

0.1 Syllabus

Prerequisites. Linear algebra. Rings and modules. It will help you if you know what is projective plane. For this you might consult notes on *Projective Geometry* of Nigel Hitchin (especially first two sections), that can be found on the page:

<http://people.maths.ox.ac.uk/hitchin/hitchinnotes/hitchinnotes.html>

There is also a nice appendix in the book of Joseph H. Silverman and John Tate. *Rational Points on elliptic curves*. The appendix is called "Projective Geometry".

Suggested reading.

1) Fulton. *Algebraic curves*. <http://www.math.lsa.umich.edu/~wful-ton/CurveBook.pdf> This is a nice book with plenty of exercises. Some material from sections 1-6 in the book is relevant to the course.

2) *Algebraic Geometry: A First Course* - Joe Harris. Some material from lectures 1-7 is relevant to the course.

3) Miles Reid, *Undergraduate Algebraic Geometry*.

4) *Basic algebraic geometry* Shafarevich, first chapter.

5) *Elementary algebraic geometry* Huleck.

The following are sources on Commutative Algebra.

5) *Introduction to Commutative Algebra* - Atiyah–Macdonald. Classical source.

6) David Eisenbud. Commutative algebra with a view towards algebraic geometry.

7) *A Primer of Commutative Algebra* - J.S. Milne.

<http://www.jmilne.org/math/xnotes/ca.html>

Office hours. This will be Wednesdays just after the classes 12-1pm.

Exercises and Exam. There will be 3-4 problem sheets. 100% of the mark is for the exam. Exam will consist of 5 problems 4 best out of 5 will count to the grade A or B.

0.2 What will be covered

1) Bézout's Theorem, first encounter.

2) Kakeya's problem, Dvir's theorem.

2) Projective spaces, homogeneous coordinates and conics.

3) Reminder on rings and ideals. Hilbert basis theorem.

4) Affine varieties and Nullstellensatz.

5) Morphisms of affine varieties, singularities, multiplicities of singular points of curves.

6) Full Bézout's Theorem (time permitted).

Acknowledgments. I would like to thank Pascal Honoré and Sveta for correcting numerous mistakes in these notes.

(these notes might still contain mistakes, if you find one, please don't hesitate to tell me.)

1 Introduction. Pascal, Bézout, Kakeya-Dvir

1.1 Pascal's and Bézout's Theorems

Let us start with the following theorem of Pascal, 1639:

Theorem 1.1 *For an arbitrary hexagon inscribed in any conic, the intersection points of lines containing pairs of opposite sides lie on a line.*

We will deduce this statement from a weak form of Bézout's theorem. Bézout's theorem is a theorem about intersection of curves on the plane given by polynomial equations $F(x, y) = 0$, $G(x, y) = 0$.

Theorem 1.2 *Let F and G be two polynomials in $K[x, y]$ without common factors. Then the number of points in the intersection of curves $F(x, y) = 0$ and $G(x, y) = 0$ is at most $\deg(F) \cdot \deg(G)$.*

This theorem generalizes the statement that a polynomial $F(x)$ in one variable has at most $\deg(F)$ distinct roots. You can check the theorem in simple cases.

A curve on the plane given by zeros of a degree two polynomial is called *conic*, while a curve given by a degree three polynomial is called *cubic*.

Proof of Pascal's theorem. We assume that the conic is *irreducible*, i.e. it is given by equation $F(x, y) = 0$, where F is an irreducible polynomial of degree two. The reducible case is left as an exercise.

Let $l_1, m_1, l_2, m_2, l_3, m_3$ be the linear functions on the plane, vanishing on the consecutive sides of the inscribed 6-gon. Consider the one parameter family of polynomials:

$$G_\lambda = l_1 l_2 l_3 + \lambda m_1 m_2 m_3$$

Pick a point p of the conic (not a vertex) and chose λ_0 so that $G_{\lambda_0}(p) = 0$.

Since the conic $F = 0$ intersects the cubic $G_{\lambda_0} = 0$ in at least 7 points and F is irreducible, according to Bézout theorem F divides G_{λ_0} ; $G_{\lambda_0} = F \cdot L$. Three points lie on $L = 0$. □

Remark 1.3 One degenerate case of this theorem is Pappus theorem, when the conic is reducible, i.e., it is a union of two lines. Pappus theorem can be proven easily using the notion of projective plane. One needs to send the intersections $l_1 \cap m_1$ and $l_2 \cap m_2$ to infinity and prove that l_3 and m_3 are parallel.

Exercise 1.4 Suppose we have a conic C on the plane and a point p on it. Suppose we can draw a line through any two points on the plane. Using Pascal's theorem guess how to draw the tangent line to C at p .

1.2 Proof of the partial case of Bézout

We are going to prove Theorem 1.2.

Recall that by $k[x_1, \dots, x_n]$ we denote the ring of polynomials with coefficients in k .

Notations. By R we denote $k[x, y]$. (F, G) is the ideal in R generated by F and G . $(F, G) = R \cdot F + R \cdot G$.

Proposition 1.5

$$\#(F = 0 \cap G = 0) \leq \dim(R/(F, G)) \leq \deg(F) \cdot \deg(G).$$

Proof. *First inequality.*

Lemma 1.6 *Let P_1, \dots, P_m be m different points in the (x, y) plane. Then for each i there is a polynomial $H_i = H_i(x, y)$ such that $H_i(P_j) = \delta_i^j$.*

Lemma 1.7 *Suppose that m points P_i from the previous lemma lie in $(F = 0) \cap (G = 0)$. Then the polynomials H_i are independent modulo (F, G) .*

Proof. Suppose there is any relation, i.e., $\sum_i c_i H_i \in (F, G)$ then each c_i equals zero (since F and G vanish at P_i). □

These two lemmas prove the first inequality.

□

Proof of second inequality.Define $\phi(d) = \frac{(d+1)(d+2)}{2}$.Let R_d be the vector space of polynomials of $\deg \leq d$.Let $W_d = R_{d-\deg F}F + R_{d-\deg G}G = \{H_1F + H_2G\}$. Of course $W_d \subset (F, G)$.**Exercise 1.8** $\dim R_d = \phi(d)$.**Lemma 1.9** For $d \geq \deg(F) + \deg(G)$ one has

$$R_{d-\deg F}F \cap R_{d-\deg G}G = R_{d-\deg F-\deg G}F \cdot G.$$

To prove the lemma we recall the following theorem from algebra.

Theorem 1.10 *The ring of polynomials is an UFD, i.e., a unique factorization domain.***Proof of lemma.** Since F and G have no common factor, a polynomial that is divisible by both F and G is divisible as well by FG .

□

Corollary 1.11

$$\dim R_d - \dim W_d = \phi(d) - \phi(d - \deg F) - \phi(d - \deg G) + \phi(d - \deg F - \deg G) = \deg F \cdot \deg G.$$

Proof. Recall that if U and V subspaces of a vector space then $\dim(U + V) = \dim(U) + \dim(V) - \dim(U \cap V)$. Applying this to $U = R_{d-\deg F}F$, $V = R_{d-\deg G}G$ and using $U + V = W_d$ with the previous lemma we get the result.

□

End of proof of second inequality.Suppose f_1, \dots, f_m are elements of R linearly independent modulo (F, G) . Let $d \geq \max_i(\deg(f_i))$. Then f_i are linearly independent in R_d modulo W_d , i.e., $m \leq \deg F \cdot \deg G$ by the corollary.

□

Exercise 1.12 Give examples of polynomials (F, G) such that:A) $\#(F = 0 \cap G = 0) < \dim(R/(F, G))$.B) $\dim(R/(F, G)) < \deg(F) \cdot \deg(G)$.

Remark 1.13 Note first that though the statement of the theorem is rather geometric (it is about number of points), the proof is rather algebraic.

Second, the statement of Bézout theorem that we proved, is about an inequality, the proof works for all field. But one can "refine" the proof in order to get "equality". In this case we should take care of points with multiplicity and take care of what happen at infinity.

Question 1.14 Could you guess what Bézout's theorem says in higher dimensions?

1.3 Kakeya conjecture over finite fields, Dvir's proof.

Now we make a jump from 19th to 21st century.

