq Z_1 \subsetneqq \cdots \subsetneqq Z_m = Y$ be a maximal chain of closed irreducible sets in Y, with respect to the induced topology. Consider the sequence $\overline{Z_0} \subsetneqq \overline{Z_1} \subsetneqq \cdots \subsetneqq \overline{Z_m} = \overline{Y}$. This is a sequence of closed sets. We claim that they are distinct and irreducible. The fact that they are distinct follows from $\overline{Z_i} \cap Y = Z_i$ (by definition of the induced topology). Suppose that $\overline{Z_i} = Y_1 \cup Y_2$, non-empty proper closed sets. Then Z_i, which is irreducible, is equal to $(Z_i \cap Y_1) \cup (Z_i \cap Y_2)$ (a union of two closed sets in the topology of Y), hence $Z_i \subset Y_j$ for some $j = 1, 2$ and the same holds for $\overline{Z_i}$.

Now, we claim that the chain $\overline{Z_0} \subsetneqq \overline{Z_1} \subsetneqq \cdots \subsetneqq \overline{Z_m} = \overline{Y}$ is maximal. Indeed, if it can be refined by adding another irreducible set Z one notes that $Y \cap Z$ is non-empty and since Z is irreducible $Y \cap Z$ is dense in Z. On the other hand $Y \cap Z$ refines the original chain $Z_0 \subsetneqq Z_1 \subsetneqq \cdots \subsetneqq Z_m = Y$ hence equal to one of its members, say Z_i. We conclude that $\overline{Z_i} = Z$. The Proposition now follows from the catenary property (Remark 2.24). Alternately, we can use Theorem 2:

It is clear that $Z_0 = \overline{Z_0}$ is a point P corresponding to a maximal ideal $\mathfrak{m}$ of $A(\overline{Y})$. So far we know that the codimension of $\mathfrak{m}$ in the ring $A(\overline{Y})$ is at least m. Now suppose given another set of prime ideals of $A(\overline{Y})$ such that $\mathfrak{m} = \mathfrak{p}_0 \supsetneqq \mathfrak{p}_1 \supsetneqq \cdots \supsetneqq \mathfrak{p}_n$. We get a sequence of closed sets of $\overline{Y}$ that we denote $Z_0 = Z_0' \subsetneqq Z_1' \subsetneqq \cdots \subsetneqq Z_n' \subset \overline{Y}$. As before, because $Z_i' \cap Y \neq \emptyset$ we conclude that $Z_0 \subsetneqq Z_1' \cap Y \subsetneqq \cdots \subsetneqq Z_n' \cap Y$, which gives $n \leq m$. We conclude that $\operatorname{codim}_{A(\overline{Y})}(\mathfrak{m}) = n$. On the other hand, since $\mathfrak{m}$ is a maximal ideal it is clearly the image of an ideal $(x - a_1, \ldots, x - a_n) \lhd k[x_1, \ldots, x_n]$

in $A(\overline{Y})$ and so $\dim_k(A(\overline{Y})/\mathfrak{m}) = \text{tr.deg.}_k(k) = 0$. Now Theorem 2 applied to $B = A(\overline{Y})$ gives $\dim(\overline{Y}) = \dim(A(\overline{Y})) = n$.

□

2.6. **A Further Algebraic Result.**

THEOREM **3. (Krull's Hauptidealsatz)** *Let R be a finitely generated k-algebra. Let $f \in R$ be an element which in neither a unit nor a zero-divisor then every minimal prime ideal $\mathfrak{p}$ containing f has codimension 1.*

Corollary 2.27. *Let $f \in k[x_1, \dots, x_n]$ be a non-constant polynomial then every irreducible component of $\mathcal{Z}(f)$ is a* **hypersurface***, i.e., a variety of dimension $n-1$.*

Remark 2.28. It is easy to prove this corollary directly. Let $\mathfrak{p}$ be a minimal prime ideal containing f. Then, $\mathfrak{p}$ contains one of the irreducible factors g of f. Then, $\mathfrak{p} \supseteq \langle g \rangle \supseteq \langle f \rangle$, and, by minimality $\mathfrak{p} = \langle g \rangle$. That is, the minimal prime ideals containing f correspond to the distinct irreducible polynomials dividing f. The ideal $\langle g \rangle$ has codimension 1. That is, there is no non-zero prime ideal $\mathfrak{q}$ properly contained in $\langle g \rangle$. If $0 \neq \mathfrak{q} \subsetneq \langle g \rangle$, take a non-zero element of $\mathfrak{q}$. It must be of the form $g^n h$, where $g \nmid h$ and $n \geq 1$. Since $g \notin \mathfrak{q}$, also $g^n \notin \mathfrak{q}$ and so $h \in \mathfrak{q}$. But, $h \in \langle g \rangle$ and so $g | h$. This is an absurd.

Remark 2.29. In fact, one can prove that every hypersurface, namely, every variety of codimension 1, is the zero set of a polynomial.

3. Projective Varieties

3.1. **Graded Rings.**

Definition 3.1. A **graded ring** R is a commutative associative ring with 1, together with a decomposition $R = \oplus_{d\geq 0} R_d$, where each R_d is an abelian group, and for every i, j we have $R_i R_j = R_{i+j}$.

The elements of R_d are called **homogenous of weight** d.

Example 3.2. $R = k[x_1, \dots, x_n]$ and for every d we let R_d be the homogenous polynomials of degree d.

Definition 3.3. An ideal $\mathfrak{a} \triangleleft R$, R a graded ring, is called a **homogenous ideal** if $\mathfrak{a} = \oplus_{d\geq 0}(\mathfrak{a} \cap R_d)$.

LEMMA **1.**

1. *The intersection, sum, product and radical of homogenous ideals are homogenous.*
2. *An ideal $\mathfrak{a}$ is homogenous if and only if $\mathfrak{a}$ is generated by homogenous elements.*
3. *A homogenous ideal $\mathfrak{a}$ is a radical ideal if and only if for each homogenous element f we have $f^n \in \mathfrak{a} \Rightarrow f \in \mathfrak{a}$.*
4. *A homogenous ideal $\mathfrak{a}$ is prime if and only if for any two homogenous elements f, g we have $fg \in \mathfrak{a}$ implies $f \in \mathfrak{a}$ or $g \in \mathfrak{a}$.*
5. *If $\mathfrak{a}$ is a homogenous ideal then $R/\mathfrak{a}$ has a natural grading.*

Proof. See [Mat] or [ZS]. Most text books leave it as an exercise. □

3.2. **Conical Sets.**

Definition 3.4. We call an algebraic set $Y \subset \mathbb{A}^n$ **conical** if $y \in Y$ implies $\alpha y \in Y$ for all $\alpha \in k$. See Figure 7.

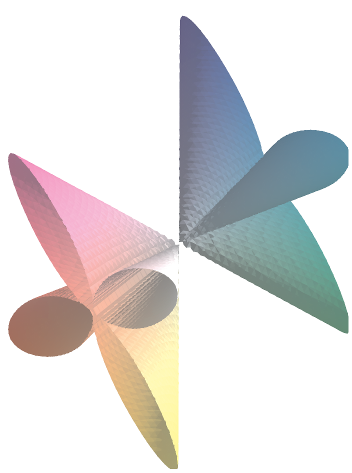


Figure 7. A Conical set

Lemma 3.5. *There is a one-one correspondence between homogenous ideals of the ring $k[x_1, \dots, x_n]$ and conical algebraic subsets of $\mathbb{A}^n$.*

Proof. Let $\mathfrak{a}$ be a homogenous ideal, then $\mathfrak{a}$ is generated by homogenous elements. Since $k[x_1, \dots, x_n]$ is noetherian, every ideal is finitely generated so $\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\{f_1, \dots, f_r\})$ for some homogenous polynomials. Let $y \in \mathcal{Z}(\{f_1, \dots, f_r\})$ then for every i we have $f_i(\alpha y) = \alpha^{\deg(f_i)} f_i(y) = 0$. Thus, $\alpha y \in \mathcal{Z}(\{f_1, \dots, f_r\})$ and we conclude that $\mathcal{Z}(\mathfrak{a})$ is a conical set.

Conversely, let Z be a conical set and let $f = f_0 + \cdots + f_d \in \mathcal{I}(Z)$, where f_i is homogenous of weight i. Let $y \in Z$ and consider the function $g : k \to k$ given by $g(\alpha) := f(\alpha y) = f_0(y) + \alpha f_1(y) \cdots + \alpha^d f_d(y)$. It is a polynomial of degree d in the variable α, which is identically zero. Thus, $f_0(y) = \cdots = f_d(y) = 0$ for all $y \in Z$. We conclude that $f_i \in \mathcal{I}(Z)$ for every $0 \leq i \leq d$. That is, $\mathfrak{a}$ is a homogenous ideal. $\square$

END OF LECTURE 3 (September 12)

3.3. **Projective Space.** Define an equivalence relation on $\mathbb{A}^{n+1}$ by

$$(a_0, a_1, \dots, a_n) \sim (\lambda a_0, \lambda a_1, \dots, \lambda a_n),$$

for any $\lambda \in k^\times$. We denote the equivalence class of $(a_0, a_1, \dots, a_n)$ by

$$(a_0 : a_1 : \cdots : a_n).$$

Definition 3.6. The **projective** ***n*****-space over** k, $\mathbb{P}^n = \mathbb{P}^n_k = \mathbb{P}^n(k)$, is the set

$$(\mathbb{A}^{n+1} - \{0\})/\sim \; = \; \{(a_0 : a_1 : \cdots : a_n) \mid (a_0, a_1, \dots, a_n) \in \mathbb{A}^{n+1} - \{0\}\}.$$

We note that the elements of $\mathbb{P}^n$ correspond to lines in $\mathbb{A}^{n+1}$ passing through the origin (Figure 8).

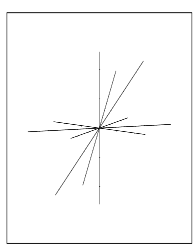


Figure 8. Lines through the origin

3.4. **Algebraic Sets in $\mathbb{P}^n$.** Let

$$S = k[x_0, \dots, x_n]$$

be the polynomial ring in $n+1$ variables. It is a graded ring, graded by degree. For every homogenous ideal $\mathfrak{a} \lhd S$ we let

$$\mathcal{Z}(\mathfrak{a}) = \{(a_0 : a_1 : \cdots : a_n) \in \mathbb{P}^n \mid f(a_0, a_1, \dots, a_n) = 0, \forall \text{ homogenous } f \in \mathfrak{a}\}.$$

It is the set of common solutions to all homogenous polynomials in $\mathfrak{a}$. Note that the condition $f(a_0 : a_1 : \cdots : a_n) = 0$ is well defined i.e., is independent of the representative, when f is homogenous.

Conversely, for any set $Y \subseteq \mathbb{P}^n$ let

$$\mathcal{I}(Y) = \langle f \in S \mid f \text{ homogenous and } f(a_0, a_1, \dots, a_n) = 0, \forall (a_0 : a_1 : \cdots : a_n) \in Y \rangle.$$

It is the (homogenous) ideal generated by all homogenous polynomials vanishing identically on Y.

Let S^+ denote the ideal $\langle x_0, \dots, x_n \rangle$. It is called the **irrelevant ideal**. Note that both $\mathcal{Z}(S^+)$ and $\mathcal{Z}(S)$ are the empty set.

Theorem 3.7. (The Fundamental Theorem) *There is* $1\colon 1$ *inclusion-reversing correspondence between closed sets in* $\mathbb{P}^n$ *and homogenous radical ideals different from the irrelevant ideal* S^+*. The correspondence is given by*

$$Y \mapsto \mathcal{I}(Y), \qquad \mathfrak{a} \mapsto \mathcal{Z}(\mathfrak{a}).$$

Under this correspondence, irreducible closed sets correspond to homogenous prime ideals. We have

$$\mathcal{Z}(\mathfrak{a}) \cup \mathcal{Z}(\mathfrak{b}) = \mathcal{Z}(\mathfrak{a} \cap \mathfrak{b}), \qquad \mathcal{Z}(\mathfrak{a}) \cap \mathcal{Z}(\mathfrak{b}) = \mathcal{Z}(\sqrt{\mathfrak{a} + \mathfrak{b}}),$$

unless $\mathcal{Z}(\mathfrak{a}) \cap \mathcal{Z}(\mathfrak{b}) = \emptyset$ *where we may need to replace* $\sqrt{\mathfrak{a} + \mathfrak{b}}$ *by* S*. In particular, the closed sets define a topology on* $\mathbb{P}^n$*, called the* **Zariski topology***.*

Proof. The proof is very similar to the proof of Theorem 2.15 making use of Lemma 1. $\square$

An irreducible non-empty algebraic set in $\mathbb{P}^n$ is called a **projective variety**; a non-empty open subset of a projective variety is called a **quasi-projective variety**.

3.5. **The Relation to Conical Sets.** Define the **conical complement** of a conical set Y in $\mathbb{A}^{n+1}$ to be $\{0\} \cup (\mathbb{A}^{n+1} \setminus Y)$. We define now an association between conical algebraic sets in $\mathbb{A}^{n+1}$ and algebraic sets in $\mathbb{P}^n$. Given a conical algebraic set Y define a set $\mathcal{P}(Y) \subset \mathbb{P}^n$ by

$$\mathcal{P}(Y) = \{(a_0 : a_1 : \cdots : a_n) \mid (a_0, a_1, \dots, a_n) \in Y \setminus \{0\}\}.$$

Given a closed algebraic set Z in $\mathbb{P}^n$ we associate to it a conical set $C(Z)$ as follows:

$$C(Z) = \{(a_0, a_1, \dots, a_n) \in \mathbb{A}^{n+1} \mid (a_0 : a_1 : \cdots : a_n) \in Z\} \cup \{0\}.$$

The proof of the following Proposition is immediate.

Proposition 3.8. *The correspondence* $Z \mapsto C(Z), Y \mapsto \mathcal{P}(Y)$ *is a* $1:1$ *correspondence between non-empty conical sets in* $\mathbb{A}^{n+1}$ *and subsets of* $\mathbb{P}^n$*. This correspondence respect intersections, unions and complements.*

Proposition 3.9. *Let* Y *be a non-empty algebraic set in* $\mathbb{P}^n$*. Then*

$$\mathcal{I}(Y) = \mathcal{I}(C(Y)).$$

In particular, the correspondence in Proposition 3.8 takes algebraic sets to algebraic sets.

Proof. The homogenous ideal $\mathcal{I}(Y)$ is generated by the homogenous polynomials f such that $f(a_0 : \cdots : a_n) = 0$ for all $(a_0 : \cdots : a_n) \in Y$. It follows that $f(a_0, \dots, a_n) = 0$ and also $f(0, \dots, 0) = 0$. Hence, $f \in \mathcal{I}(C(Y))$.

Conversely, since $\mathcal{I}(C(Y))$ is a homogenous ideal by Lemma 3.5, it is generated by homogenous polynomials. Let f be a homogenous polynomial in $\mathcal{I}(C(Y))$. Then for every $(a_0, \dots, a_n) \in C(Y)$ we have $f(a_0 : \cdots : a_n) = 0$. That is, $f \in \mathcal{I}(\mathcal{P}(C(Y))) = \mathcal{I}(Y)$. $\square$

Using the last two propositions one can get another proof of Theorem 3.7.

Definition 3.10. Let $Y \subset \mathbb{P}^n$ be an algebraic set defined by a homogenous radical ideal $\mathfrak{a}$. The **homogenous coordinate ring** of Y is $S(Y) = k[x_0, \dots, x_n]/\mathfrak{a}$.

Note that $S(Y) = A(C(Y))$ and hence $\dim(S(Y)) = \dim(Y) + 1$.

3.6. **Affine Chart on $\mathbb{P}^n$.** So far we have considered $\mathbb{P}^n$ from the perspective of a quotient of $\mathbb{A}^{n+1} \setminus \{0\}$ by $k^\times$. Now, we want to view $\mathbb{P}^n$ as composed of $n+1$ overlapping copies of $\mathbb{A}^n$. We define open sets $U_0, \dots, U_n$ of $\mathbb{P}^n$ by

$$U_i = \{(a_0 : \cdots : a_n) | a_i \neq 0\}.$$

Note that $\mathbb{P}^n \setminus U_i = \mathcal{Z}(x_i)$ so U_i is indeed open. Furthermore,

$$\mathbb{P}^n = \bigcup_{i=0}^{n} U_i.$$

Proposition 3.11. *Fix i, $0 \leq i \leq n$, and define a map*

$$\psi_i : \mathbb{A}^n \to U_i,$$

by

$$\psi(a_1, \dots, a_n) = (a_1, \dots, a_{i-1}, 1, a_i, \dots, a_n).$$

Then ψ_i is a homeomorphism.

Proof. We assume to simplify notation that $i = 0$. The map ψ_0 is given by

$$\psi_0 : \mathbb{A}^n \to \mathbb{P}^n, \qquad \psi_0(a_1, \dots, a_n) = (1, a_1, \dots, a_n).$$

We define a map

$$\varphi_0 : U_0 \to \mathbb{A}^n, \qquad \varphi_0(a_0 : a_1 : \cdots : a_n) = \left(\frac{a_1}{a_0}, \dots, \frac{a_n}{a_0}\right).$$

We note that φ_0 is well defined and is an inverse of ψ_0.

Given a polynomial $f \in k[x_1, \dots, x_n]$ define the homogenization F_f of f by

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

Here $\deg(f)$ means the maximal degree of a monomial of f. (For example, if $f(x_1, x_2) = x_1 + x_1^3 + x_1x_2$ then $F_f(x_0, x_1, x_2) = x_0^3(\frac{x_1}{x_0} + (\frac{x_1}{x_0})^3 + \frac{x_1}{x_0}\frac{x_2}{x_0}) = x_0^2 x_1 + x_1^3 + x_0x_1x_2$.) We remark that F_f is a homogenous polynomial in the variables $x_0, \dots, x_n$ and $F_f(1 : x_1 : \cdots : x_n) = f(x_1, \dots x_n)$.

Lemma 3.12. *The map φ_0 is continuous. In fact,*

$$\psi_0(\mathcal{Z}(\mathfrak{a})) = \mathcal{Z}(\langle F_f : f \in \mathfrak{a}\rangle) \cap U_0.$$

Proof. If $(x_1, \dots x_n) \in \mathcal{Z}(\mathfrak{a})$ then $F_f(\psi_0(x_1, \dots x_n)) = F_f(1 : x_1 : \cdots : x_n) = f(x_1, \dots, x_n) = 0$. This shows that $\psi_0(\mathcal{Z}(\mathfrak{a})) \subset \mathcal{Z}(\langle F_f : f \in \mathfrak{a}\rangle) \cap U_0$.

Conversely, let $(a_0 : \cdots : a_n) \in \mathcal{Z}(\langle F_f : f \in \mathfrak{a}\rangle) \cap U_0$. Then $a_0 \neq 0$ and for any $f \in \mathfrak{a}$ we have $f(a_1/a_0, \dots, a_n/a_0) = F_f(1, a_1/a_0, \dots, a_n/a_0) = 0$ because $F_f(a_0 : \cdots : a_n) = 0$. That is, $(a_1/a_0, \dots, a_n/a_0) \in \mathcal{Z}(\mathfrak{a})$ and $\psi_0(a_1/a_0, \dots, a_n/a_0) = (1 : a_1/a_0 : \cdots : a_n/a_0) = (a_0 : a_1 : \cdots : a_n)$. Therefore, $\psi_0(\mathcal{Z}(\mathfrak{a})) \supset \mathcal{Z}(\langle F_f : f \in \mathfrak{a}\rangle) \cap U_0$. $\square$

Given a homogenous polynomial $F \in k[x_0, \dots, x_n]$ define a polynomial $f_F \in k[x_1, \dots, x_n]$ by $f_F(x_1, \dots, x_n) = F(1, x_1, \dots, x_n)$. (For example, if $F(x_0, x_1, x_2) = x_0^2 x_1 + x_0 x_1 x_2$ then $f_F(x_1, x_2) = x_1 + x_1 x_2$. Note that $F_{f_F} \neq F$ though $f_{F_f} = F$.)

Lemma 3.13. *The map ψ_0 is continuous. In fact,*

$$\varphi_0(\mathcal{Z}(\mathfrak{a}) \cap U_0) = \mathcal{Z}(\langle f_F : F \in \mathfrak{a}, F \textit{ homogenous}\rangle).$$

Proof. Let $(a_1, \dots, a_n) \in \mathcal{Z}(\langle f_F : F \in \mathfrak{a}, F \text{ homogenous}\rangle)$. To show

$$\varphi_0(\mathcal{Z}(\mathfrak{a}) \cap U_0) \supset \mathcal{Z}(\langle f_F : F \in \mathfrak{a}, F \text{ homogenous}\rangle)$$

it is enough to show that $(1, a_1, \dots, a_n) \in \mathcal{Z}(\mathfrak{a}) \cap U_0$. Indeed, let $F \in \mathfrak{a}$ a homogenous polynomial. Then $F(1, a_1, \dots, a_n) = f_F(a_1, \dots, a_n) = 0$.

Conversely, let $(1 : b_1 : \dots : b_n) \in \mathcal{Z}(\mathfrak{a}) \cap U_0$. Then $f_F(b_1, \dots, b_n) = F(1, b_1, \dots, b_n) = 0$ so $(b_1, \dots, b_n) \in \mathcal{Z}(\langle f_F : F \in \mathfrak{a}, F \text{ homogenous}\rangle)$. ☐

This concludes the proof of the Proposition. ☐

Remark 3.14. The arguments above show that if $Z = \mathcal{Z}(\mathfrak{a}) \subset \mathbb{A}^n$ is an algebraic set then the closure of $\psi_0(Z)$ is $\mathcal{Z}(\langle F_f : f \in \mathfrak{a}\rangle)$.

Caveat 3.15. If $\mathfrak{a} = \langle f_1, \dots, f_r\rangle$ is an ideal of $k[x_1, \dots, x_n]$ then it need not be true that $\langle F_f : f \in \mathfrak{a}\rangle = \langle F_{f_1}, \dots, F_{f_r}\rangle$. Here is an example: Let $\mathfrak{a} = \langle x_1, x_2 - x_1^2\rangle$ then $\mathcal{Z}(\mathfrak{a}) = \{(0, 0)\}$, which maps to the point $(1, 0, 0)$ in $\mathbb{P}^2$ and therefore the closure $\overline{\mathcal{Z}(\mathfrak{a})}$ in $\mathbb{P}^2$ is still just $(1, 0, 0)$. On the other hand, let $\mathfrak{b} = \langle F_{x_1}, F_{x_2 - x_1^2}\rangle = \langle x_1, x_0 x_2 - x_1^2\rangle$ then $\mathcal{Z}(\mathfrak{b})$ has two points[8], easily calculated to be $\{(1 : 0 : 0), (0 : 0 : 1)\}$. See Figure 9.

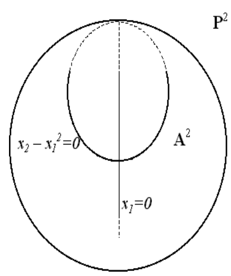


Figure 9.

For another example consider the **twisted cubic curve** T in $\mathbb{A}^3$, given parametrically as (t, t^2, t^3). It is defined by the ideal $\langle x_1 x_2 - x_3, x_1^2 - x_2\rangle$. The zero set Z of the ideal $\langle x_1 x_2 - x_0 x_3, x_1^2 - x_0 x_2\rangle$ in $\mathbb{P}^3$ is in fact reducible and thus cannot be the closure of T. Consider therefore the ideal $\langle x_1 x_2 - x_0 x_3, x_1^2 - x_0 x_2, x_2^2 - x_1 x_3\rangle$ and the zero set $Z' \subset Z$ it defines. One can verify that $\overline{T} = Z' = T \cup \{(0, 0, 0, 1)\}$ and $Z = Z' \cup C$, where C is isomorphic to $\mathbb{P}^1$.

Let us look at the structure of $\overline{T}$ around the point added at infinity: the point $(0, 0, 0, 1)$. It has non-zero x_3 coordinate and therefore we may study the situation using affine coordinates via U_3, ψ_3, φ_3. The intersection $\overline{T} \cap U_3$ is the zero set of the ideal

$$\mathfrak{c} = \langle x_1 x_2 - x_0, x_1^2 - x_0 x_2, x_2^2 - x_1\rangle$$

[8]Note that the cardinality can be deduced from Bezout's theorem!

in $\mathbb{A}^3$ with coordinates x_0, x_1, x_2. Since $\overline{T}$ is irreducible so is $\overline{T} \cap U_3$, and hence the ideal $\mathfrak{c}$ is prime. Note that in agreement with this, $k[x_0, x_1, x_2]/\mathfrak{c} \cong k[x_1, x_2]/\langle x_1 - x_2^2 \rangle \cong k[x_2]$. Furthermore, we see that $\overline{T} \cap U_3$ is isomorphic[9] to the affine line by the map $t \mapsto (t^3, t^2, t)$.

Remark 3.16. Another picture of $\mathbb{P}^n$ is obtained as follows. Via the map ψ_0 we view $\mathbb{A}^n$ as a subset of $\mathbb{P}^n$. The complement, consisting of the vectors $\{(0 : a_1 : \cdots : a_n) \mid \exists i, a_i \neq 0\}$ is naturally identified with $\mathbb{P}^{n-1}$. And so, recursively, we find:

$$\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{A}^{n-1} \cup \cdots \cup \mathbb{A}^0.$$

(Where $\mathbb{A}_0$ is just a one pointed space, associated to k - "the ring of polynomials is zero variables".)

3.7. **The Grassmannian.** The Grassmann variety is a projective variety. It, and its generalizations, had turned out to play a pivotal role in many important constructions in algebraic geometry. Incidence varieties, here meaning a closed subset of a product of two Grassmann varieties, are among these generalizations.

Let V be a vector space over k of dimension $n \geq 2$. Let $1 \leq d \leq n-1$ be an integer. The **Grassmann variety** (or **Grassmannian**) **Grass**(d, V) is a projective variety whose points are in a natural bijection with the set $G(d, V)$ of d-dimensional subspaces of V.

Consider the k-vector space $\bigwedge^d V$ of dimension $\binom{n}{d}$ (isomorphic to $\mathbb{A}^{\binom{n}{d}}$). We define a map

$$P : G(d, V) \to \mathbb{P}(\bigwedge^d V).$$

This map is called the **Plücker map** and is given as follows: Let $W \in G(d, V)$ be a subspace and let $v_1, \dots, v_d$ be a basis for W. Let

$$P(W) = v_1 \wedge \cdots \wedge v_d.$$

Note that this is well defined: if $v_1', \dots, v_d'$ is another basis for W then $v_1' \wedge \cdots \wedge v_d'$ is proportional to $v_1 \wedge \cdots \wedge v_d$. We note that the map P is **injective**. This follows from the observation that

$$W := \{v \in V : v \wedge P(W) = 0\}.$$

Hence, via P we realized $G(d, V)$ as a subset of the projective space $\mathbb{P}(\bigwedge^d V)$ of dimension $\binom{n}{d} - 1$. Our goal is to show that this set is an algebraic set, hence providing $G(d, V)$ with the structure of an algebraic variety.

Remark 3.17. We can make the situation much more explicit. Choose a basis $e_1, \dots, e_n$ for V, then

$$\{e_{i_1} \wedge \cdots \wedge e_{i_d} \mid i_1 < \cdots < i_d\}$$

is a basis to $\bigwedge^d V$. We shall use the notation $e_{i_1 \dots i_d}$ for $e_{i_1} \wedge \cdots \wedge e_{i_d}$. If

$$W = \mathrm{Span}\langle v_1, \dots, v_d \rangle$$

and $v_j = \sum_{i=1}^n a_{ij} e_i$ then $P(W) = v_1 \wedge \cdots \wedge v_d$ has coordinates (called the Plücker coordinates) equal to the $\binom{n}{d}$ maximal minors of the matrix $(a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq d}}$.

[9]We will define this notion precisely in the next lecture.

To illustrate we give two examples:

Example 3.18. Suppose that $d = 1$. Then $W = \mathrm{Span}\langle v_1\rangle$, where $v_1 = a_1e_1 + \cdots + a_ne_n$ and the Plücker coordinates are the maximal minors of the matrix $(a_1, \ldots, a_n)$ that is, $(a_1 : \cdots : a_n)$ and we get that $\mathbf{Grass}(1, n) \cong \mathbb{P}^{n-1}$.

Example 3.19. Suppose that $n = 4$ and $k = 2$. Let e_1, e_2, e_3, e_4 be a basis for V. Then $(e_1 \wedge e_2, e_1 \wedge e_3, e_1 \wedge e_4, e_2 \wedge e_3, e_2 \wedge e_4, e_3 \wedge e_4)$ is a basis for $\bigwedge^2 V$. Let

$$W = \mathrm{Span}\langle v_1, v_2\rangle,$$

where

$$v_1 = a_{11}e_1 + a_{21}e_2 + a_{31}e_3 + a_{41}e_4, \quad v_2 = a_{12}e_1 + a_{22}e_2 + a_{32}e_3 + a_{42}e_4.$$

We calculate that

$$\begin{aligned} v_1 \wedge v_2 = {} & (a_{11}a_{22} - a_{12}a_{21})e_1 \wedge e_2 + (a_{11}a_{32} - a_{31}a_{12})e_1 \wedge e_3 \\ & + (a_{11}a_{42} - a_{41}a_{12})e_1 \wedge e_4 + (a_{21}a_{32} - a_{31}a_{22})e_2 \wedge e_3 \\ & + (a_{21}a_{42} - a_{41}a_{22})e_2 \wedge e_4 + (a_{31}a_{42} - a_{41}a_{32})e_3 \wedge e_4. \end{aligned} \tag{1}$$

We get that

(2)

$$\begin{aligned} P(W) = (& a_{11}a_{22} - a_{12}a_{21}, a_{11}a_{32} - a_{31}a_{12}, \\ & a_{11}a_{42} - a_{41}a_{12}, a_{21}a_{32} - a_{31}a_{22}, a_{21}a_{42} - a_{41}a_{22}, a_{31}a_{42} - a_{41}a_{32}). \end{aligned}$$

Proposition 3.20. *The image $P(G(d, n))$ of $G(d, n)$ under the Plücker map is an algebraic subset of $\mathbb{P}(\bigwedge^d V)$. We denote it by* **Grass**(d, n) *and call it the* **Grassmann variety** *of d-dimensional subspaces.*

END OF LECTURE 4 (September 17)

Lemma 3.21. *An element $w \in \bigwedge^d V$ is of the form $w = v \wedge \alpha$ for some non-zero $v \in V$ and $\alpha \in \bigwedge^{d-1} V$ if and only if $v \wedge w = 0$.*

Proof. Choose a basis $e_1, \ldots, e_n$ of V with $e_1 = v$. Write w in the form

$$w = \sum_{i_1 < \cdots < i_d} a_{i_1,\ldots,i_d} e_{i_1,\ldots,i_d}$$

and

$$v \wedge w = \sum_{i_1 < \cdots < i_d} a_{i_1,\ldots,i_d} e_1 \wedge e_{i_1,\ldots,i_d}$$

which is zero iff for every $i_1 < \cdots < i_d$ such that $1 < i_1$ we have $a_{i_1,\ldots,i_d} = 0$. $\square$

The same argument shows the following lemma (the case $\ell = 1$ of which is the previous lemma):

$\mathbb{LEMMA}$ **2.** *Let $w \in \bigwedge^d V$ and*

$$\varphi_w : V \to \bigwedge^{d+1} V$$

be the linear map given by

$$\varphi_w(v) = v \wedge w.$$

Then $w = v_1 \wedge \cdots \wedge v_\ell \wedge \alpha$ *for some linearly independent* $v_1, \ldots, v_\ell \in V$ *and* $\alpha \in \bigwedge^{d-\ell} V$ *and only if* $\dim(\mathrm{Ker}(\varphi_w)) \geq \ell$.

Proof. (Of the Proposition) The set $P(G(d,n))$ is the set of totally decomposable vectors, which by Lemma 2, can be identified with the set of vectors w in $\bigwedge^d V$ such that $\dim(\mathrm{Ker}(\varphi_w)) \geq d$. Choosing coordinates on V, and hence on $\bigwedge^d V, \bigwedge^{d+1} V$, we can write every element $w \in \mathbb{P}(\bigwedge^d V)$ in coordinates and every linear map $\varphi \in \mathrm{Hom}(V, \bigwedge^{d+1} V)$ in coordinates. Moreover, if $\varphi = \varphi_w$ for $w \in \mathbb{P}(\bigwedge^d V)$ then these coordinates of φ are linear expressions in the coordinates of w.

The condition that the kernel of φ_w is of dimension greater or equal to d is equivalent to requiring that the image of φ_w is of dimension less or equal to $n-d$, which, in turn, is equivalent to requiring that in the matrix representation of φ_w all $n-d+1$ minors vanish. This is a collection of homogenous equations of degree $n-d+1$ in the coordinates of w. □

Example 3.22. We revisit Example 3.19. A basis for $\bigwedge^3 V$ is given by

$$e_1 \wedge e_2 \wedge e_3, e_1 \wedge e_2 \wedge e_4, e_1 \wedge e_3 \wedge e_4, e_2 \wedge e_3 \wedge e_4.$$

If we write

$$w = a_{12} e_1 \wedge e_2 + a_{13} e_1 \wedge e_3 + a_{14} e_1 \wedge e_4 + a_{23} e_2 \wedge e_3 + a_{24} e_2 \wedge e_4 + a_{34} e_3 \wedge e_4,$$

then φ_w is represented by the matrix

$$A = \begin{pmatrix} a_{23} & -a_{13} & a_{12} & 0 \\ a_{24} & -a_{14} & 0 & a_{12} \\ a_{34} & 0 & -a_{14} & a_{13} \\ 0 & a_{34} & -a_{24} & a_{23} \end{pmatrix}.$$

The variety $\mathbf{Grass}(2,4)$ is defined by the ideal whose generators are all 3×3 sub determinants of A. Namely, by the entries of the matrix $Adj(A)$. It comes out the ideal

$$\begin{aligned} I = (&a_{14}^2 a_{23} - a_{14} a_{13} a_{24} + a_{34} a_{12} a_{14}, -a_{13} a_{14} a_{23} + a_{13}^2 a_{24} - a_{34} a_{12} a_{13}, \\ &- a_{13} a_{12} a_{24} + a_{14} a_{12} a_{23} + a_{34} a_{12}^2, a_{24} a_{14} a_{23} - a_{13} a_{24}^2 + a_{34} a_{12} a_{24}, \\ &- a_{14} a_{23}^2 + a_{23} a_{13} a_{24} - a_{34} a_{12} a_{23}, -a_{13} a_{12} a_{24} + a_{14} a_{12} a_{23} + a_{34} a_{12}^2, \\ &- a_{24} a_{13} a_{34} + a_{34} a_{14} a_{23} + a_{12} a_{34}^2, -a_{14} a_{23}^2 + a_{23} a_{13} a_{24} - a_{34} a_{12} a_{23}, \\ &a_{13} a_{14} a_{23} - a_{13}^2 a_{24} + a_{34} a_{12} a_{13}, -a_{24} a_{13} a_{34} + a_{34} a_{14} a_{23} + a_{12} a_{34}^2, \\ &- a_{24} a_{14} a_{23} + a_{13} a_{24}^2 - a_{34} a_{12} a_{24}, a_{14}^2 a_{23} - a_{14} a_{13} a_{24} + a_{34} a_{12} a_{14}) \end{aligned}$$

However, this ideal is not a radical ideal. Its radical is the ideal

$$\sqrt{I} = (a_{23} a_{14} - a_{24} a_{13} + a_{12} a_{34}).$$

It's a theorem that the Grassmann variety $G(d,n)$ is always defined by a collection of quadratic polynomials.

3.7.1. *Affine neighborhoods.* We now describe affine subsets in the Grassmannian which are isomorphic to affine spaces.

Let $\Gamma \subset V$ be a fixed subspace of dimension $n-d$ and let $\lambda = P(\Gamma) \in \mathbb{P}(\bigwedge^{n-d} V)$ be its image under the Plücker map. We view λ as a linear form on $\mathbb{P}(\bigwedge^d V)$ as follows: given an element $v \in \bigwedge^d V$ we get an element $\lambda(v) := v \wedge \lambda \in \bigwedge^n V \cong k$. One checks that whether $\lambda(v) = 0$ or not is well defined and moreover writing everything in coordinates, λ is a homogenous polynomial of degree 1. We let

$$U = \mathbb{P}\left(\bigwedge^d V\right) \setminus \mathcal{Z}(\lambda),$$

an open set isomorphic to an affine space. We let

$$U_\Gamma = U \cap \mathbf{Grass}(d, n).$$

We note that

$$\begin{aligned} U_\Gamma &= \{P(W) : W \in G(d, n), P(W) \wedge \lambda \neq 0\} \\ &= \{P(W) : W \in G(d, n), V = W \oplus \Gamma\}. \end{aligned}$$

Fix some splitting $V = W_0 \oplus \Gamma$, and so an isomorphism $W_0 \cong V/\Gamma$, then we get the identification

$$U_\Gamma \cong \mathrm{Hom}(V/\Gamma, \Gamma);$$

the bijection is given by associating to $\varphi \in \mathrm{Hom}(V/\Gamma, \Gamma)$ its graph $W = (t, \varphi(t))$. Moreover, one can verify that the identification $U_\Gamma \cong \mathrm{Hom}(V/\Gamma, \Gamma) \cong k^{d(n-d)}$ respects the Zariski topology. Namely

$$U_\Gamma \cong \mathbb{A}^{d(n-d)}.$$

Here is a more explicit description. Fix a basis $e_1, \dots, e_n$ to V such that Γ is the span of $e_{d+1}, \dots e_n$. The subspaces W mapped to U_Γ are precisely those that have a basis $v_1, \dots, v_d$ with $v_j = \sum_{i=1}^n a_{ij} e_i$ such that the first $d \times d$ minor of (a_{ij}) is not zero. Since $P(W)$ does not depend on the choice of basis we may assume that the basis $v_1, \dots, v_d$ is chosen so that

$$(a_{ij}) = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ b_{1,1} & \cdots & b_{1,d} \\ \vdots & & \vdots \\ b_{n-d,1} & \cdots & b_{n-d,d} \end{pmatrix} \tag{3}$$

The Plücker coordinates, given by all $d \times d$ minors, are identified with the set of *all* sub determinant of (b_{ij}). Clearly the 1×1 minors determine the rest; this shows again that $U_\Gamma \cong \mathbb{A}^{d(n-d)}$.

To illustrate:

- If $d = 1$ then the matrix in (3) is just ${}^t(b_1, \dots, b_{n-1})$ and $U_\Gamma = \{(1, b_1, \dots, b_{n-1})\} \cong \mathbb{A}^{n-1} \subset \mathbb{P}^{n-1} = \mathbb{P}(V)$.
- If $d = 2$ and $n = 4$ (as in Examples 3.19 and 3.22) then the matrix in (3) is

$$\begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix}$$

  and $U_\Gamma = \{(1, b_{1,2}, b_{2,2}, b_{1,1}, b_{2,1}, b_{1,1}b_{2,2} - b_{1,2}b_{2,1})\}$. This is the variety in $\mathbb{A}^5 \subset \mathbb{P}^5$ defined by

$$x_5 = x_1 x_4 - x_2 x_3.$$

As each U_Γ is dense and irreducible, one consequence of this is

Corollary 3.23. *The Grassmann variety* $\mathbf{Grass}(d, n)$ *is an irreducible variety.*

4. Regular Functions and Morphisms

4.1. **The Sheaf of Regular Functions.** Let $Y \subseteq \mathbb{A}^n$ be a quasi-affine variety. We say that a function

$$h \colon Y \to k$$

is **regular at a point** P of Y if there exists an open set $U \subseteq Y$ such that $P \in U$, and there exist $f, g \in k[x_1, \ldots, x_n]$ such that $g(u) \neq 0$ for all $u \in U$ and

$$h|_U = \frac{f}{g}|_U.$$

The function h is called **regular** if it is regular at every point $P \in Y$.

Let $Y \subseteq \mathbb{A}^n$ be a quasi-affine variety and denote for every open non-empty set $U \subseteq Y$ (it is quasi-affine as well) by $\mathcal{O}(U)$ the ring of regular functions on U. Put also $\mathcal{O}(\emptyset) = \{0\}$. Then $\mathcal{O}$ is a **sheaf** in the Zariski topology on Y called the **sheaf of regular functions**. Namely:

(1) For every open sets $U \subseteq V$ we have the restriction homomorphism

$$\mathrm{res} : \mathcal{O}(V) \to \mathcal{O}(U).$$

(2) If $U = \cup U_i$ is an open cover and $f \in \mathcal{O}(U)$ satisfies $f|_{U_i} = 0$ for every i then $f = 0$.
(3) Given $f_i \in \mathcal{O}(U_i)$ such that $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$ for all i, j there exists $f \in \mathcal{O}(U)$ such that $f|_{U_i} = f_i$ for every i.

Example 4.1. Let $Y = \mathbb{A}^2$ and $U = Y \setminus \mathcal{Z}(y)$. Then $k[x, y] \subset \mathcal{O}(Y)$ but they are not equal; the function $x/y \in \mathcal{O}(U)$ and there is no function $f \in \mathcal{O}(Y)$ such that $f|_U = x/y$.

