ALGEBRAIC CURVES: LECTURE NOTES

PIOTR KOWALSKI

0. Introduction

Lecture plan

(1) Affine varieties globally: dimension, regular functions, rational functions.
(2) Affine varieties locally: smoothness, DVR rings, multiplicities of zeros and poles, intersection numbers.
(3) Projective varieties, Bezout's theorem and applications, elliptic curves.

Books Fulton "Algebraic curves", first chapter of Hartshorne's "Algebraic geometry".

Algebraic preliminaries The word *ring* will always mean *commutative ring with identity*. Homomorphisms of rings preserve identity. Let R be a ring and $A \subseteq R$. The ideal of R generated by A is denoted by (A) or AR. We have the following operations on $I, J \trianglelefteq R$:

$$I + J,\ I \cap J,\ IJ,\ \sqrt{I}.$$

An *R-algebra* is a (fixed) ring homomorphism $R \to S$. We usually say "an R-algebra S" guessing the homomorphism. If S is an R-algebra, it is also an R-module. We have the natural notion of a homomorphism of R-algebras (ring homomorphism which is also R-linear, equivalently certain diagram has to commute). If K is a field and S is a non-zero ring, then any ring homomorphism $K \to S$ is necessarily injective, so non-zero K-algebras may be identified with ring extensions of K.
Let R be a domain. If $A \subset R$ is a *multiplicative subset*, then we have the *R-algebra of fractions* (with denominators from A) denoted R_A. If P is a prime ideal in R, then $R \setminus P$ is a multiplicative subset and $R_{R\setminus P}$ is denoted R_P. The *field of fractions* of R is $R_{\{0\}}$ which we denote by R_0.
If $K \subseteq L$ is a field extension, then $\operatorname{trdeg}_K L$ is the cardinality of (any) transcendence basis of L over K. If S is a K-algebra, then by $\dim_K S$, we mean the dimension of S considered as a K-linear space.

1. Affine varieties globally

Let K be an algebraically closed field and $n \in \mathbb{N}_{>0}$. By $\mathbb{A}^n$ or $\mathbb{A}^n(K)$ we mean just K^n (the n-th Cartesian power of K), and call it *affine n-space* (over K). Elements of $\mathbb{A}^n$ are called *points* and the notation $\bar{a}, \bar{x} \in \mathbb{A}^n$ suggests that $\bar{x} = (x_1, \ldots, x_n), \bar{a} = (a_1, \ldots, a_n)$. Affine 1-space K is called *affine line* and affine 2-space K is called *affine plane*.

1.1. **Zariski topology.** In this section we will not really use the assumption that K is algebraically closed (just K being infinite will be used sometimes). Let $\bar{X} = (X_1, \ldots, X_n)$ be a tuple of variables.

Definition 1.1. For any $A \subseteq K[\bar{X}]$, let

$$V(A) := \{\bar{x} \in K^n \mid (\forall F \in A)(F(\bar{x}) = 0)\}.$$

A subset $V \subseteq \mathbb{A}^n$ is an *affine algebraic set* or a *Zariski closed set*, if there is $A \subseteq K[\bar{X}]$ such that $V = V(A)$.

Example 1.2. We have the following affine algebraic sets:

(1) Parabola ($n = 2,\ A = \{Y - X^2\}$).
(2) Hyperbola ($n = 2,\ A = \{YX - 1\}$).
(3) More generally, if $F \in K[\bar{X}] \setminus K$, then $V(F)$ is an affine algebraic set. If F is irreducible, then:
   - for $n = 2$, $V(F)$ is called *plane curve*;
   - for $n = 3$, $V(F)$ is called *surface*;
   - for $n > 3$, $V(F)$ is called *hypersurface*.
(4) Any singleton $\{\bar{a}\}$ ($A = \{X_1 - a_1, \ldots, X_n - a_n\}$).
(5) Empty set ($A = \{1\}$).
(6) Affine n-space ($A = \{0\}$).

Lemma 1.3. *Let $(A_i \subseteq K[\bar{X}])_{i<\kappa}$ and $I, J \trianglelefteq K[\bar{X}]$. Then:*

(1) *If $A_0 \subseteq A_1$, then $V(A_1) \subseteq V(A_0)$;*
(2) *$V(\bigcup A_i) = \bigcap_i V(A_i)$;*
(3) *$V(A_0) = V((A_0))$ (recall that (A_0) is the ideal generated by A_0);*
(4) *$V(I \cap J) = V(IJ) = V(I) \cup V(J)$;*
(5) *$V(I + J) = V(I) \cap V(J)$.*

Proof. We omit the easy proofs of (1) and (2).
For (3), we get by (1) that $V((A_0)) \subseteq V(A_0)$. Take any $a \in V(A_0)$ and $F \in (A_0)$. Thus there are $F_1, \ldots, F_k \in A_0$ and $G_1, \ldots, G_k \in K[\bar{X}]$ such that $F = \sum G_i F_i$. Therefore:

$$F(a) = \sum G_i(a) F_i(a) = 0.$$

Hence $a \in V((A_0))$ and $V((A_0)) = V(A_0)$.
For (4), since $IJ \subseteq I \cap J \subseteq I, J$, we get by (1) that

$$V(I) \cup V(J) \subseteq V(I \cap J) \subseteq V(IJ).$$

For the remaining inclusion take $a \in V(IJ)$ and assume that $a \notin V(I)$. Hence there is $F \in I$ such that $F(a) \neq 0$. Take any $G \in J$. Then $FG \in IJ$, so $(FG)(a) = 0$. Therefore, $G(a) = 0$ and $a \in V(J)$.
For (5) we observe by (2) and (3) that:

$$V(I) \cap V(J) = V(I \cup J) = V((I \cup J)) = V(I + J),$$

since $I + J = (I \cup J)$. □

Corollary 1.4. *Any finite subset of $\mathbb{A}^n$ is Zariski closed.*

Proof. Since we know that the singletons are Zariski closed, it is enough to use 1.3(3) and 1.3(4). □

By Lemma 1.3, Zariski closed subsets of $\mathbb{A}^n$ are indeed closed sets of a certain topology on $\mathbb{A}^n$. This topology is called *Zariski topology*. By Corollary 1.4, this topology is T_1 (points are closed). We will see soon that it is *not* Hausdorff (points can *not* be separated by open neighborhoods).