History. *Kakeya set*, is any set of points in Euclidean space which contains a unit line segment in every direction. Besicovitch – beginning of 20th century have shown that Kakeya set can have zero measure. Still there is a conjecture that the Hausdorff dimension of a Kakeya set in \mathbb{R}^n is n .

Finite fields. If K^n is a vector space over a finite field K , define a *Kakeya set* to be a subset of K^n which contains a line in every direction.

Conjecture. Thomas Wolff 1999. *Finite field Kakeya conjecture.* Let $E \subset K^n$ be a Kakeya set. Then E has cardinality at least $c_n |K|^n$, where c_n depends only on n .

This conjecture was proved by Zeev Dvir in 2008, using polynomials.

Proof. We start with the standard lemma: *Factor Lemma*.

Lemma 1.15 *Let K be a field, and $d \geq 1$ be an integer. Let $K[x]$ denote the polynomials in one variable with coefficients in K .*

1. *If $P \in K[x]$ is a non-zero polynomial of degree at most d , then the set $\{x \in K : P(x) = 0\}$ has cardinality at most d .*

2. *Conversely, given any set $E \subset K$ of cardinality at most d , there exists a non-zero polynomial $P \in K[x]$ of degree at most d that vanishes on E .*

Lemma 1.16 *Let $E \subset K^n$ be a set of cardinality less than $\binom{n+d}{d}$ for some $d \geq 0$. Then there exists a non-zero polynomial $P \in K[x_1, \dots, x_n]$ on n variables of degree at most d which vanishes on E .*

Proof. Let V be the vector space of polynomials in $K[x_1, \dots, x_n]$ of degree at most d . By combinatorics V has dimension $\binom{n+d}{d}$. On the other hand, the vector space of K -valued functions on E has dimension $< \binom{n+d}{d}$. Hence

the evaluation map $P \rightarrow (P(x))_{x \in E}$ from V to K^E is non-injective, and the claim follows. □

Proposition 1.17 *Let $P \in K[x_1, \dots, x_n]$ be a polynomial of degree at most $|K| - 1$ which vanishes on a Keakeya set E . Then P is identically zero.*

Question. Why can not we take a polynomial of degree $|F|$?

Proof. Suppose for contradiction that P is non-zero. We can write $P = \sum_{i=0}^d P_i$, where d is the degree of P , $0 \leq d \leq |K| - 1$, and P_i is the i^{th} homogeneous component. Of course, P_d is non-zero. Since P vanishes on E , d cannot be zero.

Let us fix a vector v in $K^n \setminus 0$. Since E is a Keakeya set, E contains a line $\{x + tv : t \in K\}$ for some fixed $x = x_v \in K^n$. Let us now restrict the polynomial P to the line $\{x_v + tv : t \in K\}$ so that we get the polynomial of one variable t , $P(x_v + tv)$. Clearly for all $t \in K$ we have $P(x_v + tv) = 0$. Since $P(x_v + tv)$ is a polynomial in t of degree at most $|K| - 1$, it vanishes identically by the factor lemma. We conclude that t^d coefficient of $P(x_v + tv)$, which is $P_d(v)$ as well. So, the polynomial P_d vanishes at all non-zero vectors $v \in K^n$. Since P_d is homogeneous of degree $d > 0$, P_d vanishes on all of K^n as well. Now we use the following exercise:

Exercise 1.18 Let Q be any polynomial of degree less than $|K|$ that is vanishing at each point of K^n . Prove that Q is identically zero.

Letting $Q = P_d$ we get contradiction. □

Corollary 1.19 *Every Keakeya set in K^n has cardinality at least $\binom{|K|+n-1}{|K|-1}$.*

Now, $\binom{|K|+n-1}{|K|-1} = \binom{|K|+n-1}{n} \geq \frac{|K|^n}{n!}$. This finishes the proof of Dvir's theorem. □

2 Projective space

In this section we introduce projective space and consider some examples.

2.1 Definitions and examples

Recall

Definition 2.1 By *affine space* over the field K , we mean simply the vector space $K^n = K \times \dots \times K$ (n times). This is usually denoted \mathbb{A}_K^n or just \mathbb{A}^n .

The main distinction between affine space and vector space K^n is that the origin does not play a special role in affine space.

Definition 2.2 A *projective space* over a field K is the set of one-dimensional subspaces of the vector space K^{n+1} (in other words, set of lines in K^{n+1} containing $(0, \dots, 0)$). This is denoted by \mathbb{P}_K^n or just \mathbb{P}^n .

Let us consider some examples, over various fields.

Example 2.3 0) \mathbb{P}^0 consists of one point.

- 1) $\mathbb{P}_{\mathbb{R}}^1$ is a circle.
- 2) $\mathbb{P}_{\mathbb{Z}/p\mathbb{Z}}^1$ has $p + 1$ points.
- 3) $\mathbb{P}_{\mathbb{R}}^2$ can be seen as two-sphere quotient by involution $S^2/\pm 1$. Projective plane contains projective lines (or just lines) that come from different $\mathbb{R}^2 \subset \mathbb{R}^3$.

Question. How many lines are there in $\mathbb{P}_{\mathbb{Z}/p\mathbb{Z}}^2$ where p is prime. (in $\mathbb{P}_{\mathbb{Z}/p\mathbb{Z}}^2$?)

- 4) $\mathbb{P}_{\mathbb{C}}^1$ is again a two sphere.

Relation between projective space \mathbb{P}_K^n and affine space \mathbb{A}_K^n .

Consider the vector space V^{n+1} ($V^{n+1} = K^{n+1}$) and let \mathbb{A}^n be an affine subspace of V^{n+1} that does not contain $0 \in V^{n+1}$. For every point $p \in \mathbb{A}^n$ there is a unique line that joins p with $0 \in V^{n+1}$. Thus a copy of \mathbb{A}^n is contained in \mathbb{P}^n .

Note that the piece of \mathbb{P}^n not covered by \mathbb{A}^n is \mathbb{P}^{n-1} . This \mathbb{P}^{n-1} is called sometimes *infinity* of \mathbb{A}^n .

We deduce $\mathbb{P}^n = \mathbb{A}^n \cup \dots \cup \mathbb{A}^0$.

Definition 2.4 Consider a vector subspace W^{k+1} in a vector space V^{n+1} . The set of lines through 0 in W^{k+1} define a projective subspace \mathbb{P}^k in \mathbb{P}^n . Such a subspace is called *linear subspace*. If $k = 1$ it is called *line*. If $k = n - 1$ it is called *hyperplane*.

Remark. Intersection of two linear subspaces is a linear subspace.

Projective geometry was invented by Girard Desargues who proved the following theorem:

Theorem 2.5 *Let a, b, c, A, B, C be six points in \mathbb{P}^3 that are not contained in one plane, and such that no three of these points lie on one line. Suppose that lines aA , bB , and cC intersect in one point. Then the points $ab \cap AB$, $bc \cap BC$, $ac \cap AC$ lie on one line.*

Proof. By our assumptions, then there is a unique plane that contain points a, b, c and a unique plane that contains points A, B, C . Let us prove that the intersection of two planes abc and ABC contains all three points. Indeed, $ab \subset abc$ and $AB \subset ABC$, hence $ab \cap AB \subset abc \cap ABC$. Same reasoning works for other two intersections. □

2.2 Homogeneous coordinates

To work with projective spaces it is very useful to introduce coordinates, namely *homogeneous coordinates*.

Consider projective space \mathbb{P}_K^n associated to vector space K^{n+1} . Let us introduce standard coordinates (x_0, \dots, x_n) on K^{n+1} . For any non-zero point (a_0, \dots, a_n) in K^{n+1} , the collection of points $(\lambda a_0, \dots, \lambda a_n)$, $\lambda \in K$ define a line, i.e., a point in \mathbb{P}_K^n . This point is denoted as $(a_0 : \dots : a_n)$ and the numbers a_i are called *homogeneous coordinates of the point*. They are not coordinates in the usual sense: for each point the coordinates are unique only up to multiplication by $\lambda \in K^*$. On the other hand the equation $x_i = 0$ defines a subset in \mathbb{P}_K^n .