Lemma 4.2. *A regular function $h \colon Y \to \mathbb{A}^1$ is continuous.*

Proof. Let $Z \subset \mathbb{A}^1$ be a closed set. It is enough to prove that $h^{-1}(Z)$ is a closed set. We may assume that $Z \neq \mathbb{A}^1$ and hence is a finite set. Hence, we may assume that $Z = \{a\}$ and we need to show that $T := h^{-1}(a)$ is closed in Y.

Find an open cover $Y = \bigcup_\alpha Y_\alpha$ such that for every α we have $h|_{Y_\alpha} = f_\alpha/g_\alpha$. It is enough to prove that $T \cap Y_\alpha$ is closed in Y_α for all α. But

$$T \cap Y_\alpha = Z(f_\alpha - a \cdot g_\alpha) \cap Y_\alpha.$$

□

Remark 4.3. The function $h \colon \mathbb{A}^1 \to \mathbb{A}^1$ given by

$$h(x) = \begin{cases} x & x \neq 0, 1 \\ 0 & x = 1 \\ 1 & x = 0 \end{cases}$$

is continuous but not regular.

Let $Y \subseteq \mathbb{P}^n$ be a quasi-projective variety. A function

$$h \colon Y \to \mathbb{A}^1$$

is called **regular at a point** P of Y if there exists an open set $U \subseteq Y$ such that $P \in U$, and there exist homogenous polynomials $f, g \in k[x_0, \ldots, x_n]$ of the same degree such that $\mathcal{Z}(g) \cap U = \emptyset$ and

$$h|_U = \frac{f}{g}|_U.$$

(We remark that since f and g have the same degree f/g is a well defined function.) The function h is called **regular** if it is regular at every point $P \in Y$.

Again, we may prove that this gives a sheaf on Y called the **sheaf of regular functions** and that every regular function is continuous.

Remark 4.4. Let $\psi_0 \colon \mathbb{A}^n \to \mathbb{P}^n$ be the embedding $(a_1, \dots, a_n) \mapsto (1 : a_1 : \cdots : a_n)$. If U is a quasi-affine variety then $\psi_0(U)$ is a quasi-projective variety. The notion of a regular function on U agrees with the notion of a regular function on $\psi_0(U)$. This follows from the identities, valid on U,

$$f_G/f_H = G/H \text{ (dehomogenization)}, \quad x_0^{\deg(g)-\deg(f)} F_f/F_g = f/g \text{ (homogenization)}.$$

END OF LECTURE 5 (September 19)

We shall use the term **"variety"** to mean either a quasi-affine of a quasi-projective variety. Let Y be a variety and $P \in Y$. Define

$$\mathcal{O}_{Y,P} = \varinjlim_{U \ni P} \mathcal{O}(U)$$

to be the direct limit over all open sets containing P. Being a direct limit $\mathcal{O}_{Y,P}$ is a ring. We can represent an element of $\mathcal{O}_{Y,P}$ by a pair $(U, f/g)$ where U is an open set containing P and f, g are polynomials (homogenous of the same degree, if we are in the projective case). The couples $(U, f/g)$ and $(U', f'/g')$ are identified if on $U \cap U'$ we have the equality $f/g = f'/g'$. Using this description, addition and multiplication may be described as

$$(U, f/g) \pm (V, r/s) = (U \cap V, (fs \pm rg)/gs), \qquad (U, f/g) \cdot (V, r/s) = (U \cap V, fr/gs).$$

The ring $\mathcal{O}_{Y,P}$ is called the **local ring of** P **on** Y**.** The name is justified:

Lemma 4.5. *The ring $\mathcal{O}_{Y,P}$ is a local ring whose unique maximal ideal $\mathfrak{m}$ is the set $\{(U, f/g) : (f/g)(P) = 0\}$.*

Proof. The set $\mathfrak{m}$ is the kernel of the ring homomorphism of "evaluation at P":

$$(U, f/g) \mapsto (f/g)(P).$$

This is clearly a well-defined surjective ring homomorphism $\mathcal{O}_{Y,P} \to k$ and therefore $\mathfrak{m}$ is a maximal ideal.

To prove $\mathfrak{m}$ is the unique maximal ideal of $\mathcal{O}_{Y,P}$ it is (necessary and) sufficient to prove that every $x \notin \mathfrak{m}$ is a unit. Let $x = (U, f/g)$ be such an element. Then $f(P) \neq 0$. Consider the element of $\mathcal{O}_{Y,P}$ given by $(U \setminus \mathcal{Z}(f), g/f)$. It is the inverse of x. $\square$

Let Y be a variety and define

$$K(Y) = \varinjlim_{U \neq \emptyset} \mathcal{O}(U)$$

to be the direct limit over all non-empty open sets. The limit $K(Y)$ is a ring called the **field of rational functions** or the **function field** of Y. An argument similar to the one above shows that $K(Y)$ is a field.

Let $P \in Y$ and U and open set containing P. We have natural ring homomorphisms

$$\mathcal{O}(U) \to \mathcal{O}_{Y,P} \to K(Y)$$

that are in fact injections (and so it follows that $\mathcal{O}(U)$ and $\mathcal{O}_{Y,P}$ are integral domains). For example if $f \in U$ is zero in $\mathcal{O}_{Y,P}$, i.e., $(U, f) \sim (V, 0)$ for some open set V containing P then $f = 0$ on $U \cap V$, which is a non-empty, hence dense, open set of U and it follows that $f = 0$.

Theorem 4.6. *Let $Y \subseteq \mathbb{A}^n$ be an affine variety with affine coordinate ring $A(Y)$. Then:*

1. $\mathcal{O}(Y) \cong A(Y)$.
2. *There exists a bijection between maximal ideals of $A(Y)$ and points P on Y under which $P \mapsto \mathfrak{m}_P :=$ {functions vanishing at P} and $\mathfrak{m} \mapsto \mathcal{Z}(\mathfrak{m})$.*
3. $\mathcal{O}_{Y,P} \cong A(Y)_{\mathfrak{m}_P}$ *and* $\dim(\mathcal{O}_{Y,P}) = \dim Y$.
4. $K(Y) = \mathrm{Frac}(A(Y))$ *and, in particular, is a finitely generated field extension of k of transcendence degree equal to* $\dim(Y)$.

Proof. We have a natural injective ring homomorphism

$$A(Y) \to \mathcal{O}(Y).$$

Given an element $f \in A(Y)$ we get the regular function represented on each open set U by f itself.

There is a bijection between maximal ideals of $k[x_1, \dots, x_n]$ and points of $\mathbb{A}^n$. The maximal ideal corresponding to the point $(a_1, \dots, a_n)$ is $(x_1 - a_1, \dots, x_n - a_n)$. It induces a bijection between maximal ideals containing the ideal $I(Y)$ and points on Y. On the other hand, there is a bijection between maximal ideal containing $I(Y)$ and maximal ideals of $A(Y)$. Hence a bijection between maximal ideals of $A(Y)$ and points on Y.

The map $A(Y) \to \mathcal{O}(Y)$ induces a map [10]

$$A(Y)_{\mathfrak{m}_P} \to \mathcal{O}_{Y,P},$$

under which

$$\frac{f}{g} \mapsto (Y \setminus \mathcal{Z}(g), \frac{f}{g}).$$

[10] Recall the notion of localization [Eis, Chap. 2]: Let R be a commutative ring with 1. A set $U \subset R$ is called a multiplicative set if $1 \in U$ and $u, v \in U$ implies that $uv \in U$. For example, if $\mathfrak{p}$ is a prime ideal than $R \setminus \mathfrak{p}$ is a multiplicative set. If M is an R-module (e.g. R itself) we define the localization of M in U, $M[U^{-1}]$ to be the collection of equivalence classes of tuples (m, u) for $m \in M$ and $u \in U$ where two tuples $(m, u), (n, v)$ are equivalent if for some $w \in U$ we have $w(vm - un) = 0$. We shall also use the notation m/u for the equivalence class of (m, u). One easily verifies that $R[U^{-1}]$ is a ring and that $M[U^{-1}]$ is a $R[U^{-1}]$-module. There is a natural map

$$\phi : R \to R[U^{-1}].$$

A particular case of this construction is when R is an integral domain and $U = R \setminus \{0\}$. In this case $R[U^{-1}]$ is a field, called the **quotient field of** R and denoted $\mathrm{Frac}(R)$, and the map $R \to R[U^{-1}]$ is an injection.

Given an ideal J of R we get an ideal $JR[U^{-1}]$ of $R[U^{-1}]$. Given an ideal I of $R[U^{-1}]$ we get an ideal $\phi^{-1}(I)$ of R. This sets a bijection between prime ideals of R that do not intersect U and prime ideals of $R[U^{-1}]$. In particular, if $\mathfrak{p}$ is a prime ideal of R then $R_{\mathfrak{p}}$ is a local ring. It has a unique prime ideal equal to $\mathfrak{p}R_{\mathfrak{p}}$.

Lemma 4.7. *Let B be an integral domain then $B = \cap_{\mathfrak{m}} B_{\mathfrak{m}}$ (the intersection is over all maximal ideals and is taken in $Quot(B)$).*

Proof. The inclusion $\subseteq$ is clear. Take $f/g \in \cap_{\mathfrak{m}} B_{\mathfrak{m}}$ and define an ideal

$$I = \{r \in B : r \cdot \frac{f}{g} \in B\}.$$

Suppose that $I \neq B$ and choose a maximal ideal $\mathfrak{m} \lhd B$ such that $I \subseteq \mathfrak{m}$. Since $f/g \in B_{\mathfrak{m}}$ we can write $f/g = f'/g'$ for some $f' \in B$ and $g' \in B \setminus \mathfrak{m}$. But then $g' \in I \subseteq \mathfrak{m}$. A contradiction. □

This map is an isomorphism (note that all restriction maps are injective). We have

$$A(Y) \subseteq \mathcal{O}(Y) \subseteq \cap_{P\in Y}\mathcal{O}_{Y,P} = \cap_{\text{max'l ideals}} A(Y)_{\mathfrak{m}_P} = A(Y).$$

We get therefore that $A(Y) \cong \mathcal{O}(Y)$ and assertions (2), (4) (because $K(Y) = \mathrm{Frac}(\mathcal{O}(Y))$). The only thing left is to show that $\dim(Y) = \dim(\mathcal{O}_{Y,P})$.

We have $\dim(\mathcal{O}_{Y,P})$ equal to the length of a maximal chain of prime ideals of $A(Y)$ contained in P. Since $A(Y)$ is catenary this is equal to $\dim(A(Y)) = \dim(Y)$. □

4.2. **Morphisms.**

Definition 4.8. Let X and Y be varieties. A continuous function

$$f : X \to Y$$

is called a **morphism** if for every open set U and every regular function $g : U \to k$ the function $g \circ f : f^{-1}(U) \to k$ is regular.

We note the following consequences: for every point $P \in Y$ and $Q \in X$ such that $f(Q) = P$ we get an induced ring homomorphism

$$f^* : \mathcal{O}_{Y,P} \to \mathcal{O}_{X,Q}.$$

We get a ring homomorphism

$$\mathcal{O}(Y) \to \mathcal{O}(X).$$

We get a field homomorphism,

$$K(Y) \to K(X),$$

if for every non-empty open $U \subset Y$ also $f^{-1}(U)$ is not empty. Equivalently if $f(X)$ is dense in Y. Such a morphism is called a **dominant morphism**.

Definition 4.9. A morphism $f : X \to Y$ is an isomorphism if there exists a morphism $g : Y \to X$ such that $f \circ g = id_X$ and $g \circ f = id_Y$.

Example 4.10. *The d-uple embedding.* Let d and n be positive integers. Let $N = \binom{n+d}{n} - 1$ and let $M_0, \dots, M_N$ be the monomials of degree d in the variables $x_0, \dots, x_n$. We enumerate the monomials so that $M_i = x_i^d$ for $i = 0, \dots, n$, and the rest in some arbitrary way. Define the **d-uple embedding**

$$\varphi : \mathbb{P}^n \to \mathbb{P}^N, \qquad \varphi(a) = (M_0(a) : \cdots : M_N(a)).$$

First, note that this is a well defined function. If $a = (a_0 : \cdots : a_n)$ and, say, $a_i \neq 0$, then the $M_i(a) \neq 0$ and so the vector we wrote belongs to the projective space. Secondly, although the image is calculated using a choice of representative $(a_0, \dots, a_n)$ for a, the result is independent of this choice as all the M_i are homogenous of the same degree.

The function ϕ is a morphism. To see that, note first that if F is a homogenous polynomial in the variables $y_0, \dots, y_N$ then $\phi^*(F)(x_0, \dots, x_n) = F(M_0(x_0, \dots, x_n), \dots, M_N(x_0, \dots, x_n))$ which is a homogenous polynomial of degree $\deg(F) \cdot d$. This show that f^{-1} of a closed set is a closed set and so ϕ is continuous. If f is a regular function on an open set U of $\mathbb{P}^N$, we need to show that $\varphi^*(f)$ is a regular function on $f^{-1}(U)$. We may assume that f is given on U as a ratio F/G of two homogenous polynomials of the same degree, with G non-vanishing, and so $\varphi^*(f) = F(M_0(x_0, \dots, x_n), \dots, M_N(x_0, \dots, x_n))/G(M_0(x_0, \dots, x_n), \dots, M_N(x_0, \dots, x_n))$ is a ratio of two homogenous polynomials with non-vanishing denominator.

The morphism φ is injective. Given $a = (a_0 : \cdots : a_n)$ with $a_i \neq 0$, we may assume $a_i = 1$. If $\varphi(a) = \varphi(b)$ then the i-th coordinate over $\varphi(a)$ is 1 which is proportional to the i-th coordinate of $\varphi(b)$ which is b_i^d. So $b_i \neq 0$ and so we may assume $b_i = 1$. Then the coordinate of $\varphi(a)$ that corresponds to the homogenous polynomial $x_j x_i^{d-1}$ is a_j and similarly for b. We conclude $a = b$.

Let $\mathfrak{p}$ be the kernel of the ring homomorphism

$$k[y_0, \dots, y_N] \to k[x_0, \dots, x_n], \qquad y_i \mapsto M_i.$$

The image being an integral domain, the ideal $\mathfrak{p}$ is thus prime. Let $Z = Z(\mathfrak{p})$. If $a \in \mathbb{P}^n$ and $F(y_0, \dots, y_N)$ is in $\mathfrak{p}$ then $F(M_0, \dots, M_n) = 0$ and, in particular, $F(M_0(a), \dots, M_n(a)) = 0$; that it, $\mathrm{Im}(\varphi) \subseteq Z$. In fact, they are equal. We sketch the proof of this fact, leaving the details to the reader. First, one argues that a point $P = (p_0 : \cdots : p_N)$ being on Z implies that one of its coordinates $p_0, \dots, p_n$ is not zero. This is because M_j^d can be expressed as a product of $M_0, \dots, M_n$ to various degrees, giving the same relation between the co-ordinates of P. Without loss of generality, $p_0 \neq 0$, and so we may assume $p_0 = 1$. Take $a_0 = 1$. The coordinates of P corresponding to the monomials $x_0^{d_1} x_j, j = 1, \dots, n$ give us the definition of a_j. One needs to check that $\varphi(1, a_1, \dots, a_n) = P$. This results, essentially, from writing every M_j times a suitable multiple of x_0 as a product of the monomials $x_0^{d_1} x_j, j = 1, \dots, n$.

We have established that φ is a bijective morphism $\mathbb{P}^n \to Z$. In fact, it is an isomorphism. First, we show φ is closed. To see that, note that if $f(x_0, \dots, x_n)$ is a homogenous polynomial of degree e then f^d can be written as a sum of monomials of degree de and every such monomial is a product of e monomials of degree d. That is to say, f^d is a homogenous polynomial $F(M_0, \dots, M_n)$ in $M_0, \dots, M_n$ of degree e. Thus, $f^d = \varphi^*(F(y_0, \dots, y_N))$. Since closed sets are defined by vanishing of finitely many homogenous polynomials $f_1, \dots, f_s$, by replacing f_i by f_i^d, which doesn't change the closed set, we get that the f_i are of the form $\varphi_i^F(y_0, \dots, y_N)$ for some homogenous polynomials $F_i(y_0, \dots, y_N)$. This shows that $\varphi(Z(\{f_1, \dots, f_s\})) = Z(\{F_1, \dots, F_s\}) \cap \mathrm{Im}(\varphi)$ and so is a closed set.

It is interesting to look at some examples. Consider the 2-uple embedding of $\mathbb{P}^1$ in $\mathbb{P}^2$:

$$(x_0 : x_1) \mapsto (x_0^2 : x_0 x_1 : x_1^2).$$

The image is the conic $y_0 y_2 - y_1^2 = 0$.

The 3-uple embedding of $\mathbb{P}^1$ in $\mathbb{P}^3$ is given by

$$(x_0 : x_1) \mapsto (y_0 : \cdots : y_3) = (x_0^3 : x_0^2 x_1 : x_0 x_1^2 : x_1^3).$$

The image is the zero set of the polynomials $y_0 y_3 - y_1 y_2, y_1 y_3 - y_2^2, y_0 y_2 - y_1^2$. Note that on the open set $x_1 \neq 0$ we can write the map as $x_0 \mapsto (x_0^3 : x_0^2 : x_0 : 1)$, which nothing else than the twisted cubic curve.

The 2-uple embedding of $\mathbb{P}^2$ in $\mathbb{P}^5$ is given by

$$(x_0 : x_1 : x_2) \mapsto (x_0^2 : x_1^2 : x_2^2 : x_0 x_1 : x_0 x_2 : x_1 x_2).$$

It is the variety defined by the equations $y_0 y_1 - y_3^2, y_0 y_2 - y_4^2, y_1 y_2 - y_5^2, y_3 y_4 - y_0 y_5$ (I think those suffice).

Example 4.11. *The automorphisms of* $\mathbb{P}^n$. Let $\mathrm{PGL}_{n+1}(k) = \mathrm{GL}_{n+1}(k)/Z$, where $Z = \{\mathrm{diag}(\alpha, \dots, \alpha) : \alpha \in k^*\}$ (Z is in fact the centre of $\mathrm{GL}_{n+1}(k)$). Let us also index the entries of a matrix by ij, where i, j are in the set $\{0, \dots, n\}$.The linear action of $\mathrm{GL}_{n+1}(k)$ on $\mathbb{A}^{n=1}$, induces an action of

$\mathrm{GL}_{n+1}(k)$ on $\mathbb{P}^n$ that factors through Z. Thus, we get an action of $\mathrm{PGL}_{n+1}(k)$. Every matrix acts as a morphism. This is quite clear since if M is a matrix and $\varphi_M : \mathbb{P}^n \to \mathbb{P}^n$ the map it induces,

$$\varphi_M(a) = {}^t(M \cdot {}^t a) = a \cdots {}^t M = {}^t(M_0(a) : \dots ; M_n(a))$$

where each M_i is a linear function (the coefficients are of course the entry of the i-th row of M). Then $\varphi_M^* F(x_0, \dots, x_n)$, for a homogenous degree d polynomial F, is just $F(M_0(x_0 : \dots : x_n) : \dots M_n(x_0 : \dots : x_n))$, which is again homogenous of degree d. Therefore, it is easy to check that φ^{-1} takes closed sets to closed set and regular functions to regular functions. Since $\varphi_M \circ \varphi_{M^{-1}} = \varphi_{\mathrm{Id}} = \mathrm{Id}$, it follows that every φ_M is an automorphism of $\mathbb{P}^n$. One concludes

$$\mathrm{PGL}_{n+1}(k) \hookrightarrow \mathrm{Aut}(\mathbb{P}^n).$$

It is a theorem that in fact

$$\mathrm{PGL}_{n+1}(k) = \mathrm{Aut}(\mathbb{P}^n).$$

END OF LECTURE 6 (September 24)

Proposition 4.12. *Let X and Y be two affine varieties. Let*

$$f : X \to Y$$

be a morphism and let $f^* : A(Y) \to A(X)$ be the induced homomorphism.

(1) *Let $Z \subset Y$ be a closed set defined by an ideal $J \lhd A(Y)$. Then $f^{-1}(Z)$ is the closed set of X defined by the ideal $f^*(J)A(X)$.*
(2) *Let $Z \subset X$ be a closed set defined by an ideal $J \lhd A(X)$. Then $\overline{f(Z)}$ is the closed set defined by the ideal $(f^*)^{-1}(J)$.*

Proof. We first prove (1). Let $J = \langle g_1, \dots, g_r \rangle$ then $f^*(J)A(X) = \langle f^*(g_1), \dots, (f^*)g_r \rangle$. Let $x \in X$ then $x \in f^{-1}(Z)$ iff $f(x) \in Z$, iff $g_i(f(x)) = 0$ for all i, iff $f^*(g_i)(x) = 0$ for all i, iff $x \in \mathcal{Z}(f^*(J)A(X))$.

We now prove (2). We note that $g \in \mathcal{I}(f(Z))$ iff $g(y) = 0$ for all $y \in f(Z)$, iff $g(f(x)) = 0$ for all $x \in Z$, iff $g \circ f = f^*(g) \in \mathcal{I}(Z) = J$, iff $g \in (f^*)^{-1}(J)$. That is, $\mathcal{I}(f(Z)) = (f^*)^{-1}(J)$, which gives $\overline{f(Z)} = \mathcal{Z}(\mathcal{I}(f(Z)) = \mathcal{Z}((f^*)^{-1}(J))$. ☐

Example 4.13. Let $X = \mathbb{A}^2$ with coordinates x, y and $Y = \mathbb{A}^1$ with coordinate x. Consider the function

$$f : X \to Y, \qquad f(x, y) = x.$$

We note that $f^{-1}(a) = \{(x, y) : x = a\} = \mathcal{Z}(x - a)$ is a closed set in X. This proves that f is continuous. The sheaf of regular functions on Y amounts to the following: for every finite collection of distinct points $a_1, \dots, a_n \in \mathbb{A}^1$ we have the regular functions g/h on $\mathbb{A}^1 \setminus \{a_1, \dots, a_n\}$ where $g, h \in k[x]$ and $h(a_i) \neq 0, \forall i$. This describes the ring $\mathcal{O}(\mathbb{A}^1 - \mathcal{Z}(\prod_{i=1}^n (x - a_i)))$. Note that it is equal to the localization $k[x][\prod_{i=1}^n (x - a_i)^{-1}]$.

We have $f^{-1}[\mathbb{A}^1 - \mathcal{Z}(\prod_{i=1}^n (x - a_i))] = \mathbb{A}^2 - \mathcal{Z}(\prod_{i=1}^n (x - a_i))$ and $f^*(g/h) = g/h$ is a regular function. This proves that f is a morphism.

The homomorphism of k-algebras

$$f^* : \mathcal{O}(Y) \to \mathcal{O}(X)$$

is just given by $f^* g = g$ under the interpretation $\mathcal{O}(Y) = k[x]$ and $\mathcal{O}(X) = k[x, y]$. That is

$$f^* : k[x] \to k[x, y]$$

is the natural inclusion.

Consider the closed set $Z = \{a_1, \dots, a_n\}$ in $\mathbb{A}^1$ with $J := \mathcal{I}(Z) = \langle \prod_{i=1}^n (x - a_i) \rangle$. We have $f^{-1}(Z) = \mathcal{Z}(\prod_{i=1}^n (x - a_i)) = \mathcal{Z}(f^* J k[x, y])$.

Consider the closed set $Z = \mathcal{Z}(xy - 1)$ in $\mathbb{A}^2$ with $J := \mathcal{I}(Z) = \langle xy - 1 \rangle$. Note that $f(Z) = \mathbb{A}^1 \setminus \{0\}$ and $\overline{f(Z)} = \mathbb{A}^1$. Accordingly we find $(f^*)^{-1}(J) = \{0\} = \mathcal{I}(f(Z))$.

Theorem 4.14. *Let X be any variety and let Y be an affine variety. Then there is a natural bijective map of sets*

$$\mathrm{Mor}(X, Y) \cong \mathrm{Hom}(\mathcal{O}(Y), \mathcal{O}(X)).$$

Proof. Given a morphism $f : X \to Y$ we get a homomorphism $f^* : \mathcal{O}(Y) \to \mathcal{O}(X)$.

Conversely, suppose given a homomorphism $\phi : \mathcal{O}(Y) \to \mathcal{O}(X)$. Since Y is an affine variety, $Y \subset \mathbb{A}^n$ for some n and $\mathcal{O}(Y) = A(Y) = k[x_1, \dots, x_n]/\mathcal{I}(Y)$. We define a map

$$f : X \to \mathbb{A}^n, \quad f(P) = (\phi(x_1)(P), \dots, \phi(x_n)(P)).$$

First note that the image of f is contained in Y so that in fact we defined a map $f : X \to Y$. Indeed, let $g \in \mathcal{I}(Y)$ then

$$g(\phi(x_1), \dots, \phi(x_n)) = \phi(g(x_1, \dots, x_n)) = 0,$$

hence $g(\phi(x_1)(P), \dots, \phi(x_n)(P)) = \phi(g)(P) = 0$. That is $f(X) \subset \mathcal{Z}(\mathcal{I}(Y)) = Y$.

We claim that in fact f is a morphism. We can make a general statement here:

Lemma 4.15. *Let X be any variety and let $Y \subset \mathbb{A}^n$ be an affine variety. Then a function $f : X \to Y$ is a morphism iff for every i the function $f^*(x_i) := x_i \circ f$ is regular.*

Proof. Since each x_i is a regular function on Y, if f is a morphism then $f^* x_i$ is a regular function on X.

Conversely, let $f : X \to Y$ be a function such that for every i the function $f^*(x_i) := x_i \circ f$ is regular on X. Since the regular functions on X form a ring, for every polynomial $g(x_1, \dots, x_n)$ also $f^*(g) = g(f^*(x_1), \dots, f^*(x_n))$ is a regular function. We see that pre-images of closed sets (defined by vanishing of polynomials) are sets defined by vanishing of regular functions, hence closed sets. It follows that f is continuous.

Let U be an open set of Y on which a quotient of polynomials g_1/g_2 is well defined. Then $f^{-1}(U)$ is an open set and $f^*(g_1)/f^*(g_2) = g_1(f^* x_1, \dots, f^* x_n)/g_2(f^* x_1, \dots, f^* x_n)$ is a well defined regular function. □

Coming back to the proof, we get that $f : X \to Y$ is a morphism. Clearly $f^* x_i = \phi(x_i)$ so $f^* = \phi$. This shows that our constructions are mutual inverses. □

Corollary 4.16. *Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties. Then*

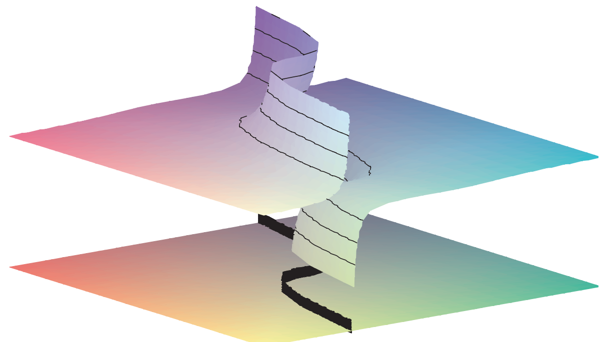
$$\begin{aligned} \mathrm{Mor}(X, Y) &= \mathrm{Hom}_{k-alg}(k[y_1, \dots, y_m]/\mathcal{I}(Y), k[x_1, \dots, x_n]/\mathcal{I}(X)) \\ &\underset{\phi(y_i) = f_i}{=} \{(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)) : g(f_1, \dots, f_m) = 0 \ \forall g \in \mathcal{I}(Y)\}. \end{aligned}$$

Example 4.17. Let $Y \subseteq \mathbb{A}^n$ be an affine variety and let $Z \subseteq \mathbb{A}^n$ be the hypersurface $\mathcal{Z}(f)$, where f is a non-zero polynomial and let $U = Y \setminus Z$. Let V be the variety in $\mathbb{A}^{n+1}$ (with coordinates $x_1, \dots, x_n, y$) given by $\mathcal{Z}(\langle \mathcal{I}(Y), y f(x_1, \dots, x_n) - 1 \rangle)$. Then

$$\alpha : V \to U, \qquad \alpha(x_1, \dots, x_n, y) = (x_1, \dots, x_n),$$

is an isomorphism.

Here is an example: Take $Y = \mathbb{A}^2$ and $Z = \mathcal{Z}(x^3 - y)$.



Indeed, α is clearly a morphism, because it is the restriction of the morphism $\mathbb{A}^{n+1} \to \mathbb{A}^n$ given by the same formula. (This morphism corresponds to the obvious inclusion of rings $k[x_1, \ldots, x_n] \hookrightarrow k[x_1, \ldots, x_n, y]$.) Define now a map

$$\beta : U \to V$$

by $\beta(x_1, \ldots, x_n) = (x_1, \ldots, x_n, 1/f(x_1, \ldots, x_n))$. Note that β is well defined function and that α and β are inverses as functions of sets. It only remains to show that β is a morphism. Using Lemma 4.15 we need only verify that $x_i \circ \beta = x_i$ is a regular function on U for every i, and that $y \circ \beta = 1/f(x_1, \ldots, x_n)$ is a regular function on U, which follows from the definition.

We obtain as a corollary that:

- $U = Y \setminus \mathcal{Z}(f)$ is affine. We remark that an open set like U is called a **principal open set** or a **basic open set** of Y.
- U has coordinate ring $A(U) \cong k[x_1, \ldots, x_n, y]/(\mathcal{I}(Y), yf - 1) = A(Y)[f^{-1}]$.

This can be applied as follows: let U be a quasi-affine variety. Let $U = U_1 \cup U_2$, a union of non-empty open sets. Then $\mathcal{O}(U) = \mathcal{O}(U_1) \cap \mathcal{O}(U_2)$ (the intersection taken in $K(U)$). For example, take $U = \mathbb{A}^2 - \{0\} = (\mathbb{A}^2 - \mathcal{Z}(x)) \cup (\mathbb{A}^2 - \mathcal{Z}(y))$. We find that $\mathcal{O}(U) = k[x, y][x^{-1}] \cap k[x, y][y^{-1}] = k[x, y]$.

END OF LECTURE 7 (October 1)

Our next task is to discuss the ring of regular functions for a projective variety, i.e., an irreducible closed set of $\mathbb{P}^n$. We first need some facts on localization on graded rings.

Let S be a graded ring and let $\mathfrak{p} \lhd S$ be a **homogenous** prime ideal. Let U be the set of homogenous elements in $S \setminus \mathfrak{p}$. Note that U is a multiplicative set. We consider now the localization $S[U^{-1}]$, $\mathbb{Z}$-graded by $\deg(f/g) = \deg(f) - \deg(g)$, and inside it the subring of elements of degree 0. We denote this ring by $S_{\mathfrak{p},0}$. It is a local ring with maximal ideal $\mathfrak{p}S[U^{-1}] \cap S_{\mathfrak{p},0}$. Note that a similar construction is valid for every multiplicative set U consisting of homogenous elements and we shall denote by $S[U^{-1}]_0$ the subring of element of degree zero in the usual localization $S[U^{-1}]$.

THEOREM **4.** *Let $Y \subseteq \mathbb{P}^n_k$ be a projective variety, defined by a homogenous prime ideal $\mathcal{I}(Y)$, with homogenous coordinate ring $S(Y) = k[x_0, \ldots, x_n]/\mathcal{I}(Y)$. Then*

1. *$\mathcal{O}(Y) = k$.*
2. *for every point P with corresponding maximal ideal $\mathfrak{m}_P \lhd S(Y)$ we have $\mathcal{O}_{Y,P} = S(Y)_{\mathfrak{m}_P,0}$.*

(3) $K(Y) \cong S(Y)_{(0),0}$.
(4) *Let* $Y_i = Y \cap U_i$, *where* $U_i = \mathbb{P}^n - \mathcal{Z}(x_i)$. *Then* $\mathcal{O}(Y_i) = A(X_i)$, *where* X_i *is the variety obtained by de-homogenizing the ideal* $\mathcal{I}(Y)$ *with respect to the variable* x_i.

For the proof we refer to [H, Thm. 3.4].

Corollary 4.18. *Any morphism* $f : X \to Y$ *from a projective variety* X *to an affine variety* $Y \subset \mathbb{A}^n$ *is constant.*

Proof. Indeed, for every i the regular function f^*x_i is constant, equal to a_i, on X. This implies that $f(X) = \{(a_1, \dots, a_n)\}$. ☐

Corollary 4.19. *A projective variety isomorphic to an affine variety is zero dimensional.*

Proof. Indeed the morphism giving the isomorphism must be constant! ☐

Corollary 4.20. *Let* $Y \subseteq \mathbb{A}^n$ *be an affine variety of dimension at least* 1. *Let* $\psi_0 : \mathbb{A}^n \to \mathbb{P}^n$ *be the embedding* $\psi_0(a_1, \dots, a_n) = (1, a_1, \dots, a_n)$. *Then*

$$\overline{\psi_0(Y)} \cap \mathcal{Z}(x_0) \neq \emptyset.$$

Proof. Else, the projective variety $\overline{\psi_0(Y)}$ is also an affine variety. ☐

5. Products, Rational Morphisms

5.1. **Products of Affine Varieties.** Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties. We take the coordinates $x_1, \dots, x_n$ on $\mathbb{A}^n$ and $x_{n+1}, \dots, x_{n+m}$ on $\mathbb{A}^m$. We define the product of X and Y to be the subset

$$X \times Y \subseteq \mathbb{A}^{n+m}$$

endowed with the induced topology. We note that $X \times Y$ is the zero set of the ideal $\langle f : f \in \mathcal{I}(X) \cup \mathcal{I}(Y) \rangle = \mathcal{I}(X) + \mathcal{I}(Y)$. It is therefore a closed set.

Remark 5.1. The topology on $X \times Y$ is usually not the product topology. Take for example $X = Y = \mathbb{A}^1$. Then $X \times Y = \mathbb{A}^2$ and the diagonal $Z(x_1 - x_2)$ is a closed subset of $X \times Y$. On the other hand, it is not a closed set in the product topology. Indeed, suppose it is. Then there exists a basic open set $U = U_1 \times U_2$, where U_1 is open in X and U_2 is open in Y, such that for all $a \in k$ the point $(a, a) \neq U$. However, for suitable finite sets we have $U_1 = \mathbb{A}^1 - \{\alpha_1, \dots, \alpha_s\}$, $U_2 = \mathbb{A}^1 - \{\beta_1, \dots, \beta_t\}$. Choose $a \in k - \{\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_t\}$. Such a exists because k is algebraically closed, hence infinite. Then the point $(a, a) \in U_1 \times U_2$; a contradiction.

Proposition 5.2. *The product $X \times Y$ is a categorical product. Namely, there are morphisms*

$$\begin{tikzcd}
& X \times Y \arrow[dl, "p_X"'] \arrow[dr, "p_Y"] & \\
X & & Y
\end{tikzcd}$$

such that given any variety S and morphisms $g_X : S \to X$ and $g_Y : S \to Y$ there exists a unique morphism $f : S \to X \times Y$ rendering the following diagram commutative:

(4)
$$\begin{tikzcd}
& S \arrow[d, dotted, "f"] \arrow[ddl, bend right, "g_X"'] \arrow[ddr, bend left, "g_Y"] & \\
& X \times Y \arrow[dl, "p_X"'] \arrow[dr, "p_Y"] & \\
X & & Y
\end{tikzcd}$$

Proof. Suppose that the proposition is true for $X = \mathbb{A}^n$ and $Y = \mathbb{A}^m$. Given morphisms $g_X : S \to X$ and $g_Y : S \to Y$ we may view them as morphisms $g_X : S \to \mathbb{A}^n$ and $g_Y : S \to \mathbb{A}^m$. We therefore obtain a unique function $f : S \to \mathbb{A}^n \times \mathbb{A}^m$ such that

$$\begin{tikzcd}
& S \arrow[d, dotted, "f"] \arrow[ddl, bend right, "g_X"'] \arrow[ddr, bend left, "g_Y"] & \\
& \mathbb{A}^n \times \mathbb{A}^m \arrow[dl, "p_X"'] \arrow[dr, "p_Y"] & \\
\mathbb{A}^n & & \mathbb{A}^m
\end{tikzcd}$$

is commutative. Since the underlying set of $X \times Y$ is certainly the direct product of the underlying set of X and Y, the morphism f has image contained in $X \times Y$. Moreover, the same argument shows f is unique (i.e., if f' is another such function then viewing f and f' just as functions of sets shows they are equal).

We now discuss the case $X = \mathbb{A}^n$ and $Y = \mathbb{A}^m$. We (of course!) define f as the function $(g_{\mathbb{A}^n}, g_{\mathbb{A}^m})$. It is clear that (4) holds. One just need to show that f is a morphism. By Lemma 4.15 it is enough to show that $x_i \circ f$ is a regular function on S for all $1 \leq i \leq n+m$. But

$$x_i \circ f = \begin{cases} x_i \circ g_{\mathbb{A}^n} & 1 \leq i \leq n \\ x_i \circ g_{\mathbb{A}^m} & n+1 \leq i \leq n+m \end{cases}.$$

These are regular functions because $g_{\mathbb{A}^n}$ and $g_{\mathbb{A}^m}$ are morphisms. □

Remark 5.3. Note that

$$\begin{aligned} A(X \times Y) &= k[x_1, \dots, x_{n+m}]/\langle \mathcal{I}(X), \mathcal{I}(Y) \rangle \\ &\cong k[x_1, \dots, x_n]/\mathcal{I}(X) \otimes_k k[x_{n+1}, \dots, x_{n+m}]/\mathcal{I}(Y) \\ &= A(X) \otimes_k A(Y). \end{aligned}$$

This, in fact, is expected. Indeed, if X and Y are affine then $X \times Y$ is affine and is a product in the category of affine varieties. Let S be an affine variety then the isomorphism that should hold for the product is

$$\begin{aligned} \mathrm{Mor}(S, X \times Y) &= \mathrm{Mor}(S, X) \times \mathrm{Mor}(S, Y) \\ &= \mathrm{Hom}_{k-alg}(A(X), A(S)) \times \mathrm{Hom}_{k-alg}(A(Y), A(S)). \end{aligned}$$

But it is easy to check that

$$\mathrm{Hom}_{k-alg}(A(X), A(S)) \times \mathrm{Hom}_{k-alg}(A(Y), A(S)) \cong \mathrm{Hom}_{k-alg}(A(X) \otimes_k A(Y), A(S)).$$

Which agrees with our observation $A(X \times Y) = A(X) \otimes_k A(Y)$. On the other hand, if we didn't have a guess to what $X \times Y$ should be concretely we could still know, by this argument, that it must be some affine[11] variety with coordinate ring $A(X) \otimes_k A(Y)$.

5.2. **Products of General Varieties.** We start our discussion of products of general varieties in the case of $\mathbb{P}^n$ and $\mathbb{P}^m$. Let Z be the image of the $\mathbb{P}^n \times \mathbb{P}^m$ (in the set theoretic sense) in the projective space $\mathbb{P}^N$, $N = (n+1)(m+1) - 1$, under the Segre embedding

$$\Psi : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^N, \qquad ((\dots, a_i, \dots), (\dots, b_j, \dots)) \mapsto (\dots, a_i b_j, \dots).$$

We know already that Ψ is a well defined, injective map whose image Z is a subvariety of $\mathbb{P}^N$. We consider $\mathbb{P}^n \times \mathbb{P}^m$ as this variety Z.

Let us consider the pull back of the coordinate ring of $\mathbb{P}^N$ to $\mathbb{P}^n \times \mathbb{P}^m$ via the Segre embedding. One immediately finds that we get polynomials $p(x_0, \dots, x_n; y_0, \dots, y_m)$ that are homogenous in each set of variables alone and of the same degree.[12] These are spanned by monomials of the form $x_0^{a_0} \cdots x_n^{a_n} y_0^{b_0} \cdots y_m^{b_m}$ with $\sum a_i = \sum b_i$.

We claim that the morphism $p_1 : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^n$ (resp. $p_2 : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^m$) is continuous. It is enough to prove that if f is a homogenous polynomial in $k[x_0, \dots, x_n]$ then $p_1^{-1}(\mathcal{Z}(f))$ is a closed set. We note that

$$p_1^{-1}(\mathcal{Z}(f)) = \{(a; b); a \in \mathcal{Z}(f), b \in \mathbb{P}^m\} = \cap_{i=0}^m \mathcal{Z}(f \cdot y_i^{\deg(f)}),$$

[11] The arguments given below in the projective case indicate why one can conclude that if $X \times Y$ is a product in the category of affine varieties, it is also a product in the category of all varieties.

[12] A good example to keep in mind is the case of $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ given by $(x_0, x_1; y_0, y_1) \mapsto (x_0 y_0, x_0 y_1, x_1 y_0, x_1 y_1)$. The image is called the **quadratic surface** in $\mathbb{P}^3$. It is defined by the equation $x_{0,0} x_{1,1} - x_{0,1} x_{1,0} = 0$. Note that a homogenous polynomial $f(x_{0,0}, x_{0,1}, x_{1,0}, x_{1,1})$ of degree d pulls back to a polynomial $f(x_0 y_0, x_0 y_1, x_1 y_0, x_1 y_1)$ which is homogenous in the variables x_0, x_1 (resp. y_0, y_1) viewing y_0, y_1 (resp. x_0, x_1 as coefficients) of degree d, in each case.

hence closed. Using this it is not hard to deduce that if X and Y are quasi-projective varieties in $\mathbb{P}^n$ and $\mathbb{P}^m$, respectively, then $X\times Y$, considered in $\mathbb{P}^N$ via the Segre embedding, is also a quasi-projective variety.