Example 1.5. Let us look at the Zariski topology on the affine line $\mathbb{A}^1 = K$. A non-zero polynomial in one variable can have only finitely many zeroes and for any finite subset $V \subset K$, there is a polynomial $F \in K[X]$ vanishing exactly on V. Therefore, a

subset $V \subset K$ is Zariski closed iff V is finite or $V = K$. Thus the Zariski topology on $\mathbb{A}^1$ is the *cofinite topology*, in particular it is not Hausdorff.

Remark 1.6. If $K = \mathbb{C}$, then we have another topology on $\mathbb{A}^n$ coming from the identification of $\mathbb{C}$ with $\mathbb{R}^2$ and the order topology on $\mathbb{R}$. We will call the latter (and much more natural) topology the *Euclidean* topology. The Zariski topology is (much) coarser than the Euclidean one, e.g. closed boxes are not closed in Zariski topology (see Example 1.5).

Remark 1.7. By Example 1.5, there are many subsets of $\mathbb{A}^2$ which are Zariski closed, but are not closed in $\mathbb{A}^2$ with the product topology $\mathbb{A}^1 \times \mathbb{A}^1$ (e.g. parabola). Hence the Zariski topology on $\mathbb{A}^2$ is *not* the product topology (note that the Euclidean topology on $\mathbb{C}^2$ *is* the product topology). Similarly for $n > 2$.

The next proposition says that for studying $V(A)$, we can concentrate on finite subsets $A_0 \subseteq A$.

Proposition 1.8. *For any $A \subseteq K[\bar{X}]$ there is a finite $A_0 \subseteq A$ such that $V(A) = V(A_0)$.*

Proof. By Hilbert's Basissatz (Basis Theorem), the ring $K[\bar{X}]$ is Noetherian, in particular the ideal (A) is finitely generated. Hence we can find a finite $A_0 \subseteq A$ such that $(A_0) = (A)$. By 1.3(3), we have

$$V(A) = V((A)) = V((A_0)) = V(A_0),$$

which is exactly what we want. □

Definition 1.9. A topological space X is called *Noetherian*, if any descending chain of closed subsets of X stabilizes.

Remark 1.10. Let X be a topological space.

(1) If X is Noetherian, then X is quasi-compact (need not be Hausdorff). However, it is not a good intuition to think about Noetherian spaces as compact spaces.
(2) Problem 1.1: X is Hausdorff and Noetherian iff X is finite with the discrete topology. Hence all "infinite, nice spaces" are *not* Noetherian.
(3) By a *subspace* of X we mean a subset with the induced topology. It is easy to see (Problem 1.0) that any subspace of a Noetherian topological space is again Noetherian. Note that compactness is not inherited by subspaces.
(4) By the example above, we see that the affine line is Noetherian.

Proposition 1.11. *$\mathbb{A}^n$ with the Zariski topology is Noetherian.*

Proof. Let us take $(V_i)_{i\in\mathbb{N}}$, a decreasing sequence of closed subsets of $\mathbb{A}^n$. For each $i \in \mathbb{N}$, there is $A_i \subseteq K[\bar{X}]$ such that $V_i = V(A_i)$. Let $I_i := (A_0 \cup \ldots \cup A_i)$. By Lemma 1.3(2,3), we have:

$$V(I_i) = V(A_0 \cup \ldots \cup A_i) = V(A_0) \cap \ldots \cap V(A_i) = V_0 \cap \ldots \cap V_i = V_i.$$

Clearly, $(I_i)_{i\in\mathbb{N}}$, is an increasing sequence of ideals of $K[\bar{X}]$. By Hilbert's Basis Theorem, $K[\bar{X}]$ is a Noetherian ring, hence there is $N \in \mathbb{N}$ such that $I_N = I_{N+1} = \ldots$. Therefore, $V_N = V_{N+1} = \ldots$, so the sequence $(V_i)_{i\in\mathbb{N}}$ stabilizes indeed. □

For any affine algebraic set $V \subseteq \mathbb{A}^n$, we consider V as a topological space with the induced Zariski topology. Then the closed subsets of V are exactly those subsets of V which are affine algebraic sets. By Problem 1.1, V is Hausdorff iff it is finite (so usually it is *not* Hausdorff). By Proposition 1.11 and Remark 1.10, V is Noetherian.

Definition 1.12. A non-empty topological space X is *irreducible* if it is not a non-trivial union of its two closed subsets, i.e. for any $Y_1, Y_2 \subseteq X$ closed, if $X = Y_1 \cup Y_2$, then $X = Y_1$ or $X = Y_2$.

Remark 1.13. Let X be a topological space.