The subset $x_i \neq 0$ in \mathbb{P}_K^n is denoted by U_i , it can be identified with \mathbb{A}_K^n . We associate to $(x_0 : \dots : x_i : \dots : x_n)$ the point $x_0/x_i, \dots, x_n/x_i$ in \mathbb{A}_K^n .

Definition 2.6 A polynomial $F \in K[x_0, \dots, x_n]$ is called *homogeneous* of degree d if all its monomials have degree d . For example $x_0 + x_1^2$ is not homogeneous, but $x_0x_1 + x_2^2 + (x_4 + x_5)^2$ is.

Consider a homogenous polynomial in $K[x_0, \dots, x_n]$, $\deg(F) = d$. Then we can consider the set of points $(x_0 : \dots : x_n)$ in \mathbb{P}^n such that $F(x) = 0$. This is a well-defined subset of \mathbb{P}^n . It is called a *hypersurface of degree d* .

Example 2.7 If $\deg(F) = 1$, then $\{F = 0\} = \mathbb{P}^{n-1}$. This is a *hyperplane*.

Example 2.8 $n = 1$. $F = \sum a_i z_0^i z_1^{d-i}$. Assume that the field that we consider is \mathbb{C} . In this case F can be decomposed as a product $F = \prod_{k=1}^d (b_k z_0 + c_k z_1)$. So the equations $F = 0$ defines the collection of points $(c_k : -b_k)$ in $\mathbb{P}_{\mathbb{C}}^1$.

2.3 Homogeneous - non-homogeneous

Recall that by U_0 we denote the subset of \mathbb{P}^n where $x_0 \neq 0$. This is an affine space and it is natural to ask how to relate a non-homogeneous equations in U_0 with a homogeneous in \mathbb{P}^n ?

$\mathbb{P}^n \rightarrow U_0$, substitute x_0 by 1.

$$x_0^2 + x_0 x_1 + x_0 x_2 + x_1 x_2 \rightarrow 1 + x_1 + x_2 + x_1 x_2.$$

$U_0 \rightarrow \mathbb{P}^n$ multiply each monomial by an appropriate power of x_0 .

$$x_1^2 x_2^2 + x_3^3 + 1 \rightarrow x_1^2 x_2^2 + x_0 x_3^3 + x_0^4.$$

The subset of point $x_0 = 0$ in \mathbb{P}^n is sometimes called *points at infinity*.

Example 2.9 Consider to circles $x_1^2 + x_2^2 = 1$ and $x_1^2 + x_2^2 = 4$ in \mathbb{C}^2 . What are their points of intersection?

Answer: obviously there are no intersections in \mathbb{C}^2 . But if we complete \mathbb{C}^2 by adding *points at infinity*, i.e. if we pass to homogeneous coordinates in $(x_0 : x_1 : x_2)$ viewing \mathbb{C}^2 as U_0 in $\mathbb{P}_{\mathbb{C}}^2$, the points of intersection are: $(0 : 1 : \pm i)$ (the homogeneous equations are $x_1^2 + x_2^2 = x_0^2$ and $x_1^2 + x_2^2 = 4x_0^2$).

Example 2.10 What are coordinates of the point at infinity in $\mathbb{R}P^2$ of the parabola $y = x^2$?

2.4 Playing with conics

Example 2.11 Suppose that $F \in K[x_0, x_1, x_2]$ is a homogeneous polynomial of degree two. Then $F = 0$ is called a *conic*. The conic is called *non-degenerate* if F is irreducible.

Lemma 2.12 Let $F = 0$ be a non-degenerate conic in \mathbb{P}_K^2 and suppose that the field K is algebraically closed, $\text{char}K \neq 2$ then in some homogeneous coordinates $(x_0 : x_1 : x_2)$ the conic is given by $x_0 x_2 - x_1^2$.

Recall that a *quadratic form* on a vector space V is a homogenous polynomial of degree two.

Proof. First we recall the following statement: for any *quadratic form* F on K^n there exists a basis v_1, \dots, v_n , such that $F(x_1v_1 + \dots + x_nv_n) = x_1^2 + \dots + x_i^2$ for some $i \in \{1, \dots, n\}$.

Recall the proof of this statement.

Associate to F the symmetric bilinear form,

$$Q(v, u) = \frac{F(v + u) - F(v) - F(u)}{2}.$$

Next we use Gram-Schmidt orthonormalization. Chose v_1 so that $F(v_1) = 1$, this is possible unless $F = 0$. Let v_1^\perp be the hyperplane in K^n composed of vectors u orthogonal to v_1 , $Q(v_1, u) = 0$. Restrict F to v_1^\perp and continue. In such a way we get the system v_1, \dots, v_n such that $Q(v_k, v_l) = 0$ unless $k = l \leq i$, $Q(v_k, v_k) = 1$ for $k \leq i$. This is the base we want.

We conclude that that the equation of irreducible conic in some coordinates is $x_0^2 + x_1^2 + x_2^2 = 0$.

Exercise. Finish the proof. □

Lemma 2.13 *Non-degenerate conic over an algebraically closed field can be identified with \mathbb{P}^1 .*

Proof. By the previous exercise we can assume that the conic is given by $x_0x_2 - x_1^2$. Then $\mathbb{P}^1 \rightarrow$ conic is: $(u_0 : u_1) \rightarrow (u_0^2 : u_0u_1 : u_1^2)$. The inverse map is $(x_0 : x_1 : x_2) \rightarrow (x_0 : x_1)$ or $(x_1 : x_2)$. □

Using this lemma we can reprove Bézout's theorem for conics.

Lemma 2.14 *For any $F_d \in K[x_1, x_2, x_3]$, a homogeneous poly of deg d either $F_d \equiv 0$ on C of $F_d = 0 \cap C$ contains no more than $2d$ points.*

Proof. We can assume that the coordinates of our conic are u_0^2, u_0u_1, u_1^2 . Then $F(u_0, u_1)$ is a homogeneous polynomial of degree $2d$. So either F has no more than $2d$ roots or F is identically zero. □

Jacob Steiner's problem 1848. Suppose we have 5 conics in general position on $\mathbb{P}_{\mathbb{C}}^2$. How many conics are tangent to these 5?

This is a difficult question. So we will do something easier for the moment.

Question 2.15 How many conics pass through given 5 points A_1, \dots, A_5 on $\mathbb{P}_{\mathbb{C}}^2$?

Step 1. The set of all conics on \mathbb{P}^2 can be identified with \mathbb{P}^5 , since a conic is given by an equation $\sum a_{ij}t_i t_j = 0$ with 6 coefficients that are defined up to multiplication by a constant. Next, if we take a point $A_1 = (t_0^1 : t_1^1 : t_2^1)$, all conics going through A_1 can be written as $\sum a_{ij}t_i^1 t_j^1$, so we have a linear equation on the coefficients a_{ij} . So these conics form a hyperplane.

So we get a question: in how many points these 5 planes intersect?

Exercise. If no 4 points lay on one line the conic is unique. If no 3, it is smooth.

Question. How many lines touch two distinct irreducible conics?

The set of all lines in \mathbb{P}^2 is \mathbb{P}^2 , it is called *dual projective plane*. Write the equation for line: $a_0 z_0 + a_1 z_1 + a_2 z_2 = 0$. Lines tangent to the conic $z_0 z_2 + z_1^2 = 0$ are characterized as follows:

The homogeneous equation $a_0 u_0^2 + a_1 u_0 u_1 + a_2 u_1^2$ in $(u_0 : u_1)$ has only one root. Then $a_1^2 - 4a_0 a_2 = 0$. I.e. the set of lines tangent to a conic forms a conic in the dual projective plane. So we have to find the number of intersections of two conics - this is Bezout. □

Jakob Steiner, was a professor of geometry at the University of Berlin. His answer to his question was $7666 = 6^5$, he was guided by a generalization of Bézout's theorem. It turned out that his answer was wrong. French naval officer de Jonquieres solved this problem in 1859, the answer is 3264. But the proof is too involved for this course.

3 Reminder on rings and Hilbert basis theorem

3.1 Reminder on rings and ideals

In this section we recall several facts about rings and ideals.