As in the affine case, we may reduce the proof that $X \times Y$ is a product to the case of $X = \mathbb{P}^n$ and $Y = \mathbb{P}^m$, which we proceed to discuss. To show $\mathbb{P}^n \times \mathbb{P}^m$ is a product one uses the following lemma:

Lemma 5.4. *Let S, T be varieties and $f : S \to T$ be a function. Let $T = \cup_i T_i$ be an open cover of T. Then f is a morphism iff for every i the set $S_i = f^{-1}(T_i)$ is open and $f|_{S_i} : S_i \to T_i$ is a morphism.*

One applies this to the following covering of $\mathbb{P}^n \times \mathbb{P}^m$:

$$\mathbb{P}^n \times \mathbb{P}^m = \cup_{i=0}^n \cup_{j=0}^m U_{i,j},$$

where $U_{i,j} = U_i \times U_j = \{(a, b) : a_i b_j \neq 0\}$. Note that $U_{i,j}$ is an open set and the induced sheaf of function on $U_{i,j}$, obtained by simultaneous de-homogenizing w.r.t. x_i and y_j, is the usual structure on $\mathbb{A}^{n+m}$.

Now, given morphisms $g_n : S \to \mathbb{P}^n$ and $g_m : S \to \mathbb{P}^m$, we obtain morphisms

$$g_n^i : g_n^{-1}(U_i) \to U_i, \qquad g_m^j : g_m^{-1}(U_j) \to U_j,$$

and hence, by the property of product for affine varieties, a unique morphism

$$f_{i,j} := (g_n^i, g_m^j) : g_n^{-1}(U_i) \cap g_m^{-1}(U_j) \to U_{i,j}.$$

One needs to check that the morphisms glue together to a global well defined function $f : S \to \mathbb{P}^n \times \mathbb{P}^m$, which is a morphism by the Lemma and to conclude by verifying that f has all the properties we want.

END OF LECTURE 8 (October 3)

Remark 5.5. If X and Y are irreducible (affine) varieties so is $X \times Y$. One has

$$\dim(X \times Y) = \dim(X) + \dim(Y).$$

5.3. **Application to Morphisms.** We draw some applications to morphisms of varieties.

Corollary 5.6. *Let X be a variety and let $\Delta : X \to X \times X$ be the diagonal morphism $\Delta(x) = (x, x)$. Then the image of Δ is closed.*

Proof. Note first that Δ is a morphism. It is induced by the universal property from the identity map $X \to X$. Let Y be a projective variety containing X as an open set. Since topology on $X \times X$ is induced from $Y \times Y$ and $\Delta(X) = \Delta(Y) \cap X \times X$ we may reduce to the case where X is projective. In this case, the diagonal is defined under the Segre embedding

$$X \times X \subset \mathbb{P}^n_{x_0,\dots,x_n} \times \mathbb{P}^n_{y_0,\dots,y_n} \to \mathbb{P}^{(n+1)^2-1}_{x_{ij}}$$

by the equations $x_{ij} = x_{ji}$, hence closed. □

Corollary 5.7. *Let $f, g : S \to Y$ be two morphisms between varieties that are equal on a non-empty open set $U \subset S$ then $f = g$.*

Proof. Consider the induced morphism
$$h = (f, g) : S \to Y \times Y.$$
Then $h^{-1}(\Delta(Y))$ is a closed set containing U hence equal to S. □

Remark 5.8. Recall that a topological space X is Hausdorff (T_2) if and only if the diagonal $\Delta(X)$ is closed in $X \times X$ in the product topology.

Our spaces are usually not Hausdorff. However, the topology on $X \times X$ is also usually not the product topology and that what allows $\Delta(X)$ to be closed in $X \times X$ in the topology we defined on it. Note that the fact that the diagonal is closed is what allowed us to prove the last corollary.

For topological spaces which are not Hausdorff (hence the diagonal is not closed) it can indeed happen that the last corollary fails. For example, take $X = Y = \{0, 1\}$ with the only non-trivial open set being $\{0\}$, and take f to be the identity and g be the constant function 0. Then $f = g$ on the open dense set $\{0\}$ though $f \neq g$.

We just saw that for varieties the diagonal is closed, hence they have a certain separated-ness property. For the spaces (called "schemes") constructed from affine varieties by the process of gluing along open sets it may be the case that the diagonal is not closed. If it is closed we call the scheme a **separated** scheme. Incidentally, the basic example of a non-separated scheme, is a favorite in topology. It is "the line with the double origin" obtained by gluing two copies of $\mathbb{A}^1$ along the common open set $\mathbb{A}^1 - \{0\}$.

5.4. **The Field of Rational Functions.** Consider a morphism $f : X \to Y$ of algebraic varieties over k. Given an open set $U \subseteq Y$ and a regular function g on U we may consider the open set $f^{-1}(U)$ and the regular function on it $g \circ f$. The couple $(f^{-1}(U), g \circ f)$ defines an element of $K(X)$ *only if* $f^{-1}(U)$ *is non-empty*. This prompts the following definition:

Definition 5.9. A morphism $f : X \to Y$ of algebraic varieties over k is called **dominant** if $f(X)$ is dense in Y.

Example 5.10. If X, Y are affine then $X = \mathcal{Z}(0)$ and $\overline{f(X)} = Z(\mathrm{Ker}(f^*))$ by Proposition 4.12, where $f^* \colon A(Y) \to A(X)$ is the corresponding ring homomorphism. Thus, f is dominant if and only if f^* is injective.

If f is dominant we obtain a well defined injective homomorphism of k-algebras
$$f^* : K(Y) \to K(X).$$
It follows that if f is dominant then $\dim(X) \geq \dim(Y)$.

Definition 5.11. Let X and Y be varieties. A **rational map** α from X to Y is an equivalence class of couples (U, f), where $U \subset X$ is an open non-empty set and $f : U \to X$ is a morphism, and where (U_1, f_1) is equivalent to (U_2, f_2) if $f_1|_{U_1 \cap U_2} = f_2|_{U_1 \cap U_2}$. (Note that $U_1 \cap U_2$ is always non-empty.) One usually uses the notation
$$X \dashrightarrow Y$$
to denote a rational map from X to Y.

Example 5.12. Let $g(x, y, z)$ be a homogenous irreducible polynomial such that $g \notin k[x, z]$. Let $X \subset \mathbb{P}^2_{x,y,z}$, $X = \mathcal{Z}(g(x, y, z))$. Let $Y = \mathbb{P}^1_{x,y}$. Let
$$f : X \dashrightarrow Y, \qquad f(x : y : z) = (x : z).$$

Then f is in fact a morphism outside the point $(0:1:0)$ (if that point belongs to X at all!). It is dominant, else its image is a point which implies $g \in k[x,z]$. Now $K(\mathbb{P}^1) = K(\mathbb{A}^1) = k(x)$, since $\mathbb{A}^1_x = \{(x:1)\}$ is open in $\mathbb{P}^1$. This field can also be written as $k[x,y]_{(0),0}$ comprised ratio of homogenous polynomials in x, y of the same degree. Similarly $K(X) = K(X \cap \{z=1\}) = \operatorname{Frac}(k[x,y]/(g(x,y,1))) = k(x)[y]/(g(x,y,1))$.

In fact, as we shall late prove, f is always a morphism. Here we illustrate this in a particular example where $g(x,y,z) = y^2z - (x^3+z^3)$ (the closure of the affine elliptic curve $y^2 = x^3+1$ in $\mathbb{P}^2$). In this example, the inclusion $k(x) \hookrightarrow k(x)[y]/(y^2-x^3-1)$, which is a quadratic field extension reflects the fact that the morphism f is $2:1$. In this affine chart, the morphism f is just $f(x,y) = x$. The point $(0:1:0)$ belongs to X though and f is not a-priori defined there. It is the only problematic point.

Choose an affine chart containing the point $(0:1:0)$. For example, the chart $\{y=1\}$. There X is given by

$$z - z^3 = x^3.$$

The morphism f can be written for $x \neq 0$ as

$$(x:y:z) \mapsto (x:z) = (1:z/x).$$

Note that on the curve X we have $z/x(1-z^2) = x^2$ and so

$$\frac{z}{x} = \frac{x^2}{1-z^2},$$

and the latter expression extends to a regular function at $x = z = 0$, expressing f as a morphism outside the closed set $x = 0, z - z^3 = 0$.

Definition 5.13. A rational map $\alpha : X \dashrightarrow Y$ is called a **birational map** if there exists a rational map $\beta : Y \dashrightarrow X$ such that $\alpha \circ \beta$ and $\beta \circ \alpha$ are equivalent to the identity morphisms. In that case we say that X and Y are **birationally equivalent**.

Remark 5.14. Corollary 5.7 shows that indeed we get equivalence relations. For example, if $(U_1, f_1) \sim (U_2, f_2) \sim (U_3, f_3)$ then on $U_1 \cap U_2 \cap U_3$ we have $f_1 = f_3$, hence $f_1 = f_3$ on $U_1 \cap U_3$ and $(U_1, f_1) \sim (U_3, f_3)$.

We call a rational map **dominant** if for one (hence, any) representative (U, f), the morphism f is dominant.

Example 5.15. Let Y' be an open non-empty subset of a variety Y than Y' and Y are birationally equivalent. If Y' is isomorphic to X' then Y' and X' are birational and if X' is also open in X then also X and Y are birational. In fact, this describes completely the equivalence we get. See Corollary 5.21.

Example 5.16. The varieties $Z = \mathcal{Z}(xy-1)$ in $\mathbb{A}^2$ and $\mathbb{A}^1$ are birationally equivalent since Z is isomorphic to $\mathbb{A}^1 \setminus \{0\}$.

Example 5.17. Let $X = \mathbb{A}^1, Y = Z(y^2 - x^3)$ and

$$f(t) = (t^2, t^3).$$

Then f is a bijective morphism which is birational morphism, because outside the point $(0,0)$ it can be inverted by

$$(x,y) \mapsto y/x.$$

Example 5.18. We have $\mathbb{P}^1 \times \mathbb{P}^1 \subset \mathbb{A}^1 \times \mathbb{A}^1 = \mathbb{A}^2 \subset \mathbb{P}^2$. This shows that $\mathbb{P}^1 \times \mathbb{P}^1$ is birational to $\mathbb{P}^2$. However, they are not isomorphic. Indeed, in $\mathbb{P}^1 \times \mathbb{P}^1$ we have two irreducible curves that don't intersect (in fact, plenty!), but in $\mathbb{P}^2$ any two such curves intersect: if the curves are defined by two homogenous polynomials $f(x_0, x_1, x_2), g(x_0, x_1, x_2)$ then the dimension of the conical set in $\mathbb{A}^3$ defined by those is at least 1 and so the dimension of the closed set in $\mathbb{P}^2$ defined by those is at least 0 and so non-empty.

Our goal is to prove the following theorem:

Theorem 5.19. *There is an anti-equivalence of categories between the category of varieties over k with morphisms being dominant rational maps, and the category of finitely generated field extensions of k with morphisms being k-algebra homomorphisms.*

Proof. Given a variety X we associate to it its field of rational functions $K(X)$. It is a finitely generated field extension of k. Given a finitely generated field extension K of k let $y_1, \dots, y_n$ be a set of generators and let B be the subring of K generated by $y_1, \dots, y_n$ over k. Then B is a homomorphic image of $k[x_1, \dots, x_n]$ which defines a variety X in $\mathbb{A}^n$ with $A(X) \cong B$. Moreover, $K(Y) \cong Quot(B) \cong K$. Hence, our functor is essentially surjective.

Given a dominant rational map $f : X \dashrightarrow Y$ we get a field injection $f^* : K(Y) \to K(X)$, which is a homomorphism of k-algebras.[13] It remains to prove the converse: given an injection of k algebras $\varphi : K(Y) \to K(X)$ there is a unique dominant rational map $f : X \dashrightarrow Y$ such that $f^* = \varphi$. For that we require a lemma of independent interest.

END OF LECTURE 9 (October 10)

Lemma 5.20. (1) *Any variety has a basis of affine open sets.*

(2) [14] *Every variety is quasi-compact. Namely, every open cover admits a finite sub cover.*[15]

Proof. Let Y be a quasi-projective variety in $\mathbb{P}^n$. Since $Y = \cup_{i=0}^n (Y \cap U_i)$, a union of open sets, we may assume Y is quasi-affine, $Y \subset \mathbb{A}^n$. Let Y' be the closure of Y in $\mathbb{A}^n$. Let U be an open set of Y, hence of Y', and P a point of U. Since $Y' - U$ is a closed set, we have

$$Y' \setminus U = \mathcal{Z}(I).$$

Since $P \notin \mathcal{Z}(I)$ there exists a polynomial $f \in I$ such that $f(P) \neq 0$. We find that

$$P \in Y' \setminus \mathcal{Z}(f) \subset U.$$

On the other hand, by Example 4.17, the set $Y' \setminus \mathcal{Z}(f)$ is affine.

Now for the second part. Let Y be a quasi-projective variety, $Y \subseteq \mathbb{P}^n$. Then, using the same decomposition as above, $Y = \cup_{i=0}^n (Y \cap U_i)$, we see that it is enough to prove the assertion for $Y \subset \mathbb{A}^n$ a quasi-affine variety. (An open cover of Y induces an open cover of $Y \cap U_i$ allowing to select a finite sub cover for each $Y \cap U_i$. There are finitely many i's, etc.) Given an open cover of Y, by passing to the complements, we arrive at the following situation. We have a collection of closed sets, whose intersection is a closed set. We need to choose a finite sub collection with the same intersection. Passing to ideals, this is just the noetherian property. □

[13] Of (U, g) is any representative than we define f^* as $g^* : K(Y) \to K(U) = K(X)$. This does not depend on the choice of representative (U, g) for f.

[14] This will not be used in the proof, but now seems a good time to prove it.

[15] The usual terminology used in north america for this property is "compact". The French use "quasi-compact" and save compact to mean Hausdorff and quasi-compact. The French terminology has taken over algebraic geometry in most cases.

Let V be an open affine set in Y and let $y_1, \dots, y_n$ be generators for $A(V)$ as a k-algebra. We know that $\mathrm{Frac}(A(V)) = K(Y)$. We may consider V as an affine variety in $\mathbb{A}^n$. Each of the functions $\varphi(y_i)$ is a rational function on X and hence we may find an open set U of X such that each $\varphi(y_i)$ is a regular function. Then the function $f : U \to V$ given by $f(t) = (\varphi(y_1)(t), \dots, \varphi(y_n)(t))$ is a well defined morphism $U \to V$ (using Theorem 4.14 and Lemma 4.15) satisfying $f^* = \varphi$.

The morphism f is dominant. If not, then $\overline{f(U)}$ is a proper closed subset of V and hence there exists a non-zero function $h \in A(V)$ that vanishes identically on $\overline{f(U)}$. We then obtain that $h \in \mathrm{Ker}(f^*)$, which is a contradiction to ϕ being injective. □

Corollary 5.21. *Let X, Y be varieties. The following are equivalent:*

1. *$X \sim Y$ (read: X is birational to Y).*
2. *There are isomorphic open sets $U \subset X$ and $V \subset Y$.*
3. *$K(X) \cong K(Y)$.*

Proof. The previous results give (2) ⇒ (3) ⇒ (1) and we need only show (1) ⇒ (2).

We know that there exist rational maps $f : X \dashrightarrow Y$, $g : Y \dashrightarrow X$, such that $f \circ g$ and $g \circ f$ are equivalent to the identity. Represent f by a pair (U_1, f_1) and g by a pair (V_1, g_1). Replace the set U_1 by $U = U_1 \cap f_1^{-1}(V_1)$ and V_1 by $V = V_1 \cap g^{-1}(U_1)$. We note that on U and V all the morphisms $f, g, f \circ g, g \circ f$ are defined. Note that, e.g. $f \circ g$ is the identity on V because it is equal to the identity on some non-empty open subset of V. □

Proposition 5.22. *Any variety X of dimension n is birational to a hypersurface Y in $\mathbb{P}^{n+1}$.*

Proof. For the proof we need to know the following

Fact 5.23. The function field of X is isomorphic to the field $k(x_1, \dots, x_n)[x_{n+1}]/(f(x_{n+1}))$, where f is a suitable irreducible polynomial with coefficients in $k[x_1, \dots, x_n]$.

Let Y' be the hypersurface in $\mathbb{A}^{n+1}$ defined by (f) and let Y be the closure in $\mathbb{P}^{n+1}$. □

Example 5.24. The curves $C : y^2 = x^3$ and $\mathbb{P}^1$ are birational. First note that $K(\mathbb{P}^1) = K(\mathbb{A}^1) = k(x)$, hence the assertion is that $k(C) \cong k(x)$. Consider the element $t = y/x \in k(C)$. Note that $k(C)$ is generated by x, y and that $k(t) \subseteq k(C)$. Now $x = t^2$ so $x \in k(t)$ and $y = tx$ so $y \in k(C)$. Hence, $k(t) = k(C)$. We also find the birational map: the inclusion $k(t) \hookrightarrow k(C)$ may be considered as coming from the morphism $C \to \mathbb{A}^1$ given by $(x, y) \mapsto x/y$. This is a well defined map f on $C - \{0\}$ whose inverse is given on $\mathbb{A}^1 - \{0\}$ by $t \mapsto (t^2, t^3)$.

Figure 10 shows this morphism. The affine line is represented by the line $x = 1$. The coordinate y on this line is the slope of the line through the origin and $(1, y)$ and its point of intersection with $y^2 = x^3$ is given by (y^2, y^3).

Note that by Bezout's theorem a line should intersect $y^2 = x^3$ in three points in $\mathbb{P}^2$. Consider the line $y = tx$ (t constant) and the curve $y^2 = x^3$ in $\mathbb{P}^2$ given, respectively by $y = tx$ and $y^2 z = x^3$. At "infinity" $(z = 0)$ they are given by $(1 : t : 0)$ and $(0 : 1 : 0)$. Hence, all intersections are accounted for by the points of intersection in $\mathbb{A}^2$. We conclude that the point $(0, 0)$ should be counted with multiplicity 2. This is affirmed by perturbing the equations slightly; see Figure 11.

Remark 5.25. Let X and Y be two varieties. Suppose that there are points $P \in X$ and $Q \in Y$ such that the local rings $\mathcal{O}_{X,P}$ and $\mathcal{O}_{Y,Q}$ are isomorphic as k-algebras. Then one can show that there are open sets $P \in U \subset X$ and $Q \in V \subset Y$ and an isomorphism of U to V that sends P to Q.

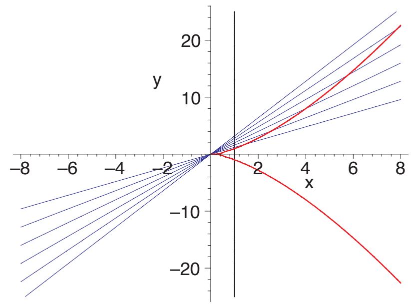


Figure 10. Birational morphism between the cuspidal curve $y^2 = x^3$ and the affine line $\mathbb{A}^1$.

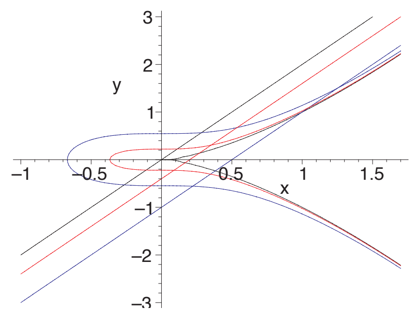


Figure 11. Perturbing the intersection between $y^2 = x^3$ and $y = 2x$.

6. Singular and Non-singular Varieties

Recall Remark 5.25: "Let X and Y be two varieties. Suppose that there are points $P \in X$ and $Q \in Y$ such that the local rings $\mathcal{O}_{X,P}$ and $\mathcal{O}_{Y,Q}$ are isomorphic as k-algebras. Then there are open sets $P \in U \subset X$ and $Q \in V \subset Y$ and an isomorphism of U to V that sends P to Q."

It shows that the local ring is in a sense containing much global information. In this lecture we shall see how to mine information from the local ring that teaches more on the truly local behavior of the variety at a point. We shall define the **tangent space** at a point – all lines that are solutions to the first order approximation of the equations defining the variety at that point, the **tangent cone** – the limit of all secants to the variety as we approach the point, and the **completion of the local ring** that provides the analytic behavior at the point.

6.1. **The Tangent Space.**

Let V be a variety and $P \in V$ a point.

Definition 6.1. The **(Zariski) tangent space** to V at P is defined as $\mathrm{Hom}_k(\mathfrak{m}/\mathfrak{m}^2, k)$, where $\mathfrak{m}$ is the maximal ideal of the local ring $\mathcal{O}_{Y,P}$. Notation: $T_{V,P}$. The space $\mathfrak{m}/\mathfrak{m}^2$ is called the **(Zariski) co-tangent space**. Notation: $T^*_{V,P}$.

The variety Y is **non-singular**(or **regular**) at P if $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \dim(Y)$. We say Y is *non-singular*, or *regular*, if it is non-singular at every point.

Remark 6.2.
1. Note that $\mathfrak{m}/\mathfrak{m}^2$ is a module over $\mathcal{O}_{Y,P}/\mathfrak{m} = k$, hence a vector space over k.
2. A local ring $(\mathcal{O}, \mathfrak{m})$ is called *regular* if $\dim(\mathcal{O}) = \dim(\mathfrak{m}/\mathfrak{m}^2)$. One always has the inequality $\dim(\mathcal{O}) \leq \dim(\mathfrak{m}/\mathfrak{m}^2)$.
3. Since we have $\dim(\mathcal{O}_{Y,P}) = \dim(Y)$ we conclude that Y is non-singular at P iff $\mathcal{O}_{Y,P}$ is a regular local ring.

We now analyze the definition above. We adopt the point of view that the tangent space at P should be a first order approximation to the variety at P. Suppose that $Y \subset \mathbb{A}^n$ is a variety of dimension r and $\mathcal{I}(Y) = \langle f_1, \dots, f_m \rangle$. Let $P = (a_1, \dots, a_n) \in Y$ and write each f_i in the variables $y_j = x_j - a_j$. The maximal ideal $\mathfrak{m}_P$ of $\mathcal{O}_{Y,P}$ is generated by the images of $y_1, \dots, y_n$. It follows that

$$\mathfrak{m}_P/\mathfrak{m}_P^2 \cong \langle y_1, \dots, y_n \rangle / \langle \{y_i y_j\}_{i,j}, f_1, \dots, f_m \rangle, \tag{5}$$

where the right hand side is calculated in the ring $k[y_1, \dots, y_n]$.

Example 6.3. Consider the nodal curve $y^2 = x^2(x+1)$ (Figure 12). we calculate the tangent space at $(0, 0)$. We have

$$\begin{aligned}\mathfrak{m}_0/\mathfrak{m}_0^2 &\cong \langle x, y \rangle / \langle x^2, xy, y^2, y^2 - x^2(x+1) \rangle \\ &\cong \langle x, y \rangle / \langle x^2, xy, y^2 \rangle \\ &\cong k^2.\end{aligned}$$

It is two dimensional and hence the curve is singular at this point. On the other hand, let us do the same calculation at the point $P = (-1, 0)$, using the variables $u = x + 1, v = y$. We find that

$$\begin{aligned}\mathfrak{m}_P/\mathfrak{m}_P^2 &\cong \langle u, v \rangle / \langle u^2, uv, v^2, v^2 - (u-1)^2 u \rangle \\ &\cong \langle u, v \rangle / \langle u^2, uv, v^2, (u^2 - 2u + 1)u \rangle \\ &\cong \langle u, v \rangle / \langle u^2, uv, v^2, u \rangle \\ &\cong k.\end{aligned}$$

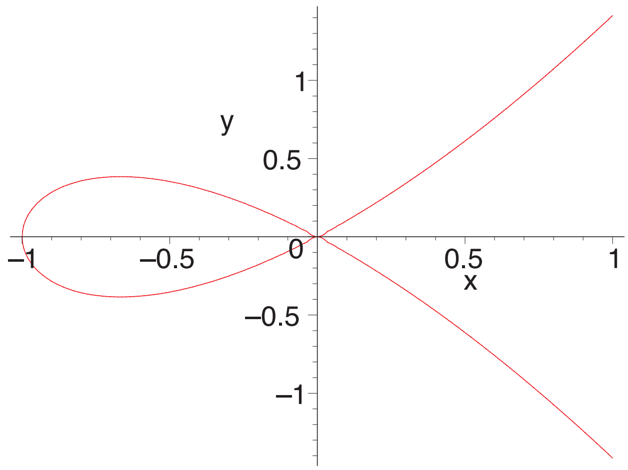


Figure 12. The nodal curve $y^2 = x^2(x+1)$.

Now, in the isomorphism (5) it is clear that only the initial terms of the relations f_i play a role. That is,

$$\begin{aligned}\mathfrak{m}_P/\mathfrak{m}_P^2 &\cong \langle y_1, \dots, y_n\rangle / \langle \{y_i y_j\}_{i,j}, \{\sum_{j=1}^n y_j \frac{\partial f_i}{\partial y_j}(0)\}_{i=1,\dots,m}\rangle \\ &\cong \oplus_{j=1}^n k y_j / V,\end{aligned} \tag{6}$$

where V is the vector space spanned by the vectors $\sum_{j=1}^n y_j \frac{\partial f_i}{\partial y_j}(0)$, $i = 1, \dots, m$. Namely, if we define the *Jacobian matrix* of Y at the point P to be

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1}(P) & \dots & \frac{\partial f_1}{\partial x_n}(P) \\ \vdots & & \vdots \\ \frac{\partial f_m}{\partial x_1}(P) & \dots & \frac{\partial f_m}{\partial x_n}(P) \end{pmatrix}$$

then we find the formula

$$\dim(\mathfrak{m}_P/\mathfrak{m}_P^2) = n - \text{rk } (\partial f_i/\partial x_j(P)).$$

We have proven the following proposition.

Proposition 6.4. *Let Y be a variety in $\mathbb{A}^n$ with $\mathcal{I}(Y) = \langle f_1, \dots, f_m\rangle$ then Y is non-singular at P if and only if*

$$\operatorname{codim}(Y) = \text{rk } (\partial f_i/\partial x_j(P)).$$

To give a tangent vector, in our definition, is to give a linear functional

$$\theta : \mathfrak{m}_P/\mathfrak{m}_P^2 \to k.$$

Such a functional is completely determined by its values $(\theta(y_1), \dots, \theta(y_n))$ that satisfy the relations

$$\sum_{i=1}^n \theta(y_i)\frac{\partial f_j}{\partial y_i}(0) = 0, \qquad j = 1, \dots, m.$$

If we interpret the vector $(\theta(y_1), \ldots, \theta(y_n))$ as defining the line

$$(\theta(y_1)t, \ldots, \theta(y_n)t), \quad t \in \mathbb{A}^1$$

through the point P, we get that the tangent space is the collection of lines ℓ through the origin such that the equations

$$f_1(\ell), \ldots, f_m(\ell)$$

vanish to a first order around P. Hence, our definition of the tangent space agrees with the intuition derived from the case of real numbers.

Example 6.5. Let us go back to the example of the nodal curve $y^2 - x^2(x+1)$. The Jacobian matrix is

$$(-3x^2 - 2x, 2y).$$

Assume first that k has characteristic different from 2. The rank of this matrix is 1 at the every point P on the curve, except at the point $(0,0)$, where it has rank 0. Thus, at every point except 0 we have $\operatorname{codim}(Y) = \operatorname{rk}(\partial f_i/\partial x_j(P))$. This shows that 0 is the only singular point.

If k has characteristic 2 then $(-3x^2 - 2x, 2y) = (-3x^2, 0)$ and the Jacobian matrix has rank 1 at every point with non-zero x coordinate. Since the only point on the curve with x coordinate equal to zero is 0, it follows again the only singular point is 0.

The tangent space at a point (x_1, y_1) is given by

$$-(3x^2 + 2x)(x - x_1) + 2y(y - y_1) = 0.$$

See Figure 13.

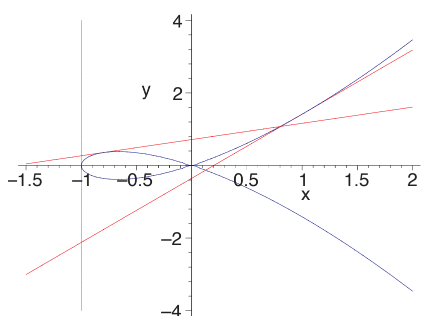


Figure 13. Tangents to the curve $y^2 = x^2(x+1)$.

END OF LECTURE 10 (October 17)

Example 6.6. Let us consider the surface $y^2 - (x^2 + z)(x+1) = y^2 - x^3 - x^2 - zx - z = 0$ in $\mathbb{A}^3$ (Figure 14). The Jacobian matrix is given by

$$(3x^2 - 2x - z, 2y, -x - 1).$$

The singular points are defined by the ideal

$$\langle y^2 - (x^2 + z)(x+1), -3x^2 - 2x - z, 2y, -x - 1\rangle.$$

Let us assume for simplicity that k has characteristic different from 2. We get then that $x = -1, y = 0, z = -1$ is the only singular point. (I recommend you check that with Macaulay, just to see that you know how to do that in more complicated examples). Note that the point $(0,0,0)$, which is a singular point on the fiber $z = 0$ of $y^2 - x^2(x+1)$, is a non-singular point of the surface.

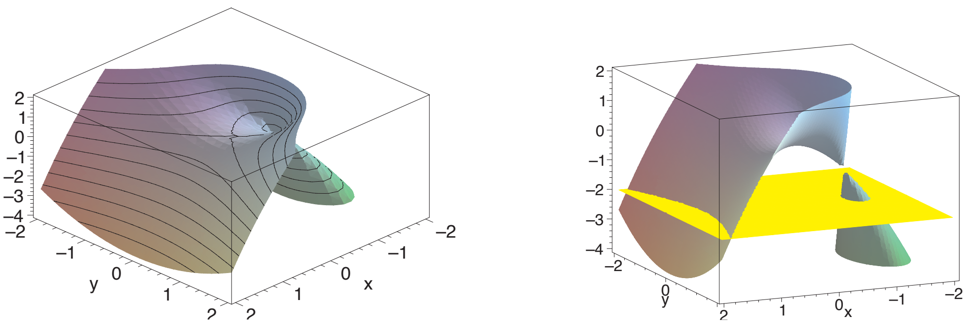


Figure 14. The surface $y^2 = (x^2 + z)(x + 1)$.

Example 6.7. Consider the twisted cubic curve $\{(t, t^2, t^3) : t \in k\}$ in $\mathbb{A}^3$. It is of codimension 2 and is equal to

$$Z(x^2 - y, x^3 - z, y^3 - z^2).$$

The Jacobian matrix is

$$\begin{pmatrix} 2x & -1 & 0 \\ 3x^2 & 0 & -1 \\ 0 & 3y^2 & -2z \end{pmatrix}$$

It has rank at least 2 at every point of $\mathbb{A}^3$ and so rank at least 2 (and hence precisely 2) at each point of the curve. It follows that the curve is non-singular. This is expected, as the curve is isomorphic to $\mathbb{P}^1$ via the 3-uple embedding; cf. page 26.

On the other hand, the higher twisted curve $\{(t^3, t^4, t^5) : t \in k\}$ in $\mathbb{A}^3$ is also of codimension 2 and is equal to

$$Z(x^4 - y^3, x^5 - z^3, y^5 - z^4).$$

(Cf. page 4.) The Jacobian matrix is

$$\begin{pmatrix} 4x^3 & -3y^2 & 0 \\ 5x^4 & 0 & -3z^2 \\ 0 & 5y^4 & -4z^3 \end{pmatrix}$$

By considering 2×2 sub determinants we see that this matrix has rank 2 at every point of the curve, except at the point $(0, 0, 0)$. See Figure 7.12.

Remark 6.8. Given a map $f : X \to Y$ we get an induced map from the tangent space of P in X to the tangent space of $f(P)$ in Y. Indeed there is a natural homomorphism of rings $\mathcal{O}_{Y,f(P)} \to \mathcal{O}_{X,P}$ taking the maximal ideal $\mathfrak{m}_{f(P)}$ of $\mathcal{O}_{Y,f(P)}$ into the maximal ideal $\mathfrak{m}_P$ of $\mathcal{O}_{X,P}$, hence inducing a map $\mathfrak{m}_{f(P)}/\mathfrak{m}_{f(P)}^2 \to \mathfrak{m}_P/\mathfrak{m}_P^2$ that induces by duality a linear map

$$T_{X,P} \to T_{Y,f(P)}.$$

In particular, if f is an isomorphism then $T_{X,P} \cong T_{Y,f(P)}$ for any $P \in X$.

6.2. **The Singular Locus.**

Theorem 6.9. *Let Y be a variety. The set of singular points of Y is a proper closed set denoted Y^{sing} and called the* **singular locus** *of Y.*

Proof. Using Lemma 5.20, we write $Y = \cup Y_\alpha$, the union taken over all open affine subsets of Y. It is enough to prove that for every α, $Y_\alpha^{\text{sing}} = Y^{\text{sing}} \cap Y_\alpha$ is a closed set and that for some α (hence for any α) it is a proper closed set.

If Y_α is affine then we have $\text{rk}(\partial f_j/\partial x_i) \leq \text{codim}(Y_\alpha)$ where $f_1, \dots, f_m$ generate $\mathcal{I}(Y_\alpha)$ in $\mathbb{A}^n$ (using the property $\dim(\mathcal{O}_{Y,P}) \leq \dim(\mathfrak{m}_P/\mathfrak{m}_P^2)$). We conclude that P is a singular point if and only if $\text{rk}(\partial f_j/\partial x_i) < \text{codim}(Y)$. This is a condition on the vanishing of all $\text{codim}(Y)$-sized minors of the Jacobian matrix, which thus defines a closed set of Y_α.

We have seen that Y is birational to a hypersurface in $\mathbb{A}^{r+1}$, where r is the dimension of Y. Hence, an open subset of Y_α is isomorphic to an open subset of that hypersurface. We conclude that it is enough to prove the theorem for hypersurfaces in $\mathbb{A}^n$.

Let $Y = \mathcal{Z}(f)$ be a hypersurface in $\mathbb{A}^n$ defined by an irreducible non-constant polynomial f. If $Y^{\text{sing}} = Y$ then we have $\partial f/\partial x_i(P) = 0$ for all $P \in Y$ and all i. It follows that for every i, $\partial f/\partial x_i \in (f)$, hence equal to zero. Therefore, if the characteristic of k is zero, f is constant which is a contradiction, and if the characteristic of k is a prime $p > 0$ then $f \in k[x_1^p, \dots, x_n^p]$ and hence of the form g^p for some polynomial $g \in k[x_1, \dots, x_n]$, which is again a contradiction to the irreducibility. $\square$

6.3. **The Tangent Cone.** The tangent space is a very crude measure for the local structure of a variety. For example, it does not allow one to distinguish between the local behavior of $y^2 = x^3$ and $y^2 = x^2(x+1)$ at the point 0. The tangent cone is a much finer invariant.

Let Y be an affine variety with coordinate ring $k[x_1, \dots, x_n]/\mathcal{I}(Y)$. We assume that $0 \in Y$ and define the tangent cone at 0. The general case is obtained by a change of variables.

Given a polynomial $f \in k[x_1, \dots, x_n]$ we write

$$f = f_r + \cdots + f_N,$$

where each f_i is homogenous of degree i and $f_r \neq 0$. We define

$$f^* = f_r$$

and call it the **leading form** of f. We further define

$$\mathcal{I}(Y)^* = \langle f^* : f \in \mathcal{I}(Y) \rangle.$$

Note that $\mathcal{I}(Y)^*$ is not necessarily a radical ideal.

Example 6.10. If $\mathcal{I}(Y) = (f)$ then $\mathcal{I}(Y)^* = (f^*)$. One inclusion is clear. For the other, note that $(fg)^* = f^*g^*$.

If $\mathcal{I}(Y) = (f_1, \dots, f_r)$ then it need not be true that $\mathcal{I}(Y)^* = (f_1*, \dots, f_r^*)$. For example, consider the ideal $I = \langle x, x + y^2 \rangle$.

Definition 6.11. The **tangent cone** for Y at 0, denoted $C_{Y,0}$ is the affine variety $\mathcal{Z}(\mathcal{I}(Y)^*)$.

Remark 6.12. Note that the tangent cone is a conical algebraic set. Note also that the tangent space at 0 to the tangent cone is contained in the tangent space to Y at 0. Indeed, take generators $f_1, \dots, f_m$ to $I = I(Y)$ such that I^* is generated by $f_1^*, \dots, f_m^*$. The cotangent space of Y is given by

$$(x_1, \dots, x_n)/(x_i x_j, (f_1)_1, \dots, (f_1)_m).$$

Here $(f_i)_1$ is the degree 1 term of f_i, that may be zero. If $f_i^* = (f_i)_1$ then the equation $(f_i)_1$ is also included in the description of the tangent space to the tangent cone. And, if $f_i^* \neq (f_i)_1$ then it means that $(f_i)_1 = 0$ and so it doesn't appear in the description of the tangent space for Y at 0. Note, however, that since the radical of I^* may be strictly larger than I^*, we may get additional equations in the description of the tangent space at zero for the tangent cone. See the example of the cuspidal curve (Example 6.14).

We shall see below that the tangent space and the tangent cones are equal at every non-singular point.

Example 6.13. Consider the nodal curve $Y : y^2 = x^2(x+1)$. The tangent cone at 0 is given by the ideal $\mathcal{I}(Y)^* = (y^2 - x^2) = (y+x)(y-x)$. See Figure 15. At the point $(-1, 0)$ we develop

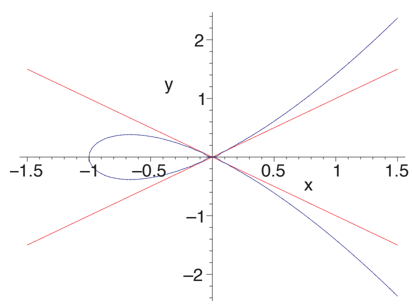


Figure 15. The tangent cone at 0 to $y^2 = x^2(x+1)$.

$y^2 - x^2(x+1)$ using the parameters $x+1$ and y to find $y^2 - x^2(x+1) = y^2 - (x+1)^3 + 2(x+1)^2 - (x+1)$ and hence the tangent cone is given by $x+1$.

Example 6.14. Consider the cuspical curve $Y : y^2 = x^3$. The tangent cone at 0 is given by the ideal $\mathcal{I}(Y)^* = (y^2)$. See Figure 16. Note that in some sense the line $y = 0$, which is the tangent cone, should be counted with double multiplicity. The tangent space at the singular point $(0, 0)$ is $\mathbb{A}^2$. Indeed

$$(x, y)/(x^2, y^2, xy, y^2 - x^3) = (x, y)/(x^2, y^2, xy)$$

is a 2 dimensional vector space. On the other hand, the radical ideal defining the tangent cone is (y) and the tangent space to it at the point $(0, 0)$ is one dimensional

$$(x, y)/(x^2, y^2, xy, y) = (x)/(x^2).$$

Definition 6.15. Let A be a local ring with maximal ideal $\mathfrak{m}$. Define the **associated graded ring** $\mathrm{gr}(A)$ by

$$\mathrm{gr}(A) = \oplus_{a=0}^{\infty} \mathfrak{m}^a / \mathfrak{m}^{a+1},$$

where $\mathfrak{m}^0 = A$ by definition.

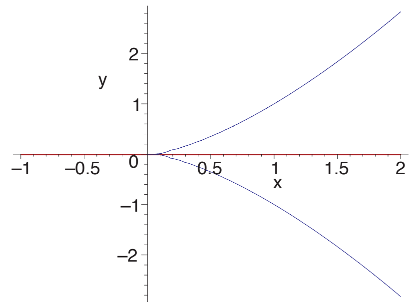


Figure 16. The tangent cone at 0 to $y^2 = x^3$.

Note that $\mathrm{gr}(A)$ is a graded k-algebra, where $k = A/\mathfrak{m}$. Suppose that $f_1, \dots, f_n$ are generators for $\mathfrak{m}$ as a k-module then

$$\mathrm{gr}(A) \cong k[x_1, \dots, x_n]/I^*,$$

where I^* is some homogenous ideal. Indeed, the graded ring homomorphism $k[x_1, \dots, x_n] \to \mathrm{gr}(A)$, $x_i \mapsto f_i \in \mathfrak{m}/\mathfrak{m}^2$ (and so a monomial $x^I = x_1^{i_1} \cdots x_n^{i_n}$ of degree a maps to $f^I = f_1^{i_1} \cdots f_n^{i_n} \in \mathfrak{m}^a/\mathfrak{m}^{a+1}$), has kernel which is a homogenous ideal.