(1) If X is irreducible, then X is connected (in the definition of irreducibility, we do not require $Y_1 \cap Y_2 = \emptyset$).
(2) If X is irreducible and Hausdorff, then X is a singleton (similar to Problem 1.1). So "nice spaces" are not irreducible.
(3) By the description of the topology on the affine line, we see that $\mathbb{A}^1$ is Noetherian and irreducible. In the next section we will find an algebraic criterium for irreducibility of an algebraic variety.
(4) Problem 1.2: Let $Y \subseteq X$. Then Y is irreducible (as a topological space with the topology induced from X) iff the closure of Y is irreducible.

Proposition 1.14. *If X is a Noetherian topological space, then:*

(1) *There are closed, irreducible $X_1, \ldots, X_k \subseteq X$ such that $X = X_1 \cup \ldots \cup X_k$ and for all $i \neq j$, we have $X_i \not\subseteq X_j$.*
(2) *If we have $X_1, \ldots, X_k$ and $X'_1, \ldots, X'_{k'}$ as above, then $k = k'$ and there is $\sigma \in \mathrm{Sym}(k)$ such that $X_1 = X'_{\sigma(1)}, \ldots, X_k = X'_{\sigma(k)}$.*

Proof. Proof of (1) is basically the same as the proof of the fact that any non-invertible non-zero element of a Noetherian domain decomposes as the product of irreducible elements. Assume X does not have a decomposition into the union of finitely many irreducible closed subsets (in short: does not have decomposition). Then X is *not* irreducible, so there are non-empty closed $X_1, X_2 \subsetneq X$ such that $X = X_1 \cup X_2$. Since X does not have decomposition, either X_1 does not have decomposition or X_2 does not have decomposition. Assume that X_1 does not have decomposition. Proceeding as above with X_1 in place of X, we get non-empty closed $X_{11}, X_{12} \subsetneq X_1$ such that $X_1 = X_{11} \cup X_{12}$ and X_{11} does not have decomposition. If we continue like this, we get a sequence of closed subsets

$$X \supsetneq X_1 \supsetneq X_{11} \supsetneq X_{111} \supsetneq \ldots$$

contradicting the assumption that X is Noetherian. Therefore X has decomposition. By throwing away the redundant X_i's, we may assume that $X_i \not\subseteq X_j$ for $i \neq j$, so (1) is proved.
Let us take $X'_1, \ldots, X'_{k'}$ from (2) and $i \leqslant k$. Then $X_i \subseteq X'_1 \cup \ldots \cup X'_{k'}$, so

$$X_i = (X'_1 \cap X_i) \cup \ldots \cup (X'_{k'} \cap X_i).$$

But X_i is irreducible, so there is $i' \leqslant k'$ such that $X_i = X'_{i'} \cap X_i$, i.e. $X_i \subseteq X'_{i'}$. Proceeding similarly, we find $j \leqslant k$ such that $X'_{i'} \subseteq X_j$. But then $X_i \subseteq X_j$, so $i = j$ and we get $X_i = X'_{\sigma(i)}$. Let $\sigma(i) := i'$. We have constructed a function $\sigma : \{1, \ldots, k\} \to \{1, \ldots, k'\}$ such that for each $i \leqslant k$, we have $X_i = X'_{\sigma(i)}$. Similarly, we get a function $\tau : \{1, \ldots, k'\} \to \{1, \ldots, k\}$ such that for each $j \leqslant k'$, we have $X'_j = X_{\tau(j)}$. But then for any $i \leqslant k$, we have

$$X_{\tau(\sigma(i))} = X'_{\sigma(i)} = X_i,$$

so $\tau(\sigma(i)) = i$. Similarly, for each $j \leqslant k'$, we have $\sigma(\tau(j)) = j$. Hence $k = k'$ and σ is a permutation. □

The closed subsets $X_1, \ldots, X_k$ from Proposition 1.14 are called the *irreducible components* of X.

Definition 1.15. Let V be an affine algebraic set. We call V an *affine variety*, if it is irreducible as a topological space with the Zariski topology.

We can now directly apply Proposition 1.14.

Proposition 1.16. *Every affine algebraic set can be expressed uniquely as a finite union of affine varieties, no one containing another.*

Example 1.17. Union of affine line and parabola, or line and points etc. But we still do not know whether e.g. hyperbola or parabola is irreducible. In the next section we will learn an algebraic criterium for irreducibility.

Definition 1.18. Let X be a topological space. The *dimension* of X, denoted $\dim(X)$, is the supremum of $k \in \mathbb{N}$ such that there is a strictly decreasing (or increasing) sequence of irreducible closed subsets of X:

$$X \supsetneq X_0 \supsetneq X_1 \supsetneq \ldots \supsetneq X_k.$$

(Note that the empty set is not considered to be irreducible.)

Problem 1.3: If X is Noetherian and T_1 (points are closed), then $\dim(X) = 0$ iff X is finite.

There is a Noetherian topological space X such that $\dim(X) = \infty$.

Let V be an affine algebraic set. By the *dimension* of V, denoted $\dim(V)$, we mean the dimension of V as a Noetherian topological space (with the Zariski topology).

Example 1.19. We can see that $\dim(\mathbb{A}^1) = 1$, since $\mathbb{A}^1$ is irreducible and a proper closed subset of $\mathbb{A}^1$ is irreducible iff it is a singleton.

Definition 1.20. An *affine algebraic curve* (or just *affine curve*) is an affine algebraic variety C such that $\dim(C) = 1$.

We know so far that the affine line is an affine curve. In the next section we will find algebraic criteria to decide whether an algebraic variety is a curve (in particular to prove that hyperbola and parabola are indeed curves as they ought to be).