Definition 3.1 A commutative ring is a set R with multiplication and addition $\cdot, + : R \times R \rightarrow R$ such that

1. $(R, +)$ is an abelian group;
2. for all $a, b, c \in R$, $a(bc) = (ab)c$;

3. for all $a, b \in R$, $ab = ba$ (all rings in this course will be commutative);
4. there exists an element $1_R \in R$ (necessarily unique) such that $1_R \cdot a = a \cdot 1_R = a$, $\forall a \in R$;
5. $a(b + c) = ab + bc$.

Definition 3.2 Suppose that R is a commutative ring. A subset $\emptyset \neq I \subset R$ of R is said to be an *ideal* of R if $x + y \in I$ whenever $x, y \in I$ and $ax \in I$ whenever $x \in I$ and $a \in R$.

Example 3.3 $2\mathbb{Z}$ is an ideal in \mathbb{Z} . If R is any ring, then $I = \{0\}$ is an ideal.

Definition 3.4 For a field K a K -*algebra* is a commutative ring containing K as a subring. An example is $K[X_1, \dots, X_n]$.

Definition 3.5 A ring *homomorphism* is a map $\varphi : R \rightarrow S$ of rings R and S such that

$$\varphi(ab) = \varphi(a)\varphi(b), \quad \varphi(a + b) = \varphi(a) + \varphi(b), \quad \forall a, b \in R,$$

and $\varphi(1_R) = 1_S$. The kernel $\text{Ker}(\varphi) \subset R$ is defined to be

$$\text{Ker}(\varphi) := \{a \in R : \varphi(a) = 0 \in S\}.$$

Exercise 3.6 $\text{Ker}(\varphi)$ is an ideal of R (check it).

Definition 3.7 A non-zero commutative ring $R \neq \{0\}$ is said to be an *integral domain* if

$$\forall a, b \in R \quad (ab = 0 \Rightarrow a = 0, \text{ or } b = 0).$$

Definition 3.8 If R is a ring and $I \subset R$, then I is said to be a *maximal ideal* of R if $I \neq R$ and if there are no ideals J of R such that $I \subsetneq J \subsetneq R$. The ideal I is called *prime* if for any a, b with $ab \in I$, a or b are in I .

Exercise 3.9 If R is a ring and I is an ideal of R , then R/I is a field iff I is a maximal ideal. R/I is an integral domain iff I is prime.

Definition 3.10 The *radical* of an ideal I in a commutative ring R , denoted by $\text{Rad}(I)$ or \sqrt{I} , is defined as

$$\text{Rad}(I) = \{r \in R \mid r^n \in I \text{ for some positive integer } n\}.$$

An ideal I is called *radical* if $I = \text{Rad}(I)$.

Exercise 3.11 Show that the radical of an ideal is an ideal and that $\text{Rad}(\text{Rad}(I)) = \text{Rad}(I)$.

Definition 3.12 If $\emptyset \neq A \subset R$ is a subset of a ring R , then the ideal generated by A is the smallest ideal of R containing A . Equivalently, it is the collection of all finite linear combinations of elements of A , that is,

$$\left\{ \sum_{i=1}^N b_i x_i : N \in \mathbb{N}, b_i \in R, x_i \in A \right\}.$$

An ideal generated by the elements x_1, \dots, x_n is denoted (x_1, \dots, x_n) .

Definition 3.13 An ideal $I \subset R$ is said to be *finitely generated* if there exists a finite subset $A = \{x_1, \dots, x_n\} \in R$ such that $I = (x_1, \dots, x_n)$.

Finally we come to a lemma, characterizing *Noetherian* rings.

Lemma 3.14 *Let R be a ring. Then the following two conditions are equivalent:*

- (i) *(the ascending chain condition) if $I_0 \subset I_1 \subset I_2 \dots$ are proper ideals of R , then there exists N , such that $\forall n > N$ $I_n = I_N$;*
- (ii) *every ideal of R is finitely generated.*

Proof by contrapositive. (i) \Rightarrow (ii). If $I \subset R$ is not finitely generated, then choose $I_{n+1} = I_n + Rx_{n+1}$, where $x_{n+1} \notin I_n = (x_0, \dots, x_n)$.

(ii) \Rightarrow (i). If $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \dots$ are ideals in R then $I = \bigcup_{i \in \mathbb{Z}_+} I_i$ is an ideal in R , but it can not be finitely generated. □

Definition 3.15 A ring R is called *Noetherian* if every ideal of R is finitely generated.

Example 3.16 The ring of continuous functions on $[0, 1]$ is not Noetherian, indeed we can consider the sequence of ideals I_n , of functions vanishing on $[0, \frac{1}{n}]$.

3.2 Hilbert basis theorem

Theorem 3.17 *If R is Noetherian, then so is $R[X]$.*

Proof. Let I be an ideal in $R[X]$. We claim that I is finitely generated. Choose $f_1 \in I \setminus (0)$ with minimal degree; if $I \neq (f_1)$, choose $f_2 \in I \setminus (f_1)$ with minimal degree. If this process terminates, we are done. If not, let a_i be the leading coefficient of f_i , and form the ideal $J = (a_1, a_2, a_3, \dots)$ in R . Since R is Noetherian, we have $J = (a_1, \dots, a_N) = J_N$ for some N .

Now we will deduce a contradiction, we will show that the ideal $I_N, I_N := (f_1, \dots, f_N)$ equals I . Indeed, if $I_N \neq I$ then according to our construction there exists an element f_{N+1} in $I \setminus I_N$ of minimal possible degree. Moreover, $a_{N+1} = \sum_{i=1}^N r_i a_i$ since $a_{N+1} \in J = J_N$. Now set

$$g = \sum_{i=1}^N r_i f_i X^{\deg f_{N+1} - \deg f_i}.$$

Since g is a linear combination of the f_i , we have $g \in I_N$. Next $\deg(g) = \deg f_{N+1}$, and both polynomials have the same leading term. Thus $\deg(f_{N+1} - g) < \deg f_{N+1}$. But since $f_{N+1} - g \in I \setminus I_N$, this contradicts the minimality of $\deg f_{N+1}$. □

Corollary 3.18 *For any field K the ring $K[X_1, \dots, X_n]$ is Noetherian.*

Proof. We prove this statement by induction. The ring $K[x]$ is Noetherian by Hilbert basis theorem, since K is Noetherian. Now $K[x_1, \dots, x_n] = K[x_n][x_1, \dots, x_{n-1}]$, i.e., the polynomial ring in n variables with coefficients in K can be seen as the polynomial ring in $n - 1$ with coefficients in $K[x_n]$. Hence it is Noetherian by both induction and Hilbert basis theorem. □

Recall that the a ring R is said to be finitely generated over its subring A if there exists $r_1, \dots, r_n \in R$ such that $\forall r \in R$ we have $r = P(r_1, \dots, r_n)$, where $P \in A[x_1, \dots, x_n]$ is a certain polynomial.

More generally, the following corollary holds:

Corollary 3.19 *Let A be a Noetherian ring and R be a ring finitely generated over A then R is Noetherian.*

Proof. Suppose that R is generated by (r_1, \dots, r_n) . Take the ring $A[x_1, \dots, x_n]$ (it is Noetherian by Hilbert basis theorem) and consider the surjective homomorphism $A[x_1, \dots, x_n] \rightarrow R$ sending x_i to r_i . Then since ACC holds for ideals in $A[x_1, \dots, x_n]$ it should also hold for ideals in R . □

Example 3.20 Consider the set of all polynomials $f(x, y)$ in two variables, whose restriction to the x -axis is constant. This defines a subring $R \subset k[x, y]$. A polynomial in R can be written

$$f(x, y) = \text{constant} + yg(x, y).$$

The ideals $(y), (y, yx), (y, yx, yx^2), \dots$ in R are all different (as ideals in R).

3.3 Finite generation of the ring of invariants

In this subsection we prove the famous theorem of Hilbert on finite generation of the ring of invariants.

This theorem was a motivation for Hilbert to prove "Hilbert basis theorem".

Definition 3.21 An *automorphism* of a ring R is a bijective map $R \rightarrow R$ preserving addition and multiplication.

We say that a group G is acting on a ring R if there is a homomorphism of groups $G \rightarrow \text{Aut}(R)$.