Let Y be an affine variety in $\mathbb{A}^n$ and say $0 \in Y$. The maximal ideal of 0 in Y is $\mathfrak{m} := (x_1, \dots, x_n)/\mathcal{I}(Y)$. Then $A := \mathcal{O}_{Y,0}$ is a local ring with maximal ideal $\mathfrak{m}A$ because it is the localization of $A(Y)$ at $\mathfrak{m}$:

$$A = (k[x_1, \dots, x_n]/\mathcal{I}(Y))_{\mathfrak{m}}.$$

We calculate now the associated graded ring $\mathrm{gr}(A)$. We use a subscript a to denote homogenous elements of weight a.

$$\begin{aligned}
\mathrm{gr}(A) &= \oplus_{a=0}^{\infty} (\mathfrak{m}A)^a/(\mathfrak{m}A)^{a+1} \\
&\cong \oplus_{a=0}^{\infty} \mathfrak{m}^a/\mathfrak{m}^{a+1} \\
&= \oplus_{a=0}^{\infty} (x_1, \dots, x_n)^a/\langle (x_1, \dots, x_n)^{a+1}, \mathcal{I}(Y) \cap (x_1, \dots, x_n)^a \rangle \\
&= \oplus_{a=0}^{\infty} (x_1, \dots, x_n)^a/\langle (x_1, \dots, x_n)^{a+1}, \mathcal{I}(Y)^*_a \rangle \\
&= \oplus_{a=0}^{\infty} [k[x_1, \dots, x_n]/\mathcal{I}(Y)^*]_a \\
&\cong k[x_1, \dots, x_n]/\mathcal{I}(Y)^*.
\end{aligned}$$

(In passing to the second line we used that $\mathfrak{m}^a/\mathfrak{m}^{a+1} = (\mathfrak{m}A)^a/(\mathfrak{m}A)^{a+1}$. This follows from the fact that localization is an exact functor; we localize at $\mathfrak{m}$ the sequence $0 \to \mathfrak{m}^{a+1} \to \mathfrak{m}^a \to \mathfrak{m}^a/\mathfrak{m}^{a+1} \to 0$ and the fact that the localization of $\mathfrak{m}^a/\mathfrak{m}^{a+1}$ in $\mathfrak{m}$ is just $\mathfrak{m}^a/\mathfrak{m}^{a+1}$.) We proved:

Proposition 6.16. *Let Y be an affine variety. The tangent cone to Y at a point $P \in Y$ is isomorphic to $\mathrm{gr}(\mathcal{O}_{Y,P})$.*

In fact, the Proposition doesn't quite make sense in the category of varieties, as we are always supposed to work with rings without nilpotents and $\mathrm{gr}(\mathcal{O}_{Y,P})$ may have nilpotents. See Example 6.14. The statement in the theory of varieties is thus that the tangent cone is the affine variety associated to the k-algebra $\mathrm{gr}(\mathcal{O}_{Y,P})/\mathfrak{n}$, where $\mathfrak{n}$ is the ideal of nilpotent elements of $\mathrm{gr}(\mathcal{O}_{Y,P})$.

Note that the proposition allows us an intrinsic definition of the tangent cone to any variety Y at any of its points P as $\mathrm{gr}(\mathcal{O}_{Y,P})$ (or $\mathrm{gr}(\mathcal{O}_{Y,P})/\mathfrak{n}$ if we insist on sticking to varieties). It is a fact that for every local ring A, $\dim(A) = \dim \operatorname{gr}(A)$. We conclude that the dimension of the tangent cone is equal to the dimension of the variety.

Note also that the tangent space $\operatorname{Hom}(\mathfrak{m}_P/\mathfrak{m}_P^2, k)$ is isomorphic to k^n for some n and if we think about it as an affine variety that its ring of regular functions is canonically the k-algebra $\operatorname{Sym}(\mathfrak{m}_P/\mathfrak{m}_P^2)$. There is a canonical surjective homomorphism

$$\operatorname{Sym}(\mathfrak{m}_P/\mathfrak{m}_P^2) \to \operatorname{gr}(\mathcal{O}_{Y,P})$$

induced from the inclusion $\mathfrak{m}_P/\mathfrak{m}_P^2 \to \operatorname{gr}(\mathcal{O}_{Y,P})$, which induces a surjective homomorphism

$$\operatorname{Sym}(\mathfrak{m}_P/\mathfrak{m}_P^2) \to \operatorname{gr}(\mathcal{O}_{Y,P})/\mathfrak{n},$$

that gives a canonical embedding

$$C_{Y,P} \hookrightarrow T_{Y,P}.$$

Now, since $\dim C_{Y,P} = \dim Y$ and $\dim T_{Y,P} \geq \dim Y$ with equality iff P is non-singular, we conclude:

Corollary 6.17. *The inclusion $C_{Y,P} \hookrightarrow T_{Y,P}$ is an isomorphism iff P is non-singular.*

We shall come back to the tangent cone when we discuss blow-up of varieties.

END OF LECTURE 11 (October 22)

6.4. **The Completion of Local Ring.** This is another way to study the local behavior of a variety at a point. We recall here that a local ring $(A, \mathfrak{m})$ is called **complete** if $A \cong \widehat{A} := \varprojlim A/\mathfrak{m}^n$. If $(A, \mathfrak{m})$ a local ring then $\widehat{A}$ is a complete local ring. The main theorem one employs is

Theorem 6.18. (Cohen's Structure Theorem) *Let $(A, \mathfrak{m})$ be a complete regular local ring of dimension n that contains a field, then*

$$A \cong k[[x_1, \dots, x_n]],$$

where $k = A/\mathfrak{m}$. Moreover, this isomorphism can be chosen so that the images of $x_1, \dots, x_n$ are any desired set of generators for $\mathfrak{m}/\mathfrak{m}^2$.

It follows that if X is a variety over k, P a non-singular point of X and $f_1, \dots, f_n$ are elements of the maximal ideal $\mathfrak{m}_P$ of P in X that generate $\mathfrak{m}_P/\mathfrak{m}_P^2$ then there exists an isomorphism

$$\widehat{\mathcal{O}}_{X,P} \cong k[[x_1, \dots, x_n]],$$

such that f_i maps to x_i.

In general, if $\psi : X \to Y$ is a morphism and $P \in X$, we get a homomorphism

$$\widehat{\mathcal{O}}_{Y,\psi(P)} \to \widehat{\mathcal{O}}_{X,P}, \tag{7}$$

which is an isomorphism if ψ is an isomorphism (even locally around P and $\psi(P)$). A morphism ψ is called **étale** if we have an isomorphism in (7) for every point $P \in X$.

Example 6.19. Let X be the curve $y^2 = x^2(x+1)$ in $\mathbb{A}^2$ and $P = (0,0)$. One can show that

$$\widehat{\mathcal{O}}_{X,P} \cong k[[x,y]]/(y^2 - x^2(x+1)) \cong k[[u,v]]/(uv).$$

7. Gröbner bases

Let k be a field. A **monomial order** on $k[x_1, \dots, x_n]$ is a relation $>$ on the set of monomials $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ such that:

(1) $>$ is a linear order.
(2) If $x^\alpha > x^\beta$ then for every x^γ we have $x^{\alpha+\gamma} > x^{\beta+\gamma}$.
(3) It is a well-ordering. Namely, any non-empty set of monomials has a minimal element under $>$.

There are many monomial orders. The one we will be using most is the lexicographic order, but other orders (such as, graded lexicographic order, graded reverse lexicographic order) are useful as well. In the **lexicographic order** we say that a monomial $x^\alpha > x^\beta$ if in the vector $\alpha - \beta$, which is a vector in $\mathbb{Z}^n$, the first left most entry that is not zero is positive. Having a monomial order allows us to speak of the largest monomial (in the order sense) that appears in a polynomial f. We will call it the **leading term** $\mathrm{LT}(f)$ of f. Note that it doesn't have to be a monomial x^α whose total weight $|\alpha| = \alpha_1 + \cdots + \alpha_n$ is maximal.

7.0.1. *Division algorithm.* One can define a **division algorithm** in $k[x_1, \dots, x_n]$ with respect to a monomial order.

Let $F = (f_1, \dots, f_s)$ be an ordered set of polynomials in $k[x_1, \dots, x_n]$. Then any polynomial $f \in k[x_1, \dots, x_n]$ can be written uniquely as

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

where the a_i's and r are polynomials, and for each i, either $a_i f_i = 0$ or $\mathrm{LT}(f) \geq \mathrm{LT}(a_i f_i)$, and either $r = 0$ or r is a linear combination of monomials none of which is divisible by any of the leading terms of $f_1, \dots, f_s$. r is called the **remainder** *of the division of f by F.*

Remark 7.1. Note that for $k[x]$ with the usual order (in fact, there isn't any other in that case), this is the familiar division with residue in a Euclidean ring.

The division algorithm can be proven by induction on the leading term of f. If the leading term of f is divisible by the leading term of some f_i, then take the minimal i so that this occurs and for some a_i we have $\mathrm{LT}(a_i f_i) = \mathrm{LT}(f)$ and so $f - a_i f_i$ will have a leading term that is smaller then f's. One uses induction at this point. If the leading term of f is not divisible by any of the leading terms of f_i then put the leading term of f into the remainder and apply induction to f minus its leading term.

You will notice that the statement as given is not complete and not accurate. Still, remarkably, that is how it is formulated in several very successful books on the subject. The point that has to be added is in which way the order of the basis matters. It is exactly when carrying out the inductive process as in the sketch of proof. One checks for each $i = 1, 2, \dots, s$ in turn whether the next step can be carried out. One takes the *first* i such that $\mathrm{LT}(f_i)$ divides the leading term of the polynomial left at this point.

Example 7.2. Take $F = (f_1, f_2) = (y^2 - 1, xy - 1)$ and $f = x^2y + xy^2 + y^2$. The leading term of f is x^2y and it is not divisible by the leading term of f_1, but is divisible by xy which is the leading term of f_2. We have then $f - x(xy - 1) = xy^2 + y^2 + x$. The leading term now is xy^2 which is divisible by the leading term of f_2. We subtract $x(y^2 - 1)$ and get $xy^2 + y^2 + x - x(y^2 - 1) = y^2 + 2x$. The leading term of this polynomial is divisible by that of f_1 and we now consider $y^2+2x-(y^2-1)=2x+1$. The remainder $2x+1$ is a sum of monomials none of which is divisible by the leading term of f_1 or f_2 and so is the remainder. Altogether,

$$x^2y+xy^2+y^2=(x+1)\cdot(y^2-1)+x\cdot(xy-1)+2x+1.$$

On the other hand, if we take $F=(xy-1,y^2-1)$ we get the following. At the first step we reduce to $f-x(xy-1)=xy^2+y^2+x$. The leading term now is xy^2 and it is divisible by the leading term of $xy-1$ and so we get $xy^2+y^2+x-y(xy-1)=y^2+y+x$. The leading term now is x and it is not divisible by the leading terms of $xy-1, y^2-1$. However, the polynomial y^2+y+x is not yet the remainder because one of its terms, namely y^2 is divisible by the leading term of y^2-1. Thus, we write $y^2+y+x-(y^2-1)=x+y+1$. At this point we are left with a polynomial $x+y+1$ none of its terms is divisible by the leading terms of f_1, f_2 and so it is the remainder. Thus, we get

$$x^2y+xy^2+y^2=(x+y)\cdot(xy-1)+1\cdot(y^2-1)+x+y+1.$$

7.0.2. *Monomial ideals and Dickson's lemma.* An ideal I of $k[x_1,\dots,x_n]$ is called a **monomial ideal** it is generated by monomials as an ideal. That is, for some set of monomials $\{x^\alpha:\alpha\in A\subset\mathbb{Z}^n_{\geq 0}\}$ we have $I=\langle\{x_\alpha:\alpha\in A\}\rangle$. Hilbert's nullstellensatz guarantees that I has a finite basis. However, a strong statement is true.

Lemma 7.3. *(Dickson's lemma) Let I be a monomial ideal then I has a finite basis consisting of monomials.*

7.0.3. *Gröbner bases.* Let I be an ideal. Let $\langle \mathrm{LT}(I)\rangle$ be the (monomial) ideal generated by all leading terms of elements of I. Using Dickson's lemma, there are then polynomials $g_1,\dots,g_s$ in I such that $\langle \mathrm{LT}(I)\rangle=\langle \mathrm{LT}(g_1),\dots,\mathrm{LT}(g_s)\rangle$. Such a set is called a **Gröbner basis** of I. The following lemma gives some basic properties of a Gröbner basis.

Lemma 7.4. *If $\{g_1,\dots,g_s\}$ is a Gröbner basis then it is a basis for I. Furthermore, the leading term of every polynomial in I is divisible by some $\mathrm{LT}(g_i)$. Conversely, given a set $\{g_1,\dots,g_s\}$ of elements of I such that the leading term of every polynomial in I is divisible by some $\mathrm{LT}(g_i)$, the set $\{g_1,\dots,g_s\}$ is a Gröbner basis for I (and hence, by the first part, a basis of I as well).*

Proof. The second part is clear as in that case $\langle \mathrm{LT}(g_1),\dots,\mathrm{LT}(g_s)\rangle=\langle \mathrm{LT}(I)\rangle$.

For the first part, let $f\in I$ and perform division with residue in $g_1,\dots,g_s$:

$$f=a_1g_1+\cdots+a_sg_s+r,$$

where, $r\neq 0$, no term in the remainder r is divisible by $\mathrm{LT}(g_i)$ for any i. But, $r\in I$ and so

$$\mathrm{LT}(r)\in\langle \mathrm{LT}(I)\rangle=\langle \mathrm{LT}(g_1),\dots,\mathrm{LT}(g_s)\rangle.$$

Suppose $r\neq 0$. So we can write

$$\mathrm{LT}(r)=\sum h_i\mathrm{LT}(g_i).$$

Expanding the right hand side linearly, we find a sum of linear terms, each of which is divisible by some $\mathrm{LT}(g_i)$ and so this must hold for the left hand side too. Contradiction. Thus, $r=0$. The argument also shows that the leading term of every polynomial in I is divisible by some $\mathrm{LT}(g_i)$. $\square$

Theorem 7.5. *Let I be an ideal and choose a Gröbner basis $\{g_1,\dots,g_s\}$ for it. Then a polynomial f belongs to I if and only if in the division of f by $G=(g_1,\dots,g_s)$ the residue is zero.*

Proof. That follows from the argument we have just given. □

7.0.4. *Buchberger's Criterion.* The question that remains is how to find Gröbner bases for a given ideal. Let f and g be non-zero polynomials with leading monomials x^α, x^β respectively. Let $\gamma = (\gamma_1, \dots, \gamma_n)$ with $\gamma_i = \max(\alpha_i, \beta_i)$ and let

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

Example 7.6. If $f = x^3y^2 - x^2y^3 + x$, $g = 3x^4y + y^2$ then the leading terms are respectively x^3y^2 and $3x^4y$. Here $\gamma = (4,2)$ and $S(f,g) = \frac{x^4y^2}{x^3y^2} \cdot (x^3y^2 - x^2y^3 + x) - \frac{x^4y^2}{3x^4y} \cdot (3x^4y + y^2) = x \cdot (x^3y^2 - x^2y^3 + x) - \frac{1}{3}y \cdot (3x^4y + y^2) = -x^3y^3 + x^2 - \frac{1}{3}y^3$.

Theorem 7.7. *(Buchberger) Let $G = (g_1, \dots, g_s)$ be a basis for an ideal I. Then G is a Gröbner basis if for all $i \neq j$ the remainder of division of $S(g_i, g_j)$ by G is zero.*

Buchberger's criterion gives an effective algorithm for finding Gröbner bases. Start with any finite basis G for the ideal I. Add to G the remainder upon division by G of a pair $S(f,g)$, if there are $f, g \in G$ such that this remainder is not zero (if there's more than one pair f, g choose one arbitrarily). Note that if the remainder of $S(f,g)$ is not zero then $\mathrm{LT}(S(f,g))$ does not belong to $\langle \mathrm{LT}(G) \rangle$ because it is not divisible by any element of $\mathrm{LT}(G)$. Thus, the ideal generated by $\mathrm{LT}(G \cup S(f,g))$ strictly contains the ideal generated by $\mathrm{LT}(G)$. This shows that this process must end. Thus, at some point we get a set G such that each $S(f,g)$, $f, g \in G, f \neq g$, has remainder zero when divided by G and by Buchberger's criterion such G is a Gröbner basis for I.

END OF LECTURE 12 (October 24)

7.1. **Applications of Gröbner bases.** We give here a few initial applications. We shall see more applications later on, but we would still nonetheless be just scratching the surface. The theory of Gröbner became the central computational tool in algebraic geometry and is able to answer of host of important and natural questions (such as, when are two ideals are equal, how to calculate the radical of an ideal, how to calculate sum and intersection of ideals and much more). We refer to Cox, Little and O'Shea: *Ideals, Varieties, and Algorithms* for a gentle and much more complete introduction to the subject of Gröbner bases and many of their applications.

7.1.1. *The membership problem.* Let I be an ideal, presented by a basis G. Then the membership problem for I can be solved. Namely, given a polynomial f there is a finite procedure to determine if $f \in I$. Indeed, first make from G a Gröbner basis, still denoted G, as described above. Next, divide f by G. $f \in I$ if and only if the remainder is zero.

7.1.2. *Calculating the radical of an ideal.* This is based on the following lemma.

Lemma 7.8. *$f \in \sqrt{I}$ if and only if $1 \in I + (x_{n+1}f - 1)$, an ideal in $k[x_1, \dots, x_{n+1}]$.*

The lemma then reduces checking if $f \in \sqrt{I}$ to the membership problem for the ideal $I + (x_{n+1}f - 1)$, which we have solved.

7.1.3. *The tangent cone.* Using the method of Gröbner bases we can find a way to compute the tangent cone. Consider the case of $Y \subset \mathbb{A}^n$ with variables $x_1, \ldots, x_n$ and the usual lexicographic order $x_1 > \cdots > x_n$. Denote

$$\mathcal{I}(Y) = I = \langle f_1, \ldots, f_s \rangle.$$

Let J be the ideal of $k[x_0, \ldots, x_n]$ given by

$$J = \langle F_1, \ldots, F_s \rangle,$$

where F_i is the homogenization of f_i with respect to x_0.[16] We take on $k[x_0, \ldots, x_n]$ the lexicographic order $x_0 > x_1 > \cdots > x_n$. Let $G_1, \ldots, G_t$ be any Gröbner basis for J with respect to this order. Let

$$g_i = G_i(1, x_1, \ldots, x_n)$$

be the de-homogenization of G_i relative to x_0.

Proposition 7.9. *We have the equality of ideals*

$$I^* = \langle g_1^*, \ldots, g_t^* \rangle.$$

Proof. Let $g \in I$. We want to prove that

$$g^* \in \langle g_1^*, \ldots, g_t^* \rangle.$$

Write $g = \sum p_i \cdot f_i$ for some polynomials $p_i \in k[x_1, \ldots, x_n]$, and let G, P_i and F_i be the corresponding homogenizations with respect to x_0. We have then for suitable $a, a_1, \ldots, a_s$ that $x_0^a G = \sum x_0^{a_i} P_i F_i \in J$. We have the expression

$$x_0^a G = x_0^b g^* + \text{terms of lower degree in } x_0.$$

We can also write $x_0^a G$ using the Gröbner basis as

$$x_0^a G = \sum Q_i G_i$$

and because of the formalism of Gröbner bases we have that

$$\mathrm{LT}(Q_i G_i) \leq \mathrm{LT}(x_0^a G), \qquad i = 1, \ldots, t,$$

which implies that

$$\deg_{x_0}(Q_i G_i) \leq b, \qquad i = 1, \ldots, t.$$

It follows that $x_0^b g^*$ is the sum of those terms in $Q_i G_i$ that have x_0-degree exactly b and, moreover, those are the terms of highest x_0-degree. Equivalently, g^* is the sum of the terms of lowest total degree in $Q_i(1, x_1, \ldots, x_n) G_i(1, x_1, \ldots, x_n)$, which, in turn, belong to J. $\square$

Example 7.10. For plane curves $Y = Z(f(x, y))$, where $f(x, y)$ is an irreducible polynomial there is nothing new here. If we homogenize f we get $J = (F)$ and F is a Gröbner basis (this holds for any principal ideal). Thus, we find that the ideal I^* is generated by f^*, which is nothing new. The tangent cone at zero is then a union of irreducible plane curves corresponding to the irreducible polynomials dividing f. For example, for the curve

$$x^2 y + x y^2 = x^4 + y^4$$

(see Figure 7.10), the leading term is

$$x^2 y + x y^2 = x \cdot y \cdot (x + y).$$

[16] Note that J is usually not the homogenization of I.

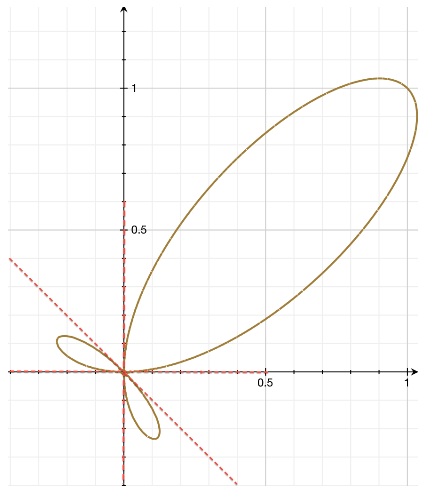


Figure 17. The plane curve $x^2y + xy^2 = x^4 + y^4$.

Example 7.11. Let us look at the **pinch**. This is the surface

$$xy^2 = z^2.$$

(See Figure 7.11). The leading term is z^2 which gives as the tangent cone the plane $z = 0$. The

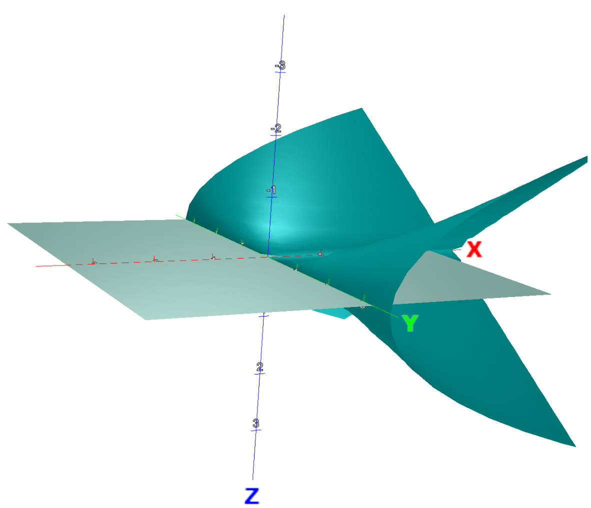


Figure 18. The pinch singularity $xy^2 = z^2$.

tangent space is the whole space.

Example 7.12. For out last example we look at the very twisted curve, the singular curve (t^3, t^4, t^5) in $\mathbb{A}^3$. See Figure 7.12.

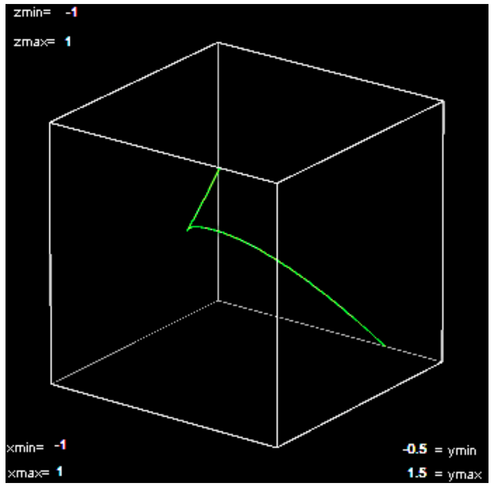


Figure 19. The twisted curve (t^3, t^4, t^5).

We assume characteristic zero. The curve is defined by the ideal

$$x^4 - y^3, \quad y^5 - z^4, \quad x^5 - z^3.$$

The Jacobian matrix is

$$\begin{pmatrix} 4x^3 & -3y^2 & 0 \\ 0 & 5y^4 & -4z^3 \\ 5x^4 & 0 & -3z^2 \end{pmatrix}$$

One quickly verities that the point $(0, 0, 0)$ is the only singular point and that the tangent space there is 3-dimensional. If we homogenize the equations we find $x^4 - uy^3, y^5 - uz^4, x^5 - u^2z^3$. It is not a Gröbner basis (calculate the S-polynomial of the first two generators) and creating a Gröbner basis will be too laborious to do by hand. We resort to a trick. Consider the ideal generated by the leading terms of the 3 equations we have. It is $K = \langle y^3, z^3\rangle$. We know that the tangent cone has dimension 1 and the radical of the ideal defining it is contained in the radical of the ideal K. But the radical of K is $\langle y, z\rangle$ which is a prime ideal. Thus, it defines the tangent cone.

8. Blow-up

The construction of blow-up is an example of a birational map, but, more important, it is one of the canonical approaches to resolving singularities:

Let X be a variety and $Y \to X$ a morphism which is surjective and birational. Assume that Y is non-singular then we say Y is a resolution of singularities for X. While the process of blow-up does not guarantee the resolution of singularities, it is certainly one of the first places to look!

8.1. **Definition of Blow-up.** Consider the variety $\mathbb{A}^n \times \mathbb{P}^{n-1}$ with coordinates $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ respectively (note the non-orthodox choice of indices). The closed sets are defined by zeros of polynomials $f(x_1, \ldots, x_n, y_1, \ldots, y_n)$ homogenous in the y_i's. As a reminder of that we shall write $f(x_1, \ldots, x_n; y_1 : \cdots : y_n)$ for such a polynomial.

Definition 8.1. The **blow-up of $\mathbb{A}^n$ at zero** is the closed set $X = \mathrm{Bl}_0(\mathbb{A}^n)$ of $\mathbb{A}^n \times \mathbb{P}^{n-1}$ given by the equations

$$x_i y_j = x_j y_i, \qquad i, j = 1, \ldots, n.$$

An example is provided in Figure 20 for the case $n = 2$. The Figure shows the part of the blow up lying in $\mathbb{A}^2 \times \mathbb{A}^1 \subset \mathbb{A}^2 \times \mathbb{P}^1$ as it lies over $\mathbb{A}^2$.

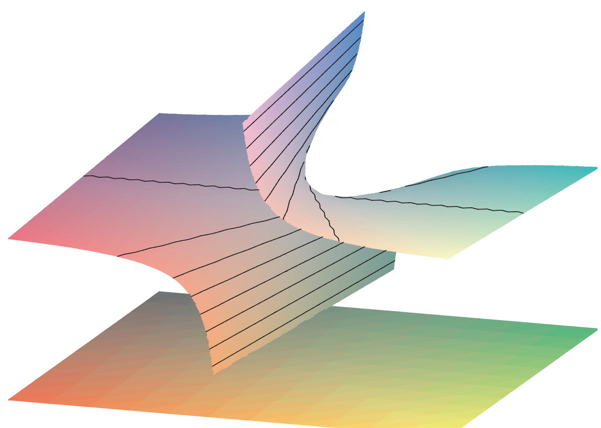


Figure 20. Blow-up of $\mathbb{A}^2$ at the origin.

Scholie. Consider the ring $k[x_1, \ldots, x_n][y_1, \ldots, y_n]$, where we think about this ring as $A[y_1, \ldots, y_n]$, where $A = k[x_1, \ldots, x_n]$ are the "scalars", and the ring is graded by the degree of polynomials in the y_i. In a certain sense, made precise best through the theory of schemes, this ring gives the projective space over $\mathbb{A}^n$. For example, assigning a particular value to $x_1, \ldots, x_n$ (that is, a point of $\mathbb{A}^n$) we get a homomorphism $A = k[x_1, \ldots, x_n] \to k$ and we obtain from $k[x_1, \ldots, x_n][y_1, \ldots, y_n]$ the ring of polynomials $k[y_1, \ldots, y_n]$ with algebraic sets defined by homogenous polynomials. In that sense, In that sense, we see that $A[y_1, \ldots, y_n]$ is a description of

$$\begin{tikzcd} P \times \mathbb{P}^{n-1} \arrow[r, hook] \arrow[d] & \mathbb{A}^n \times \mathbb{P}^{n-1} \arrow[d] & & k[y_1, \ldots, y_n] & A[y_1, \ldots, y_n] \arrow[l, two heads] . \\ P \arrow[r, hook] & \mathbb{A}^n \arrow[r, phantom, "\leftarrow \Vert \rightarrow"] & & k \arrow[u, hook] & A \arrow[l, two heads] \arrow[u, hook] \end{tikzcd}$$

Consider the ideal $I = (x_1, \dots, x_n)$ defining the point $(0, \dots, 0)$ on $\mathbb{A}^n$. Recall that we have constructed a graded ring $\oplus_{d=0}^{\infty} I^d$. There is a surjective graded rings homomorphism

$$A[y_1, \dots, y_n] \to \oplus_{d=0}^{\infty} I^d$$

that takes a monomial y^J ($J = (j_1, \dots, j_n)$ a multi-index) to $x^J \in I^d$, where $d = |J|$. Namely, it is the unique homomorphism of graded A algebras taking A isomorphically to itself $A = I^0$, and taking y_i to $x_i \in I$. Let K be the kernel of this homomorphism. It is a graded ideal where K_d are sums degree d monomials in the variables $y_1, \dots, y_d$ multiplied by coefficients being elements of A, namely $\sum_{|J|=d} f_J(x_1, \dots, x_n) y^J$, such that $\sum_{|J|=d} f_J(x_1, \dots, x_n) x^J = 0$. For example, K_1 is k-linear the span of elements of the form $x_i y_j - x_j y_i$, and using this it is not hard to show that

$$K = \langle x_i y_j - x_j y_i : i, j = 1, \dots, n \rangle.$$

Thus, we have

$$\begin{tikzcd}
\{0\} \times \mathbb{P}^{n-1} \arrow[r, hook] \arrow[d, two heads] & \mathbb{A}^n \times \mathbb{P}^{n-1} \arrow[d, two heads] & \mathrm{Bl}_0(\mathbb{A}^n) \arrow[l, hook'] \arrow[dl] \\
\{0\} \arrow[r, hook] & \mathbb{A}^n &
\end{tikzcd}
\qquad \leftarrow \Big\| \rightarrow \qquad
\begin{tikzcd}
k[y_1, \dots, y_n] & A[y_1, \dots, y_n] \arrow[l, two heads] \arrow[r, two heads] & \frac{k[x_1,\dots,x_n][y_1,\dots,y_n]}{\langle \{x_i y_j - x_j y_i\} \rangle} \\
k \arrow[u, hook] & A \arrow[l, two heads] \arrow[u, hook] \arrow[ur, hook] &
\end{tikzcd}$$

Theorem 8.2. *The morphism $\varphi : \mathrm{Bl}_0(\mathbb{A}^n) \to \mathbb{A}^n$ has the following properties:*

(1) $\varphi : \mathrm{Bl}_0(\mathbb{A}^n) \setminus \varphi^{-1}(0) \to \mathbb{A}^n \setminus \{0\}$ *is an isomorphism.*

(2) $\varphi^{-1}(0) \cong \mathbb{P}^{n-1}$ *and there is a natural bijection between lines through the origin in $\mathbb{A}^n$ and points in $\varphi^{-1}(0)$ (called the* ***exceptional fibre****). If ℓ is a line and p_ℓ the corresponding point in $\mathbb{P}^{n-1}$ then*

$$\overline{\varphi^{-1}(\ell - \{0\})} \cap \varphi^{-1}(0) = p_\ell.$$

(3) $\mathrm{Bl}_0(\mathbb{A}^n)$ *is irreducible.*

Proof. First note that φ is a morphism, since it is a restriction of the projection morphism

$$p_1 \colon \mathbb{A}^n \times \mathbb{P}^{n-1} \to \mathbb{A}^n, \qquad p_1(x_1, \dots, x_n; y_1 : \dots y_n) = (x_1, \dots, x_n).$$

We note that there is a natural isomorphism

$$\varphi^{-1}(0) = \{(0, \dots, 0; y_1 : \dots : y_n) : (y_1 : \dots : y_n) \in \mathbb{P}^{n-1}\} \cong \mathbb{P}^{n-1}.$$

Given $x \in \mathbb{A}^n - \{0\}$, say $x = (x_1, \dots, x_n)$, with $x_i \neq 0$, define

$$g(x) = (x_1, \dots, x_n; x_1 : \dots : x_n).$$

The function g is well defined and is easily checked to be a morphism given the property

$$g^* f(x_1, \dots, x_n, y_1, \dots, y_n) = f(x_1, \dots, x_n; x_1 : \dots : x_n).$$

To show that $g = \varphi^{-1}$ on $\mathbb{A}^n - \{0\}$ we just need to show that $\varphi|_{X - \varphi^{-1}(0)}$ is injective.

Suppose $x = (x_1, \dots, x_n; y_1 : \dots : y_n) \in \mathrm{Bl}_0(\mathbb{A}^n) - \varphi^{-1}(0)$ then there exists an i such that $x_i \neq 0$. This implies that for all j we have

$$y_j = y_i x_j x_i^{-1},$$

which implies that $(y_1 : \dots : y_n)$ is uniquely determined by x. Hence (1) follows.

To prove (2) we write a line ℓ in $\mathbb{A}^n$ passing through 0 as $\ell = \{t(\ell_1, \dots, \ell_n) : t \in k\}$. Then $p_\ell = (\ell_1 : \cdots : \ell_n)$, which sets up a natural bijection

$$\{\text{Lines through } 0\} \leftrightarrow \text{points in } \varphi^{-1}(0)$$

by

$$\ell \leftrightarrow (0, \dots, 0; \ell_1 : \dots, \ell_n).$$

Now,

$$\varphi^{-1}(\ell - \{0\}) = \{(t\ell_1, \dots, t\ell_n; \ell_1 : \dots, \ell_n) : t \neq 0\}.$$

Let $f(x_1, \dots, x_n, y_1, \dots, y_n)$ be a polynomial, homogenous in the y_i's, that vanishes on $\varphi^{-1}(\ell - \{0\})$. Thinking on the restriction of f to $\varphi^{-1}(\ell - \{0\})$ as a polynomial in t we see that also $f(0, \dots, 0; \ell_1 : \dots, \ell_n) = 0$ and therefore $(0, \dots, 0, \ell_1 : \dots, \ell_n) \in \overline{\varphi^{-1}(\ell - \{0\})} \cap \varphi^{-1}(0)$. On the other hand, let $f_1, \dots, f_{n-1}$ be the (homogenous) linear equations defining ℓ in $\mathbb{A}^n$. Let

$$F_i(x_1, \dots, x_n; y_1 : \cdots : y_n) = f_i(y_1, \dots, y_n).$$

Then the forms F_i vanish on $\varphi^{-1}(\ell - \{0\})$ and hence

$$\overline{\varphi^{-1}(\ell - \{0\})} \cap \varphi^{-1}(0) \subseteq \mathcal{Z}(F_1, \dots, F_{n-1}) \cap \varphi^{-1}(0) = \{(0, \dots, 0; \ell_1 : \cdots : \ell_n)\}.$$

It remains to prove (3). Since $\mathrm{Bl}_0(\mathbb{A}^n)$ is closed and since $\varphi^{-1}(0) \subseteq \overline{\mathrm{Bl}_0(\mathbb{A}^n) - \varphi^{-1}(0)}$ it is enough to prove that $\mathrm{Bl}_0(\mathbb{A}^n) - \varphi^{-1}(0)$ is irreducible. But

$$\mathrm{Bl}_0(\mathbb{A}^n) - \varphi^{-1}(0) \cong \mathbb{A}^n - \{0\},$$

which is irreducible, being an open set of the irreducible space $\mathbb{A}^n$. □

Scholie. The surjective ring homomorphism

$$A[y_1, \dots, y_n] \to \oplus_{d=0}^{\infty} I^d$$

can be composed with another surjective graded ring homomorphism

$$A[y_1, \dots, y_n] \to \oplus_{d=0}^{\infty} I^d \to \oplus_{d=0}^{\infty} I^d/I^{d+1},$$

the kernel of which is the graded ideal of $A[y_1, \dots, y_n]$ with degree 0 elements being I, degree 1 elements generated over k by $\{x_i y_j\}$, etc. Namely, the ideal generated by I in $A[y_1, \dots, y_n]$. This provides a diagram

$$\begin{tikzcd}
A[y_1, \dots, y_n] \arrow[r] & \frac{k[x_1,\dots,x_n][y_1,\dots,y_n]}{\langle\{x_i y_j - x_j y_i\}\rangle} \arrow[r] & k[y_1, \dots, y_n] \\
A \arrow[u, hook] \arrow[r, equal] & A \arrow[u, hook] \arrow[r] & A/I = k \arrow[u, hook]
\end{tikzcd}$$

And this diagram corresponds to the diagram

$$\begin{tikzcd}
\mathbb{A}^n \times \mathbb{P}^{n-1} & \mathrm{Bl}_0(\mathbb{A}^n) \arrow[l, hook'] \arrow[d, "\varphi"] & \varphi^{-1}(0) \cong \mathbb{P}^{n-1} \arrow[l, hook'] \arrow[d, "\varphi"] \\
\mathbb{A}^n \arrow[u, leftarrow] \arrow[r, equal] & \mathbb{A}^n & 0 \arrow[l]
\end{tikzcd}$$

The moral is that the diagram of rings

$$A[y_1, \dots, y_n] \to \oplus_{d=0}^{\infty} I^d \to \oplus_{d=0}^{\infty} I^d/I^{d+1},$$

describes completely the blow-up of $\mathbb{A}^n$ at zero, with the projection to $\mathbb{A}^n$ and the special fibre. Furthermore the isomorphism

$$\mathrm{gr}(\mathcal{O}_{\mathbb{A}^n,0}) = \oplus_{d=0}^{\infty} I_{\mathfrak{m}}^d / I_{\mathfrak{m}}^{d+1} = \oplus_{d=0}^{\infty} I^d / I^{d+1},$$

(here $\mathfrak{m} = I = (x_1, \dots, x_n)$ and we only introduce it so that not to denote the localization of I at I by I_I) shows that we can identify the special fibre in the blow-up of $\mathbb{A}^n$ at 0 with the projectivation of the tangent cone of $\mathbb{A}^n$ at the point 0.

8.2. **Projective Version.** It is sometime more convenient to deal with a projective version of the construction. We consider $\mathbb{P}^n \times \mathbb{P}^{n-1}$ and the variety X' defined in $\mathbb{P}^n \times \mathbb{P}^{n-1}$ by the same equations as before

$$x_i y_j = x_j y_i, \qquad i, j = 1, \dots, n.$$

Note that if $x_0 \neq 0$ we may assume that $x_0 = 1$ and we reduce to the previous case. If $x_0 = 0$ then there is some i such that $x_i \neq 0$ and then

$$y_j = y_i x_j x_i^{-1},$$

which show that the y_i are uniquely determined by the x_i's as long as we are away from the point $(1 : 0 : \cdots : 0)$. One concludes that

Theorem 8.3. *Let $P = (1 : 0 : \cdots : 0)$. The morphism $\varphi : X' \to \mathbb{P}^n - \{P\}$ has the following properties:*

(1) *$\varphi : X' \setminus \varphi^{-1}(P) \to \mathbb{P}^n \setminus \{P\}$ is an isomorphism.*

(2) *$\varphi^{-1}(P) \cong \mathbb{P}^{n-1}$ and there is a natural bijection between lines through P in $\mathbb{P}^n$ and points in $\varphi^{-1}(P)$. If ℓ is a line and p_ℓ the corresponding point in $\mathbb{P}^{n-1}$ then*

$$\overline{\varphi^{-1}(\ell - \{P\})} \cap \varphi^{-1}(P) = p_\ell.$$

(3) *X' is irreducible.*

END OF LECTURE 13 (October 29)

8.3. **Blow-up of Subvarieties at a point.** Let $Y \subseteq \mathbb{A}^n$ be a variety with $0 \in Y$ such that $\dim(Y) \geq 1$. Let us take our cue from the completely algebraic description given for the blow-up of $\mathbb{A}^n$ at 0 to figure out what the blow-up of Y at 0 might be.

Let $A = k[x_1, \dots, x_n]$, $\bar{A} = A(Y) = A/I(Y)$, $I = (x_1, \dots, x_n)$ and $\bar{I} = I/I(Y)$. We often use the notation $\underline{x}$ for $x_1, \dots, x_n$ and $\underline{y}$ for $y_1, \dots, y_n$. When we write $f(\underline{x}; \underline{y})$ we always mean an element of $A[y_1, \dots, y_n]$ that is homogenous of some degree in the variables $\underline{y}$.