1.2. **Coordinate rings.** We want to express some properties of affine algebraic sets in algebraic terms. The assumption that K is algebraically closed will be needed for this. For any set Y, let $\mathrm{Func}(Y, K)$ denote the set of all functions from Y to K. It has a natural K-algebra structure (K embeds into $\mathrm{Func}(Y, K)$ as the subfield of constant functions). For $F \in K[\bar{X}]$, let us denote (only for a while) by $\tilde{F}$ the corresponding polynomial function from $\mathbb{A}^n$ to K. By the definition of the ring operations in $K[\bar{X}]$, the map

$$K[\bar{X}] \ni F \mapsto \tilde{F} \in \mathrm{Func}(\mathbb{A}^n, K)$$

is a homomorphism of K-algebras.

Problem 1.4: If $F \neq G$, then $\tilde{F} \neq \tilde{G}$.

By Problem 1.4, we can identify $K[\bar{X}]$ with a K-subalgebra of $\mathrm{Func}(\mathbb{A}^n, K)$ consisting of polynomial functions, and we will not write $\tilde{F}$ anymore.

Definition 1.21. If $V \subseteq \mathbb{A}^n$, then the *(affine) coordinate ring of* V (or *ring of polynomial functions on* V) is:

$$K[V] := \{f \in \mathrm{Func}(V, K) \mid (\exists F \in K[\bar{X}])(F|_V = f)\}.$$

It is easy to see that $K[V]$ above is a K-subalgebra of $\mathrm{Func}(V, K)$.

Problem 1.5: If $V \subset \mathbb{A}^n$ is finite, then $K[V] = \mathrm{Func}(V, K)$.

Therefore, $K[V] \cong_K K^{|V|}$, the Cartesian power of the field K (considered with the coordinate-wise K-algebra structure). By Problem 1.4, $K[\mathbb{A}^n] = K[\bar{X}]$.

We have a natural epimorphism of K-algebras:

$$K[\bar{X}] \ni F \mapsto F|_V \in K[V].$$

We denote its kernel by $I(V)$, it is the *ideal of* V.

Lemma 1.22. *The ideal $I(V)$ is* radical*, i.e. $I(V) = \sqrt{I(V)}$.*

Proof. Let us take $F \in \sqrt{I(V)}$. There is $k \in \mathbb{N}$ such that $F^k \in I(V)$. It means that for each $v \in V$, we have $0 = F^k(v) = F(v)^k$. Hence for each $v \in V$, $F(v) = 0$, thus $F \in I(V)$. □

Clearly

$$I(V) = \{F \in K[\bar{X}] \mid (\forall \bar{x} \in V)(F(\bar{x}) = 0)\},$$

and we have an isomorphism of K-algebras:

$$K[V] \cong K[\bar{X}]/I(V).$$

Lemma 1.23. *Let $(V_i \subseteq \mathbb{A}^n)_{i<\kappa}$ and $J \trianglelefteq K[\bar{X}]$. Then:*

1. *If $V_0 \subseteq V_1$, then $I(V_1) \subseteq I(V_0)$;*
2. *$I(\bigcup V_i) = \bigcap I(V_i)$;*
3. *$J \subseteq I(V(J))$;*
4. *$V(I(V_0))$ is the* Zariski closure *(i.e. the closure in the Zariski topology) of V_0.*

Proof. We omit easy proofs of (1), (2) and (3). For (4), let $\bar{V}_0$ be the Zariski closure of V_0. It is also easy to see that $V_0 \subseteq V(I(V_0))$. Since $V(I(V_0))$ is Zariski closed, it is enough to show that for any Zariski closed $W \subseteq \mathbb{A}^n$ such that $V_0 \subseteq W$, we have $V(I(V_0)) \subseteq W$. There is $J \trianglelefteq K[\bar{X}]$ such that $W = V(J)$. Hence $V_0 \subseteq V(J)$. By (3) and (1), we have:

$$J \subseteq I(V(J)) \subseteq I(V_0).$$

By Lemma 1.3(1), $V(I(V_0)) \subseteq V(J) = W$. □

We aim to describe $I(V(I))$ for $I \trianglelefteq K[\bar{X}]$. We will need another famous theorem of Hilbert. We just give an idea of the proof of this theorem. The most natural (full) proof uses basic model theory and will be given in my other course. This is the place, where we use the assumption that K is algebraically closed.

Theorem 1.24 (**Weak Hilbert's Nullstellensatz**)**.** *Let $I \trianglelefteq K[\bar{X}]$. If $I \neq K[\bar{X}]$, then $V(I) \neq \emptyset$.*

Idea of the proof. Let $F_1, \ldots, F_r \in I$ be such that $I = (F_1, \ldots, F_r)$, and let k be the subfield of K generated by the coefficients of $F_1, \ldots, F_r$. Since $I \neq K[\bar{X}]$, I extends to a maximal $\mathfrak{m} \trianglelefteq K[\bar{X}]$. Let $L := K[\bar{X}]/\mathfrak{m}$ and $\Phi : K \to L$ denote the following composition:

$$K \xrightarrow{\subseteq} K[\bar{X}] \longrightarrow K[\bar{X}]/\mathfrak{m} = L.$$

Since Φ is a homomorphism of fields, it is an embedding. Hence we can identify K with a subfield of L. Let

$$\bar{v} := (X_1 + \mathfrak{m}, \ldots, X_n + \mathfrak{m}) \in L^n.$$

It is easy to check (but some care is necessary) that

$$F_1(\bar{v}) = 0, \ldots, F_r(\bar{v}) = 0.$$

Let $l := k(\bar{v})$. Now, *if* there is an k-algebra homomorphism $\Psi : l \to K$, then $\Psi(\bar{v}) \in V(I)$, so $V(I)$ is non-empty. This homomorphism exists for example if $\mathrm{trdeg}_k K$ is infinite (enough to take the transcendence degree over the prime field). By using model theory, the (incomplete) homomorphism argument can be replaced with an *elementary extension* argument. We will not go into details here. □

There are many algebraic proofs of Weak Hilbert's Nullstellensatz. We will not discuss any of them here.