An *invariant* of the action is an element $r \in R$ such that $g(r) = r$ for all $g \in G$. The subset of invariant elements forms a sub ring of R that is denoted R^G and is called the *ring of invariants*.

Definition 3.22 Let A be an algebra over K . A is said to be *finitely generated* if there exist a collection of elements a_1, \dots, a_n in A such that for any $a \in A$ there exists a polynomial $f \in K[x_1, \dots, x_n]$ such that $a = f(a_1, \dots, a_n)$.

Theorem 3.23 *Suppose that a finite group G is acting on the polynomial ring $R = \mathbb{C}[x_1, \dots, x_n]$ preserving the degree of polynomials. Then the ring R^G of invariants is a finitely generated \mathbb{C} -algebra.*

Proof of finite generation of invariants. Let I be the ideal generated by the elements of R^G without free term. Note that I is generated by homogeneous polynomials in R^G , and since R is Noetherian I should be generated

by a finite collection i_1, \dots, i_k of such polynomials. (otherwise ACC would not hold in R). We want to show that i_1, \dots, i_k generate R^G as an ALGEBRA (which is much stronger than saying they generate IDEAL I).

We use *Reynolds operator* ρ given by taking average under action of G $\rho(a) = \frac{1}{|G|} \sum_{g \in G} g(a)$. **Key properties:** $\rho(a) \in R^G$ for all $a \in R$, $\rho(ab) = a\rho(b)$ if $a \in R^G$, $\rho(1) = 1$.

We show by induction on degree of a homogeneous polynomial x that if $x \in R^G$ then it is in algebra generated by i_j 's. Indeed, we know

$$x = a_1 i_1 + \dots + a_k i_k$$

for some a 's in R as x is in I . Apply Reynolds operator:

$$x = \rho(x) = \rho(a_1) i_1 + \dots + \rho(a_k) i_k$$

Since x and i_j are homogeneous, we may assume that a_j are homogeneous of degree less than x . Then by induction $\rho(a_j)$ is in the algebra generated by i_j 's as it has degree less than that of x , and so x is in this algebra as well. \square

Gordon apparently said about this proof: "This is not math; this is theology".

4 Varieties and Nullstellensatz

Recall:

Definition 4.1 A field K is called *algebraically closed* if every non-constant single-variable polynomial with coefficients in K has at least one root in K .

The field of complex numbers is the main example (for us), it is algebraically closed by the Fundamental theorem of algebra.

Definition 4.2 A subset $V \subset A_K^n$ is said to be an affine variety if there exist polynomials $f_1, \dots, f_N \in K[x_1, \dots, x_n]$ such that $(x_1, \dots, x_n) \in V$ if and only if $f_i(x_1, \dots, x_n) = 0$, for all $i \in \{1, \dots, N\}$.

4.1 From ideals to varieties

Remark 4.3 Recall that according to Hilbert basis theorem each ideal in $K[X_1, \dots, X_n]$ is generated by finite number of elements f_1, \dots, f_N . To each ideal $I \subset K[X_1, \dots, X_n]$ we can associate $V(I)$:

$$V(I) = \{P \in \mathbb{A}_K^n : f(P) = 0 \text{ for all } f \in I\}.$$

This is an affine variety.

Proposition 4.4 *The map from ideals in $R = K[X_1, \dots, X_n]$ to affine varieties in \mathbb{A}_K^n has the following properties:*

1. $V(\{0\}) = \mathbb{A}_K^n$ (here by $\{0\}$ we mean the zero ideal in R); $V(R) = \emptyset$;
2. $I \subset J$ implies $V(I) \supset V(J)$;
3. $V(I) \cup V(J) = V(I \cap J)$;
4. $\bigcap_{\nu} V(I_{\nu}) = V(\sum_{\nu} I_{\nu})$.

Here I, J, I_{ν} are ideals in R , and $\sum_{\nu} I_{\nu}$ denotes the ideal consisting of finite combinations of elements in I_{ν} with the coefficients in R .

Proof.

1, 2. These properties are clear.

3. We have $V(I) \subset V(I \cap J)$ since $I \cap J \subset I$. Similarly $V(J) \subset V(I \cap J)$, hence $V(I) \cup V(J) \subset V(I \cap J)$.

Now assume that $P \in V(I \cap J)$. If P is not in $V(I)$, then there is some $f \in I$ with $f(P) \neq 0$. Similarly, if P is not in $V(J)$, then there is some $g \in J$ with $g(P) \neq 0$. Then $f \cdot g \in I \cap J$ and $(f \cdot g)(P) \neq 0$. This contradicts $P \in V(I \cap J)$.

4. Let $P \in \bigcap_{\nu} V(I_{\nu})$; then $f_{\nu}(P) = 0$ for all $f_{\nu} \in I_{\nu}$ for all ν , hence $f(P) = 0$ for all finite linear combinations $f \in \sum_{\nu} I_{\nu}$. This shows that $\bigcap_{\nu} V(I_{\nu}) \subset V(\sum_{\nu} I_{\nu})$.

On the other hand, $I_{\mu} \subset \sum_{\nu} I_{\nu}$ for every μ , hence $V(\sum_{\nu} I_{\nu}) \subset V(I_{\mu})$ for every μ , and therefore $V(\sum_{\nu} I_{\nu}) \subset \bigcap_{\mu} V(I_{\mu})$. □

4.2 From Varieties to Ideals: The Vanishing Ideal

We saw how to associate a variety to an ideal, now let us go the opposite way.

Definition 4.5 If $V \subset \mathbb{A}^n$ (just a subset, though a variety is more useful) then $I(V) \subset K[X_1, \dots, X_n]$ is defined by

$$I(V) = \{f \in K[X_1, \dots, X_n] : f(P) = 0, \forall P \in V\}.$$

Remark 4.6 First of all $V \subset V(I(V))$. For arbitrary subsets $V \subset \mathbb{A}^n$, it is possible to have $V \neq V(I(V))$. For example, if $K = \mathbb{C}$, $n = 1$, $V = \mathbb{Z}$, then $I(V) = \{0\}$, and $V(I(V)) = \mathbb{C} \neq \mathbb{Z}$.

Lemma 4.7 For any affine variety V we have $V(I(V)) = V$.

Proof. We have $V \subset V(I(V))$: if $f \in I(V)$, then $f(P) = 0$ for any $P \in V$, hence $P \in V(I(V))$.

Now assume that V is the zero set of polynomials $f_1, \dots, f_m \in K[X_1, \dots, X_n]$. Then $f_1, \dots, f_m \in I(V)$, hence $(f_1, \dots, f_m) \subset I(V)$, and therefore $V(I(V)) \subset V((f_1, \dots, f_m)) = V$. □

Note now, $I \subset I(V(I))$, but $I \neq I(V(I))$ in general. Example, $K = \mathbb{C}$, $n = 1$, and $I = (X^2)$. Then $V(I) = \{0\}$ but $I(V(I)) = (X) \neq (X^2)$.

Proposition 4.8 If V is an affine variety, then $I(V) = \text{Rad}(I(V))$.

Proof. Since $I \subset \text{Rad}(I)$ for any ideal I , we only have to show that $\text{Rad}(I(V)) \subset I(V)$. Assume that $f \in \text{Rad}(I(V))$. Then $f^n \in I(V)$ for some n , hence $f^n(P) = 0$ for all $P \in V$. This implies $f(P) = 0$, hence $f \in I(V)$. □

Conclusion: vanishing ideals have the property that they coincide with their radical. In particular, (X^2) is not the vanishing ideal of a variety because $\text{Rad}(X^2) = (X)$.

Thus we can only hope to get a bijection between affine varieties and radical ideals (these are ideals that coincide with their radical). This is exactly the statement of Nullstellensatz.

Theorem 4.9 (Hilbert's Nullstellensatz). If K is an algebraically closed field, then for each ideal I in $K[X_1, \dots, X_n]$ we have $I(V(I)) = \text{Rad}(I)$.