We expect that the graded ring $\oplus_{d=0}^{\infty} \bar{I}^d$ should be the blow-up of Y at 0 and the graded ring $\oplus_{d=0}^{\infty} \bar{I}^d / \bar{I}^{d+1}$ be the exceptional fibre. We have a graded homomorphism

$$\oplus_{d=0}^{\infty} \bar{I}^d \twoheadrightarrow \oplus_{d=0}^{\infty} \bar{I}^d / \bar{I}^{d+1},$$

whose kernel is $\oplus_{d=0}^{\infty} \bar{I}^{d+1}$. We also have a graded homomorphism which is the composition of two graded homomorphisms (the first one takes y_i to $x_i \in I$, namely, in the first graded piece of $\oplus_{d=0}^{\infty} \bar{I}^d$):

$$A[y_1, \dots, y_n] \twoheadrightarrow \oplus_{d=0}^{\infty} I^d \twoheadrightarrow \oplus_{d=0}^{\infty} \bar{I}^d,$$

whose kernel J is a graded ideal whose elements in degree d are

$$J_d = \langle \{ f(\underline{x}; \underline{y}) : f \text{ homogenous of degree } d \text{ in } \underline{y}, f(\underline{x}; \underline{x}) \in I(Y)_{\geq d} \} \rangle.$$

Thus,

$$J = \langle \{ f(\underline{x}; \underline{y}) : f(\underline{x}; \underline{x}) \in I(Y) \} \rangle.$$

Thus, if we think of the blow-up of Y at 0 as the ring $\oplus_{d=0}^{\infty} \bar{I}^d$, we see that it is the closed subvariety of $\mathbb{A}^n \times \mathbb{P}^{n-1}$ defined by the ideal J. We also remark that the ring $\oplus_{d=0}^{\infty} \bar{I}^d / \bar{I}^{d+1}$ is non-other than $\mathrm{gr}(\mathcal{O}_{Y,0})$ and therefore when we view it as associated to a subvariety of $\mathbb{A}^n \times \mathbb{P}^{n-1}$, via

$$A[y_1, \ldots, y_n] \twoheadrightarrow \oplus_{d=0}^{\infty} \bar{I}^d \twoheadrightarrow \oplus_{d=0}^{\infty} \bar{I}^d / \bar{I}^{d+1},$$

it is defined by the ideal which is the kernel of this composition; one calculates that this is the ideal

$$\langle \{ f(0; \underline{y}) : f(\underline{x}; \underline{y}) \text{ homogenous}, f(\underline{x}; \underline{x}) \in I(Y) \} \rangle.$$

Furthermore, because of the interpretation as $\mathrm{gr}(\mathcal{O}_{Y,0})$, it is the projectivization of the tangent cone of Y at 0.

We summarize the picture in two huge diagrams. One of algebras, the other of algebraic varieties. The homomorphisms are always graded and when we talk of inclusions such at $A \hookrightarrow A[\underline{y}]$ we always mean that A is embedded in the 0-th graded piece.

$$\begin{tikzcd}
A[\underline{y}] \arrow[r, two heads] & \oplus_{d=0}^{\infty} I^d \arrow[r, two heads] \arrow[d, two heads] & \oplus_{d=0}^{\infty} I^d / I^{d+1} \arrow[d, two heads] \\
 & \oplus_{d=0}^{\infty} \bar{I}^d \arrow[r, two heads] & \oplus_{d=0}^{\infty} \bar{I}^d / \bar{I}^{d+1} \\
A \arrow[uu, hook] \arrow[uur, hook] \arrow[r, two heads] & \bar{A} \arrow[u, hook] \arrow[r, two heads] & k \arrow[u, hook]
\end{tikzcd}$$

And the geometric content of this is

$$\begin{tikzcd}
A^n \times \mathbb{P}^{n-1} \arrow[dd, "\varphi"] & Bl_0(\mathbb{A}^n) \arrow[l, hook'] \arrow[ddl] & \varphi^{-1}(0) = \mathrm{Projec}(C_{\mathbb{A}^n,0}) \arrow[l, hook'] \\
 & Bl_0(Y) \arrow[u, hook] \arrow[d] & Bl_0(Y) \cap \varphi^{-1}(0) = \mathrm{Projec}(C_{Y,0}) \arrow[l, hook'] \arrow[u, hook] \arrow[d] \\
\mathbb{A}^n & Y \arrow[l, hook'] & \{0\} \arrow[l, hook']
\end{tikzcd}$$

Unfortunately, at present we lack a completely rigorous language to handle blow-up this way (in particular, we seem to be making ad hoc definitions as to when we should take "homogenous theory" and when not). This would be the language of schemes. Hence, we now develop the same theory but using a different construction. However, as the results will show we get exactly the same final answer. It should be stressed that the approach we have just sketched, that goes completely through the algebra, is the more powerful. There are many situations where re-writing it in classical explicit terms is very difficult, if not impossible.

Definition 8.4. Let $Y \subseteq \mathbb{A}^n$ be a variety with $0 \in Y$ such that $\dim(Y) \geq 1$. The **blow-up of** Y **at** 0 is defined as

$$\widetilde{Y} = \overline{\varphi^{-1}(Y - \{0\})}.$$

Remark 8.5. Note that $\widetilde{Y}$ (also called the **strict transform of** Y) has the property that $\widetilde{Y} - \varphi^{-1}(0) \cong Y - \{0\}$. We call $\widetilde{Y} \cap \varphi^{-1}(0)$ the **exceptional fibre**.

Figure 21 shows an affine piece of the blow up of the nodal curve $y^2 = x^2(x+1)$. It is given as the intersection of the pre-image of this nodal curve in $\mathbb{A}^2 \times \mathbb{P}^1$ (shown in blue) with the blow up of $\mathbb{A}^2$ at the origin. Figure 22 shows a close up on the neighborhood of zero. Note that the two

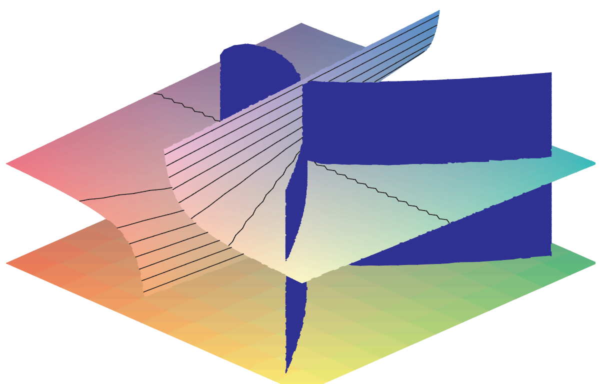


Figure 21. Blow-up of $y^2 = x^2(x+1)$ at its singular point $(0,0)$.

branches at zero separate at the blow-up. The blow up of the nodal curve is not singular anymore.

Theorem 8.6. *In the notation above we have:*

(1) $\mathcal{I}(\widetilde{Y}) = \langle \{ f(x_1, \dots, x_n, y_1, \dots, y_n); f(x_1, \dots, x_n, x_1, \dots, x_n) \in \mathcal{I}(Y)\}\rangle$. *(Note that this contains* $\{x_i y_j - x_j y_i\}$*.)*

(2) *Let* C *be the cone in* $\mathbb{A}^n$ *lying over the projective closed set* $\widetilde{Y} \cap (\{0\} \times \mathbb{P}^{n-1})$ *(thought of as a projective closed set in* $\mathbb{P}^{n-1}$*, and let* $C_{Y,0}$ *be the tangent cone to* Y *at* 0*. Then*

$$C \cong C_{Y,0}.$$

In words, the exceptional fiber of $\widetilde{Y}$ *is the projectivation of the tangent cone to* Y *at the origin.*

(3) $\widetilde{Y}$ *is irreducible and* $\varphi : \widetilde{Y} \to Y$ *is a birational moprhism.*

Proof. (1) Let $f \in \mathcal{I}(\widetilde{Y})$ then $\forall (x_1, \dots, x_n) \in Y - \{0\}$ we have $f(x_1, \dots, x_n; x_1 : \dots : x_n) = 0$. This gives $f(x_1, \dots, x_n, x_1, \dots, x_n) \in \mathcal{I}(Y - \{0\}) = \mathcal{I}(Y)$.

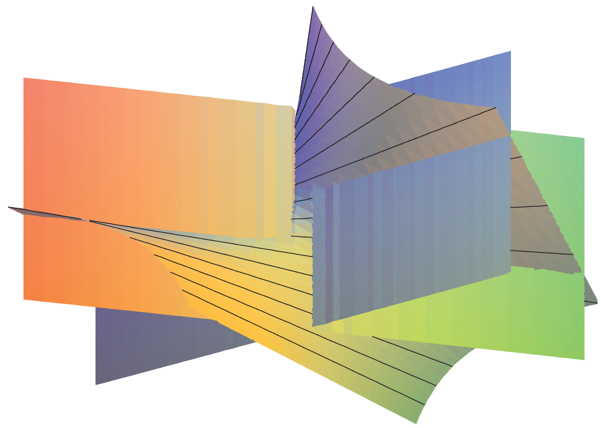


Figure 22. Blow-up of $y^2 = x^2(x+1)$ at its singular point $(0,0)$: Close-up.

Conversely, let $f(x_1,\dots,x_n;y_1,\dots,y_n)$ be such that $f(x_1,\dots,x_n,x_1,\dots,x_n) \in \mathcal{I}(Y)$. Then $f \in \mathcal{I}(\widetilde{Y})$ if and only if $f \equiv 0$ on $\varphi^{-1}(Y - \{0\})$. But $f(\varphi^{-1}(x_1,\dots,x_n)) = f(x_1,\dots,x_n,x_1:\dots:x_n) = 0$.

(2) Let J be the ideal

$$J = \langle \{f(0,\dots,0;y_1:\dots:y_n) : f(x_1,\dots,x_n,x_1,\dots,x_n) \in \mathcal{I}(Y)\}\rangle.$$

Note that $\mathcal{Z}(J) = \widetilde{Y} \cap \{0\} \times \mathbb{P}^{n-1}$. We need to show

$$J = \mathcal{I}(Y)^*.$$

Let $f \in \mathcal{I}(Y)$, $f = f_r + \dots$ its decomposition into homogenous elements, where $f_r \neq 0$. Then $f_r \in \mathcal{I}(Y)^*$ and $\mathcal{I}(Y)^*$ is generated by such elements. Write

$$f = f_r + \sum_i g_{r+1,i}h_{r+1,i} + \sum_i g_{r+2,i}h_{r+2,i} + \dots,$$

where $g_{s,i}$ is homogenous of weight r and $h_{s,i}$ is homogenous of weight $s-r$. Let

$$F = f_r(y_1,\dots,y_n) + \sum_i g_{r+1,i}(y_1,\dots,y_n)h_{r+1,i}(x_1,\dots,x_n) \\ + \sum_i g_{r+2,i}(y_1,\dots,y_n)h_{r+2,i}(x_1,\dots,x_n) + \dots.$$

Then $F(0,\dots,0;y_1:\dots:y_n) = f_r(y_1,\dots,y_n) \in J$, hence $\mathcal{I}(Y)^* \subseteq J$.

Conversely, let $f(0,\dots,0;y_1,\dots,y_n) \in J$. Then $f(x_1,\dots,x_n;y_1,\dots,y_n)$ is homogenous of weight r with respect to the variables y_i and therefore we may write

$$f(x_1,\dots,x_n;y_1,\dots,y_n) = g_1(x_1,\dots,x_n)h_1(y_1,\dots,y_n) + \dots + g_s(x_1,\dots,x_n)h_s(y_1,\dots,y_n),$$

with h_i the distinct monomials of weight r. Let a_i be the constant term of g_i. If each $a_i = 0$ then $f(0,\dots,0;y_1,\dots,y_n) = 0$. Thus, we may assume that some $a_i \neq 0$. We now write

$$f(x_1,\dots,x_n;y_1,\dots,y_n) = a_1h_1(y_1,\dots,y_n) + \dots + a_sh_s(y_1,\dots,y_n) \\ + \text{terms of pos. } x\text{-degree and } y\text{-degree } r.$$

We know that $f(x_1,\dots,x_n,x_1,\dots,x_n)\in\mathcal{I}(Y)$ and using the last expression we write

$$f(x_1,\dots,x_n,x_1,\dots,x_n)=a_1h_1(x_1,\dots,x_n)+\cdots+a_sh_s(x_1,\dots,x_n) \\ +\text{ higher order terms},$$

which is an element on $\mathcal{I}(Y)$. Note that there is no cancellation between the terms $a_1h_1(x_1,\dots,x_n)+\cdots+a_sh_s(x_1,\dots,x_n)$. We therefore conclude that $f(0,\dots,0;y_1:\dots,y_n)=a_1h_1(y_1,\dots,y_n)+\cdots+a_sh_s(y_1,\dots,y_n)\in\mathcal{I}(Y)^*$.
(3) As $Y-\{0\}$ is irreducible, $\widetilde{Y}-\varphi^{-1}(0)$ is irreducible, open and dense in $\widetilde{Y}$ and so $\widetilde{Y}$ is irreducible algebraic set. Thus, a variety. Further, $\varphi:\widetilde{Y}-\varphi^{-1}(0)\to Y-\{0\}$ is an isomorphism between open dense sets of $\widetilde{Y}$ and Y, respectively. Therefore, φ is a birational morphism. □

Corollary 8.7. *Let Y be a positive dimensional affine variety such that $0\in Y$. Choose generators $g_1,\dots,g_t$ for $\mathcal{I}(Y)$ such that $g_1^*,\dots,g_t^*$ generate the ideal $\mathcal{I}(Y)^*$. For each polynomial $h\in k[x_1,\dots,x_n]$ we define a polynomial $H_h\in k[x_1,\dots,x_n,y_1,\dots,y_n]$ as follows: write $h=h_r+h_{r+1}+\cdots+h_s$ with h_a homogenous of weight a, and write each h_a in the form $h_a=\sum_j h'_{a,j}h''_{a,j}$ where $h''_{a,j}$ is homogenous of weight r (there is an arbitrary choice involved here). Define then*

$$H_h=h_r(y_1,\dots,y_n)+(\sum_j h'_{r+1,j}(x_1,\dots,x_n)h''_{r+1,j}(y_1,\dots,y_n))+\cdots \\ +(\sum_j h'_{s,j}(x_1,\dots,x_n)h''_{s,j}(y_1,\dots,y_n)).$$

Consider the ideal

$$I=\langle\{x_iy_j-x_jy_i:i,j\}\cup\{H_{g_i}:i=1,\dots,t\}\rangle$$

of $k[x_1,\dots,x_n,y_1,\dots,y_n]$. Then

$$\mathcal{Z}(I)=\widetilde{Y}.$$

Proof. Outside the special fiber the equations just reduce to the equations $g_1,\dots,g_t$. Thus, the only thing we need to verify is that $\mathcal{Z}(I)\cap\varphi^{-1}(0)=\widetilde{Y}\cap\varphi^{-1}(0)$. However $\mathcal{Z}(I)\cap\varphi^{-1}(0)$ is the set $\{(0,\dots,0;y_1:\cdots:y_n):H_{g_i}(0,\dots,0;y_1:\cdots:y_n)=0,\ i=1,\dots,t\}=\{(0,\dots,0;y_1:\cdots:y_n):g_i^*(y_1:\cdots:y_n)=0,\ i=1,\dots,t\}$, which, by our choice of g_i, is the projectivation of the tangent cone to Y at 0. We conclude by part (2) of Theorem 8.6. □

Remark 8.8. Note that we do not claim that I is a radical ideal.

8.4. **Examples.** Suppose that Y is a hypersurface containing 0. Say $Y=\mathcal{Z}(f)$. Then $\widetilde{(Y)}$ is the zero set of the equations $x_iy_j=x_jy_i$ and the polynomial H_f.

Here are concrete examples. If $f=x_1^2+x_2^2-x_3^2$ then Y is the cone in $\mathbb{A}^3$ and the blow-up is defined by $x_1y_2=x_2y_1, x_1y_3=x_3y_1, x_2y_3=x_3y_2$ and $y_1^2+y_2^2-y_3^2$.

If $f=x_1x_2^2+x_1x_2x_3^2+17x_1^3x_2^2$ then the blow up is defined by $x_1y_2=x_2y_1, x_1y_3=x_3y_1, x_2y_3=x_3y_2$ and $y_1y_2^2+x_3y_1y_2y_3+17x_2^2y_1^3$ (or by $y_1y_2^2+x_1y_2y_3^2+17x_1^2y_1y_2^2$).

8.4.1. *The nodal curve.* We consider the nodal curve $Y : x_2^2 = x_1^2(x_1+1)$ in $\mathbb{A}^2$. In this case $\widetilde{Y} \subset \mathbb{A}^2_{x_1,x_2} \times \mathbb{P}^1_{y_1,y_2}$ is the zero set of the ideal

$$\langle y_2^2 = y_1^2(x_1+1), \;\; x_1y_2 - x_2y_1\rangle.$$

This is a closed curve whose intersection with $\varphi^{-1}(0)$ is $(0,0;1:\pm 1)$. The cone over this intersection is $y_1^2 - y_2^2$, which is (as it should be) the tangent cone of Y at 0.

I claim that $\widetilde{Y}$ is non-singular. Take first $y_1 = 1$ then we have the equations in $\mathbb{A}^3_{x_1,x_2,y_2}$

$$y_2^2 - x_1 - 1 = 0, \quad x_1y_2 - x_2 = 0.$$

The Jacobian matrix is

$$\begin{pmatrix} -1 & 0 & 2y_2 \\ y_2 & -1 & x_1 \end{pmatrix},$$

which always has rank 2. Hence, this piece of $\widetilde{Y}$ is non-singular. Now take $y_2 = 1$ to obtain equations in $\mathbb{A}^3_{x_1,x_2,y_1}$

$$y_1^2(x_1+1) - 1 = 0, \quad x_1 - x_2y_1 = 0$$

that give the Jacobian

$$\begin{pmatrix} y_1^2 & 0 & 2y_1(x_1+1) \\ 1 & -y_1 & -x_2 \end{pmatrix}.$$

Since for $y_2 = 1$ we cannot have $y_1 = 0$, we conclude that the rank of the Jacobian is always 2 and it follows that this piece of $\widetilde{Y}$ is also non-singular.

8.4.2. *The cuspidal curve.* We consider the cuspidal curve $Y : x_2^2 = x_1^3$ in $\mathbb{A}^2$. In this case $\widetilde{Y} \subset \mathbb{A}^2_{x_1,x_2)x_2} \times \mathbb{P}^1_{y_1,y_2}$ is the zero set of the ideal

$$\langle y_2^2 = y_1^2x_1, \;\; x_1y_2 - x_2y_1\rangle.$$

This is a closed curve whose intersection with $\varphi^{-1}(0)$ is $(0,0;1:0)$. The cone over this intersection is y_2, which is (as it should be) the tangent cone of Y at 0.

I claim that $\widetilde{Y}$ is non-singular. Take first $y_1 = 1$ then we have the equations in $\mathbb{A}^3_{x_1,x_2,y_2}$

$$y_2^2 - x_1 = 0, \quad x_1y_2 - x_2 = 0.$$

The Jacobian matrix is

$$\begin{pmatrix} -1 & 0 & 2y_2 \\ y_2 & -1 & x_1 \end{pmatrix},$$

which always has rank 2. Hence, this piece of $\widetilde{Y}$ is non-singular. Now take $y_2 = 1$ to obtain equations in $\mathbb{A}^3_{x_1,x_2,y_1}$

$$y_1^2x_1 - 1 = 0, \quad x_1 - x_2y_1 = 0$$

that give the Jacobian

$$\begin{pmatrix} y_1^2 & 0 & 2y_1x_1 \\ 1 & -y_1 & -x_2 \end{pmatrix}.$$

Since for $y_2 = 1$ we cannot have $y_1 = 0$, we conclude that the rank of the Jacobian is always 2 and it follows that this piece of $\widetilde{Y}$ is also non-singular.

8.4.3. *The Cone.* Consider the cone $Y : x_1^2 + x_2^2 - x_3^2 = 0$ in $\mathbb{A}^3_{x_1,x_2,x_3}$. The tangent cone to Y at zero is Y itself. The strict transform $\widetilde{Y}$ of Y is defined by the equations

$$\langle y_1^2 + y_2^2 - y_3^2,\ x_1y_2 - x_2y_1,\ x_1y_3 - x_3y_1,\ x_2y_3 - x_3y_y\rangle.$$

(1) The special fibre $\widetilde{Y} \cap \varphi^{-1}(0)$ is given by the projective equation

$$C_1 :\ y_1^2 + y_2^2 - y_3^2 = 0.$$

I claim that this curve in $\mathbb{P}^2$ is isomorphic to $\mathbb{P}^1$. For that we shall use the projection from a point. Consider the change of coordinates $y_2 \mapsto (y_2 - y_3)$ and the curve

$$C_2 :\ y_1^2 + (y_2 - y_3)^2 - y_3^2 = y_1^2 + y_2^2 - 2y_2y_3 = 0.$$

If $(y_1 : y_2 : y_3) \in C_2$ then $(y_1 : y_2 - y_3 : y_3) \in C_1$. Let us consider the projection from the point $P = (0 : 0 : 1)$ onto $\mathbb{P}^1 \cong Z(y_3 = 0)$ given by

$$\pi : \mathbb{P}^2 - \{P\} \to \mathbb{P}^1, \quad \pi(y_1 : y_2 : y_3) = (y_1 : y_2).$$

One checks that this gives an isomorphism

$$C_2 - \{P\} \to \mathbb{A}^1 = \{(t : 1 : 0)\} \subset \mathbb{P}^2.$$

Indeed this map is given by $(y_1 : y_2 : y_3) \mapsto (y_1/y_2 : 1 : 0)$ and its inverse is $(t : 1 : 0) \mapsto (t : 1 : (1 + t^2)/2)$. [17] Now, I claim that the isomorphism

$$C_2 - \{P\} \to \mathbb{A}^1 = \{(y_1 : y_2 : 0) : y_2 \neq 0\} \subset \mathbb{P}^2$$

can be extended to an isomorphism

$$C_2 \to \mathbb{P}^1.$$

Note that on C_2 we have the equality

$$(y_1 : y_2) = (2y_3 - y_2 : y_1),$$

when all magnitudes are defined. The rational function $C_2 \dashrightarrow \mathbb{P}^1$ given by

$$(y_1 : y_2 : y_3) \to (2y_3 - y_2 : y_1 : 0)$$

is well defined in a neighborhood of P and agrees with π elsewhere. It takes P to $(1 : 0 : 0)$ and hence induces and isomorphism of C_2 with $\mathbb{P}^1$.

(2) Local structure of $\widetilde{Y}$. Let $Z \subset \mathbb{P}^2$ be the rational curve $y_1^2 + y_2^2 - y_3^2 = 0$.
- $y_1 \neq 0$. In this case we have that

$$x_2 = x_1(y_2/y_1), \quad x_3 = x_1(y_3/y_1).$$

This gives an isomorphism

$$\Phi_1 : \mathbb{A}^1 \times Z - \{(0 : 1 : \pm 1)\} \to \widetilde{Y} \cap \{y_1 \neq 0\}$$

[17] As an aside we remark that this induces a birational map

$$\mathbb{A}^1 \to C_1$$

under which $t \mapsto (t : 1 : (1 + t^2)/2) \mapsto (t : 1 - (1 + t^2)/2 : (1 + t^2)/2)$. Notice that this induces a bijection between $t \in \mathbb{Q}$ and the rational solutions to C_1 which are the rational Pythagorean triples different from $(0 : -1 : 1)$. If we write $t = p/q$ then the corresponding triple is

$$(p/q : 1 - (1 + (p/q)^2)/2 : (1 + (p/q)^2)/2) = (2pq : q^2 - p^2 : q^2 + p^2).$$

by the formula

$$\Phi_1(t; y_1, y_2, y_3) = (t, t(y_2/y_1), t(y_3/y_1); y_1, y_2, y_3).$$

In particular, we deduce that

$$\widetilde{Y} \sim \mathbb{A}^1 \times \mathbb{P}^1.$$

- $y_2 \neq 0$. In this case we have that

$$x_1 = x_2(y_1/y_2), \quad x_3 = x_2(y_3/y_2).$$

This gives an isomorphism

$$\Phi_2 : \mathbb{A}^1 \times Z - \{(1 : 0 : \pm 1)\} \to \widetilde{Y} \cap \{y_1 \neq 0\}$$

by the formula

$$\Phi_2(t; y_1, y_2, y_3) = (t(y_1/y_2), t, t(y_3/y_2); y_1, y_2, y_3).$$

- $y_3 \neq 0$. In this case we have that

$$x_1 = x_3(y_1/y_3), \quad x_2 = x_3(y_2/y_3).$$

This gives an isomorphism

$$\Phi_3 : \mathbb{A}^1 \times Z - \{(1 : \pm i : 0)\} \to \widetilde{Y} \cap \{y_1 \neq 0\}$$

by the formula

$$\Phi_3(t; y_1, y_2, y_3) = (t(y_2/y_3), t(y_1/y_3), t; y_1, y_2, y_3).$$

(3) $\widetilde{Y}$ as a line bundle over $\mathbb{P}^1$.

Definition 8.9. Let X, Z be varieties and $\pi : X \to Z$ a morphism. We say that X is a **line bundle** over Z if the following holds: there exists an open cover of Z, say $Z = \cup U_\alpha$, and isomorphisms

$$\phi_\alpha : \pi^{-1}(U_\alpha) \to \mathbb{A}^1 \times U_\alpha$$

with the following properties:

A. The diagram commutes

$$\begin{tikzcd}
\pi^{-1}(U_\alpha) \arrow[r, "\phi_\alpha"] \arrow[d, "\pi"'] & \mathbb{A}^1 \times U_\alpha \arrow[d, "p_2"] \\
U_\alpha \arrow[r, equal] & U_\alpha
\end{tikzcd}$$

B. For every $u \in U_\alpha \cap U_\beta$ the induced map

$$\phi_\beta(\cdot, u)^{-1} \circ \phi_\alpha(\cdot, u) : \mathbb{A}^1 \to \mathbb{A}^1$$

is a linear map.

To prove that the natural morphism $\widetilde{Y} \to \mathbb{P}^1$ given by

$$(x_1, x_2, x_3; y_1, y_2, y_3) \mapsto (y_1, y_2, y_3)$$

is a line bundle, we need to verify that the transition maps given above for the covering $\{y_1 \neq 0\}, \{y_2 \neq 0\}, \{y_3 \neq 0\}$ are linear on the fibers. We verify one case: we have

$\Phi_2^{-1}(\Phi_1(t; y_1 : y_2 : y_3)) = \Phi_2^{-1}((t, t(y_2/y_1), t(y_3/y_1); y_1 : y_2 : y_3)) = (t(y_2/y_1); y_1 : y_2 : y_3)$, which is indeed linear when $(y_1 : y_2 : y_3)$ is fixed.

END OF LECTURE 14 (October 31)

8.5. **Blow up of an affine variety at an affine subvariety.**

§ Blowing up at subvarieties.

Have discussed $\mathbb{A}^n \supseteq Y \ni \{0\}$
$I = (x_1, .., x_n)$

$$\begin{array}{ccc} Bl_0(\mathbb{A}^n) & \supseteq & Bl_0(Y) \\ \updownarrow & & \updownarrow \\ \bigoplus_{d=0}^{\infty} I^d & \twoheadrightarrow & \bigoplus \bar{I}^d \end{array} \qquad \bar{I} = I/I(Y)$$

Let Y be an affine variety, $I(Y)$, $A(Y) = A/I(Y)$ where $A = k[x_1, .., x_n]$.
Let $Z \subseteq Y$ be an algebraic set, $Z = Z(I)$ with $I \supseteq I(Y)$. $\bar{I} = I \bmod I(Y)$

$$\bigoplus_{d=0}^{\infty} I^d \twoheadrightarrow \bigoplus_{d=0}^{\infty} \bar{I}^d$$

<u>Definition</u>: $Bl_Z(\mathbb{A}^n)$ is ~~the~~ Proj. $(\bigoplus_{d=0}^{\infty} I^d)$

and $Bl_Z(Y)$ is Proj $(\bigoplus_{d=0}^{\infty} \bar{I}^d)$.

By Proj we mean that homogeneous ideals define the subvarieties, homog. elements the regular fcns and so on.

Let $g_1, .., g_N$ be generators of I over A.

$$\begin{tikzcd}
A[y_1,\dots,y_N] \arrow[r, two heads, "\alpha"] & \bigoplus_{d=0}^{\infty} I^d \arrow[r] \arrow[d, "\beta"] & \bigoplus_{d=0}^{\infty} I^d/I^{d+1} \arrow[d] \\
& \bigoplus_{d=0}^{\infty} \bar{I}^d \arrow[r, two heads] & \bigoplus_{d=0}^{\infty} \bar{I}^d/\bar{I}^{d+1} \\
A \arrow[uu, hook] \arrow[uur, hook] \arrow[r] & A(Y) \arrow[u, hook] \arrow[r, two heads] & A(Z) = A(Y)/\bar{I} \arrow[u, hook]
\end{tikzcd}$$

$$\begin{tikzcd}
\mathbb{A}^n \times \mathbb{P}^{N-1} \arrow[dd, "\varphi"] & Bl_Z(\mathbb{A}^n) \arrow[l, hook'] \arrow[ddl, "\varphi"'] & \cancel{Bl_Z(\ldots)}\ \varphi^{-1}(Z) \arrow[l, hook'] \arrow[d] \\
& Bl_Z(Y) \arrow[u, hook] \arrow[d] & \varphi^{-1}(Z) \cap Bl_Z(Y) \arrow[l, hook'] \arrow[d] \\
\mathbb{A}^n & Y \arrow[l, hook'] & Z \arrow[l, hook']
\end{tikzcd}$$

So $Bl_Z(\mathbb{A}^n)$ is the algebraic set corresponding to $\sqrt{\mathrm{Ker}(\alpha)}$, $Bl_Z(Y)$ is the algebraic set corresponding to $\sqrt{\mathrm{Ker}(\beta\circ\alpha)}$.

<u>A useful trick:</u>

$$\bigoplus_{d=0}^{\infty} I^d \hookrightarrow A[t] \quad \text{as graded } A\text{-algebras}$$

special case of:

$$\bigoplus_{d=0}^{\infty} \bar{I}^d \hookrightarrow A(Y)[t] \quad \text{as graded } A\text{-algebra.}$$

$$(f_0, f_1, f_2, \dots) \longmapsto \sum_{i=0}^{\infty} f_i t^i \qquad \text{(well-defined)}$$

Corollary: $\bigoplus \bar{I}^d$ is an integral domain.

$\Longrightarrow$ $\ker(\alpha)$, $\ker(\beta\circ\alpha)$ are prime ideals

$\Longrightarrow$ $Z \subseteq Y$, Y variety then $Bl_Z(Y)$ is a variety.

Note that in weight 0, $\ker(\alpha)_0 = \{0\}$, $\ker(\beta\alpha)_0 = \{0\}$

This implies that $\varphi: Bl_Z(\mathbb{A}^n) \setminus \varphi^{-1}(Z) \xrightarrow{\sim} \mathbb{A}^n \setminus Z$.

$\varphi: Bl_Z(Y) \setminus \varphi^{-1}(Z) \xrightarrow{\sim} Y \setminus Z$.

Examples:

1. $Y = \mathbb{A}^n$, $Z = Z(f)$. $I = \langle f \rangle$.

$$\begin{aligned} A[y] &\longrightarrow \bigoplus_{d=0}^{\infty} I^d \quad \text{is an isomorphism} \\ y &\longmapsto f \end{aligned}$$

$Bl_Z(\mathbb{A}^n)$ is defined by the homogeneous polynomial

$\{0\}$ in $\mathbb{A}^n \times \mathbb{P}^0 \simeq \mathbb{A}^n$.

That is, $Bl_Z(\mathbb{A}^n) = \mathbb{A}^n$.

The special fiber is defined by the kernel

$A[y] \longrightarrow \bigoplus_{d=0}^{\infty} I^d / I^{d+1}$ which is the principal ideal

generated by $f \in A$. That is, the special fiber

is $Z \times \mathbb{P}^0 \simeq Z$.

Nothing changes.

(2) $Y = \mathbb{A}^n$, $Z = Z(f_1, f_2)$, f_1, f_2 irreducible

polynomials that are non-associate. and $\langle f_1, f_2 \rangle \neq A$.

(For example $f_1 = x_1$, $f_2 = x_2$).

$$A[y_1, y_2] \longrightarrow \bigoplus_{d=0}^{\infty} I^d$$

$$y_i \longmapsto f_i$$

the kernel J contains $f_2 y_1 - f_1 y_2$.

<u>Proposition</u>: $J = \langle f_1 y_2 - f_2 y_1 \rangle$.

<u>Proof</u>:

$$
\begin{array}{ccccc}
A[y_1, y_2] & \xrightarrow{\alpha} & A[y_1,y_2]/\langle f_1 y_2 - f_2 y_1\rangle & \longrightarrow & \bigoplus_{d=0}^{\infty} I^d \\
 & & & & \cong \\
 & & & & A[f_1 t, f_2 t] \\
 & & & & \cap \\
 & & & & A[t].
\end{array}
$$

Let us calculate dimⁿˢ.

$$\dim A[y_1,y_2]/\langle f_1 y_2 - f_2 y_1\rangle \underset{\text{Krull}}{=} n+2-1 = n+1$$

$$\dim A[f_1 t, f_2 t] = \dim \mathrm{Frac}(A[f_1 t, f_2 t]) = \dim \mathrm{Frac}(A[t]) = n+1$$

$$\Rightarrow \quad A[y_1,y_2]/\langle f_1 y_2 - f_2 y_1\rangle \cong \bigoplus_{d=0}^{\infty} I^d.$$

$\dim(B/\mathfrak{p}) = \dim(B) - ht(\mathfrak{p})$

<u>Remark</u>: The argument just requires that $\langle f_1 y_2 - f_2 y_1\rangle$ is a prime homogenous ideal $\iff \gcd(f_1, f_2) = 1$.

For a different proof that works in more general situations, see Eisenbud + Harris Propⁿ IV-25

What is the special fibre?

$$\mathrm{Ker}\left(A[y_1, y_2] \longrightarrow \bigoplus_{d=0}^{\infty} I^d / I^{d+1}\right) ?$$

This is $\alpha^{-1}\left(\bigoplus_{d=0}^{\infty} I^{d+1}\right)$.

This is just $\langle f_1, f_2 \rangle$.

Given a generator $f_1^a f_2^b$ of I^{d+1} with, say, $b>0$, the element $f_2 \cdot y_1^a y_2^{b-1}$ is a preimage, unique up to kernel α. But $\ker(\alpha)$, $f_2 y_1^a y_2^{b-1}$ both belong to $\langle f_1, f_2 \rangle$.

$\Longrightarrow$ The special fibre is the closed subvariety defined by the homogeneous-in-the-y_i's ideal $\langle f_1 f_2 \rangle \subseteq A[y_1, y_2]$. Thus

$$\cong Z \times \mathbb{P}^1.$$

We have a section

$$\begin{aligned} \mathbb{A}^n - Z &\longrightarrow \mathbb{A}^n \times \mathbb{P}^1 \\ (\underline{a}) &\longmapsto (\underline{a};\, f_1(\underline{a}) : f_2(\underline{a})) \end{aligned}$$

The image is defined by $f_1 y_2 - f_2 y_1$. Over Z, this becomes the zero equation ✓.

A sequence of elements $f_1, \dots, f_s$ of a ring A is called a regular sequence if $\langle f_1, \dots, f_s \rangle \neq A$ and for all i $f_i \bmod \langle f_1, \dots, f_{i-1} \rangle$ is not a zero divisor.

Example: $A = k[x_1, \dots, x_n]$, f_1, f_2 irreducible polynomials that are non-associate and $\langle f_1, f_2 \rangle \neq A$.

Then (f_1, f_2) and (f_2, f_1) are a regular sequence.

We have the following for a regular sequence with $I = \langle f_1, f_2, \dots, f_s \rangle$ in a ring A:

$$\bigoplus_{d=0}^{\infty} I^d \cong (A[y_1, \dots, y_s])/K$$

where K is generated by $\{ f_i y_j - f_j y_i : \substack{i=1,\dots,s \\ j=1,\dots,s} \}$

(That's not so easy!) From that one concludes easily

$$\bigoplus_{d=0}^{\infty} I^d / I^{d+1} \cong A/I\,[y_1, \dots, y_s]$$

Cor: $Y \supseteq Z$, $Z \leftrightarrow I = \langle f_1, \dots, f_s \rangle$ and assume $f_1, \dots, f_s$ is a regular sequence. Then $Bl_Z(Y)$ is defined in $Y \times \mathbb{P}^{s-1}$ by $\{ f_i y_j - f_j y_i : i, j \}$ and the special fibre is $\cong Z \times \mathbb{P}^{s-1}$.

9. Integral Extensions and Finite Morphisms

9.1. **Integral Extensions.**

Definition 9.1. Let $A \subset B$ be rings (always commutative with 1). An element $b \in B$ is called **integral** over A if b satisfies a monic polynomial $f(x) \in A[x]$. That is, exist some $a_0, \dots, a_{n-1}$ in A such that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0.$$

The extension $A \subset B$ is called an **integral extension** if every element of B is integral over A.

Example 9.2. Let $A = \mathbb{Z}$ and $B = \mathbb{Q}$. Then $b \in \mathbb{Q}$ is integral over $\mathbb{Z}$ if and only if $b \in \mathbb{Z}$. Indeed, if $b \in \mathbb{Z}$ then b solves $x - b \in \mathbb{Z}[x]$. Conversely, write $b = c/d$ for relatively prime integers c and d, $d > 0$. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with integer coefficients that b satisfies. Substituting b for x and multiplying by d^n we obtain

$$c^n = -(da_{n-1}c^{n-1} + \cdots + d^n a_0).$$

Since d divides the right hand side, we get that $d|c^n$. But $(d, c) = 1$. Therefore, $d = 1$.

Example 9.3. Let k be an algebraically closed field, $f(x) \in \mathbb{F}[x]$ a non-constant polynomial and $n > 0$ an integer. Consider the extension of rings $k[x] \subset k[x, y]/(y^n - f(x))$. This is an integral extension. Clearly y is integral over $k[x]$. We shall see soon (Corollary 9.6) that the collection of elements of $A(X)$ that are integral over $k[x]$ forms a ring. Thus, since x and y are integral over $k[x]$, it follows that the whole extension $k[x] \subset k[x, y]/(y^n - f(x))$ is integral.

Example 9.4. Consider the extension $k[x] \subset k[x, y]/(xy - 1) = k[x, x^{-1}]$. This is not an integral extension. Let $f_1, \dots, f_r$ be elements of $k[x^{\pm 1}]$. Then in $\oplus_{i=1}^r k[x]f_i$ the negative powers of x are bounded. Thus, we cannot have $\oplus_{i=1}^r k[x]f_i = k[x^{\pm 1}]$.

Proposition 9.5. *Let $A \subset B$ be rings and $b \in B$. The following are equivalent:*

(1) b is integral over A.

(2) $A[b]$ is a finitely generated module over A (i.e., exist $b_1, \dots, b_n$ in $A[b]$ such that $A[b] = Ab_1 + \cdots + Ab_n$).

(3) $A[b] \subset M \subset B$, where M is finitely generated A-module.

(4) Exists a faithful $A[b]$-module K, finitely generated over A. ("faithful" means that if $a \in A[b]$ and $ak = 0$ for all $k \in K$ then $a = 0$).

Proof. **(1) implies (2) :** For some $a_0, \dots, a_{n-1}$ we have $b^n = -(a_{n-1}b^{n-1} + \cdots + a_0)$. I claim that

$$A[b] = A + Ab + \cdots + Ab^{n-1}.$$

Let J denote the right hand side. It is enough to prove that $b^r \in J$ for every $r \geq n$. For $r = n$ this is the identity $b^n = -(a_{n-1}b^{n-1} + \cdots + a_0)$. Assume that $b^r \in J$ then $b^r = \alpha_0 + \alpha_1 b + \cdots + \alpha_{n-1}b^{n-1}$ for suitable $\alpha_i \in A$. Therefore $b^{r+1} = \alpha_0 b + \alpha_1 b^2 + \cdots + \alpha_{n-2}b^{n-1} + \alpha_{n-1}b^n$. Since $\alpha_{n-1}b^n$ belongs to J and $\alpha_0 b + \alpha_1 b^2 + \cdots + \alpha_{n-2}b^{n-1}$ belongs to J we get $b^{r+1} \in J$.

(2) implies (3): Take $M = A[b]$.

(3) implies (4): Take $K = M$. Since $1 \in K$, if $r \in A[b]$ annihilates K then, in particular, $r \cdot 1 = 0$. Thus $r = 0$ and K is a faithful $A[b]$-module.

(4) implies (1): Say that

$$K = Ac_1 + \cdots + Ac_n$$

for some $c_i \in K$. Consider the A-linear map

$$\phi_b : K \to K, \quad \phi_b(d) = bd.$$

Write

$$\phi_b(c_j) = \sum_{i=1}^{n} a_{ij} c_i, \quad a_{ij} \in A.$$

The matrix T, given by

$$T = b \cdot I_n - (a_{ij}),$$

acts as zero on the vector ${}^t(c_1, \dots, c_n)$.

Let $\mathrm{Adj}(T)$ be the adjoint matrix to T. Then the transformation $\mathrm{Adj}(T) \cdot T^t(c_1, \dots, c_n) =$, which gives $\det(T) \cdot I_n^t(c_1, \dots, c_n) = 0$. This implies that $\det(T)$ kills any element of K. Since K is a faithful $A[b]$-module, that implies that $\det(T) = 0$. Expanding $\det(T)$, we see that for suitable $r_i \in A$ we have

$$b^n + r_{n-1} b^{n-1} + \dots + r_0 = 0.$$

$\square$

Corollary 9.6. *(1) The* **integral closure** *of A in B, defined as*

$$\{b \in B : b \text{ is integral over A}\},$$

and denoted $N_B(A)$, is a sub-ring of B containing A.

(2) $N_B(N_B(A)) = N_B(A)$.

Proof. We first remark that if $A \subset B \subset C$ are three rings such that B is a finitely generated A-module and C is a finitely generated B-module then C is a finitely generated A module. Indeed, let $B = Ab_1 + \dots + Ab_m$ for some $b_i \in B$ and $C = Bc_1 + \dots + Bc_n$ for some $c_i \in C$. Then $C = \sum_{i=1,j=1}^{m,n} b_i c_j$. Furthermore, by induction, we get that if $A = B_0 \subset B_1 \subset \dots \subset B_n$ are rings and B_i is finitely generated B_{i-1}-module for every $i \geq 1$, then B_n is a finitely generated A-module.