Corollary 1.25 (**Hilbert's Nullstellensatz**). *For $I \trianglelefteqslant K[\bar{X}]$, we have $I(V(I)) = \sqrt{I}$.*

Proof. By Lemma 1.23(3), we have $I \subseteq I(V(I))$. By 1.22, we have $\sqrt{I} \subseteq I(V(I))$. For the opposite inclusion, let us take a non-zero $G \in I(V(I))$ and $F_1, \ldots, F_r \in I$ such that $I = (F_1, \ldots, F_r)$. Let us define

$$J := (F_1, \ldots, F_r, X_{n+1}G - 1) \trianglelefteqslant K[\bar{X}, X_{n+1}].$$

Take any $(\bar{v}, v) \in \mathbb{A}^{n+1}$. If for each $i \leqslant r$, we have $F_i(\bar{v}) = 0$, then $\bar{v} \in V(I)$. Thus $G(\bar{v}) = 0$, since $G \in I(V(I))$. Therefore

$$(X_{n+1}G - 1)(\bar{v}, v) = 0 - 1 \neq 0.$$

We have obtained that $V(J) = \emptyset$. By Weak Hilbert's Nullstellensatz, $J = K[\bar{X}, X_{n+1}]$. Hence there are $H_1, \ldots, H_{r+1} \in K[\bar{X}, X_{n+1}]$ such that

$$1 = \sum_{i=1}^{r} H_i F_i + H_{r+1}(X_{n+1}G - 1). \tag{1}$$

Consider the following homomorphism of K-algebras:

$$\Psi : K[\bar{X}, X_{n+1}] \to K(\bar{X}); \quad \Psi(X_i) = X_i \text{ for } i \leqslant n,\ \Psi(X_{n+1}) = G^{-1}$$

(here we use $G \neq 0$). After applying Ψ to (the both sides of) (1) we get the following equality in $K(\bar{X})$

$$1 = \sum_{i=1}^{r} H_i(\bar{X}, G^{-1}) F_i(\bar{X}). \tag{2}$$

Let N be the maximum of the degrees of H_i with respect to the variable X_{n+1}. Multiplying the both sides of (2) by G^N we get:

$$G^N = \sum_{i=1}^{r} G^N H_i(\bar{X}, G^{-1}) F_i(\bar{X}), \tag{3}$$

where for each $i \leqslant r$, we have $G^N H_i(\bar{X}, G^{-1}) \in K[\bar{X}]$. By (3), $G^N \in I$, therefore $G \in \sqrt{I}$. □

We can prove now the algebraic characterization of irreducibility.

Proposition 1.26. *Let $V \subseteq \mathbb{A}^n$ be Zariski closed. The following are equivalent:*

1. *V is irreducible,*
2. *$I(V)$ is prime,*
3. *There is a prime ideal $P \trianglelefteqslant K[\bar{X}]$ such that $V = V(P)$,*
4. *$K[V]$ is a domain.*

Proof. Since $K[V] \cong K[\bar{X}]/I(V)$, we get the equivalence (2) $\Leftrightarrow$ (4).
For the implication (1) $\Rightarrow$ (2) assume that V is irreducible and take $F, G \in K[\bar{X}]$ such that $FG \in I(V)$. Then

$$V \subseteq V(FG) = V(F) \cup V(G).$$

Since V is irreducible, $V \subseteq V(F)$ or $V \subseteq V(G)$. It means that $F \in I(V)$ or $G \in I(V)$, so $I(V)$ is prime.
For the implication (2) $\Rightarrow$ (3) we take $P = I(V)$. Since V is Zariski closed, we get by Lemma 1.23(4):

$$V(P) = V(I(V)) = V.$$

For the implication (3) $\Rightarrow$ (1) assume that $V = V(P)$ for a prime ideal P and take Zariski closed $V_1, V_2 \subseteq \mathbb{A}^n$ such that $V = V_1 \cup V_2$. By 1.23(2) and Hilbert Nullstellensatz, we have

$$I(V_1) \cap I(V_2) = I(V_1 \cup V_2) = I(V(P)) = \sqrt{P} = P.$$

Since P is prime, $P = I(V_1)$ or $P = I(V_2)$. By Lemma 1.23(4), $V = V_1$ or $V = V_2$, so V is irreducible. □

Remark 1.27. For the equivalences (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (4) we do not need the assumption that K is algebraically closed. However this assumption is necessary for the crucial equivalence with (3) (see Problem 1.6).

Clearly, I may be not prime and $V(I)$ may be still irreducible, e.g. for $I = (X^2)$.

Corollary 1.28. *If $F \in K[\bar{X}]$ is irreducible (as an element of the ring $K[\bar{X}]$), then the hypersurface $V(F)$ is an affine variety.*

Proof. Since $K[\bar{X}]$ is UFD (Gauss Theorem) and F is irreducible, F is prime. Therefore, the ideal (F) is prime. By 1.26(4), $V(F)$ is irreducible. □

Problem 1.6: Find $F \in \mathbb{R}[X, Y]$ which is irreducible such that $V(F) \cap \mathbb{R}^2$ is non-empty and not irreducible.

Example 1.29. We can finally give some examples of affine varieties and their coordinate rings.