Corollary 4.10 For K algebraically closed take an ideal $I \subset K[X_1, \dots, X_n]$. $V(I) = \emptyset$ iff there are $f_1, \dots, f_k \in I$ and $g_1, \dots, g_k \in K[X_1, \dots, X_n]$ such that:

$$\sum g_i f_i = 1.$$

Proof. One direction is clear. If we can write 1 as a linear combination of f_1, f_2, \dots, f_k then f_1, f_2, \dots, f_k cannot vanish simultaneously.

Suppose now $V(I) = \emptyset$. Then by Nullstellensatz $\text{Rad}(I) = I(V(I)) = I(\emptyset) = K[X_1, \dots, X_n]$. So $1 \in \text{Rad}(I)$. But this means that $1 \in I$ as well. \square

Corollary 4.11 *Let K be an algebraically closed field. Then every maximal ideal of $K[X_1, \dots, X_n]$ is of the form $m_a = (X_1 - a_1, X_2 - a_2, \dots, X_n - a_n)$, where a_1, a_2, \dots, a_n are elements of K .*

Proof. Let I be a maximal ideal. Then $1 \notin I$, so that there is at least one point $(a_1, a_2, \dots, a_n) \in \mathbb{A}^n$ contained in $V(I)$. It follows that $I \subset (X_1 - a_1, X_2 - a_2, \dots, X_n - a_n)$. As I is maximal, the result follows. \square

Example 4.12 A typical application. Let $P(x, y) \in \mathbb{C}[x, y]$ be an irreducible polynomial, and suppose that $Q(x, y)$ vanishes at the curve $P(x, y) = 0$. Then Q is divisible by P .

Proof. Use the fact that (P) is a prime ideal (and so $\text{Rad}((P)) = (P)$) in $\mathbb{C}[x, y]$, since $\mathbb{C}[x, y]$ is a UFD.

4.3 Irreducible varieties

Definition 4.13 An affine variety $V \subset \mathbb{A}_K^n$ is *irreducible* if there does not exist a decomposition

$$V = V_1 \cup V_2, \quad \text{with } V_1, V_2 \neq V$$

of V as a union of two affine varieties.

Example 4.14 $V(xy) \subset \mathbb{A}_K^2$ is the set consisting of the two coordinate axes, and is obviously the union of $V(x)$ and $V(y)$, hence reducible.

Proposition 4.15 *a) Let $V \subset \mathbb{A}_K^n$ be an affine variety and $I(V)$ the corresponding ideal. Then V is irreducible iff $I(V)$ is prime.*

b) Any affine variety V has a unique expression

$$V = V_1 \cup \dots \cup V_r$$

with V_i irreducible and V_i doesn't belong to V_j for $i \neq j$.

Proof.

a) We will prove that V is reducible iff $I(V)$ is not prime.

(\Rightarrow) Suppose $V = V_1 \cup V_2$ with $V_1, V_2 \subsetneq V$ affine varieties. Then $V_1 \subsetneq V$ means that there exists $f_1 \in I(V_1) \setminus I(V)$ (here we use $V(I(V)) = V$), and similarly $V_2 \subsetneq V$ gives $f_2 \in I(V_2) \setminus I(V)$. Now the product $f_1 f_2$ vanishes at all points of V , and so $f_1 f_2 \in I(V)$. So $I(V)$ is not prime.

(\Leftarrow) Suppose $I(V)$ is not prime; then there exist $f_1, f_2 \notin I(V)$ such that $f_1 f_2 \in I(V)$. Let $I_1 = (I(V), f_1)$ and $V(I_1) = V_1$; then $V_1 \subsetneq V$; similarly setting $I_2 = (I(V), f_2)$ and $V(I_2) = V_2$ gives $V_2 \subsetneq V$. But $V \subset V_1 \cup V_2$, since for all $P \in V$, $f_1 f_2(P) = 0$ implies that either $f_1(P) = 0$ or $f_2(P) = 0$. □

5 Morphisms, singularities, non-singularities, and dimension

5.1 Morphisms

Just as an affine variety is given by polynomials, a *morphism* (algebraic term for a map) of affine varieties is given by polynomials.

Example 5.1 The simplest example of a morphism of affine varieties is a polynomial map

$$\mathbb{A}^n \rightarrow \mathbb{A}^m, \quad x \rightarrow (F_1(x), F_2(x), \dots, F_m(x))$$

where by *polynomial map* we mean that each of the components F_i of F is a polynomial in the n coordinates x_1, \dots, x_n in \mathbb{A}^n .

Definition 5.2 Let $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$ be affine varieties. A map $F : V \rightarrow W$ is a *morphism of algebraic varieties* if it is the restriction of a polynomial map on the ambient affine spaces $\mathbb{A}^n \rightarrow \mathbb{A}^m$.

A morphism is called *isomorphism* if it admits an inverse morphism, that is it is bijective and its inverse is also a morphism.

Example 5.3 An affine change of coordinates of \mathbb{A}^n . Chose

$$L_i(x) = \lambda_{i1}x_1 + \dots + \lambda_{in}x_n + \mu_i$$

and consider the map $\mathbb{A}^n \rightarrow \mathbb{A}^n, x \rightarrow (L_1(x), \dots, L_n(x))$.

It is a morphism and is an isomorphism if the matrix λ_{ij} is invertible.

Example 5.4 The projection $\mathbb{A}^2 \rightarrow \mathbb{A}^1$, $(x, y) \rightarrow x$ is a morphism but not an isomorphism, since it is not bijective.

Example 5.5 Let C be $V(x - y^2)$ in \mathbb{A}^2 . Then $\mathbb{A}^1 \rightarrow \mathbb{A}^2$, $t \rightarrow (t^2, t)$ gives an isomorphism of \mathbb{A}^1 and C . The inverse morphism from C to \mathbb{A}^1 is $(x, y) \rightarrow y$.

Remark 5.6 Consider $V = V(xy - 1) \subset \mathbb{A}^2$. Then the projection $(x, y) \rightarrow x$ sends V bijectively to $\mathbb{A}^1 \setminus 0$. $\mathbb{A}^1 \setminus 0$ is not an affine variety according to our definition. So this is one of incompleteness of our definition.

Remark 5.7 A bijective morphism between two affine varieties need not be an isomorphism. Consider the morphism $\mathbb{A}^1 \rightarrow V(x^3 - y^2) \in \mathbb{A}^2$, $t \rightarrow (t^2, t^3)$. This is a bijective morphism. But the inverse map is given by $(x, y) \rightarrow \frac{y}{x}$, and $\frac{y}{x}$ is not a polynomial function on \mathbb{A}^2 . Indeed one needs to show that $\frac{y}{x}$ is not equal to the restriction of $F \in K[x, y]$ to $V(x^2 - y^3)$.

5.2 Singularity, non-singularity, and dimension

Good thing about working with polynomials is that you can take their derivative without calculating a limit. I.e., the derivative of a polynomial is given by an algebraic operation, it works over any field. This is important because the definition can be generalized then to other rings.

Definition 5.8 Derivative on polynomials in $k[x]$ is defined as follows:

$$\frac{d}{dx}x^n = nx^{n-1}, \quad \forall n \in \mathbb{N}, \quad \frac{d}{dx}1 = 0.$$

Remark 5.9 Derivative is a k -linear map $k[x] \rightarrow k[x]$. There is one subtlety: if k is of characteristic p , then $\frac{d}{dx}x^{pn} = 0$.

This rule extends in an obvious way to polynomials of several variables $k[x_1, \dots, x_n]$, so we get an algebraic definition of partial derivative $\frac{\partial f}{\partial x_i}$.

Now, we will start to define *tangent plane* to irreducible affine variety.

Definition 5.10 Let $V \subset \mathbb{A}^n$ be an irreducible *hypersurface*, given by the polynomial equation $f = 0$, where $f \in k[x_1, \dots, x_n]$ is irreducible. For $P = (a_1, \dots, a_n) \in V$, we define the tangent plane $T_P V \subset \mathbb{A}^n$ as

$$T_P V = \{(x_1, \dots, x_n) \mid \sum_{i=1}^n \frac{\partial f}{\partial x_i}(P)(x_i - a_i) = 0\}.$$

Remark 5.11 The space $T_P V$ is clearly an affine subspace of \mathbb{A}_k^n .

Example 5.12 The tangent space of the variety $V(x^3 - y^2) \subset \mathbb{A}_k^2$ at zero is the whole plane.