We use this as follows. Let $b_1, \dots, b_n$ be elements of B integral over A. Then $A[b_1, \dots, b_n]$ is a finitely generated A module. Indeed, let $B_i = A[b_1, \dots, b_i]$. Note that b_i is integral over B_{i-1}, therefore, by the proposition, B_i is a finitely generated B_{i-1}-module.

We now prove (1). We notice that given $b_1, b_2 \in N_B(A)$ we have $A[-b_1], A[b_1 + b_2], A[b_1 b_2]$ each contained in the finitely generated A-module $A[b_1, b_2]$. Hence, by the proposition, $-b_1, b_1 + b_2, b_1 b_2$ are integral over A. Finally, clearly $a \in A$ solves $x - a$. That is $A \subset N_B(A)$.

Let $b \in N_B(N_B(A))$. Then $b^n + a_{n-1} b^{n-1} + \dots a_0 = 0$ for some $a_i \in N_B(A)$. Then we see that b is integral over $A[a_0, \dots, a_{n-1}]$. Therefore $A[a_0, \dots, a_{n-1}, b]$ is finite over $A[a_0, \dots, a_{n-1}]$, which, in turn, is finite over A. Therefore $A[a_0, \dots, a_{n-1}, b]$ is finite over A and contains $A[b]$. The proposition gives that b is integral over A. I.e., that $b \in N_B(A)$. $\square$

END OF LECTURE 15 (November 5)

Before proceeding to study integral extensions in more depth, we provide several results that explain the relevance of the concept to algebraic geometry.

9.2. **Noether's normalization lemma.** Let $f : X \to Y$ be a dominant morphism of affine varieties. The induced ring homomorphism

$$f^* : A(Y) \to A(X)$$

is injective. Indeed, if $f^*g = 0$ then $g(f(X)) = 0$ and hence $g(\overline{f(X)}) = g(Y) = 0$, so $g = 0$. Hence, we may consider $A(Y)$ as a subring of $A(X)$ via f^*,

$$A(Y) \subseteq A(X).$$

Recall that the two natural operations on closed sets of taking pre-images and the closure of the image correspond to natural operations on ideals as follows:

- Let $\mathfrak{m} \lhd A(X)$ be an ideal and $\mathfrak{n} = \mathfrak{m} \cap A(Y) \lhd A(Y)$. Then
$$\overline{f(\mathcal{Z}(\mathfrak{m}))} = \mathcal{Z}(\mathfrak{n}).$$
- Let $\mathfrak{n} \lhd A(Y)$ be an ideal and $\mathfrak{n}A(X)$ the ideal of $A(X)$ it generates. Then
$$f^{-1}(\mathcal{Z}(\mathfrak{n})) = \mathcal{Z}(\mathfrak{n}A(X)).$$

Definition 9.7. A morphism $f : X \to Y$ is called **finite** if $A(X)$ is a finitely generated module over $f^*(A(Y))$. This implies that $A(X)$ is an integral extension of $A(Y)$; every element of $A(X)$ is integral over $A(Y)$. Conversely, if every element of $A(X)$ is integral over $A(Y)$, since $A(X)$ is finitely generated as a ring over k hence over $A(Y)$, it follows that $A(X)$ is a finitely generated $A(Y)$-module.

The following theorem explains one way the concept of finite morphism is central to algebraic geometry.

Theorem 9.8. *(**Noether's Normalization Lemma**) Let k be an algebraically closed field*[18] *and let A be a finitely generated k-algebra. There exist elements $y_1, \dots, y_r$ of A, such that $y_1, \dots, y_r$ are algebraically independent over k and A is integral over $k[y_1, \dots, y_r]$.*

Proof. Let $x_1, \dots, x_n$ be generators for A over k as a ring. Thus, $A = k[x_1, \dots, x_n]$. We may assume that $x_1, \dots, x_r$ are algebraically independent over k and that $x_{r+1}, \dots, x_n$ are algebraic over $k[x_1, \dots, x_r]$. The proof now proceeds by induction on n.

If $n = r$, whatever r is, then there is nothing to prove. Else, $n > r$ and x_n is algebraic over $k[x_1, \dots, x_{n-1}]$. Therefore, there is a polynomial f in n variables, say $f \in k[t_1, \dots, t_n]$, such that $f \neq 0$ and

$$f(x_1, \dots, x_n) = 0.$$

Let us write f as a sum of its homogenous parts

$$f = f_0 + f_1 + \cdots + f_e,$$

where $f_e \neq 0$ (while the other f_i may be zero, of course). Write $F = f_e$. It is a non-zero homogenous polynomial in the variables $t_1, \dots, t_n$ and of degree $e > 0$. Now, there exist $\lambda_1', \dots, \lambda_n'$ in k such that

$$F(\lambda_1', \dots, \lambda_n') \neq 0,$$

and $\lambda_n' \neq 0$. Otherwise, for every $\lambda_n' \neq 0$, we have $F(\lambda_1', \dots, \lambda_n') = 0$, which implies $F \equiv 0$, by continuity. Since F is homogenous, we deduce that there exists $\lambda_1, \dots, \lambda_{n-1}$ in k such that

$$F(\lambda_1, \dots, \lambda_{n-1}, 1) \neq 0.$$

[18] The lemma is correct for any field k and the proof given works for any infinite field k.

Define new variables by

$$x_1' = x_1 - \lambda_1 x_n, \ \ldots, \ x_{n-1}' = x_{n-1} - \lambda_{n-1} x_n.$$

Then, $f(x_1' + \lambda_1 x_n, \ldots, x_{n-1}' + \lambda_{n-1} x_n, x_n) = 0$. By expanding (where $I = (i_1, \ldots, i_n)$ is multi-index notation) we find

$$\begin{aligned}
0 &= f(x_1' + \lambda_1 x_n, \ldots, x_{n-1}' + \lambda_{n-1} x_n, x_n) \\
&= \sum_{|I|=e} a_I \cdot x_n^{i_n} \cdot \prod_{j=1}^{n-1} (x_j' + \lambda_j x_j)^{i_j} + \sum_{|I|<e} a_I \cdot x_n^{i_n} \cdot \prod_{j=1}^{n-1} (x_j' + \lambda_j x_j)^{i_j} \\
&= x_n^e \cdot \sum_{|I|=e} a_I \cdot \lambda_1^{i_1} \cdots \lambda_{n-1}^{i_{n-1}} + \text{ lower order terms in } x_n \\
&= F(\lambda_1, \ldots, \lambda_{n-1}, 1) \cdot x_n^e + \text{ lower order terms in } x_n.
\end{aligned}$$

More explicitly, by dividing by the scalar $F(\lambda_1, \ldots, \lambda_{n-1}, 1)$, we find that

$$0 = x_n^e + \alpha_{e-1} x_n^{e-1} + \cdots + \alpha_0, \qquad \alpha_i \in k[x_1', \ldots, x_{n-1}'].$$

This proves that x_n is integral over $k[x_1', \ldots, x_{n-1}']$ and so $A = k[x_1', \ldots, x_{n-1}', x_n]$ is a finitely generated $k[x_1', \ldots, x_{n-1}']$-module . By induction, for suitable algebraically independent elements $y_1, \ldots, y_s$ of $k[x_1', \ldots, x_{n-1}']$, we have that $k[x_1', \ldots, x_{n-1}']$ is a finitely generated $k[y_1, \ldots, y_s]$-module and so A is a finitely generated $k[y_1, \ldots, y_s]$-module. And so, every element of A is integral over $k[y_1, \ldots, y_s]$. ☐

Remark 9.9. Note that in fact, the r appearing the statement of the theorem is an invariant of the ring A. That is, every maximal set of algebraically independent elements has the same cardinality r. If A is an integral domain, this r is just the transcendence degree of $\mathrm{Frac}(A)$ over k.

Corollary 9.10. *Let X be an affine algebraic set. Then there is a finite morphism*

$$f : X \to \mathbb{A}^r,$$

for some r.

Proof. Apply Noether's normalization lemma for $A = A(X)$. There exists elements $y_1, \ldots, y_r$ of $A(X)$ that are algebraically independent over k and such that $A(X)$ is a finitely generated $k[y_1, \ldots, y_r]$-module. Identifying $k[y_1, \ldots, y_r]$ with the affine coordinate ring of $\mathbb{A}^r$, we get a finite morphism $X \to \mathbb{A}^r$. ☐

The beauty of this proof of Noether's lemma is that it allows us to effectively construct the morphism f. We illustrate this in some simple examples.

Example 9.11. Consider the affine variety $X = \{(x, y) : xy = 1\}$. Its affine coordinate ring is $A(X) = k[x, y]/(xy - 1)$. Although $k[x] \subset A(X)$, this inclusion induces the morphism $X \to \mathbb{A}^1$, $(x, y) \mapsto x$, and this is *not* a finite morphism (Example 9.4).

Let us apply Noether's lemma. y solves the polynomial $f = xy - 1$, whose highest homogenous part is $F = xy$. We find that $F(1, 1) \neq 0$ and we perform the change of variable $x' = x - y$, giving

$$0 = f(x' + y, y) = (x' + y)y - 1 = y^2 + x'y - 1.$$

This shows that y is integral over $k[x']$. Geometrically, this is saying that the morphism

$$\varphi : X \to \mathbb{A}^1, \quad \varphi(x, y) = x - y,$$

is a finite morphism.

Example 9.12. (The cone over the **quadric surface**). Let $X : xy - zw = 0$, a 3-dimensional affine variety in $\mathbb{A}^4_{x,y,z,w}$. X is the affine cone over projective quadric surface

$$S = \{(x : y : z : w) | xy - zw = 0\}, \qquad S \subset \mathbb{P}^3_{x,y,z,w}.$$

The surface S is the image of $\mathbb{P}^1 \times \mathbb{P}^1$ under the Segre embedding,

$$\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3, \qquad ((a_0, a_1), (b_0, b_1)) \mapsto (a_0b_0, a_1b_1, a_0b_1, a_1b_0).$$

The quadric surface is ruled in two ways: It is a family of $\mathbb{P}^1$'s parameterized by $\mathbb{P}^1$ in two different ways. One is the family $\{t\} \times \mathbb{P}^1$ for $t \in \mathbb{P}^1$. The other is the family $\mathbb{P}^1 \times \{t\}$ for $t \in \mathbb{P}^1$. It is also related to the blow-up of $\mathbb{A}^2$ at the origin. We leave it to the reader to explore this relation.

At any rate, the extension $k[x, y, z] \subseteq k[x, y, z, w]/(xy - zw)$ is not integral. To see this, it is convenient to use the facts (to be proven below) that a finite morphism is a closed surjective and **quasi-finite** (i.e., all the fibres have finite cardinality) map. The morphism $X \to \mathbb{A}^3$ corresponding to this inclusion is $(x, y, z, w) \mapsto (x, y, z)$. This morphism is not surjective. It misses the points $\{(x, y, z) : xy \neq 0, z = 0\}$ (and, in fact, none else). The fibres are not finite either. For example, the fibre over $(a, 0, 0)$ is $\{(a, 0, 0, w) : w \in k\} \cong \mathbb{A}^1$.

Let us apply Noether's lemma. We have the equation $f = xy - zw$ that w satisfies. We have $F = f$ and $F(0, 0, 1, 1) \neq 0$. Make a change of variables $z' = z - w$. Then $f(x, y, z' + w, w) = 0$. We find that $xy - (z' + w) \cdot w = 0$, or $w^2 - z'w + xy = 0$. This shows that w is integral over $k[x, y, z']$. Otherwise said, we have a finite morphism

$$X \to \mathbb{A}^3, \qquad (x, y, z, w) \mapsto (x, y, z - w).$$

9.3. **Results about integral extensions and their geometric interpretation.**

Proposition 9.13. *Let $A \subseteq B$ be an integral extension. Let U be a multiplicative set in A. Then the extension*

$$A[U^{-1}] \subseteq B[U^{-1}]$$

is an integral extension.

Proof. Let $u \in U$, $b \in B$. Suppose that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0 \qquad a_i \in A.$$

Then,

$$(\frac{b}{u})^n + \frac{a_{n-1}}{u}(\frac{b}{u})^{n-1} + \cdots + \frac{a_0}{u^n} = 0,$$

and this shows that $\frac{b}{u}$ is integral over $A[U^{-1}]$. □

Geometric Content: Let $f : X \to Y$ be a finite morphism of affine varieties through which $A(Y) \subseteq A(x)$. Consider the special case where $U = \{1, g, g^2, \dots\}$ for $g \in A$ such that $Z(g)$ is not empty. Let

$Y_0 = Y \backslash Z(g)$ and $X_0 = f^{-1}(Y_0) = X \backslash Z(g)$. We have $A(Y_0) = A(Y)[g^{-1}]$ and $A(X_0) = A(X)[g^{-1}]$. The extension $A(Y_0) \subseteq A(X_0)$ is thus an integral extension. That is,

$$f : X_0 \to Y_0$$

is also a finite morphism. In fact, this is true for any open subset Y_0 in Y and $X_0 = f^{-1}(Y_0)$, but it will be easier to deduce that later. In fact, later we shall also see that if for every such g, $f : X_0 \to Y_0$ is finite, then f is finite. Thus, the notion of a finite morphism is a local notion. We shall return to that after Proposition 9.15.

Proposition 9.14. *Let $A \subseteq B$ be an integral extension. Let P be an ideal of B and $\mathfrak{p} = P \cap A$. The extension*

$$A/\mathfrak{p} \subseteq B/P$$

is an integral extension.

Proof. Let $b \in B$. Suppose that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0 \qquad a_i \in A.$$

Then, reducing modulo P, using a bar to denote reduction, we find

$$\bar{b}^n + \bar{a}_{n-1}\bar{b}^{n-1} + \cdots + \bar{a}_0 = 0 \text{ in } B/P.$$

We can interpret $\bar{a}_i$ as in $A/\mathfrak{p}$ and so $\bar{b}$ is integral over $A/\mathfrak{p}$. ☐

Geometric Content: Let $f : X \to Y$ be a finite morphism of affine algebraic sets. Let $Z \subset X$ be a closed subset. Then

$$f : Z \to \overline{f(Z)}$$

is also a finite morphism of affine algebraic sets. (We shall see later that a finite morphism is closed, so in fact $f(Z) = \overline{f(Z)}$.)

END OF LECTURE 16 (November 7)

Proposition 9.15. *Let $A \subseteq B$ be an extension of commutative rings. The following are equivalent.*

1. *$A \subseteq B$ is an integral extension.*
2. *For every multiplicative set U in A the extension $A[U^{-1}] \subseteq B[U^{-1}]$ is an integral extension.*
3. *For every maximal ideal $\mathfrak{m}$ of A, the extension $A_{\mathfrak{m}} \subseteq B_{\mathfrak{m}}$ is an integral extension. (Here, $B_{\mathfrak{m}}$ means B localized at the multiplicative set $A - \mathfrak{m}$.)*

Proof. We have shown (1) ⇒ (2) in Proposition 9.13 and (2) ⇒ (3) is obvious. We show now that (3) ⇒ (1).

Consider the exact sequence of A-modules

$$0 \to N_B(A) \to B \to B/N_B(A) \to 0.$$

To show that $B/N_B(A) = 0$ it is enough to show that $(B/N_B(A))_{\mathfrak{m}} = 0$ for every maximal ideal $\mathfrak{m}$ of A. Since localization is an exact functor, we have

$$(B/N_B(A))_{\mathfrak{m}} = B_{\mathfrak{m}}/(N_B(A))_{\mathfrak{m}}.$$

We know that the extension $A_{\mathfrak{m}} \subseteq B_{\mathfrak{m}}$ is integral. Let $\frac{b}{s} \in B_{\mathfrak{m}}$. It solves some equation

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_{n-1}}{s_{n-1}}\right)\left(\frac{b}{s}\right)^{n-1} + \cdots + \left(\frac{a_0}{s_0}\right) = 0,$$

for some $a_i \in A, s_i \in A - \mathfrak{m}$. By passing to a common denominator, we may assume $s_{n-1} = \cdots = s_0$. And so,

$$\left(\frac{b}{s}\right)^n + \left(\frac{a_{n-1}}{s_0}\right)\left(\frac{b}{s}\right)^{n-1} + \cdots + \left(\frac{a_0}{s_0}\right) = 0.$$

Multiplying through by $s^n s_0^n$ we find that

$$\left(\frac{s_0 b}{1}\right)^n + \left(\frac{s s_0 a_{n-1}}{1}\right)\left(\frac{s_0 b}{1}\right)^{n-1} + \cdots + \left(\frac{s^n s_0^{n-1} a_0}{1}\right) = 0$$

in the ring $B_\mathfrak{m}$. That means that for some $s_1 \in A - \mathfrak{m}$ we have

$$s_1\left((s_0 b)^n + (s s_0 a_{n-1})(s_0 b)^{n-1} + \cdots + (s^n s_0^{n-1} a_0)\right) = 0,$$

and so,

$$s_1^n\left((s_0 b)^n + (s s_0 a_{n-1})(s_0 b)^{n-1} + \cdots + (s^n s_0^{n-1} a_0)\right) = 0,$$

hence,

$$(s_1 s_0 b)^n + s_1 s s_0 a_{n-1}(s_1 s_0 b)^{n-1} + \cdots + s_1^n s^n s_0^{n-1} a_0 = 0.$$

This shows that $s_1 s_0 b \in N_B(A)$ and so that $\frac{b}{s} \in (N_B(A))_\mathfrak{m}$. [19] Thus, $B_\mathfrak{m}/(N_B(A))_\mathfrak{m} = 0$. □

Geometric Content: Let $f : X \to Y$ be a morphism of affine algebraic sets. Then f is finite, if and only if for all $y \in Y$ the extension of rings $\mathcal{O}_{Y,y} \subseteq (\mathcal{O}_X)_{\mathfrak{m}_y}$ is integral, where $\mathfrak{m}_y$ is the maximal ideal corresponding to y in $A(Y)$. So the property of being finite can be studied locally at a point.

Let $f : X \to Y$ be a morphism between affine varieties. Let $y \in Y$ and let $Y_0 \subseteq Y$ be an open affine neighbourhood of Y, say $Y_0 = Y - Z(g)$. Then $f : X \to Y$ is finite at the point y, in the sense that $\mathcal{O}_{Y,y} \subseteq (\mathcal{O}_X)_{\mathfrak{m}_y}$ is integral, if and only if $f : f^{-1}(Y_0) \to Y_0$ is finite at y. Note that $f^{-1}(Y_0) = X - Z(g)$ and so is also affine.

Given now any dominant morphism $f : X \to Y$ of varieties, we say that f is a **finite** morphism if there is a covering of $Y = \cup_\alpha Y_\alpha$ by affine subsets such that $\forall\alpha$, $f^{-1}(Y_\alpha)$ is affine and $f^{-1}(Y_\alpha) \to Y_\alpha$ is a finite morphism. One can then use the proposition above to show that if $Y = \cup_\alpha Y'_\alpha$ by affine subsets such that $\forall\alpha$, $f^{-1}(Y'_\alpha)$ is affine then $f^{-1}(Y'_\alpha) \to Y'_\alpha$ is a finite morphism. And, of course, the statement that f is a finite morphism can be check locally at every point. We thus see that we may as well keep discussing just the affine case, which is technically easier.

Proposition 9.16. *Let $A \subseteq B$ be an integral extension of integral domains. Then A is a field if and only if B is a field.*

Proof. Suppose that A is a field. Let $b \in B$, $b \neq 0$. Then, for some minimal n and $a_i \in A$, we have

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0.$$

Note that $a_0 \neq 0$, else $b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) = 0$, which gives, because B is an integral domain and $b \neq 0$, $b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1 = 0$. This contradicts the minimality of n. Thus, we have

$$b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) \cdot (-a_0)^{-1} = 1,$$

showing that b is invertible.

[19] The argument we just gave shows more generally that $N_B(A)[U^{-1}] = N_{B[U^{-1}]}(A[U^{-1}])$.

Conversely, assume that B is a field. Let $a \in A$, $a \neq 0$. The element $a^{-1} \in B$ and is integral over A. Thus, for suitable $a_i \in A$, we have

$$a^{-n} + a_{n-1}a^{-(n-1)} + \cdots + a_0 = 0.$$

Multiply by a^{n-1} to get

$$a^{-1} = -(a_{n-1} + \cdots + a_0 a^{n-1}) \in A.$$

□

Corollary 9.17. *Let $A \subseteq B$ be an integral extension. Let $\mathfrak{q}$ be a prime ideal of B and $\mathfrak{p} = \mathfrak{q} \cap A$. Then q is a maximal ideal if and only if $\mathfrak{p}$ is a maximal ideal.*

Proof. First note that $\mathfrak{p}$ is prime and we have an extension of integral domains $A/\mathfrak{p} \subseteq B/\mathfrak{q}$, which is an integral extension by Proposition 9.14. Then, $\mathfrak{q}$ is maximal iff $B/\mathfrak{q}$ is a field, iff $A/\mathfrak{p}$ is a field, iff $\mathfrak{p}$ is maximal. □

Geometric Content: Let $f : X \to Y$ be a finite morphism. The image of a subvariety of X is zero-dimension if and only if it is zero-dimensional. In particular, *a finite morphism is quasi-finite*. Indeed, let $y \in y$ and pick an irreducible component of the closed set $f^{-1}(y)$. Since its image is zero-dimensional, it is zero-dimensional. That shows that the fibre, which is the affine variety corresponding to $A(X)/\sqrt{\mathfrak{m}_y A(x)}$, is zero dimensional, hence consists of finitely many points.

Proposition 9.18. *Let $A \subseteq B$ be an integral extension. Let $\mathfrak{p} \subset A$ be a prime ideal. There exists a prime ideal $\mathfrak{q}$ of B such that $\mathfrak{q} \cap A = \mathfrak{p}$.*

Proof. Consider the integral extension (Proposition 9.13)

$$A_{\mathfrak{p}} \subseteq B_{\mathfrak{p}}.$$

(That is, if $U = A - \mathfrak{p}$, $A[U^{-1}] \subseteq B[U^{-1}]$.) Let $\tilde{\mathfrak{q}}$ be any maximal ideal of $B_{\mathfrak{p}}$. Then $\tilde{\mathfrak{q}} \cap A_{\mathfrak{p}}$ is a prime ideal, hence a maximal ideal by Corollary 9.17. Thus,

$$\tilde{\mathfrak{q}} \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}},$$

because $\mathfrak{p}A_{\mathfrak{p}}$ is the unique maximal ideal of $A_{\mathfrak{p}}$. Let $\mathfrak{q}$ be the unique prime ideal of B such that

$$\mathfrak{q}B_{\mathfrak{p}} = \tilde{\mathfrak{q}}.$$

(This uses that for a ring R and multiplicative set U there is a bijection between the prime ideals $\mathfrak{a}$ of R that are disjoint with U and the prime ideals of $R[U^{-1}]$, under $\mathfrak{a} \mapsto \mathfrak{a}[U^{-1}]$.) We claim that

$$(\mathfrak{q} \cap A)_{\mathfrak{p}} = \tilde{\mathfrak{q}} \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}.$$

If so, then both $\mathfrak{p}$ and $\mathfrak{q} \cap A$ are prime ideals and give under localization in $\mathfrak{p}$ the same ideal. Thus, $\mathfrak{p} = \mathfrak{q} \cap A$ and the proof is done. As to the claim, it follows from a general and simple lemma about localizations given just after the discussion of the geometric content of the proposition. □

Geometric Content: Let $f : X \to Y$ be a finite morphism.

(1) Taking $\mathfrak{p}$ to be a maximal ideal we find that *a finite morphism is surjective*.
(2) Let $Z_Y \subset Y$ be a subvariety. Then there is a subvariety $Z_X \subset X$ such that $f(Z_X) = Z_Y$ (we shall see soon that f is closed; at this point we really can only say that $\overline{f(Z_X)} = Z_Y$.)

Lemma 9.19. *Let A be a ring, $U \subset A$ a multiplicative set and M_1, M_2 two submodules of an A-module M. Then,*

$$(M_1 \cap M_2)[U^{-1}] = M_1[U^{-1}] \cap M_2[U^{-1}]$$

(everything viewed in $M[U^{-1}]$).

Proposition 9.20. *Let $A \subset B$ be an integral extension. Let $\mathfrak{q}_1 \subset \mathfrak{q}_2$ be prime ideals of B. Then $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A$ implies that $\mathfrak{q}_1 = \mathfrak{q}_2$.*

Proof. Let $\mathfrak{p} = \mathfrak{q}_1 \cap A$. We have an integral extension

$$A - \mathfrak{p} \subseteq B_{\mathfrak{p}}.$$

We also have

$$\mathfrak{q}_i B_{\mathfrak{p}} \cap A_{\mathfrak{p}} = (\mathfrak{q}_i \cap A)_{\mathfrak{p}} = \mathfrak{p} A_{\mathfrak{p}}.$$

Thus, $\mathfrak{q}_i B_{\mathfrak{p}}$ are maximal ideals (Corollary 9.17), $\mathfrak{q}_1 B_{\mathfrak{p}} \subseteq \mathfrak{q}_2 B_{\mathfrak{p}}$ and so $\mathfrak{q}_1 B_{\mathfrak{p}} = \mathfrak{q}_2 B_{\mathfrak{p}}$. This implies $\mathfrak{q}_1 = \mathfrak{q}_2$ by the correspondence for prime ideals under localization. □

Geometric Content: Let $f : X \to Y$ be a finite morphism. A chain of distinct irreducible sets $Z_1 \subset \cdots \subset Z_n$ in X has distinct images in Y (even after taking closure). In particular, $\dim(X) \leq \dim(Y)$. On the other $K(Y) \subset K(X)$ and hence $\dim(Y) = \text{trans. deg.}_k(K(Y)) \leq \text{trans. deg.}_k(K(X)) = \dim(X)$. Thus, *if $f : X \to Y$ is a finite morphism then* $\dim(X) = \dim(Y)$.

Theorem 9.21. *(Cohen-Seidenberg) Let $A \subset B$ be an integral extension.*

(1) (Going-up) Let $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ be prime ideals of A. Let $\mathfrak{q}_1$ be a prime ideal of B such that $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. Then there exist prime ideals of B, $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$, such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$.

(2) (Going-down) Assume that A and B are also domains and that A is integrally closed (i.e., $N_{Quot(A)}(A) = A$). Let $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ be prime ideals of A. Let $\mathfrak{q}_n$ be a prime ideal of B such that $\mathfrak{q}_n \cap A = \mathfrak{p}_n$. Then there exist prime ideals of B, $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$, such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$.

Proof. (Of part (1) of the theorem).To prove (1), we may assume that $n = 2$. The general case follows by induction. We have then the following situation: $\mathfrak{p}_1 \subset \mathfrak{p}_2$, $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$.

$$\begin{tikzcd}
\mathfrak{q}_1 \arrow[r, dash, "\subset"] \arrow[d, dash] & ? \arrow[d, dash] \\
\mathfrak{p}_1 \arrow[r, dash, "\subset"] & \mathfrak{p}_2
\end{tikzcd}$$

Consider the integral extension $A/\mathfrak{p}_1 \subset B/\mathfrak{q}_1$. The ideal $\mathfrak{p}_2/\mathfrak{p}_1$ is a prime ideal of $A/\mathfrak{p}_1$. Proposition 9.18 gives a prime ideal $\mathfrak{q}$ of $B/\mathfrak{q}_1$ such that $\mathfrak{q} \cap A/\mathfrak{p}_1 = \mathfrak{p}_2/\mathfrak{p}_1$. Let $\mathfrak{q}_2$ be the preimage in B of $\mathfrak{q}$. Then $\mathfrak{q}_2$ is a prime ideal containing $\mathfrak{q}_1$ (hence $\mathfrak{p}_1$) and $(\mathfrak{q}_2 \cap A)/\mathfrak{p}_1 = \mathfrak{q}_2/\mathfrak{q}_1 \cap A/\mathfrak{p}_1 = \mathfrak{p}_2/\mathfrak{p}_1$. It follows that $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$. □

We do not prove part (2) of the theorem here. A proof can be found, for example, if the book by Atiyah - Macdonald.

Corollary 9.22. *Let $f : X \to Y$ be a finite morphism between affine varieties. Then f is a closed map.*

Proof. It is enough to show that if $X_1 \subseteq X$ is an irreducible closed set then $\overline{f(X_1)}$ is closed. Choose $y \in \overline{f(X_1)}$. Then, if X_1 corresponds to a prime ideal $\mathfrak{q}_1$ of $A(X)$, then $\overline{f(X_1)}$ corresponds to the prime ideal $\mathfrak{p}_1 = \mathfrak{q}_1 \cap A(Y)$ of $A(Y)$, and y corresponds to a maximal ideal $\mathfrak{p}_2 \supseteq \mathfrak{p}_1$. By "Going up" there is a prime ideal $\mathfrak{q}_2$ of $A(X)$, such that $\mathfrak{q}_2 \cap A(Y) = \mathfrak{p}_2$. In fact, by Corollary 9.17, $\mathfrak{q}_2$ is maximal too and thus corresponds to a point $x \in X$ such that $f(x) = y$. Since $\mathfrak{q}_2 \supseteq \mathfrak{q}_1$, in fact $x \in X_1$ and so $y \in f(X_1)$. □

Geometric Content of "Going up": Let $f : X \to Y$ be a dominant integral morphism. Given a chain of closed irreducible sets $Y_1 \supset \cdots \supset Y_n$ in Y, first there exists a closed irreducible set X_1 of X such that $f(X_1) = Y_1$. (This is Proposition 9.18). For any such X_1 there exists a chain $X_1 \supset \cdots \supset X_n$ of closed irreducible sets in X, such that for every i we have $f(X_i) = Y_i$.

Part (2) of the theorem has a similar interpretation, only that one starts from a given X_n such that $f(X_n) = Y_n$ and has to find$X_1 \supset \cdots \supset X_n$.

END OF LECTURE 17 (November 12)

9.4. **Normalization.** As usual, k is our algebraically closed field. We begin by citing a theorem of Emmy Noether that is true in much greater generality than stated here.

Theorem 9.23. *(**" finiteness of integral closure"**) Let A be a finitely generated integral domain over k. Let $K = \mathrm{Frac}(A)$ be the field of fractions. Let L/K be a finite extension. The ring $N_L(A)$ is a finitely generated A-module and a finitely generated k-algebra.*

An integral domain B is called **integrally closed** if $B = N_K(B)$, where $K = \mathrm{Frac}(B)$. Taking the case $L = K$ we find:

Corollary 9.24. *Given an affine variety Y there is a canonical affine variety X, such that $A(X)$ is integrally closed and a finite birational morphism*

$$f : X \to Y.$$

The variety X is called the **normalization** of Y. Integral closure commutes with localization, namely, if $A \subset B$ and $U \subset A$ is a multiplicative set, then $N_B(A)[U^{-1}] = N_{B[U^{-1}]}(A[U^{-1}])$ (this was essentially proven in Proposition 9.15). Therefore, the construction of X is local, at least in the following sense. Let $Y_0 \subseteq Y$ be a basic open affine set, $Y_0 = Y - Z(g)$, and let $X_0 = f^{-1}(Y_0)$. Then X_0 is the normalization of Y_0. Indeed, $A(X_0) = A(X)[g^{-1}]$, which is the integral closure of $A(Y)[g^{-1}] = A(Y_0)$.

Theorem 9.25. *A regular local ring is integrally closed. Namely, if $(R, \mathfrak{m}_R)$ is a local ring such that $\dim(R) = \dim_{R/\mathfrak{m}_R}(\mathfrak{m}_R/\mathfrak{m}_R^2)$ then R is integrally closed.*

We shall not prove this theorem, but we use it in the sequel.

Let Y be an affine variety and Y^{sing} its singular locus. It is a closed set by Theorem 6.9. The complement $Y - Y^{\mathrm{sing}}$ is thus a union of open affine sets whose coordinate rings are of the form $A(Y)[g^{-1}]$. For every point $y \in Y - Y^{\mathrm{sing}}$, $\mathcal{O}_{Y,y}$ is a regular local ring, hence integrally closed. Let $\mathfrak{m}_y$ be the corresponding maximal ideal of $\mathcal{O}(Y - Z(g)) = A(y)[g^{-1}]$. Then $A(X)[g^{-1}]$ is the integral closure of $A(Y)[g^{-1}]$ and so $A(X)[g^{-1}]_{\mathfrak{m}_y}$ is the integral closure of $A(X)[g^{-1}]_{\mathfrak{m}_y} = \mathcal{O}_{Y,y}$. Thus, $A(X)[g^{-1}]_{\mathfrak{m}} = A(X)[g^{-1}]_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ of $A(Y)[g^{-1}]$ and thus, $A(X)[g^{-1}] = A(Y)[g^{-1}]$.

Corollary 9.26. *Let $f : X \to Y$ be the normalization of Y then f is a morphism over the non-singular locus of Y.*

That is, X is obtained from a "modification" of Y^{sing}. Let us look at some examples:

Example 9.27. Let Y be the cusp $\{(x, y) : x^2 = y^3\}$. We have a morphism

$$f : \mathbb{A}^1 \to Y, \qquad t \mapsto (t^2, t^3).$$

The morphism gives us the inclusion $A(Y) \subset k[t]$ and in fact $A(Y) = k + t^2k[t]$. t is integral over $A(Y)$ as it solves the monic polynomial $u^2 - t^2 \in A(Y)[u]$. Thus, $k[t] \subseteq N_{k(t)}(A(Y)) \subseteq N_{k(t)}(k[t]) = k[t]$, where the last equality follows from a lemma we shall prove momentarily. It follows that $\mathbb{A}^1 \to Y$ is the normalization of Y.

Note that the morphism f is indeed an isomorphism outside the singular locus of Y, namely outside the point $(0, 0)$. The inverse is given by

$$(x, y) \mapsto y/x.$$

We note that the process of normalization resolved the singularity.

Lemma 9.28. *Let R be a UFD then R is integrally closed.*

Proof. Let $\frac{a}{b} \in \text{Frac}(R)$ with $\gcd(a, b) = 1$. Suppose that $\frac{a}{b}$ is integral over R, then, for some $r_i \in R$,

$$(\frac{a}{b})^n + r_{n-1}(\frac{a}{b})^{n-1} + \cdots + r_0 = 0.$$

This implies that $a^n + r_{n-1}ba^{n-1} + \cdots + b^n r_0 = 0$ and so that $b|a$. Therefore, b is a unit and $\frac{a}{b} \in R$. □

Example 9.29. Consider now the nodal curve $Y = \{(x, y) = y^2 = x^2(x+1)\}$. We have a morphism

$$f : \mathbb{A}^1 \to Y, \qquad t \mapsto (t^2 - 1, t(t^2 - 1)).$$

Under this morphism $A(Y) = k + (t^2 - 1)k[t]$. Once more $N_{k(t)}(A(Y)) \supseteq k[t]$, as t solves the polynomial $u^2 - t^2 \in A(Y)[u]$. The same reasoning as in the previous example gives that $N_{k(t)}(A(Y)) = k[t]$ and so that $f : \mathbb{A}^1 \to Y$ is the normalization of Y. Outside the singular locus, $Y^{\text{sing}} = \{(0, 0)\}$, f is an isomorphism with an inverse given by $(x, y) \mapsto y/x$. In this case, the singular point of Y is replace by two points $\{\pm 1\}$ on $\mathbb{A}^1$; again, the normalization resolved the singularities of Y.

This example shows that a finite morphism can be generically an isomorphism, yet not injective.

Example 9.30. Consider now the pinch $Y = \{(x, y, z) : xy^2 = z^2\}$. Let $f(x, y, z) = xy^2 - z^2$. Then $(\partial f/\partial x, \partial f/\partial y, \partial f/\partial z) = (y^2, 2xy, -2z^2)$ and we find that the singular locus is defined by the equation $y = 0$ and is given by the line

$$Y^{\text{sing}} = \{(x, 0, 0) : x \in k\} \cong \mathbb{A}^1.$$

Let $t = z/y$. The function field of Y is $k(x, y)[z]/(z^2 - xy^2) = k(x, y)[t]/(t^2 - x) = k(y, t)$. The integral closure of $A(Y) = k[x, y, z]/(z^2 - xy^2)$ certainly contains $k[x, y, t] = k[y, t]$ and so equal to this ring. The inclusion $k[x, y, z]/(z^2 - xy^2) \subseteq k[x, t]$ is given by

$$x \mapsto t^2, \quad y \mapsto y, \quad z \mapsto yt.$$

This provides us with a morphism

$$f : \mathbb{A}^2_{y,t} \to Y, \qquad (y,t) \mapsto (t^2, y, yt),$$

which is the normalization of Y.

Outside the singular locus, we can invert the map by

$$(x,y,z) \mapsto (y, z/y).$$

The singular locus $\{(x,0,0)\} \cong \mathbb{A}^1$ is replaced by $\{(0,t)\} \cong \mathbb{A}^1$ and the map $\mathbb{A}^1 \to AA^1$ that we get form $(0,t) \mapsto (t^2,0,0)$ is $t \mapsto t^2$. It is a map that identifies t with $-t$. Thus, the pinch is obtained from $\mathbb{A}^2$ by pinching $\mathbb{A}^2$ along the t-axis, in an origami-like fashion, identifying t and $-t$.

Let X be a **normal affine variety**, that is, a variety equal to its normalization. The ring $A(X)$ is integrally closed and noetherian. Let $\mathfrak{p}$ be a prime ideal of height 1 in $A(X)$; it corresponds to an irreducible co-dimension 1 subvariety of X. The local ring $A(X)_{\mathfrak{p}}$ is an integrally closed ring, noetherian and or dimension 1.

In general, let B be a domain that is integrally closed, noetherian and of dimension 1 then B is called a **Dedekind domain**. The simplest example is $B = \mathbb{Z}$, the integers. The ring $A(X)_{\mathfrak{p}}$ is also a Dedekind domain, but it is also a local ring. We shall see that such rings are very special. Namely, we shall see that it is a discrete valuation ring; conversely, we shall see that a discrete valuation ring is a local Dedekind ring.

9.5. **Discrete valuation rings.** Let K be a field. A discrete valuation on K is a function

$$v : K^\times \to \mathbb{R},$$

extended by $v(0) = +\infty$, that satisfies:

(1) $v(xy) = v(x) + v(y)$ and $v(K^\times)$ is a rank 1 subgroup of $\mathbb{R}$;
(2) $v(x+y) \geq \min\{v(x), v(y)\}$.

As v is a discrete valuation if and only if $\alpha \cdot v$ is a discrete valuation for every positive real scalar α, we often assume that $v(K^\times) = \mathbb{Z}$ (and say v is **normalized**).

Lemma 9.31. *The following holds:*

(1) $v(1) = 0$ *and* $v(x^{-1}) = -v(x)$*;*
(2) $v(-1) = 0$ *and* $v(-x) = x$*;*
(3) *If* $v(x) > v(y)$ *then* $v(x+y) = v(y)$*.*

Proof. (1) follows from the fact that v is a homomorphism of groups. As $0 = v(1) = v((-1)^2) = 2v(-1)$ we get $v(-1) = 0$ and then $v(-x) = v(-1) + v(x) = v(x)$. ☐

Given a discrete valuation, put

$$R = \{k \in K : v(k) \geq 0\}, \qquad \mathfrak{m} = \{k \in K : v(k) > 0\}.$$

Then R is called a **discrete valuation ring**.

Proposition 9.32. $(R, \mathfrak{m})$ *is a local noetherian ring of dimension* 1*, which is integrally closed. In fact, R is PID. If the valuation on R normalized and* $\pi \in R$ *is a* **uniformizer***, that is, an element such that* $v(\pi) = 1$*, then the ideals of R are*

$$R \supsetneq (\pi) \supsetneq (\pi^2) \supsetneq \cdots \supsetneq (0).$$

Proof. Given Lemma 9.31, it is a simple matter to check that R is a ring and $\mathfrak{m}$ an ideal. Further, to show R is local it is enough to show that $R-\mathfrak{m} = R^\times$. But if u is a unit of R then $v(u^{-1}) = -v(u)$; both $v(u)$ and $v(u^{-1})$ are non-negative. Thus, $v(u) = 0$ and $u \in R - \mathfrak{m}$. Conversely, if $u \in R - \mathfrak{m}$ then $v(u) = 0$ and so $v(u^{-1}) = 0$ so $u^{-1} \in R$ and not only in K.

Given a non-zero ideal I, let $n = \min\{v(r) : r \in I\}$. $n < \infty$ and there is an element $r \in I$ such that $v(r) = n$. Let $x \in I$ then $v(x/r) = v(x) - v(r) \geq 0$ and so $x/r \in R$ and $x = r \cdot (x/r)$ shows that $I = (r)$. Also, $v(r/\pi^n) = 0$ and so $r = \pi^n u$, for some unit $u \in R^\times$, and it follows that $I = (\pi^n)$. Note that this characterization of n such that $I = (\pi^n)$ shows that all the ideals listed above are distinct.