(1) Let $V = V(Y - X^2) \subseteq \mathbb{A}^2$ (parabola). The polynomial $Y - X^2$ is irreducible, so by Corollary 1.28, V is an affine variety. Since the ideal $(Y - X^2)$ is prime, we get by Hilbert Nullstellensatz that $I(V) = (Y - X^2)$. Therefore

$$K[V] \cong_K K[X, Y]/(Y - X^2) \cong_K K[X].$$

Note that $K[V] \cong_K K[\mathbb{A}^1]$ which suggests that parabola is "isomorphic" to the affine line. We will make sense out of it and see that it is true.

(2) Let $V = V(YX - 1) \subseteq \mathbb{A}^2$ (hyperbola). Similarly as above, V is an affine variety and $K[V] \cong_K K[X, Y]/(XY - 1)$.
Problem 1.7: $K[V]$ is not isomorphic to $K[\mathbb{A}^1]$.

(3) Let $V = V(Y^2 - X^3)$. Problem 1.8: $K[V]$ is not UFD.
In particular $K[V]$ is not isomorphic to $K[\mathbb{A}^1]$. Actually, the fact that $K[V]$ is not UFD (or rather, not *normal*) is related to the fact that V is *singular at* $(0, 0)$ (again, we will make it precise later). This is very typical: algebraic properties of the coordinate ring of V reflect geometric properties of V.

Corollary 1.30. *Let $V \subseteq \mathbb{A}^n$ be an affine algebraic set. There is a bijective correspondence (inverting inclusions) between the set of radical (resp. prime) ideals of $K[V]$ and the set of Zariski closed subsets (resp. irreducible Zariski closed subsets) of V.*

Proof. By Proposition 1.26 and Hilbert Nullstellensatz (and 1.3(1), 1.23(1)), we have such correspondences for $V = \mathbb{A}^n$. For an arbitrary V let us concentrate on prime ideals. Since $K[V] = K[\bar{X}]/I(V)$, the set of prime ideals of $K[V]$ corresponds to the set of prime ideals of $K[\bar{X}]$ containing $I(V)$. But the latter set corresponds exactly (again by the references above) to the set of irreducible Zariski closed subsets of V. □

We recall a definition from ring theory.

Definition 1.31. Let R be a ring. The *Krull dimension* of R, denoted $\dim(R)$, is the supremum of $k \in \mathbb{N}$ such that there is a strictly increasing (or decreasing) sequence of prime ideals of R:

$$P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_k.$$

Example 1.32. It is usually not easy to calculate the Krull dimension of a ring. We describe it in some simple cases.

- If k is a field, then $\dim(k) = 0$, because the 0-ideal is a unique prime ideal of k.
- Problem 1.9: If R is PID and not a field, then $\dim(R) = 1$.
- Nagata has constructed a Noetherian ring of infinite Krull dimension.

Proposition 1.33. *Let V be an affine algebraic set. Then* $\dim(V) = \dim(K[V])$

Proof. It follows directly from the definitions and Corollary 1.30. □

In the case of coordinate rings, there is an easier description of the Krull dimension, but it is difficult to prove. First we need one more definition.

Definition 1.34. Let V be an irreducible affine variety. Then $K(V)$ denotes the field of fractions of $K[V]$ (which is a domain by 1.26(4)) and it is called *the field of rational functions on V*.

We will not give a real proof of the following theorem (recall that R_0 denotes the field of fractions of R).

Theorem 1.35. *Let R be a finitely generated K-algebra which is a domain. Then we have:*

$$\dim(R) = \operatorname{trdeg}_K R_0.$$

A very brief idea of the proof. Let us assume first that $R = K[\bar{X}]$ and consider the following chain of prime ideals

$$(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq (X_1, \ldots, X_n).$$

Hence $\dim(K[\bar{X}]) \geqslant n$. The other inequality is more difficult and is proved by induction on n by finding an appropriate quotient ring.
For the general case, by Noether's Normalization Theorem there are $r_1, \ldots, r_d \in R$ which are algebraically independent over K and such the the ring extension $K[r_1, \ldots, r_d] \subseteq R$ is *finite*, i.e. R is a finitely generated $K[r_1, \ldots, r_d]$-module. Then the field extension $K(r_1, \ldots, r_d) \subseteq R_0$ is also finite, hence algebraic and $\operatorname{trdeg}_K R_0 = d$.
Clearly $K[r_1, \ldots, r_d] \cong K[X_1, \ldots, X_d]$, so $\dim(K[r_1, \ldots, r_d]) = d$. Now we have to use the fact that the Krull dimension does not change in finite extensions so $\dim(R) = d$. □

Remark 1.36. A finitely generated algebra over a field is called an *affine domain*. Theorem 1.35 holds for any affine domain (we do not need the assumption that K is algebraically closed).

Corollary 1.37. *Let V be an affine variety. Then*

$$\dim(V) = \operatorname{trdeg}_K K(V).$$

Proof. The K-algebra $K[V]$ is finitely generated as an image of $K[\bar{X}]$ and it is a domain, so we can use 1.33 and 1.35. □

Corollary 1.38. *Let V be a plane curve. Then* $\dim(V) = 1$. *(So, a plane curve is an affine curve.)*

Proof. Let $F \in K[X,Y]$ be irreducible such that $V = V(F)$. Then $K[V] \cong K[X,Y]/(F)$ and let us identify this two K-algebras. We consider $K[X,Y]/(F)$ as a ring extension of K. Let

$$t := X + (F) \in K[V] \subseteq K(V), \quad s := Y + (F) \in K[V] \subseteq K(V).$$

Case 1 $t \in K$.
Then $X - t \in (F)$, so $F | X - t$ in $K[X,Y]$. Since F and $X - t$ are irreducible, $(F) = (X - t)$, so

$$K[X,Y]/(F) = K[X,Y]/(X - t) \cong K[Y].$$

Then $K(V) \cong K(Y)$, so $\operatorname{trdeg}_K K(V) = 1$, OK.