Definition 5.13 A point P of hypersurface $f = 0$ is called singular if $\frac{\partial f}{\partial x_i}(P) = 0$ for all i . Otherwise the point is called non-singular.

Lemma 5.14 Let $L \subset \mathbb{A}_k^n$ be an affine line through the point P on V . Then P is a multiple root of $f|_L$ iff $L \subset T_P V$.

Proof. The line L has a parametrization

$$L := x_i = a_i + bt_i,$$

where $P = (a_1, \dots, a_n)$ and (b_1, \dots, b_n) is a vector in the direction of L . Let $g := f|_L$, i.e.,

$$g(t) = f(a_1 + b_1 t, \dots, a_n + b_n t).$$

Since $P = (a_1, \dots, a_n) \in V$ we have

$$g(0) = f(P) = 0.$$

So g has a multiple root at 0 if and only if

$$\frac{\partial g}{\partial t}(0) = 0 \iff \sum_{i=1}^n b_i \frac{\partial f}{\partial x_i}(P) = 0 \iff L \subset T_P V,$$

here the last equivalence follows directly from the equation of $T_P V$. □

Lemma 5.15 A nonzero proper principal ideal $(f) \in k[X_1, \dots, X_n]$ is prime if and only if f is irreducible.

Theorem 5.16 Let V be an irreducible hyper-surface in \mathbb{A}_k^n given by $f = 0$ where $f \in k[X_1, \dots, X_n]$ is an irreducible polynomial. Then the set of non-singular points of V is non-empty.

We just treat the case when $\text{char}(k) = 0$. We need this to be able to use the following simple fact:

Exercise 5.17 Let $f \in k[x_1, \dots, x_n]$. Suppose that $\text{char}(k) = 0$, and suppose $\frac{\partial f}{\partial x_i} = 0$ for all i . Then f is a constant.

Proof. We have $\text{Sing } V = V(f, \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n})$. Note that since f is irreducible, the ideal (f) is prime (Lemma 5.15) and in particular radical, and so $(f) = I(V)$. Hence, if $V = \text{Sing } V$, then for each $i \in \{1, \dots, n\}$, $\frac{\partial f}{\partial x_i} \in I(V)$ so by Nullstellensatz we have

$$\frac{\partial f}{\partial x_i} \in \text{rad}(I(V)).$$

On the other hand by Proposition 4.8 $I(V)$ is radical, i.e., $\text{rad}(I(V)) = I(V) = (f)$. So for each $i \in \{1, \dots, n\}$, there exists $g_i \in K[X_1, \dots, X_n]$ such that $\frac{\partial f}{\partial x_i} = g_i f$. But $\deg_{x_i} g_i f > \deg_{x_i} \frac{\partial f}{\partial x_i}$ unless $g_i = 0$. We conclude that $\frac{\partial f}{\partial x_i} = 0$ for all i , and since $\text{char } k = 0$, $f = \text{const}$ (see exercise). This is a contradiction. □

5.3 General case.

Definition 5.18 For a polynomial $f \in k[x_1, \dots, x_n]$ and a point $P = (a_1, \dots, a_n)$, the *linear part* of f at P is defined by

$$f_P^{(1)} := \sum_{i=1}^n \frac{\partial f}{\partial x_i}(P)(x_i - a_i).$$

Now, we consider an irreducible affine variety $V \subset \mathbb{A}_k^n$.

Definition 5.19 The *tangent space* to an irreducible variety V at a point $P \in V$ is defined by the following intersection of affine hyperplanes:

$$T_P V := \bigcap_{f \in I(V)} (f_P^{(1)} = 0) \subset \mathbb{A}_k^n.$$

Finally we come to the definition of dimension.

Definition 5.20 For an irreducible affine variety V , we define the dimension of V by

$$\dim V = \min\{\dim T_P V \mid P \in V\}.$$

6 Singularities of curves and multiplicity of intersection

In this final section we look closer into curves and introduce further algebraic notions in order to formulate the final version of Bézout's theorem.

We assume that the field is algebraically closed unless the opposite is specified.

6.1 Multiplicities

In this subsection we define multiplicities of singular points of curves.

Take a polynomial $F \in k[x, y]$, consider the curve $F = 0$ in \mathbb{A}_k^2 . Take a point $P \in F = 0$. The *multiplicity* of curve $F = 0$ at point P is defined as follows:

Definition 6.1 Consider the Taylor decomposition of F at $P = (x_0, y_0)$

$$F(x_0 + x, y_0 + y) = F_d(x, y) + \dots + F_{d+k}(x, y)$$

where F_d is non zero and F_i is a homogeneous polynomial of degree i for all i . Then d is called *multiplicity* of the curve $F = 0$ at (x_0, y_0) .

Remark 6.2 *Interpretation.* For a point $P \in \{F = 0\}$ consider all lines L in \mathbb{A}_k^2 that contain the point. The restriction $F|_L$ has zero at P of certain multiplicity. The minimum of such multiplicities is the multiplicity of P .

Example 6.3 1) Let $F \in k[x, y]$ be an irreducible polynomial of degree 3. Then the cubic $F = 0$ can have at most one singular point and the point has multiplicity 2. Let us prove this.

First, if a cubic $F = 0$ has multiplicity > 2 , then in its Taylor decomposition the first term is cubic, i.e., $F(x - x_0, y - y_0)$ is a homogeneous polynomial of degree 3 in $(x - x_0, y - y_0)$, hence reducible.

Next, if $F = 0$ has at least two singular points of multiplicity 2, then consider the line L through these two points. The restriction $F|_L$ has two roots of multiplicity at least 2, hence $F|_L = 0$ and so F is reducible.

2) More complicated example. If F is irreducible of degree 4 $F = 0$ has at most 3 singular points.

6.2 Local ring

Now we introduce an important notion, the *local ring* O_P of a point $P \in \mathbb{A}_K^2$.

Definition 6.4 Let $k(x, y)$ be the *fraction field* of the ring $k[x, y]$. Define by O_P the subring of $k(x, y)$ consisting of elements that can be expressed as fractions $\frac{F}{G}$ with $G(P) \neq 0$.

For an element $\phi = \frac{F}{G} \in O_P$ we define $\phi(P) = \frac{F(P)}{G(P)}$.

Let us list the basic properties the local ring O_P .

1) O_P is a subring of $k(x, y)$, and the map $\phi \rightarrow \phi(P)$ is a homomorphism of O_P onto k which is the identity on $k \in O_P$.

Let $M_P = \{\phi \in O_P : \phi(P) = 0\}$ be the kernel of the homomorphism. Then

2) $O_P = k + M_P$, and $O_P/M_P \cong k$.

3) An element $\phi \in O_P$ has a multiplicative inverse in O_P if and only if $\phi \notin M_P$.

4) Every ideal of O_P other than O_P itself, is contained in M_P , and so M_P is the unique maximal ideal of O_P .

This brings us to the definition:

Definition 6.5 A ring having a unique maximal ideal is called a *local ring*.

6.3 Multiplicity of intersection

Finally we come to Bézout's theorem. So, let F and G be two polynomials in $k[x, y]$ without common factors. The weak form of Bézout's theorem stated

$$\#(F = 0 \cap G = 0) \leq \deg(F) \cdot \deg(G).$$

In our proof of *weak form* of Bézout relied on the following inequality:

$$\#(F = 0 \cap G = 0) \leq \dim(k[x, y]/(F, G)).$$

Our goal now will be to replace the left hand side of this inequality by a "*correct*" expression.

Definition 6.6 Denote by $(F, G)_P$ the ideal generated by F and G in O_P . Then the *intersection index* is defined as the dimension of the vector space $O_P/(F, G)_P$.

For two curves $C_1 := \{F = 0\}$, $C_2 := \{G = 0\}$ we use the notation for intersection index $I(C_1 \cap C_2, P)$.

Now we can formulate *half of Bézout*.

Theorem 6.7 *Let f_1 and f_2 be two polynomials without common factors in $k[x, y]$. Let C_1 be the curve $f_1 = 0$, C_2 be the curve $f_2 = 0$. Then*

$$\sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P) = \dim(k[x, y]/(f_1, f_2)).$$

The proof of this theorem will be composed of several lemmas.