Since R is a PID it is a UFD, hence integrally closed by Lemma 9.28. □

Corollary 9.33. *A dvr is a local Dedekind ring.*

Proof. The list of ideals shows that ring is noetherian. (π) is not only the only maximal ideal, but also the only prime ideal besides zero because for $n > 1$ we have $\pi \cdot \pi^{n-1} \in (\pi^n)$, but $\pi \notin (\pi^n)$ and $\pi^{n-1} \notin (\pi^n)$. □

END OF LECTURE 18 (November 14)

Theorem 9.34. *A local Dedekind ring* $(R, \mathfrak{m})$ *is a dvr.*

Proof.
Step 1: $\mathfrak{m}$ is a principal ideal. Let $a \neq 0, a \in \mathfrak{m}$. For $b \in R - Ra$, consider the ideal

$$(a : b) = \{r \in R : r \cdot \frac{b}{a} \in R\} = \{r \in R : rb \in Ra\}.$$

Note that $1 \notin (a : b)$. Choose b among $R - Ra$ such that the ideal $(a : b)$ is maximal relative to inclusion. This is possible because R is noetherian. We claim that $(a : b)$ is a prime ideal. Indeed, suppose that $xy \in (a : b)$ and $x \notin (a : b)$ and $y \notin (a : b)$. Therefore, $yb \notin Ra$ and so $(a : yb)$ is among the ideals we consider. Note also, that $(a : yb) \supseteq (a : b)$ and, furthermore $x \in (a : yb)$. It follows that $(a : yb) \supsetneq (a : b)$ and that is contradiction. Therefore, $(a : b)$ is prime. Since R has dimension 1 and $(a : b) \neq \{0\}$ (for example, $a \in (a : b)$), it follows that

$$\mathfrak{m} = (a : b).$$

We will show now that $\mathfrak{m} = R \cdot \frac{a}{b}$. Firstly, from the definition,

$$\mathfrak{m} \cdot \frac{b}{a} = (a : b)\frac{b}{a} \subseteq \mathfrak{m}.$$

If equality doesn't hold then $\frac{b}{a} \cdot \mathfrak{m} \subseteq \mathfrak{m}$. Viewing $\mathfrak{m}$ as a finitely generated R-module (using that R is noetherian), we see that it is a faithful $R[\frac{b}{a}]$-module and so $\frac{b}{a}$ is integral over R. Since R is integrally closed, $\frac{b}{a} \in R$. But the $b \in Ra$, which is a contradiction. Thus, $\frac{b}{a} \cdot \mathfrak{m} = R$ and so $\mathfrak{m} = R \cdot \frac{a}{b}$; in particular $\frac{a}{b} \in \mathfrak{m}$ and it follows $\mathfrak{m}$ is a principal ideal. Let $\pi = \frac{a}{b}$. Then,

$$\mathfrak{m} = (\pi).$$

Step 2: any ideal of R is principal. Suppose not, and, using the noetherian property again, choose an ideal I that is maximal among the non-principal ideals. Then $I \subset \mathfrak{m} = R\pi$. It follows that

$$I = \pi^{-1}\pi I \subseteq \pi^{-1} I \subseteq T.$$

If $I = \pi^{-1}I$ then, as above, π^{-1} is integral and so $\pi^{-1} \in R$ and thus $\mathfrak{m} = R$, which is an absurd. Thus, $I \subsetneqq \pi^{-1}I$. It follows that $\pi^{-1}I$ is a principal ideal, but then so is I! That's a contradiction and so all ideals are principal.

Step 3: R **is a dvr.** We know now that R is a PID, hence a UFD. It has a unique maximal ideal, hence a unique irreducible element π up to units. Every element x of the fraction field of R can therefore be written as $x = \pi^n u$, for some $n \in \mathbb{Z}$ and $u \in R^\times$, uniquely determined by x. We define

$$\mathrm{val}(x) = \mathrm{val}(\pi^n u) = n.$$

Clearly,

$$R = \{x : \mathrm{val}(x) \geq 0\}.$$

If $x = \pi^n u, y = \pi^m v$ then $xy = \pi^{n+m}(uv)$ and we find that $\mathrm{val}(xy) = \mathrm{val}(x) + \mathrm{val}(y)$. Suppose, without loss of generality, that $n \leq m$. Then $x + y = \pi^n(u + \pi^{m-n}v)$. As $u + \pi^{m-n}v \in R$, $\mathrm{val}(u + \pi^{m-n}v) \geq 0$ and so

$$\mathrm{val}(x) \leq \mathrm{val}(y) \implies \mathrm{val}(x+y) = \mathrm{val}(x) + \mathrm{val}(u + \pi^{m-n}v) \geq \mathrm{val}(x).$$

This gives, in general, that

$$\mathrm{val}(x+y) \geq \min\{\mathrm{val}(x), \mathrm{val}(y)\}.$$

Thus, val is a valuation and the proof is complete. $\square$

Corollary 9.35. *Let X be an affine variety and $\mathfrak{p}$ a prime ideal of height 1, corresponding to an irreducible variety $Z \subset X$ of codimension 1. Define the* **local ring of** X **at** Z *by*

$$\mathcal{O}_{X,Z} = A(X)_{\mathfrak{p}}.$$

Then, if X is normal, $\mathcal{O}_{X,Z}$ is a discrete valuation ring with valuation denoted ord_Z. Given a function $f \in K(X)$ we say that f **vanishes to order** n **along** Z *if $\mathrm{ord}_Z(F) = n$. If $n \geq 0$ we say that f has a* **zero of order** n*, while if $n \leq 0$ we say that f has a* **pole of order** n*.*

Proof. The ring $\mathcal{O}_{X,Z}$ is noetherian, being a localization of a noetherian ring; it is of dimension 1 because $\mathfrak{p}$ is of height 1; it is an integral domain because X is a variety; it is integrally closed being a localization of an integrally closed domain $A(X)$ as X is normal. Thus, $\mathcal{O}_{X,Z}$ is a local Dedekind ring, hence a dvr. The rest is just definitions. $\square$

Remark 9.36. Let $f \in K(X)$ such that $\mathrm{ord}_Z(f) \geq 0$. Then $f \in \mathfrak{p}\mathcal{O}_{X,Z}$. This implies that locally $f = \frac{f_1}{f_2}$, a ratio of regular functions such that $f_1 \in \mathfrak{p}$ and $f_2 \notin \mathfrak{p}$. Thus, the function f is well-defined on an open non-empty subset U of Z (for instance, $U = Z - Z(f_2)$) and identically zero there. Thus, f vanishes on Z, where ever it has a well-defined value. Conversely, let f be a function in $K(X)$, well-defined and identically zero on an open non-empty set of Z. Then $f \in \mathfrak{p}\mathcal{O}_{X,Z}$.

This shows that ord_Z really measures order of vanishing along Z.

Example 9.37. Let $X = \mathbb{A}^n$ and $Z = Z(g)$, where g is an irreducible polynomial. As $k[x_1, \dots, x_n]$ is UFD, every function f can be written as $f = g^n u$, where g doesn't divide u; that is, where $u \in \mathcal{O}_{X,Z}^\times$. We have

$$\mathrm{val}_Z(f) = n.$$

Example 9.38. If X is not normal, we cannot in general define the order of vanishing along a subvariety Z. For example, suppose that X is the cuspidal curve $y^2 = x^3$. The singular point $P = (0, 0)$ has a local ring that is not a dvr, because a dvr is regular local ring. Can we talk about order of vanishing at P. Suppose that there is such a notion. Then x vanishes to order a and y to order b, we expect that x^3 vanishes to order $3a$ and y^2 to order $2b$ and then $2b = 3a$. Therefore, $b > a$ and so we would expect that y/x vanished at P and, at any rate, is well defined at P. But in that case, the uniformization

$$\mathbb{A}^1 \to X, \qquad t \mapsto (t^2, t^3),$$

is an isomorphism with inverse

$$(x, y) \mapsto y/x.$$

That is a contradiction, as one is non-singular and the other is.

Corollary 9.39. *Let X be a* **curve***, that is, X is an irreducible quasi-projective variety of dimension* 1*. Suppose that for all $x \in X$, $\mathcal{O}_{X,x}$ is an integrally closed domain then X is non-singular.*

Proof. $\mathcal{O}_{X,x}$ is then a local Dedekind ring, hence a dvr. But then, $\mathcal{O}_{X,x}/\mathfrak{m}_x \cong \mathfrak{m}_x/\mathfrak{m}_x^2$ by a map induced by multiplication by a uniformizer. Thus, $\mathcal{O}_{X,x}$ is a regular local ring of dimension 1. $\square$

The last corollary suggest a method of resolving the singularities of a curve Y. Cover Y by open affine curves Y_α and let X_α be the normalization of Y_α, with finite morphisms $f_\alpha : X_\alpha \to Y_\alpha$. The curves X_α should "glue" to a global quasi-affine curve X and the morphisms f_α to a global morphism $f : X \to Y$. If so, by construction f will also be a birational morphism, an isomorphism outside Y^{sing}, and X non-singular. This idea is sound, but we don't have yet the technology to prove it. We will eventually do just that (cf. proof of Theorem 10.6). We remark that there is another approach that works through taking an embedding of Y in a projective space and taking the normalization of $S(Y)$, the homogenous coordinate ring. See [Mum, III §8].

10. Curves

10.1. **The idea, the goal and some consequences.** Let Y be an affine curve. We are familiar with the correspondence

$$\{\text{points } y \in Y\} \quad \longleftrightarrow \quad \{\text{maximal ideals of } A(Y)\},$$

given by $y \mapsto \mathfrak{m}_y$. If Y is projective, we have a difficulty constructing a similar correspondence. Of course, we could use the homogenous coordinate ring of Y and its maximal ideals, but unlike in the affine case, the homogenous coordinate ring depends on the embedding of Y in a projective space and typically two different embeddings do not yield isomorphic rings. Nonetheless, we note that there is another approach that works in the affine case. There is an injective map

$$Y \;\hookrightarrow\; \{\text{local rings of } K(Y)\}, \qquad y \mapsto \mathcal{O}_{Y,y}.$$

This map is indeed injective, because for different points we localize $A(Y)$ at different maximal ideals to obtain the local rings. Note that we can recover the maximal ideals by $\mathcal{O}_{Y,y} \cap A(Y)$. This approach generalizes well to the case where Y is quasi-projective as the local ring of a point *is* an intrinsic notion that doesn't depend on the projective embedding. Thus, for Y quasi projective, we have a function

$$Y \;\longrightarrow\; \{\text{local rings of } K(Y)\}, \qquad y \mapsto \mathcal{O}_{Y,y}.$$

Lemma 10.1. *This map is injective.*

Proof. Let $P \neq Q$ be distinct points of Y and say $Y \subseteq \mathbb{P}^n$. We claim that there exists a function f that is zero at P and non-zero at Q. Let $g = 1/f$. Then $g \in \mathcal{O}_{Y,Q}$ and $g \notin \mathcal{O}_{Y,P}$. When $n = 1$, $P = (\alpha : \beta)$ and T a point distinct from P and Q, $T = (\gamma : \delta)$, take $\frac{\beta x - \alpha y}{\delta x - \gamma y}$. To construct f for $n > 1$ we argue by induction on n. Choose a hyperplane $H \subseteq \mathbb{P}^n$ such that $P, Q \in H$. If $Y \subset H$ as $H \cong \mathbb{P}^{n-1}$ we may consider Y already as contained in $\mathbb{P}^{n-1}$ and use induction. Else $Y \cap H$ consists of finitely many points and so we can choose a hyperplane $J_0 \subset H$ of codimension 1 that contains P and not Q, and a hyperplane $L_0 \subset H$ of codimension 1 that contains neither P or Q. Linear algebra gives hyperplanes J and L of $\mathbb{P}^n$ that intersect H at J_0 and L_0, respectively. J and L are defined by the vanishing of linear forms j and ℓ, respectively. Let $f = j/\ell$. Then f is a rational function vanishing at P, well-defined and non-vanishing at Q. $\square$

Let K/k be a **function field of dimension** 1; that is K/k is a finitely generated field extension such that the transcendence degree of K over k is 1. These are precisely the fields arising a fields of rational functions of curves Y over k. Call a dvr $R \subset K$ a **dvr of** K/k if the valuation gives value 0 to k^times and the fraction field of R is K.

Consider now a particular case is when Y is a non-singular curve over k. In that case, we have an injection

$$Y \;\hookrightarrow\; \{\text{dvr's of } K(Y)/k\}, \qquad y \mapsto \mathcal{O}_{Y,y}.$$

One of the main points of this chapter is that if Y is projective, this is a bijection. Let us push our discussion a bit further. Suppose now that Y is any affine curve and let $P \in Y$ be a singular point. Then $\mathcal{O}_{Y,P}$ is *not* a dvr. Let $\tilde{Y} \to Y$ be the normalization of Y in $K(Y)$ and let $Q_1, \dots, Q_r$ be the points of $\tilde{Y}$ lying above P. Then, we have an injection

$$\mathcal{O}_{Y,P} \subseteq \mathcal{O}_{\tilde{Y},Q_i}$$

and each $\mathcal{O}_{\tilde{Y},Q_i}$ is a dvr of $K(Y)/k$. So, the process of resolution of singularities obtained by passing from Y to $\tilde{Y}$ is reflected by replacing the ring $\mathcal{O}_{Y,P}$ by the dvr $\mathcal{O}_{\tilde{Y},Q_i}$, $i = 1, \dots, r$. All this suggest that in some sense, a projective non-singular curve Y should be thought of as the collection of dvr's of $K(Y)/K$.

After developing a language allowing us to make sense of this idea, we will be able to prove one of the main results of this chapter. Namely, that the following three categories are equivalent:

(1) Projective non-singular curves and dominant morphisms.
(2) Quasi-projective curves with dominant rational maps.
(3) Function fields K/k of dimension 1 and k-algebra homomorphisms.

END OF LECTURE 19 (November 19)

We remark that the equivalence of (2) and (3) - to be precise, an anti-equivalence - is already known to us from our discussion of rational morphisms and birational equivalence. There is also a canonical function from (1) to (2): A projective curve is in particular a quasi-projective curve and a dominant morphism is an example of a dominant rational map.

Let us now illustrate what the equivalence means. For example, it implies the following: Given any quasi-projective curve Y, there is a smooth projective curve X, such that $X \sim Y$, equivalently $K(X) = K(Y)$. X is unique up to isomorphism. Further, given a dominant rational map $f : Y_1 - - \to Y_2$, and smooth projective curves $X_i \sim Y_i$, there exists a unique morphism $\phi : X_1 \to X_2$ such that the following diagram commutes

$$\begin{tikzcd} X_1 \arrow[r, "\phi"] \arrow[d, dashed] & X_2 \arrow[d, dashed] \\ Y_1 \arrow[r, dashed, "f"] & Y_2 \end{tikzcd}$$

In particular, if Y_1, Y_2 are themselves smooth projective curves and $f : Y - - \to Y_2$ is a rational map then f extends uniquely to a morphism $Y_1 \to Y_2$.

For example, we can use these statements to conclude that if Y is smooth projective and $Y_0 \subseteq Y$ is an affine curve then any automorphism $Y_0 \to Y_0$ extends uniquely to an automorphism $Y \to Y$.

10.2. **Abstract non-singular curves.** Let K/k be a function field of dimension 1; as always, k algebraically closed. Let C_K be the set of dvr's of K/k. The following lemma will be used repeatedly.

Lemma 10.2. *Let $x \in K$. Then $\{R \in C_K : x \notin R\}$ is a finite set. Let $y \in K$, $y \neq 0$. Then $\{R \in C_K : y \in \mathfrak{m}_R\}$ is a finite set.*

Proof. The case $x = 0$ is trivial. Suppose that $x \neq 0$ and put $y = 1/x$. If $x \notin R$ then $y \in \mathfrak{m}_R$, and vice-versa. Therefore, it is enough to prove the second statement of the lemma.

If $y \in k^\times$, then $y \in R^\times$ for any $R \in C_K$, so the set $\{R \in C_K : y \in \mathfrak{m}_R\}$ is empty. Let then $y \in K - k$. Since k is algebraically closed, y is transcendental over k. We have

$$k[y] \subset R \subset K.$$

Let B be the integral closure of $k[y]$ in K. Since $K/k(y)$ is algebraically and finitely generated, B is a finitely generated k-algebra that is a finite $k[y]$-module. Moreover, the quotient field of B is

K (every element of K is integral over some localization of $k[y]$ - look at the minimal polynomial of that element of $k(y)$). Thus, B corresponds to a smooth affine curve Y with $A(Y) = B$ and $K(Y) = K$.

Note that $k[y] \subset R$ implies that $B = N_K(k[y]) \subseteq N_K(R) = R$, because R is integrally closed and its fraction field is K. So $B \subset R$ for any dvr R of K/k such that $y \in \mathfrak{m}_R$. Let

$$\mathfrak{n}_R = \mathfrak{m}_R \cap B.$$

The ideal $\mathfrak{n}_R$ is a prime ideal of B, which is a Dedekind ring. Therefore $\mathfrak{n}_R$ is a maximal ideal, corresponding to some point $P \in Y$. We have

$$\mathcal{O}_{Y,P} = B_{\mathfrak{n}_R} \subseteq R.$$

Note that $B_{\mathfrak{n}_R}$ is a dvr of K/k too. We claim that in fact $B_{\mathfrak{n}_R} = R$. Indeed, as $\mathfrak{n}_R = \mathfrak{m}_R \cap B$, a uniformizer of $\mathfrak{n}_R$ belongs to $\mathfrak{m}_R$ and hence has positive valuation relative to the valuation of R. Therefore, up to a positive scaling factor, the valuation v of $B_{\mathfrak{n}_R}$ is obtained by restricting the valuation of R. But then both rings are equal to $\{k \in K : v(k) \geq 0\}$, hence equal.

Thus, $y \in \mathfrak{m}_R$ implies that $y \in \mathfrak{m}_P$. That is, y vanishes at P. But $y \neq 0$ so it vanishes at finitely many points. □

Corollary 10.3. *Any dvr of K/k is the local ring of some point on a smooth affine curve Y with $K(Y) = K$. In particular, $R/\mathfrak{m}_R = k$.*

To define abstract non-singular curves - or AC for short - we consider the following space (in fact, a special case of AC).

- The points of the space are C_K. It is a space with infinitely many points.
- The topology is the co-finite topology.
- We define a sheaf of functions $\mathcal{O}$: for $U \subseteq C_K$ we let

$$\mathcal{O}(U) = \cap_{R \in U} R.$$

We note that the function field of this space, namely $\varinjlim_{U \neq \emptyset} \mathcal{O}(U)$, is just K. Also, the local ring of a point R, namely $\varinjlim_{U \text{ s.t. } R \in U} \mathcal{O}(U) = R$ (use Lemma 10.2). Every element of $f \in \mathcal{O}(U)$, we shall refer to such an element temporarily as "abstract function", defines a "real function" $f : U \to k$ by the formula

$$f(R) = f \pmod{\mathfrak{m}_R} \in R\mathfrak{m}_R = k.$$

The "real function" f determines the "abstract function" f; indeed, if f and g define the same "real function", then $f - g \in \mathfrak{m}_R$ for all $R \in U$, which is an infinite set. By Lemma 10.2, $f - g = 0$. We can therefore easily identify "abstract functions" with "real functions".

We now define an **abstract non-singular curve**, or **AC** for short, to be a non-empty open set U of C_K (for some function field K/k of dimension 1) with the induced topology and sheaf of regular functions. We will see shortly that we may think about AC as a curve, but until we have established that, if we want to consider morphisms between varieties and AC's, we have to enlarge the category of varieties by including also all AC for any function field K/k of dimension 1. If V_1, V_2 are objects then a morphism $f : V_1 \to V_2$ is a continuous function such that for all $U \subseteq V_2$ open and a "real function" $g : U \to k$, the "real function" $g \circ f : f^{-1}(U) \to k$ is a regular function. That means that if V_1 is curve, this "real function" arises from an "abstract function" in the manner discussed above. We get a category this way that contains the category of varieties.

10.3. **Curves and abstract curves.**

Proposition 10.4. *Every non-singular quasi-projective curve Y is isomorphism to some AC.*

Proof. Let $K = K(Y)$ and $U \subseteq C_K$ be the set

$$U = \{\mathcal{O}_{Y,P} : P \in Y\}.$$

We shall show below that U is open. Suppose that for the time being then U is an AC. Define

$$\varphi : Y \to U, \qquad P \mapsto \mathcal{O}_{Y,P}.$$

As we have noted before, this is a bijection. Let $V \subseteq Y$ be open, then

$$\mathcal{O}(V) = \cap_{P\in Y}\mathcal{O}_{Y,P}.$$

(This just expresses the fact that being regular is a local property.) It follows that

$$\mathcal{O}(V) = \mathcal{O}(\varphi(V))$$

and therefore that φ is an isomorphism.

Now, to show U is open, it is enough to show that $C_K - U$ is finite, and, so, it is enough to show that U contains a non-empty open set. We may therefore assume that Y is affine. In that case, the proof of Lemma 10.2, show that

$$U = \{ \text{ dvr } R \text{ of } K/k : R \supset A(Y)\}.$$

Let $x_1, \dots, x_n$ be generators of $A(Y)$. Then,

$$U = \{R \in C_K : x_i \in R, i = 1, \dots, n\} = \cap_{i=1}^n \{R \in C_K : x_i \in R\}.$$

By Lemma 10.2, each set $\{R \in C_K : x_i \in R\}$ is co-finite and so U is co-finite too. □

Proposition 10.5. *Let X be an AC, $P \in X$ and Y a projective variety. Any morphism*

$$\varphi : X - \{P\} \to Y$$

extends uniquely to a morphism $X \to Y$.

Proof. Suppose that $Y \subseteq \mathbb{P}^n$, then the morphism $\varphi : X - \{P\} \to Y$ induces a morphism $\varphi : X - \{P\} \to \mathbb{P}^n$. Suppose that this morphism can be extended to $\varphi : X \to PP^n$, then $\varphi^{-1}(Y)$ is closed and contains $X - \{P\}$, hence equal to X (closed sets, except for X itself, are finite). Therefore the morphism $\varphi : X \to PP^n$ necessarily factors through Y and gives us an extension $\varphi : X \to Y$. Note that this extension is unique, because two morphisms agreeing on an open dense set, $X - \{P\}$ in our case, are equal everywhere.

Thus, we may consider the problem of extending a morphism $\varphi : X - \{P\} \to \mathbb{P}^n$ to a morphism $\varphi : X \to \mathbb{P}^n$.

Let $U \subseteq \mathbb{P}^n$ be the open set whose points are $\{a \in \mathbb{P}^n : a_i \neq 0, i = -, \dots, n\}$. We may assume that $\varphi(X - \{P\}) \cap U \neq \emptyset$. Indeed, if not, then $\varphi(x - \{P\}) \subset \cup_{i=0}^n Z(x_i)$. As $X - \{P\}$ is irreducible (proper finite sets are finite, after all) so is $\varphi(x - \{P\})$ and thus, there is an i such that $\varphi(x - \{P\}) \subseteq Z(x_i) \cong \mathbb{P}^{n-1}$. Thus, making use that the case of $n = 0$ it trivial and arguing by induction, we may assume this doesn't happen and so that $\varphi(X - \{P\}) \cap U \neq \emptyset$.

Let $f_{ij} = \varphi^*(x_i/x_j)$. This is a regular function of $\varphi^{-1}(U)$, which is a non-empty open set. Thus, $f_{ij} \in K$. Let us denote the valuation on P (P, recall, is a dvr) by v, and let $r_i = v(f_{i0})$. Then

$$v(f_{ij}) = v(f_{i0}/f_{j0}) = r_i - r_j.$$

Choose an a such that

$$v(f_{a0}) = \min\{v(f_{00}), v(f_{10}), \dots, v(f_{n0})\}.$$

Then,

$$v(f_{ia}) = r_i - r_a \geq 0, \forall i.$$

That is, $f_{0a}, \dots, f_{na} \in P$. Extend φ by defining

$$\varphi(P) = (f_{0a}(P), \dots, f_{na}(P)).$$

This is well-defined as all the functions f_{ia} are regular at P and not all vanish at P: $f_{aa} \equiv 1$. We need to show φ is a morphism. To begin with, to show that φ pulls-back regular functions to regular functions, it is enough to deal with an arbitrarily small open set containing $\varphi(P)$.

Note that $\varphi(P) \in V := \{x; x_a \neq 0\}$ and that is an affine open subset of $\mathbb{P}^n$ with affine coordinate ring $k[x_0/x_a, \dots, x_n/x_a]$. As $\varphi^*(x_i/x_a) = f_{ia}$ is regular at P, and regularity at any other point of $\varphi^{-1}(V)$ is already known, φ^* takes regular functions on V to regular functions on $\varphi^{-1}(V)$. Given a $V_1 \subseteq V$ open and $g \in \mathcal{O}(V)$ it follows easily, by writing g locally as a fraction of regular functions on V, that $\varphi^*(g)$ is regular on $\varphi^{-1}(V_1)$.

Finally, to show φ is continuous, we need to show that the pre image of a closed set is closed. A quick examination of the situation reveals that the only problem may occur when there is closed set $Z \supseteq \varphi(X - \{P\})$ such that $\varphi(P) \notin Z$. But then, if we define a function g by $g(Z) \equiv 0, g(P) = 1$, then g is a regular function on $\varphi(X)$. Thus, $\varphi^*(g)$ is regular on X; but this is a function that is zero on $X - \{P\}$ and 1 at P, and that's a contradiction. $\square$

END OF LECTURE 20 (November 21)

Here are some remarks concerning Proposition 10.5:

(1) The proposition applies to the case where X is a quasi-projective smooth curve, because we know such are isomorphic to abstract curves.

(2) The proposition fails if Y is not projective. Let $X = \mathbb{P}^1, P = (1:0), Y = \mathbb{A}^1$ and

$$\varphi : \mathbb{P}^1 - \{(1:0)\} \to \mathbb{A}^1, \qquad (x:y) \mapsto x/y.$$

Then φ doesn't extend to $\mathbb{P}^1$ as any morphism from a projective variety to an affine variety is constant (Corollary 4.18).

(3) The proposition fails when $\dim(X) > 1$. For example, let $X = \mathbb{A}^2, P = (0,0)$, Y some projective closure of $\mathrm{Bl}_P(\mathbb{A}^2)$. Let

$$\varphi : \mathbb{A}^2 - \{(0,0)\} \to Y, \qquad (a_1, a_2) \mapsto (a_1, a_2; a_1 : a_2).$$

The φ is an isomorphism from $\mathbb{A}^2 - \{(0,0)\}$ to the open set $Y-$ special fibre, which cannot be extended to X.

(4) The proof of Proposition prop extension makes use of the fact that we can write a function into a projective space in many ways. If locally around P,

$$Q \mapsto (f_0(Q) : \dots : f_n(Q)),$$

then we may say that this is also the map (up to rational equivalence)

$$Q \mapsto (f_0/f_a(Q) : \dots : \underset{a}{1} : \dots : f_n/f_a(P))).$$

The index a was chosen so that to make this expression well defined at P, and hence locally around P. This proof is very useful for explicit computations.

For instance, in Example 5.12 we considered a curve $Y = Z(g(x, y, z)) \subseteq \mathbb{P}^2_{x,y,z}$. And, we have constructed a morphism

$$\varphi : X - \{(0 : 1; 0)\} \to \mathbb{P}^1 = Y, \qquad (x : y : z) \mapsto (x; z).$$

We know now that this morphism can always be extended to X and how to do it. If φ is not dominant then it's constant and we are done. If $P = (0 : 1; 0) \notin X$, there is not problem, of course. Else, $P \in X$ and φ is dominant. The proof tells us to consider the two functions $1, \frac{z}{x}$ at P. If $\frac{z}{x}$ is regular at P then extend φ by $\varphi(P) = (1 : \frac{z}{x}(P))$. Else, necessarily $\frac{x}{z}$ is regular at P and extend φ by $\varphi(P) = (\frac{x}{z}(P) : 1)$. Note that if both $\frac{x}{z}$ and $\frac{z}{x}$ are regular, then indeed $(1 : \frac{z}{x}(P)) = (\frac{x}{z}(P) : 1)$.

Theorem 10.6. *The abstract curve C_K is isomorphic to a projective non-singular curve Y.*

Proof. Every point $R \in C_K$ has an open neighbourhood U^R isomorphic to an affine non-singular curve Y^R. As $C_K - U^R$ is finite, we can write

$$C_K = \cup_{i=1}^m U^i, \qquad U^i \cong Y_i^\circ \subseteq Y_i,$$

where Y_i° is a non-singular curve and Y_i its closure in some projective space $\mathbb{P}^{n_i}$. By Proposition 10.5, the morphism $\varphi_i : U_i \to Y_i$ extends to a morphism

$$\varphi_i : C_K \to Y_i.$$

Consider the product $\prod_{i=1}^m Y_i$ which is a closed irreducible subset of $\mathbb{P}^{n_1} \times \cdots times \mathbb{P}^{n_m}$ and so a projective variety. We have a morphism

$$\varphi = (\varphi_1, \dots, \varphi_m) : C_K \to \prod_{i=1}^m Y_i.$$

Let Y be the closure of $\varphi(C_K)$. Note that $Y \subset \prod_{i=1}^m Y_i$ and so the projection maps $p_i : \prod_{i=1}^m Y_i \to Y_i$ are defined on Y. $\varphi(C_K)$ is dense in Y and has dimension 1 as its projection onto Y_i is dominant (for any i). Y is thus a curve and $K(Y) \subseteq K$. Our goal is to show that the morphism $\varphi : C_K are Y$ is an isomorphism.

Let $R \in C_K$. Then $R \in U_i$ for some i. We have the following commutative diagram

$$\begin{tikzcd} C_K \arrow[r, "\varphi"] & Y \arrow[d, "p_i"] \\ U_i \arrow[u, hook] \arrow[r, "\varphi_i"] & Y_i \end{tikzcd}$$

All the morphisms are dominant and we conclude that

$$\mathcal{O}_{Y_i, \varphi_i(R)} \subseteq \mathcal{O}_{Y, \varphi(R)} \subseteq \mathcal{O}_{C_K, R} = R.$$

As φ_i is an isomorphism, we get equalities through out, and so $\mathcal{O}_{Y, \varphi(R)} \cong R$. That implies that $K(Y) = K$ and that φ is injective (recall, that if $x, y \in Z$, a quasi-projective variety, then $\mathcal{O}_{Z,x} = \mathcal{O}_{Z,y} \Leftrightarrow x = y$). The morphism φ is also surjective.

Let $P \in Y$. We claim that there exists a dvr R of K/k such that $R \supseteq \mathcal{O}_{Y,P}$. Indeed, as Y is a curve, there exists an open set $U \subseteq Y$ that is affine and such that $P \in U$. Let $\tilde{U}$ be its normalization in $K(Y)$. We have a finite birational morphism $f : \tilde{U} \to U$. Let $\tilde{P}$ be a point of $\tilde{U}$ such that $f(\tilde{P}) = P$. Then, $\mathcal{O}_{Y,P} = \mathcal{O}_{U,P} \subseteq \mathcal{O}_{\tilde{U},\tilde{P}}$, which is a dvr R since $\tilde{U}$ is a non-singular curve. We obtain then a point $R \in C_K$ such that

$$\mathcal{O}_{Y,\varphi(R)} = R \supseteq \mathcal{O}_{Y,P}.$$

We claim that this implies $P = \varphi(R)$; that is, if x, y are points on a curve Z and $\mathcal{O}_{Z,x} \subsetneq \mathcal{O}_{Z,y}$ then $x = y$. For that, it is enough to show that if $x \neq z$ then there exists a function on Z that vanishes at x and not at y to obtain a contradiction. Embed Z in a projective space $\mathbb{P}^N$. One can obtain such a function as a ratio of two linear forms F/G. We leave the details as an east exercise (one looks for a hyperplane passing through x and not through y, and another hyperplane passing through none of $\{x, y\}$).

At this point we know that $\varphi : C_K \to Y$ is a bijective morphism. But, we can cover C_K and Y by open sets U_i and $\varphi(U_i)$ respectively, on which φ restricts to an isomorphism, because the composition $U_i \to C_K \xrightarrow{\varphi} Y \xrightarrow{p_i} Y_i$ is the isomorphism φ_i. Namely, the inverse of $\varphi|_{U_i}$ is the morphism $\varphi_i^{-1} \circ p_i$. Thus, φ is an isomorphism. $\square$

Corollary 10.7. *Any AC is isomorphic to some non-singular quasi-projective curve.*

Proof. We have $U \subseteq C_K \cong Y$, where Y is a non-singular projective curve and so U can be identified with an open subset of Y and therefore is a quasi-projective non-singular curve. $\square$

Corollary 10.8. *Every non-singular quasi-projective curve Y° is isomorphic to an open subset of a non-singular projective curve Y.*

Proof. Indeed, by Proposition 10.4, Y° is an AC. Use the previous corollary. $\square$

Corollary 10.9. *Every curve Y' is birationally equivalent to a non-singular projective curve Y, $Y' \sim Y$.*

Proof. Indeed $Y' \sim Y^\circ$, where Y° is the non-singular locus of Y'. Use the previous corollary. $\square$

10.4. **An equivalence of categories.**

Theorem 10.10. *The following categories are equivalent:*

1. *Projective non-singular curves and dominant morphisms.*
2. *Quasi-projective curves with dominant rational maps.*
3. *Function fields K/k of dimension 1 and k-algebra homomorphisms.*

Proof. We already know the equivalence of (2) and (3) as a special case of Corollary 5.21. $\square$

10.4.1. *Normalization.* Let X be a quasi-projective curve. Then there is a quasi-projective non-singular curve and a finite birational morphism $\tilde{X} \to X$. To show that, it is enough to consider the case where X is projective, the general case follows by restricting to a subset. In that case, let $\tilde{X}$ be the non-singular projective model of X. The inclusion $K(X) \subseteq K(\tilde{X})$ produce a rational morphism $\tilde{X} \to X$, which, by Proposition 10.5, extends to a morphism $f : \tilde{X} \to X$. As the inclusion of function fields is actually an equality, this morphism is birational. Further, $\tilde{X}$ is normal, being non-singular. The morphism f is in fact surjective. Given a point $x \in X$, choose a dvr R of K/k such that $\mathcal{O}_{X,x} \subseteq R$. R corresponds to a point $t \in \tilde{X} \cong C_K$. Consider $f(t)$. If $f(t) \neq x$, we can find a rational function g on X that vanishes at $f(t)$ and is invertible at x. Then $f^*(g)$ vanishes at t and so is in the maximal ideal of R, but is a unit in $\mathcal{O}_{X,x}$. A contradiction.

We can cover X by open affine subsets U such that $f^{-1}(U)$ is affine. But then $f : f^{-1}(U) \to U$ produces an injection of rings $A(U) \subseteq A(f^{-1}(U))$. Passing to integral closure in $K(X)$ we get $B(U) \subseteq A(f^{-1}(U))$, as $A(f^{-1}(U))$ is integrally closed, being a ring of regular functions of a non-singular affine curve, and where we have let $B(U)$ be the integral closure of $A(U)$. We claim that $B(U)$ is equal to $A(f^{-1}(U))$.

Let t be a point of $A(f^{-1}(U))$ and R the corresponding local ring. Let R_1 be the local ring of $f(t)$. Then $R_1 \subseteq R$ and both are dvr of K/k. We saw that this implies $R = R_1$ (see the proof of Lemma lemma curves). This, in turn implies that the map $f : f^{-1}(U) \to U$ is injective because if $f(t_1) = f(t_2)$ then t_1, t_2 have the same local ring and so are equal. Thus, the inclusion $B(U) \subseteq A(f^{-1}(U))$ is surjective too. We have equality. That means that locally $\tilde{X}$ is the normalization of X and so $\tilde{X}$ is the normalization of X.

Fact: The following theorem holds true. It is not very hard to prove, but we will not have time to prove it this semester. For the proof see, for example, [Sha, Volume 1, §5.2].

Theorem 10.11. *Let X be a projective variety and $f : X \to Y$ a morphism into a quasi-affine variety Y. The image of f is closed.*

The following corollary follows immediately, noting that we may replace Y also by its closure in some projective space.

Corollary 10.12. *A dominant morphism $f : X \to Y$ from a projective variety into a quasi-affine variety is surjective. In fact, Y is then necessarily projective. In particular, any dominant morphism between projective curves in surjective.*

10.4.2. *Degree.* Let $f : X \to Y$ be a dominant morphism between non-singular curves. Define the **degree** of f as

$$\deg(f) := [K(X) : K(Y)].$$

This is a finite number, as $K(X)$ and $K(Y)$ are both of transcendence degree 1 over k and finitely generated over k. It follows from Theorem 10.10 that $\deg(f) = 1$ if and only if f is an isomorphism.

10.4.3. *Hyperelliptic curves.* We ask to classify all the diagrams

$$f : X \to \mathbb{P}^1,$$

where X is a non-singular projective curve and f is a surjective morphism of degree 2. Such a curve X is called **hyperelliptic**. Note that what we are doing is classifying all pairs (X, f) up to isomorphism, which is not the same as classifying all X up to isomorphism. Using Theorem 10.10, this is the same as classifying all quadratic extensions

$$k(t) = K(\mathbb{P}^1) \subset K.$$

The discussion brakes now naturally into two cases.

(1) The characteristic of k is not 2. In this case, Kummer's theory applies. Such extensions correspond canonically to non-trivial elements of $k(t)^\times / k(t)^{\times 2}$. To a polynomial $g(t)$, which is not a square, one associate the curve $y^2 = g(t)$, equivalently, the function field $k(t)[y]/(y^2 - g(t))$.

(2) The characteristic of k is 2. Here one uses Artin-Schreier theory. Such extensions correspond canonically to nontrivial elements in $k(t)/S$, where $S = \{f^2 - f : f \in k(t)\}$. To a polynomial $g(t)$ one associates the curve $y^2 - y = g(t)$, that is, the function field $k(t)[y]/(y^2 - y - g(t))$.

END OF LECTURE 21 (November 26)

10.5. **Ramification, Genus and the Hurwitz genus formula.** Let $f\colon X \to Y$ be a dominant morphism of non-singular projective curves. f is surjective. Let $y \in Y$ and let $x \in X$ with $f(x) = y$. Then, we have an inclusion of dvr's

$$\mathcal{O}_{Y,y} \subseteq \mathcal{O}_{X,x}.$$

Let π_y be a uniformizer of $\mathcal{O}_{Y,y}$ and let e_x, the **ramification number** at x, be

$$e_x = \mathrm{val}_x(f^*(\pi_y)).$$

The morphism f is called **unramified at** x if $e_x = 1$ and **unramified** if $e_x = 1$ for all $x \in X$.

We assume throughout that $\mathrm{char}(F) \nmid \deg(f)$**.**

Fact. The morphism f is ramified at finitely many points (if at all). For all $y \in Y$,

$$\sum_{f(x)=y} e_x = \deg(f(x)).$$

Therefore, most the fibres of f are unramified and have precisely $\deg(f)$ points.

Example 10.13. Let $X = Y = \mathbb{P}^1$. Let $f(x:y) = (x^n : y^n)$. If we let $t = x/y$ then $K(\mathbb{P}^1) = k(t)$ and the inclusion f^* is

$$k(t) \to k(t), \qquad t \mapsto t^n.$$

Therefore,

$$\deg(f) = n.$$

The map f is ramified at two points at most: $0 = (0:1)$ and $\infty = (1:0)$. At the point 0 we have the affine chart $\mathbb{A}^1 \subset \mathbb{P}^1$, $t \mapsto (t:1)$ and the map is written as $t \mapsto t^n$. We see that $f^*(t) = t^n$ and t is a local parameter at 0. Thus, $e_0 = n$. At ∞, we take the variable $u = 1/t = y/x$ as a coordinate at the affine chart $\mathbb{A}^1 \subset \mathbb{P}^1$, $u \mapsto (1:u)$. The map is $u \mapsto u^n$ and so also $e_\infty = n$.

10.5.1. *Genus.* It is a fact that to every non-singular projective curve X one can associate an integer $g(X) \in \mathbb{Z}_{\geq 0}$, called the **genus** of X. The best definitions of the genus use either cohomology groups, or holomorphic differential, and we hadn't studied those. Thus, instead of defining the genus we will explain how to compute it.

Theorem 10.14. (**Hurwitz's genus formula**) *Let $f\colon X \to Y$ be a dominant morphism of projective non-singular curves. Then,*

$$2g(X) - 2 = \deg(f) \cdot (2g(Y) - 2) + \sum_{x \in X} (e_x - 1).$$

Note that the sum $\sum_{x\in X}(e_x - 1)$ is really a finite sum, because all point of X, except the finitely many ramification points, satisfy $e_x - 1 = 0$.

Let X be any projective non-singular curve and pick an $f \in K(X)$ that is not constant. Then f defines a rational morphism $f\colon X - \to Y$. But then, by Proposition 10.5, f is actually a morphism $f : X \to \mathbb{P}^1$ and so we can calculate $g(X)$ by analyzing f and knowing that $g(\mathbb{P}^1) = 0$.

It is amusing that in fact we can conclude from the genus formula that

$$g(\mathbb{P}^1) = 0.$$

Indeed, let $n > 1$ and consider the raising-to-n-power map $\mathbb{P}^1 \to \mathbb{P}^1$ of Example 10.13. Let $g = g(\mathbb{P}^1)$. We have

$$2g - 2 = n(2g - 2) + 2(n - 1).$$

Solving, we find that $g = 0$. The converse is also true: a non-singular projective curve of genus 0 is isomorphic to $\mathbb{P}^1$. In general, the curves of genus $g > 1$ are parameterized by a quasi-projective variety of dimension $3g-3$ and the curves of genus 1 by a variety of dimension 1. These statements go back to Riemann, in fact.