Case 2 $t \notin K$.
We will show that $\{t\}$ is the transcendence basis of $K(V)$. Since $t \notin K$ and K is algebraically closed, $\{t\}$ is algebraically independent. Now it is enough to show that $K(t) \subset K(V)$ is algebraic. Since $K(V) = K(t,s)$, it is enough to show that s is algebraic over $K(t)$. Let

$$G(Y) := F(t,Y) \in K(t)[Y].$$

If $G = 0$, then t is algebraic over K, a contradiction. So $G \neq 0$ and $G(s) = F(t,s) = 0$, OK. □

Remark 1.39. The above corollary is generalized as follows:
Let $F \in K[\bar{X}] \setminus K$ and V be an irreducible component of $V(F)$. Then $\dim(V) = n - 1$. To prove it, one needs to know Krull's Principal Ideal Theorem (Hauptidealsatz).

To avoid usage of Theorem 1.35 in the case of curves, we can use Problem 1.11 below.

Problem 1.10: V is a point iff $\operatorname{trdeg}_K K(V) = 0$.

Problem 1.11: If $\operatorname{trdeg}_K K(V) = 1$, then V is a curve.

1.3. **The category of affine algebraic sets.** Let $V \subseteq \mathbb{A}^n$, $W \subseteq \mathbb{A}^m$ and $Z \subseteq \mathbb{A}^r$ be affine algebraic sets.

Definition 1.40. A function $\Phi : V \to W$ is a *morphism*, if there are $f_1, \ldots, f_m \in K[V]$ such that for each $v \in V$ we have

$$\Phi(v) = (f_1(v), \ldots, f_m(v)).$$

In other words, a morphism is a polynomial function. Note that the set of morphism from V to $\mathbb{A}^1$ is exactly $K[V]$.
It is easy to see that if $\Phi : V \to W$ and $\Psi : W \to Z$ are morphism, then $\Psi \circ \Phi : V \to Z$ is a morphism (the composition of polynomial functions is a polynomial function) and

such that id_V is a morphism. Therefore we obtain the *category of affine algebraic sets*. As in any category, a morphism $\Phi : V \to W$ is an *isomorphism*, if there is a morphism $\Psi : W \to V$ such that $\Psi \circ \Phi = \mathrm{id}_V$ and $\Phi \circ \Psi = \mathrm{id}_W$. If there is an isomorphism between V and W, then we write $V \cong W$. As usual we have:

- $V \cong V$;
- if $V \cong W$, then $W \cong V$;
- if $V \cong W$ and $W \cong Z$, then $V \cong Z$.

Example 1.41. We have noticed that parabola $V = V(Y - X^2)$ should be isomorphic to affine line. Let

$$\Phi : \mathbb{A}^1 \to V, \quad \Phi(x) = (x, x^2), \qquad \Psi : V \to \mathbb{A}^1, \quad \Psi(x, y) = x.$$

Then we have

$$\Psi(\Phi(x)) = \Psi(x, x^2) = x, \quad \Phi(\Psi(x, y)) = \Phi(x) = (x, x^2) = (x, y).$$

Therefore $V \cong \mathbb{A}^1$.

Example 1.42. We may be used to algebraic situations where a bijective homomorphism is an isomorphism. It is not the case here! For example, if $\mathrm{char}(K) = p > 0$, then

$$\mathrm{Fr} : \mathbb{A}^1 \to \mathbb{A}^1, \quad \mathrm{Fr}(x) = x^p.$$

The Frobenius morphism is bijective, but it is not an isomorphism, since there is no polynomial F such that $F(X^p) = X$. Later, we will also give an example in characteristic 0.

We will explain now the notion of morphism on the level of coordinate rings.

Definition 1.43. For a morphism $\Phi : V \to W$ let:

$$\Phi^* : K[W] \to K[V], \quad \Phi^*(f) = f \circ \Phi.$$

We know that the composition of morphisms is a morphism, so it is well defined. Note that we invert arrows which always brings some difficulties.
It is obvious that Φ^* is a K-algebra homomorphism, since for $v \in V$ and $f, g \in K[W]$ we have

$$\begin{aligned}[\Phi^*(f \cdot g)](v) &= (f \cdot g)(\Phi(v)) = f(\Phi(v)) \cdot g(\Phi(v)) \\ &= [(f \circ \Phi) \cdot (g \circ \Phi)](v) = (\Phi^*(f) \cdot \Phi^*(g))(v),\end{aligned}$$

and similarly for the addition and the scalar multiplication.