Lemma 6.8

$$\dim(O_P/(f_1, f_2)_P) \leq \dim(R/(f_1, f_2)),$$

in particular the intersection multiplicity $I(C_1 \cap C_2, P)$ is finite.

Proof. Note first, that any finite set of elements in O_P can be written over a common denominator.

Let $\frac{g_1}{h}, \dots, \frac{g_r}{h}$ be elements of O_P , linearly independent modulo $(f_1, f_2)_P$. Then the elements g_1, \dots, g_r are linearly independent modulo (f_1, f_2) . Indeed any combination of g_i that belongs to (f_1, f_2) produces the combination of $\frac{g_i}{h}$ that belongs to $(f_1, f_2)_P$. □

Corollary 6.9 $O_P = k[x, y] + (f_1, f_2)_P$.

Proof. Indeed, we can find a finite set of elements $\frac{g_i}{h}$ that span O_P modulo $(f_1, f_2)_P$. At the same time $\frac{1}{h} \in O_P$. So g_i span O_P modulo $(f_1, f_2)_P$ as well. □

Proposition 6.10 *Suppose that $P \in C_1 \cap C_2$. Let r satisfy $r \geq \dim(O_P/(f_1, f_2)_P)$. Then $M_P^r \subset (f_1, f_2)_P$.*

Proof. We need to prove that for any collection of r elements t_1, \dots, t_r in M_P their product is in $(f_1, f_2)_P$.

Define the sequence of ideals J_i in O_P :

$$J_i = t_1 \dots t_i O_P + (f_1, f_2)_P \quad \text{for } 1 \leq i \leq r, \quad J_{r+1} = (f_1, f_2)_P.$$

Then

$$M \supset J_1 \supset \dots \supset J_r \supset J_{r+1} = (f_1, f_2)_P.$$

Since $r > \dim(M_P/(f_1, f_2)_P)$, it follows that $J_i = J_{i+1}$ for some i .

If $i = r$ then $t_1 \dots t_r \in J_{r+1} = (f_1, f_2)_P$ and we are done. If $i < r$ then

$$t_1 t_2 \dots t_i = t_1 t_2 \dots t_{i+1} \phi + \psi \quad \text{with } \phi \in O_P, \text{ and } \psi \in (f_1, f_2)_P,$$

$$t_1 t_2 \dots t_i (1 - t_{i+1} \phi) = \psi \in (f_1, f_2)_P$$

$$t_1 \dots t_r = \psi (1 - t_{i+1} \phi)^{-1} t_{i+1} \dots t_r \in (f_1, f_2)_P.$$

□

Lemma 6.11 *Let $P \in C_1 \cap C_2$, and let $\phi \in O_P$. Then there exists a polynomial $g \in k[x, y]$ such that*

$$g \equiv \phi \pmod{(f_1, f_2)_P},$$

$$g \equiv 0 \pmod{(f_1, f_2)_Q} \quad Q \neq P.$$

Proof. By the weak version of Bézout's theorem we know that the number of points in $C_1 \cap C_2$ is finite. By a simple lemma proven in the beginning of the course, there is a polynomial $h(x, y)$ such that $h(P) = 1$ and $h(Q) = 0$ for all $Q \in C_1 \cap C_2$, $Q \neq P$. I.e. $h^{-1} \in O_P$, $h \in M_Q$ for other points Q . Hence there exists $r > 0$ such that $h^{-r} \in O_P$, $h^r \in (f_1, f_2)_Q$.

Now, since $O_P = k[x, y] + (f_1, f_2)_P$, there is a polynomial f such that $f \equiv \phi h^{-r} \pmod{(f_1, f_2)_P}$. Then $g = fh^r$ solves the problem.

□

Corollary 6.12 *The map*

$$\pi : k[x, y] \rightarrow \prod_{P \in C_1 \cap C_2} \frac{O_P}{(f_1, f_2)_P}$$

given by $f \rightarrow (\dots, f \pmod{(f_1, f_2)_P}, \dots)$, $P \in C_1 \cap C_2$ is surjective.

Proof. Follows immediately from the last proposition.

□

Consider now the kernel of homomorphism π . Clearly $(f_1, f_2) \subset \ker(\pi)$. So to finish the proof of Theorem 6.7 it suffices to prove the following:

Proposition 6.13 $\ker(\pi) = (f_1, f_2)$.

Proof. Let $f \in \ker(\pi)$. To show that $f \in (f_1, f_2)$ we consider the set:

$$I_f = \{g \in k[x, y] : gf \in (f_1, f_2)\}.$$

It is clear that I_f is an ideal, and we just need to prove that 1 belongs to I_f , i.e. $I_f = k[x, y]$. To prove this we will show that $V(I_f)$ is empty. Then applying Nullstellensatz we get the statement.

$V(I_f) = \emptyset$. Since $(f_1, f_2) \subset I_f$, we have $V(I_f) \subset C_1 \cap C_2$. Chose now $P \in C_1 \cap C_2$. Since $f \in \ker(\pi)$, we have $f \in (f_1, f_2)_P$, $f = (f_1g_1 + f_2g_2)/g$ with $g(P) \neq 0$. And we deduce $fg \in (f_1, f_2)$. So $g \in I_f$ and $P \notin V(I_f)$. □

Proof of Theorem 6.7. It follows from the proposition, that we have the isomorphism of the following two vector spaces. Hence their dimensions coincide

$$k[x, y]/(f_1, f_2) \cong \prod_{P \in C_1 \cap C_2} \frac{O_P}{(f_1, f_2)_P}$$

□

Here is an immediate corollary of the theorem:

Corollary 6.14 *Suppose that curves $C_1 = 0$ and $C_2 = 0$ intersect at exactly one point P . Then the intersection index of $I(C_1 \cap C_2, P)$ equals $\dim(k[x, y]/(f_1, f_2))$.*

Example 6.15 Consider two curves $x^2 - y^3 = 0$ and $x^2 + y^3 = 0$ in $\mathbb{A}_{\mathbb{C}}^2$. Let us calculate the index of their intersection at $(0, 0)$.

Note first that these curves intersect only at $(0, 0)$. So we can use the corollary. Next, clearly $(x^2 - y^3, x^2 + y^3) = (x^2, y^3)$. Now the base of the quotient space $k[x, y]/(x^2, y^3)$ is given by monomials $x^i y^j$, $i = 0, 1$, $j = 0, 1, 2$. I.e., $I(C_1 \cap C_2, 0) = 6$.

Exercise 6.16 Suppose that F and G are two polynomials without common factors and $F(P) = G(P) = 0$. Prove that for any polynomial H , $I((F = 0) \cap (G = 0), P) = I((F = 0) \cap (G + HF = 0), P)$.

Here is the almost final version of Bézout's theorem for this course. Let F and G be polynomials without common factors. Suppose the corresponding curves C_1 and C_2 don't intersect at the infinity of \mathbb{A}_k^2 . Then $\deg F \cdot \deg G = \sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P)$.

6.4 What should you definitely know?

Everything are supposed to know is contained in these notes, and in exercises with solutions. Especially you should know the following:

- 1) Projective space. Points at infinity. Desargue's theorem and its proof.
- 2) Bézout's theorem in the weak form (understand but don't need to know the proof). Understand solution to exercise 11 from first assessment.
- 3) Affine varieties, irreducible affine varieties (why \mathbb{C}^n is irreducible?).
- 4) Been able to find singular points of affine varieties (there are several problems of this type in the second assessment).
- 5) Been able to solve problem 14 from the second assessment.
- 6) Know Hilbert basis theorem and Hilbert theorem on finite generation the ring of invariants. Understand the proof of Hilbert theorem on finite generation of the ring of invariants. Know what Nullstellensatz says and know its corollaries. Been able to solve problem 11 from the second assessment.
- 7) Know what is a morphism of affine varieties.
- 8) Know what are multiplicities of curves, and what is intersection index of curves in $\mathbb{A}_{\mathbb{C}}^2$. Been able to calculate this index in simple cases. Understand Corollary 6.14, and been able to solve exercise 5 from third exercise sheet.

In general. The more you know the better.