Example 10.15. Let k be a field of characteristic different from 2. Let $f(t) \in k(t)^\times$ be a square-free, non constant, polynomial. Let X° be the affine curve $y^2 = f(t)$. It is a non-singular curve as

$$(-f'(t), 2y) = (0, 0),$$

for a point (a, b) on the curve implies that $b = 0$ and hence a is a root of f. But then $f'(a) = 0$ implies that a is a double root of f and that's a contradiction. We have the morphism of degree 2,

$$\varphi : X^\circ \to \mathbb{A}^1, \qquad \varphi(t, y) = t.$$

If $a \in \mathbb{A}^1$ and is not a root of f, there are two pre-images, namely $\{(a, \pm\sqrt{f(a)})\}$. Let a be a root of f, then at a, the function $t - a$ is a uniformizer and since $f(t) = (t - a)g(t)$, where $g(a) \neq 0$, we find that $g(t) \in \mathcal{O}^\times_{\mathbb{A}^1,a}$. Therefore, $f(t)$ is also a uniformizer at a.

Now, on the curve X°, the functions y and $x - a$ (equivalently, $g(t)$), generate the maximal ideal at the point $P = (a, 0)$. Since $\mathfrak{m}_P/\mathfrak{m}_P^2$ is 1-dimensional, either $f(t)$ or y are uniformizers at P. We also have the relation $y^2 = f(t)$, from which follows that $\mathrm{val}_P(f(t)) = 2\mathrm{val}_P(y)$. It follows that y is the uniformizer and $e_P = 2$.

Let X be a projective non-singular curve containing X°. The morphism φ extend to a morphism of degree 2,

$$\varphi : X \to \mathbb{P}^1.$$

Note that, taking into account multiplicities, we have already accounted for all the points lying over $\mathbb{A}^1$; they all lie on X°. Thus $X - X^\circ = \varphi^{-1}(\infty)$, which is either one point (that we then denoted P_∞), or two points (that we denote Q_∞, R_∞). Applying Hurwitz formula we find

$$2 \cdot g(X) - 2 = 2(2 \cdot 0 - 2) + \deg(f) + \epsilon, \qquad \epsilon = \begin{cases} 1 & |\varphi^{-1}(\infty)| = 1 \\ 0 & |\varphi^{-1}(\infty)| = 2 \end{cases}$$

Parity considerations now force the following conclusions:

(1) If $\deg(f)$ is even, $|\varphi^{-1}(\infty)| = 2$ and

$$g(X) = \frac{\deg(f) - 2}{2}.$$

(2) If $\deg(f)$ is odd, $|\varphi^{-1}(\infty)| = 1$ and
$$g(X) = \frac{\deg(f) - 1}{2}.$$

Remark 10.16. Over the complex numbers X is topologically a compact oriented surface. Thus, topologically, X is a handle body and its genus is the number of holes.

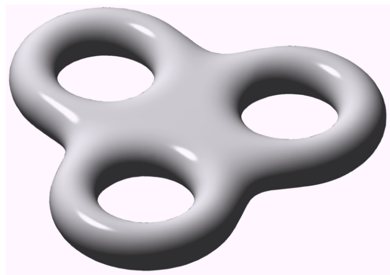


Figure 23. Genus 3

Example 10.17. Let X be a non-singular plane curve defined by an irreducible homogenous polynomial $g(x, y, z)$ of degree d. Then,
$$g(X) = \frac{(d-1)(d-2)}{2}.$$
Therefore, the genera of plane curves are $0, 1, 3, 6, 10, \dots$. Thus, for example, a non-singular curve of genus 2 cannot be embedded in $\mathbb{P}^2$. That is why in Example 10.15 we used some round-about arguments instead of taking the projective closure of X° in $\mathbb{P}^2$ and doing direct calculations.

Let us illustrate the formula for the case of a **Fermat curve**
$$X: \quad x^d + y^d + z^d = 0.$$
Let us assume that $\mathrm{char}(\mathbb{F}) \nmid d$. Then X is a non-singular curve. The morphism
$$f : X \to \mathbb{P}^1, \qquad (x : y : z) \mapsto (x : y),$$
is defined everywhere. Writing $K(\mathbb{P}^1) = k(\frac{x}{y})$ we have $K(X) = k(\frac{x}{y})[\frac{z}{y}]/((\frac{z}{y})^d + (\frac{x}{y})^d + 1)$, and f induces the obvious inclusion $K(\mathbb{P}^1) \subseteq K(X)$. It follows that f has degree d. If $(a : b)$ is a point such that $a^d + b^d \neq 0$ then there are precisely d pre images.

There are d points $(a : b)$ on $\mathbb{P}^1$ such $a^d + b^d = 0$. Such a point can be written as $(\zeta : 1)$, where $\zeta^d = -1$. Its unique pre image is $P = (\zeta : 1 : 0)$. Thus, we can conclude that $e_P = d$ (using $\sum_{f(x)=y} e_x = \deg(f)$). Let us verify that directly:

In the coordinates $\tilde{u} = \frac{x}{y}, v = \frac{z}{y}$ the equation of the curve is $v^d = -\tilde{u}^d - 1$, the morphism is $(\tilde{u}, v) \mapsto \tilde{u}$ and the point on $\mathbb{A}^1$ is $(\zeta, 0)$. Let $u = \tilde{u} - \zeta$. Then,
$$v^d = -(u + \zeta)^d - 1 = -u^d - d\zeta u^{d-1} - \cdots - d\zeta^{d-1} u.$$
The morphism is $(u, v) \mapsto u$ and the point is $P = (0, 0)$. Note that $\mathrm{val}_P(u) > 0$ as u certainly vanishes at P. Thus, by the strong triangle inequality, we find
$$d \cdot \mathrm{val}_P(v) = \mathrm{val}_P(-u^d - d\zeta u^{d-1} - \cdots - d\zeta^{d-1} u) = \mathrm{val}_P(u).$$

It follows that v is a uniformizer at P and $e_P = d$. We find that $2g(X) - 2 = -2d + d(d-1)$, which implies

$$g(X) = \frac{(d-1)(d-2)}{2}.$$

10.6. **Singularities of plane curves.** Let $X \subset \mathbb{P}^2_{x,y,z}$ be a plane curve. Suppose that the point $P = (0:0:1) \in X = Z(G(x,y,z))$, where G is a homogenous irreducible polynomial. Let $g(x,y)$ be the dehogenization of G relative to the variable z. The **multiplicity of** X **at** P**,** m_P**,** is defined to be the degree of g^*. Recall out notation: we expand $g = g_m + \dots + g_r$ as a sum of homogenous polynomials in x, y of degrees $m, \dots, r$, respectively, where $g_m \neq 0$. Then $g^* = g_m$. The multiplicity m_P at any other point $P = (p_1, \dots, p_n)$ is defined by making a linear change of coordinates to get to the case $P = 0$. Note that the curve is singular at P if and only if $m_P > 1$.

Example 10.18. $y^2 - x^3$ has multiplicity 2 at $(0,0)$, as does $y^2 - x^2(x+1)$. The curve $x^2y + xy^2 = x^4 + y^4$ has multiplicity 3 at $(0,0)$.

Since g^* is a homogenous polynomial in x, y of degree m - the multiplicity at 0 - we can write

$$g^* = \prod_{i=1}^{m} (\alpha_i x + \beta_i y).$$

If none of the forms $\alpha_i x + \beta_i y$ is a scalar multiple of the other, we call 0 an **ordinary point**. If $m = 2$, we talk about an **ordinary double point** (or a **node**), if $m = 3$ about **ordinary triple point** and so on.

Example 10.19. For $y^2 - x^3$, $g^* = y^2 = y \cdot y$ and 0 is not an ordinary point. For $y^2 - x^2(x+1)$, $g^* = y^2 - x^2 = (x+y)(x-y)$ and 0 is an ordinary double point. For $x^2y + xy^2 - x^4 - y^4$, $g^* = x^2y + yx^2 = x \cdot y \cdot (x+y)$ and 0 is an ordinary triple point.

Theorem 10.20. *Let X be a plane curve of degree d with r ordinary singular points and let $\tilde{X}$ be its normalization (the non-singular projective model of $K(X)$). Then,*

$$g(\tilde{X}) = \frac{(d-1)(d-2)}{2} - \sum_{P \text{ singular}} \frac{m_P(m_P - 1)}{2}.$$

Since $g(\tilde{X}) \geq 0$, we find:

Corollary 10.21. *The number of singular points on X is at most $\frac{(d-1)(d-2)}{2}$.*

We remark that this holds true without the assumption that the singularities are ordinary. More information about all that can be found in [Har]. For the proof of the theorem, see [Ful, Chapter 8, Proposition 5].

Example 10.22. The degree of $X: \quad y^2z = x^2(x+z)$ is 3. The only singular point (including at infinity) is 0 and its multiplicity is 2. We find that $g(\tilde{X}) = \frac{(3-1)(3-2)}{2} - \frac{2(2-1)}{2} = 0$. In fact, we know that already. We have considered the paramaterization

$$\varphi : \mathbb{P}^1 \to X,$$

given on the affine chart $(t:1)$ by $t \mapsto (t^2 - 1, t(t^2 - 1))$, and so, in projective coordinates by

$$(x:y) \mapsto (x^2y - y^3 : x^3 - xy^2 : y^3).$$

It is easy to see that φ has degree 1. It follows that $\tilde{X}$ is the normalization of X and indeed it has genus 0.

END OF LECTURE 22 (November 28)

10.7. **Projection from a point.** Let $P \in \mathbb{P}^n$, $n \geq 1$. The lines through P are parameterized by $\mathbb{P}^{n-1}$. Indeed, the point P corresponds to a one dimensional subspace $k \cdot P$ in $\mathbb{A}^{n+1}$ and the lines through P then correspond to two dimensional subspaces of $\mathbb{A}^{n+1}$ containing $k \cdot P$ and so to one dimensional subspaces of $\mathbb{A}^{n+1}/k \cdot P \cong \mathbb{A}^n$. Each such line through P is isomorphic to $\mathbb{P}^1$. Any two distinct points P, Q in $\mathbb{P}^n$ lie on a unique line; that line is the image of the plane spanned by P and Q in $\mathbb{A}^{n+1}$

For example, suppose that $P = (0 : \cdots : 1)$ (we can always achieve that after an automorphism of $\mathbb{P}^n$). Then, given a point $(\alpha_0 : \cdots : \alpha_{n-1}) \in \mathbb{P}^{n-1}$, the line through P it defines is given as the image of $\mathbb{P}^1$ under the morphism

$$\mathbb{P}^1 \to \mathbb{P}^n, \qquad (s : t) \mapsto (s\alpha_0 : \cdots : s\alpha_{n-1} : t),$$

which is the image of the plane spanned by $(\alpha_0, \ldots, \alpha_{n-1}, 0)$ and $(0, \ldots, 0, 1)$ in $\mathbb{A}^{n+1}$.

For a general point $P \in \mathbb{P}^n$ we define the **projection from a point** morphism

$$\pi_P : \mathbb{P}^n - \{P\} \to \mathbb{P}^{n-1}.$$

The morphism π_P takes a point Q to the line passing through P and Q; that line is viewed as a point on $\mathbb{P}^{n-1}$. For example, of $P = (0 : \cdots : 0 : 1)$ we get the morphism

$$\pi_P(x_0 : x_1 : \cdots : x_n) \mapsto (x_0 : x_1 : \cdots : x_{n-1}).$$

Note that indeed, $\pi_P^{-1}((x_0 : x_1 : \cdots : x_{n-1})) = \{(sx_0 : sx_1 : \cdots : sx_{n-1} : t) \mid (s : t) \in \mathbb{P}^1\}$ is a line through P and the point $(x_0 : x_1 : \cdots : x_n)$.

There is another way to view this map. Consider the blow up of $\mathbb{P}^n$ at the point P, $f : \mathrm{Bl}_P(\mathbb{P}^n) \to \mathbb{P}^n$. The point P is replaced by the variety parametrizing the lines passing through it, namely by $\mathbb{P}^{n-1}$. For every point Q different from P the strict transform of the line ℓ_Q through P and Q is a closed subvariety of $\mathrm{Bl}_P(\mathbb{P}^n)$ that intersects the special fibre at a unique point $\pi_P(Q)$. Let Y be a closed algebraic set of $\mathbb{P}^n$ such that $P \notin Y$. The union of the lines $\cup_{Q \in Y} \ell_Q$ is a projective algebraic set as well, denoted (temporarily) Y_{sus} - this something we take as fact for now, and make a few further remarks on later when we discuss how to calculate the image of Y under the projection π_P. We note that $\pi_P(Y)$ is equal to $\widetilde{Y_{\mathrm{sus}}} \cap f^{-1}(P)$, where $\widetilde{Y_{\mathrm{sus}}}$ is the strict transform of Y_{sus}, and so is closed.

We will be interested in particular in the case where Y is a curve (not containing P) and in the image of Y under π_P, which is a curve as well. The properties of the curve $\pi_P(Y)$ depend on the relative position of P and Y and so we need some techniques first to exclude problematic relative positions.

10.7.1. *Secant varieties.* Let $Y \subseteq \mathbb{P}^n$ be a quasi-projective variety. For every P, Q on Y, consider the line through P and Q. The collection of these lines is parameterized by some subset of $\mathrm{Grass}(2, n+1)$. It can be described as the image of a rational morphism

$$Y \times Y \dashrightarrow \mathrm{Grass}(2, n+1).$$

The **secant variety** of Y, $\mathscr{S}(Y)$ is the closure of the image of that morphism. It is a variety of dimension at most $2\dim(Y)$ (and in fact the dimension is lower only in very rare cases).

Let V be the tautological plane bundle over $\mathrm{Grass}(2, n+1)$. It is a variety contained in $\mathrm{Grass}(2, n+1) \times \mathbb{A}^{n+1}$ such that its fibre over a point of the Grassmannian is precise the plane in $\mathbb{A}^{n+1}$ that the point parameterizes. We have a diagram

$$\begin{tikzcd} V \arrow[d] & V|_{\mathscr{S}(Y)} \arrow[l, hook'] \arrow[d] \arrow[r, "\varphi"] & \mathbb{P}^n \\ \mathrm{Grass}(2, n+1) & \mathscr{S}(Y) \arrow[l, hook'] \end{tikzcd}$$

Here the fibre over a point $t \in \mathscr{S}(Y)$, goes to the projective line in $\mathbb{P}^N$ which is the secant to the curve parameterized by t.

Suppose that Y is a curve. Then $\mathscr{S}(Y)$ is 2-dimensional at most and so $\mathrm{Im}(\varphi)$ is at most 3-dimensional. Therefore, if $Y \subset \mathbb{P}^n$, $n \geq 4$, there is an open set U of $\mathbb{P}^n$ with the property that if $P \in U$ then the line through P and any other point Q of Y is not a secant of Y. Otherwise said, for $P \in U$, π_P is injective on Y.

10.7.2. *Variety of tangents.* Let $X \subseteq \mathbb{A}^n$ be an affine non-singular variety. For every $x \in X$ we may identify the tangent space $T_{X,x}$ of X at x with a subset of $\mathbb{A}^n$. For example, if $x = 0$, the tangent space is the subspace cut by the linear relations $\sum_i x_i \frac{\partial f_j}{\partial x_i}(0)$ as f_j ranges over the ideal $I(X)$. We can also view the tangent space in the affine space as $x + T_{X,x}$. When x varies over X we get an algebraic subset of $\mathbb{A}^n$.

Suppose now that X is projective and is a non-singular variety in $\mathbb{P}^n$. By covering $\mathbb{P}^n$ by affine spaces, we have for every $x \in X$ an affine subspace of dimension $d = \dim(X)$ passing through x and identified with $T_{X,x}$. We take the closure of $x + T_{X,x}$; it is a linear subvariety of dimension d isomorphic to $\mathbb{P}^d$. Denote it $\mathbb{T}_{X,x}$. By a **tangent line** to X at P we mean a line in $\mathbb{P}^n$ that passes through x and lies on $\mathbb{T}_{X,x}$. Such a line defines a point in $\mathrm{Grass}(2, n+1)$. The closure of all the points obtained this way is called the **variety of tangents** $\mathscr{T}_1(X)$. It is a closed subset of $\mathrm{Grass}(2, n+1)$; in fact, it is a closed subset of $\mathscr{S}(X)$. If X is curve then $\mathscr{T}_1(X)$ is 1 dimensional, unless X is a line itself.

It follows that the same set U found above has the additional property that for $P \in U$, any line passing through P and a point Q of Y is not a tangent line to Y.

Theorem 10.23. *Let Y be a non-singular projective curve in $\mathbb{P}^n$, where $n \geq 4$. There exists a point $P \notin Y$ such that $\pi_P(Y)$ is a projective non-singular curve in $\mathbb{P}^{n-1}$ isomorphic to Y.*

The proof of the theorem can be found in [H, IV, Corollary 3.6], and in more elementary language in [Sha, II.5, Corollaries 1,2].

Corollary 10.24. *Any projective non-singular curve is isomorphic to a projective non-singular curve in $\mathbb{P}^3$.*

We remark that one can also prove, using similar ideas the following

Theorem 10.25. *Every curve is birational to a projective plane curve with ordinary double points.*

The proof can be found in [H, IV.3]; see also [Har]. This explains the interest in studying plane curves with ordinary singularities, and, even more specifically, with only ordinary double points. Note that there is a link between the degree, the number of singular points and the genus. For example, if X is projective non-singular and of genus 2 then it is possibly isomorphic to a plane curve of degree 4 with one ordinary double point, or a plane curve of degree 5 with 4 ordinary double points, etc. The advantage of this view point is that the family of degree d plane curves is easily parametrized.

10.7.3. *Resultants.* What is still lacking in our discussion is how to calculate the image of the projection from a point. The main tool is resultants. A first reference is [Har, pp. 34-37]. Let f, g be polynomials in the variable z and coefficients in the ring $k[x_1, \dots, x_n]$. The **resultant** of f and g, $\mathrm{Res}(f, g)$, is a polynomial in the ring $k[x_1, \dots, x_n]$. It is defined as follows. Write

$$f(z) = \sum_{i=0}^{m} a_i z^i, \qquad g(z) = \sum_{i=0}^{n} b_i z^i,$$

where a_i, b_j are in $k[x_1, \dots, x_n]$ and $a_m \neq 0, b_n \neq 0$. We let

$$\mathrm{Res}(f,g) = \det \begin{pmatrix} a_0 & \cdots & \cdots & a_m & & & & & \\ & a_0 \cdots & \cdots & & a_m & & & & \\ & & \ddots & & \ddots & & & & \\ & & & & & a_0 & \cdots & \cdots & a_m \\ b_0 & \cdots & \cdots & & b_n & & & & \\ & b_0 & \cdots & \cdots & & b_n & & & \\ & & \ddots & & & \ddots & & & \\ & & & b_0 & \cdots & \cdots & & & b_n \end{pmatrix}$$

This is an $(m+n) \times (m+n)$ matrix; there are n rows of a's and m rows of b's. The main property of the resultant is that the polynomials $f(z), g(z)$ have a common factor, if and only if their resultant is zero.

As before, suppose that the point we are projecting from is $P = (0 : \cdots : 0 : 1)$ and we choose as coordinates on $\mathbb{P}^n$ the variables $x_1, \dots, x_n, z$ (to conform with the resultant notation). Then one has the following theorem (cf. [Har], loc. cit.).

Theorem 10.26. *Let Y be a closed algebraic set in $\mathbb{P}^n$ not containing P. Then $\pi_P(Y)$ is the closed subvariety of $\mathbb{P}^{n-1}_{x_1,\dots,x_n}$ defined by the ideal*

$$\langle \{\mathrm{Res}(f, g) : f, g \in I(Y)\} \rangle.$$

Remark 10.27. This theorem holds also when $P \in Y$, as long as every irreducible component of Y containing P is positive dimensional.

The answer provided by the theorem to our computation problem, is not really satisfactory, as the ideal is presented using an infinite set of generators. However, if we are projecting a curve from $\mathbb{P}^3$ to $\mathbb{P}^2$ we can be more optimistic, as the image will be defined by one irreducible polynomial, and now we know where to look for it. In general, the interpretation $\pi_P(Y) = \widetilde{Y_{\mathrm{sus}}} \cap f^{-1}(P)$, gives another approach to calculation equation to $\pi_P(Y)$.

Example 10.28. Consider the twisted cubic Y in $\mathbb{P}^3$. It is given by the equations $x_0x_2 - x_1^2 = 0$, $x_0x_3 - x_1x_2 = 0$, $x_1x_3 - x_2^2 = 0$. (So on the affine patch $x_3 = 1$ these are the points (t^3, t^2, t).) We switch the coordinates x_3 and x_1 and now we have the generators

$$x_0x_2 - x_3^2, \quad x_0x_1 - x_3x_2, \quad x_1x_3 - x_2^2.$$

The point $P = (0:0:0:1)$ is not on the curve. Let us calculate the projection of the curve from the point P. We are looking for a curve in $\mathbb{P}^2$. Let us calculate the resultant of the polynomials

$$f(x_3) = x_1x_3 - x_2^2, \qquad g = -x_3x_2 + x_0x_1.$$

We have

$$\mathrm{Res}(f,g) = \det \begin{pmatrix} -x_2^2 & x_1 \\ x_0x_1 & -x_2 \end{pmatrix} = x_2^3 - x_1^2x_0.$$

As this is an irreducible polynomial, there is no need to calculate further. This is the image.

The morphism $Y \to \pi_P(Y)$ is bijective and so, since we are dealing with curves (!), birational. (Assume for simplicity that we are characteristic zero.). The image is the closure of the cuspidal curve $x_2^3 - x_1^2 = 0$. It has a unique singular point, the point $q = (1:0:0)$ and it is not ordinary. (Else, we would find that genus is $(2-1)(2-2)/2 - m_q(m_q-1)/2 < 0$, but we have also checked that before directly.) That suggests that the curve $(s:0:0:t)$ is tangent to the curve Y at some point. Consider the point $Q = (1:0:0:0)$. Dehomegenizing the equations relative to x_0, we find that in the affine chart $x_0 \neq 0$, the curve is given by

$$f_1 = x_2 - x_3^2 = 0, \quad f_2 = x_1 - x_2x_3 = 0, \quad f_3 = x_1x_3 - x_2^2 = 0.$$

The Jacobian matrix at $(0,0,0)$ is

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

The tangent space in $\mathbb{A}^3$ is $k \cdot (0,0,1)$ and it is embedded in $\mathbb{P}^3$ as $\{(1:0:0:t) : t \in k\}$. The tangent space $\mathbb{T}_P(Y)$ in $\mathbb{P}^3$ is thus the closure of the set $\{(1:0:0:1) : t \in k\}$, namely, $\{(s:0:0:t) : (s:t) \in \mathbb{P}^1\}$.

11. Intersections in a Projective Space

11.1. **The Problem.** Intersection theory is originally motivated by counting problems and by the problem of guaranteeing the existence on non-trivial solutions to a system of equations.

A classical problem in the field of enumerative geometry is the problem of counting conics satisfying certain conditions. To fix ideas consider circles in the plane: $a(x^2+y^2)+bxz+cyz+dz^2=0$. These can be thoughts of as the conics in $\mathbb{P}^2$ that pass through the points $(1:\pm 1:0)$. Note that such a circle corresponds bijectively to a point $(a:b:c:d) \in \mathbb{P}^3$. The family of circles tangent to a given circle forms a quadric hypersurface in $\mathbb{P}^3$. One thus expects that the number of circles tangent to three given circles (in general position) should be computable as the intersection of three quadrics in $\mathbb{P}^3$ and, drawing from Bezout's theorem, should perhaps be equal to $2^3 = 8$. This is indeed true.[20]

Bezout's theorem also illustrates nicely the other motivation we have raised. One knows that there are plenty of solutions to a homogenous polynomial $f_1(x, y, z)$ of degree m_1 in the variables x, y, z. But are there always solutions to a system $f_1 = \cdots = f_n = 0$ of such equations? When the number of equations is 2, Bezout's theorem provides a precise answer: there are $m_1 m_2$ such solutions counting multiplicities.

The generalization of these topics to higher dimensions and spaces besides $\mathbb{P}^n$ is the topic of intersection theory. In particular, the correct definition of intersection that allows multiplicities to be taken into account (needed for Bezout's theorem and for enumerative geometry).

11.2. **The Hilbert Polynomial.** This is some beautiful piece of pure algebra. I shall refer to Hartshorne for some of the proofs.

Definition 11.1. Let $S = \oplus_{d\geq 0} S_d$ be a graded ring. Let M be an S module. We say that M is a **graded S-module** if we have

$$M = \oplus_{d\in\mathbb{Z}} M_d, \quad S_d \cdot M_e \subseteq M_{d+e},$$

for all integers d, e. Note that we do not restrict the grading on M to be positive.

Example 11.2. Let $Y \subseteq \mathbb{P}^n$ be a closed algebraic set. Let $S = k[x_0, \cdots, x_n]$ and $S(Y) = S/\mathcal{I}(Y)$. Then $S(Y)$ is a graded S module.

Definition 11.3. Let $S = k[x_0, \cdots, x_n]$ and let M be a graded S-module. Define

$$\phi_M : \mathbb{Z} \to \mathbb{Z}, \quad \phi_M(\ell) = \dim_k(M_\ell).$$

Theorem 11.4. (Hilbert-Serre) *Let $S = k[x_0, \cdots, x_n]$ and M be a finitely-generated graded S-module. There is a unique polynomial $P_M(x) \in \mathbb{Q}[x]$ such that*

$$\phi_M(\ell) = P_M(\ell), \quad \forall \ell \gg 0.$$

Furthermore,

$$\deg(P_M) = \dim \mathcal{Z}(\operatorname{Ann} M),$$

where Ann M *is the ideal of all elements $s \in S$ such that $s \cdot m = 0$ for all $m \in M$.*

[20] It turns out that also the circles tangent to a given line are parameterized by a quadric, but the number of circles tangent to three different lines (in general position) is 4 and not 8, due to non-generic intersection of these quadrics. See [Ful, p. 192].

Definition 11.5. Let $Y \subseteq \mathbb{P}^n$ be a closed algebraic set of dimension r. The **Hilbert polynomial** of Y, denoted $P_Y(x)$, is the polynomial $P_{S(Y)}(x)$ of the graded S-module $S(Y)$. The **degree** of Y is defined as $r!$ times the leading coefficient of P_Y. Thus,

$$P_Y(x) = \frac{\deg(Y)}{\dim(Y)!} x^{\dim(Y)} + \text{lower order terms}.$$

We would like to calculate the Hilbert polynomials of some projective varieties in order to see what information they contain.

Lemma 11.6. *Let $0 \to M_1 \to M \to M_2 \to 0$ be an exact sequence of S-modules. Then*

$$\phi_M = \phi_{M_1} + \phi_{M_2}.$$

Proof. Clear. For every ℓ we have an exact sequence of k-vector spaces

$$0 \to (M_1)_\ell \to (M)_\ell \to (M_2)_\ell \to 0.$$

$\square$

Proposition 11.7. *Let $Y \subseteq \mathbb{P}^n$ be a closed set. Then*

(1) *If $Y \neq \emptyset$ then $\deg(Y)$ is a positive integer.*
(2) *If $Y = Y_1 \cup Y_2$, where Y_1 and Y_2 are of the same dimension and $\dim(Y_1 \cap Y_2) < \dim(Y) = r$ then $\deg(Y) = \deg(Y_1) + \deg(Y_2)$.*
(3) *Let $Y = \{y_1, \dots, y_m\}$ be a finite collection of distinct points. Then $P_Y = m$.*
(4) *The Hilbert polynomial of $\mathbb{P}^n$ is*[21]

$$P_{\mathbb{P}^n}(x) = \binom{x+n}{n} = \frac{1}{n!}(x+n)(x+n-1)\cdots(x+1).$$

In particular, $\deg(\mathbb{P}^n) = 1$.
(5) *Let Y be a hypersurface generated by an irreducible polynomial of degree d. Then*

$$P_Y(x) = \binom{x+n}{n} - \binom{x+n-d}{n}.$$

In particular, $\deg(Y) = d$.

Proof. (1) Since P_Y is a numeric polynomial of degree $r = \dim(Y)$ and leading coefficient say c, we have that $r! \cdot c$ is a non-zero integer. Since for large x we have $P_Y(x) \sim cx^r \sim \dim_k(S(Y)_x)$ we must have $c \geq 0$.

(2) Let I_1, I_2 be the ideals of Y_1, Y_2. Then $I = I_1 \cap I_2$ is also a radical ideal and it corresponds to $Y_1 \cup Y_2$. Let $J = I_1 + I_2$. We have then an exact sequence of S-modules

$$0 \to S/I \to S/I_1 \oplus S/I_2 \to S/J \to 0,$$

where the first map is induced from the diagonal homomorphism $S \to S/I_1 \oplus S/I_2$ and the second homomorphism is $(a_1 + I_1, a_2 + I_2) \mapsto a_1 - a_2 + J$. This gives us that

$$\begin{aligned} P_{Y_1 \cup Y_2} &= P_{S/I} \\ &= P_{S/I_1 \oplus S/I_2} - P_{S/J} \\ &= P_{S/I_1} + P_{S/I_2} - P_{S/J} \\ &= P_{Y_1} + P_{Y_2} - P_{S/J}. \end{aligned} \tag{8}$$

[21]For any integer n the symbol $\binom{z}{n}$ stands for the polynomial $\frac{1}{n!}z(z-1)\cdots(z-n+1)$.

Since both P_{Y_1} and P_{Y_2} are polynomials of degree r of leading coefficients $\deg(Y_1)/r!$ and $\deg(Y_2)/r!$, and since $P_{S/J}$ is a polynomial of degree $\dim \mathcal{Z}(J) = \dim(Y_1 \cap Y_2) < r$, the assertion follows.

Remark 11.8. Note that if $J = I_1 + I_2$ is a **radical** ideal, then

$$P_{Y_1 \cup Y_2} = P_{Y_1} + P_{Y_2} - P_{Y_1 \cap Y_2},$$

because in that case we can identify J with $\mathcal{I}(Y_1 \cap Y_2)$, unless J is the irrelevant ideal. One checks that in that case the equality is still true.

(3) Assume first that $m = 1$. Then Y consists of a single point. There exists a coordinate x_i such that $x_i(Y) \neq 0$. I claim that $k[x_i] \cong S(Y)$ as graded rings. First, since the homomorphism $k[x_i] \to S(Y)$ is graded, if it is not injective then x_i^n is in the kernel for some n, which is clearly a contradiction. Second, to show this is a surjective homomorphism it is enough to show that every x_j is in the image. If $x_j \notin \mathcal{I}(Y)$ then for some $\alpha \in k$ we have $\alpha x_i(Y) - x_j(Y) = 0$ which shows that $\alpha x_i - x_j \in \mathcal{I}(Y)$. It follows that $S(Y)_\ell$ is one dimensional for every ℓ and hence that $P_Y(x) = 1$.

Assume now that we proved the result for $Y_1 = \{y_1, \ldots, y_d\}$ and consider $d+1$ distinct points $Y = \{y_1, \ldots, y_d, x\}$. Write $Y = Y_1 \cup Y_2$, where $Y_2 = \{x\}$. Then, since $Y_1 \cap Y_2 = \emptyset$ we can use the previous result and especially Remark 11.8.

(4) This follows immediately from the fact that the number of distinct monomials of degree d in $x_0, \ldots, x_n$ is $\binom{d+n}{n}$. (To a monomial $x_0^{a_0} \cdots x_n^{a_n}$ associate the increasing vector $(1+a_0, 2+a_0+a_1, \ldots, n+a_0+\cdots+a_{n-1})$, a choice of n elements from the set $\{1, \ldots, n+d\}$.)

(5) We first make a definition:

Definition 11.9. Let M be a graded R-module and let $d \in \mathbb{Z}$. Define $M(d)$ to be the module M but with a new grading such that

$$M(d)_\ell = M_{d+\ell}.$$

Note that for $R = S$ we have that

$$\phi_{M(d)}(x) = \phi_M(d+x).$$

Let now f be homogenous and irreducible polynomial of degree d in S. We have an exact sequence of graded S-modules

$$0 \to S(-d) \xrightarrow{f} S \to S/(f) \to 0.$$

We conclude that

$$\begin{aligned}
\phi_Y(x) &= \phi_S(x) - \phi_{S(-d)}(x) \\
&= \phi_{\mathbb{P}^n}(x) - \phi_{\mathbb{P}^n(x-d)} \\
&= \binom{x+n}{n} - \binom{x+n-d}{n} \\
&= \frac{1}{n!}(x+n)(x+n-1)\cdots(x+1) - \frac{1}{n!}(x-d+n)(x-d+n-1)\cdots(x-d+1) \\
&= \frac{d}{(n-1)!}x^{n-1} + \text{lower order terms.}
\end{aligned}$$

□

11.3. **Intersection Multiplicities.**

Proposition 11.10. *Let M be a finitely generated graded module over a noetherian graded ring S. Then there exists a filtration*

$$0 = M^0 \subset M^1 \subset \cdots \subset M^r = M$$

by graded submodules such that for every i we have

$$M^i/M^{i-1} \cong (S/\mathfrak{p}_i)(\ell_i),$$

where $\mathfrak{p}_i$ is a homogenous prime ideal of S and $\ell_i \in \mathbb{Z}$. Furthermore:

(1) *If $\mathfrak{p}$ is a homogenous prime ideal of S then*

$$\mathfrak{p} \supseteq \operatorname{Ann}(M) \iff \exists i, \;\; \mathfrak{p} \supseteq \mathfrak{p}_i.$$

In particular, the minimal elements of the set $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are the minimal primes of the ideal $\operatorname{Ann}(M)$*. We shall call them the* **minimal primes of** M*.*

(2) *For each minimal prime $\mathfrak{p}$ of M, the number of times that $\mathfrak{p}$ occurs in the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ is equal to the length of $\mathfrak{M}_\mathfrak{p}$ over the local ring $S_\mathfrak{p}$ (and hence is independent of the filtration). This number is called the* **multiplicity** *of $\mathfrak{p}$ in M and denoted $\mu_\mathfrak{p}(M)$.*

Let $Y \subseteq \mathbb{P}^n$ be a projective variety and let $H \subseteq \mathbb{P}^n$ be a hypersurface not containing Y. Then, essentially by an exercise we did but see also [H, Thm. 7.2], every irreducible component Z of $Y \cap H$ has dimension $r-1$. Let $\mathfrak{p}$ be the homogenous prime ideal of Z.

Definition 11.11. The intersection multiplicity $i(Y, H; Z)$ of Y and H at Z is

$$\mu_\mathfrak{p}\left[S/(\mathcal{I}(Y) + \mathcal{I}(H))\right].$$

Note that $M = S/(\mathcal{I}(Y) + \mathcal{I}(H))$ has annihilator $\mathcal{I}(Y) + \mathcal{I}(H)$ and $\mathcal{Z}(\mathcal{I}(Y) + \mathcal{I}(H)) = Y \cap H$, hence $\mathfrak{p}$ is a minimal prime ideal for M and the intersection multiplicity is well defined.

11.4. **Intersection Theory in $\mathbb{P}^n$.**

Theorem 11.12. *Let $Y \subseteq \mathbb{P}^n$ be a variety of positive dimension and let $H \subset \mathbb{P}^n$ be a hypersurface not containing Y. Let $Z_1, \dots, Z_s$ be the irreducible components of $Y \cap H$. Then*

$$\sum_{j=1}^{s} i(Y, H; Z_j) \cdot \deg(Z_j) = \deg(Y) \cdot \deg(H).$$

Corollary 11.13. (Bezout's Theorem) *Two distinct plane curves of degree m and n intersect at mn points, counting multiplicities.*

Example 11.14. Let $Y : y^2z - x^3 = 0$ be the cuspidal curve and $H : x = 0$ be a line, both in $\mathbb{P}^2_{x,y,z}$. In this case $\mathcal{I}(Y) = (y^2z - x^3), \mathcal{I}(H) = (x)$ and $\mathcal{I}(Y) + \mathcal{I}(H) = (x, y^2z - x^3) = (x, y^2z)$. We see that

$$Y \cap H = \{(0:0:1), (0:1:0)\}.$$

We proceed to calculate the intersection multiplicities. Let $M = k[x, y, z]/(x, y^2z) \cong k[y, z]/(y^2z)$. M is naturally a module over $k[y, z]$ and the module structure over $k[x, y, z]$ comes from the module structure over $k[y,z]$ via the homomorphism $k[x,y,z] \to k[y,z]$ taking x to 0. Consider the filtration

$$0 = M^0 \subset M^1 = (yz)/(y^2z) \subset M^2 = (z)/(y^2z) \subset M^3 = M = k[y,z]/(y^2z).$$

We see that

$$M^3/M^2 \cong k[y,z]/(z), \quad M^2/M^1 \cong (k[y,z]/(y))(1), \quad M^1 \cong (k[y,z]/(y))(2).$$

Or, as $k[x,y,z]$-modules

$$M^3/M^2 \cong k[x,y,z]/(x,z), \quad M^2/M^1 \cong (k[x,y,z]/(x,y))(1), \quad M^1 \cong (k[x,y,z]/(x,y))(2).$$

The list of ideals we get are

$$\mathfrak{p}_1 = \mathfrak{p}_2 = (x,y), \; \mathfrak{p}_3 = (x,z).$$

(Note that these are indeed the minimal prime ideals containing $\mathrm{Ann}(M)$). We conclude that

$$i(Y,H;(0:0:1)) = 2, \qquad i(Y,H;(0:1:0)) = 1.$$

This affirm Bezout's theorem and also the expectation, based on perturbation, that the intersection multiplicity at $(0:0:1)$ is two. See Figure 24.

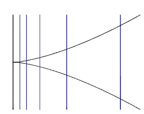


Figure 24. Intersection multiplicity at 0

Proof. (of Theorem 11.12) Let $M = S/(\mathcal{I}(Y) + \mathcal{I}(H))$ and let H be defined by a homogenous irreducible polynomial f of degree d. We shall calculate the Hilbert polynomial P_M in two ways and get the result by comparing the leading coefficients.

We have an exact sequence of graded S-modules

$$0 \to (S/\mathcal{I}(Y))(-d) \xrightarrow{f} S/\mathcal{I}(Y) \to M \to 0.$$

Therefore,

$$P_M(x) = P_Y(x) - P_Y(x-d).$$

If Y has dimension r and degree e we have

$$P_Y(x) = \frac{e}{r!}x^r + \text{lower order terms},$$

which gives

$$P_M(x) = \frac{de}{(r-1)!}x^{r-1} + \text{lower order terms}.$$

On the other hand, we can calculate P_M using the filtration of M. If the filtration is

$$0 = M^0 \subset M^1 \subset \cdots \subset M^q = M,$$

such that for every i we have

$$M^i/M^{i-1} \cong (S/\mathfrak{p}_i)(\ell_i),$$

then

$$\begin{aligned}
P_M(x) &= \sum_{i=1}^{q} P_{M_i}(x) \\
&= \sum_{i=1}^{q} P_{S/\mathfrak{p}_i}(x+\ell_i) \\
&= \sum_{i=1}^{q} P_{\mathcal{Z}(\mathfrak{p}_i)}(x+\ell_i) \\
&= \sum_{i=1}^{q} \frac{\deg(\mathcal{Z}(\mathfrak{p}_i))}{(\dim(\mathcal{Z}(\mathfrak{p}_i))-1)!} x^{\dim(\mathcal{Z}(\mathfrak{p}_i))} + \text{lower order terms.}
\end{aligned}$$

The leading term depends only on these $\mathfrak{p}_i$ giving varieties of dimension $\geq r-1$. These are the minimal prime ideals of M and they all give varieties of dimension $r-1$. It only remains to note that each such prime $\mathfrak{p}$ contributes to the leading term exactly $i(Y, H; \mathcal{Z}(\mathfrak{p}))\frac{\deg(\mathcal{Z}(\mathfrak{p}))}{(r-1)!}$. $\square$

To have a more complete theory we would like to have similar theorems for arbitrary two closed algebraic sets in $\mathbb{P}^n$ and a more intuitive, or easy to calculate, notion of multiplicity. Both can indeed be developed. For multiplicites, in the case of curves, see [H, Ex. 5.3-5.4].

References

[Eis] Eisenbud, David: Commutative algebra. With a view toward algebraic geometry. Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.

[Ful] Fulton, William: Intersection theory. Second edition. Springer Verlag, New York, Berlin, Heidelberg. 1998.

[Har] Harris, J.: Algebraic Geometry. Springer GTM, vol. 133.

[H] Hartshorne, R.: Algebraic geometry. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[Lang] Lang, Serge: Algebra. Second edition. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1984.

[Mat] Matsumura, H.: Commutative algebra. Second edition. Mathematics Lecture Note Series, 56. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.

[Mum] Mumford, David: The red book of varieties and schemes. Lecture Notes in Mathematics, 1358. Springer-Verlag, Berlin, 1988.

[Sha] Shafarevich, I.: Basic Algebraic Geometry, volumes 1 and 2. Second edition. Springer.

[ZS] Zariski, O.; Samuel, P.: Commutative algebra. Vols. I, II. With the cooperation of I. S. Cohen. Corrected reprinting of the 1958 edition. Graduate Texts in Mathematics, No. 28, 29. Springer-Verlag, New York-Heidelberg-Berlin, 1975.