Proposition 1.44. (1) *If $\Psi : V \to W$ and $\Phi : W \to Z$ are morphism, then*

$$(\Phi \circ \Psi)^* = \Psi^* \circ \Phi^*, \quad (\mathrm{id}_V)^* = \mathrm{id}_{K[V]}.$$

(2) *The map $\Psi \mapsto \Psi^*$ is a bijection between the set of morphisms from V to W and the set of K-algebra homomorphisms from $K[W]$ to $K[V]$.*
(3) *For any finitely generated K-algebra R which is* reduced *(i.e. has no nilpotent elements), there is an affine algebraic set V such that $R \cong_K K[V]$.*

Proof. (1) is a very easy diagram chase.
For (2), let us notice first that *polynomial functions separate points*, i.e. by Problem 1.5, for any $w, w' \in W$, if $w \neq w'$ then there is $t \in K[W]$ such that $t(w) = 0, t(w') = 1$. Let us take two different morphisms $\Phi, \Psi : V \to W$. Then there is $v \in V$ such that $\Phi(v) \neq \Psi(v)$. Hence we find $t \in K[W]$ such that $t(\Phi(v)) = 0, t(\Psi(v)) = 1$, hence

$\Phi^*(t)(v) \neq \Psi^*(t)(v)$, so $\Phi^* \neq \Psi^*$.
Let us take a K-algebra homomorphism $\gamma : K[W] \to K[V]$. We have a morphism

$$\Psi : V \to \mathbb{A}^m, \quad \Psi = (\gamma(X_1|_W), \ldots, \gamma(X_m|_W)).$$

We will check that $\Psi(V) \subseteq W$ and $\gamma = \Psi^*$.
To show that $\Psi(V) \subseteq W$, it is enough to show that for any $F \in I(W)$, we have $F \circ \Psi = 0$. Since γ is a K-algebra homomorphism and the restriction map is a homomorphism we have:

$$\begin{aligned} F \circ \Psi &= F(\gamma(X_1|_W), \ldots, \gamma(X_m|_W)) \\ &= \gamma(F(X_1|_W, \ldots, X_m|_W)) \\ &= \gamma(F|_W) \\ &= 0. \end{aligned}$$

To show that $\gamma = \Psi^*$, we take $f \in K[W]$ and $F \in K[X_1, \ldots, X_m]$ such that $F|_W = f$. By computations as above, we have:

$$\begin{aligned} \Psi^*(f) &= f \circ \Psi \\ &= F \circ \Psi \\ &= \gamma(F|_W) \\ &= \gamma(f). \end{aligned}$$

For (3), let us take a finitely generated reduced K-algebra R. Then R is isomorphic to $K[X_1, \ldots, X_d]/I$ for some $d \in \mathbb{N}$ and $I \trianglelefteq K[X_1, \ldots, X_d]$. Since R is reduced, I is radical (Problem 2.1). By Hilbert's Nullstellensatz, $I = I(V(I))$, so $R \cong K[V(I)]$. □

The above proposition says that the category of affine algebraic sets is *antiequivalent* or *dually equivalent* to the category of finitely generated reduced K-algebras. In other words, these two categories are "the same" after inverting arrows.

Corollary 1.45. *If V, W are affine algebraic sets, then $V \cong W$ if and only if $K[V] \cong_K K[W]$.*

2. Affine varieties locally

In this section we will be interested in the local properties of an affine variety around a given point. Let $V \subseteq \mathbb{A}^n, W \subseteq \mathbb{A}^m, Y \subseteq \mathbb{A}^r$ be affine varieties.

2.1. **Rational maps.** We will first regard a rational function on a variety as an actual function.

Definition 2.1. Let $f \in K(V)$. We define the *domain* of f, denoted $\mathrm{dom}(f)$, as the set of points $v \in V$ such that there are $f_1, f_2 \in K[V]$ such that $f = f_1/f_2$ and $f_2(v) \neq 0$.

If $v \in \mathrm{dom}(f)$ and f_1, f_2 are as above, then we define $f(v)$ as $f_1(v)/f_2(v)$. Clearly the value $f(v)$ does not depend on the choice of representatives $f_1, f_2 \in K[V]$. So we have a function:

$$f : \mathrm{dom}(f) \to K.$$

Problem 2.2: $\mathrm{dom}(f)$ is (Zariski) open in V.

Definition 2.2. Let $f \in K(V)$ and $v \in V$. Then:

- f is *regular* at v, if $v \in \mathrm{dom}(f)$;
- $\mathcal{O}_{V,v} := \{f \in K(V) \mid v \in \mathrm{dom}(f)\}$;

- f is *regular*, if f is regular at each $v \in V$, i.e. if $\mathrm{dom}(f) = V$.

Example 2.3. Let $V = \mathbb{A}^1$ and $f = 1/X$. Then $\mathrm{dom}(f) = \mathbb{A}^1 \setminus \{0\}$.

For any $W \subseteq V$, let

$$I_V(W) := \{f \in K[V] \mid f|_W = 0\}.$$

Problem 2.3: For any $v \in V$, the ideal $I_V(v)$ $(= I_V(\{v\}))$ is maximal.

Before the next result (the description of $\mathcal{O}_{V,v}$) let us recall that a *local ring* is a ring with a unique maximal ideal. A ring is local if and only if the set of non-invertible elements is an ideal (necessarily the unique maximal ideal). For any domain R and prime ideal $P \trianglelefteq R$, the localization ring R_P is local with the maximal ideal

$$PR_P := \left\{\frac{a}{b} \in R_0 \mid a \in P, b \in R \setminus P\right\}.$$

We naturally identify R_P with the following subring of R_0:

$$\left\{\frac{a}{b} \in R_0 \mid a \in R,\ b \in R \setminus P\right\}.$$

For any multiplicative subset $S \subset R$, we consider R as a subring of R_S.

Fact 2.4. *For any $v \in V$, $\mathcal{O}_{V,v} = K[V]_{I_V(v)}$.*

Proof. This is just checking the definitions. For any $f \in K(V)$, we have $f \in K[V]_{I_V(v)}$ if and only if there are $a \in K[V], b \in K[V] \setminus I_V(v)$ such that $f = a/b$ which happens if and only if $v \in \mathrm{dom}(f)$. □

Definition 2.5. For $v \in V$, $\mathfrak{m}_{V,v}$ denotes the maximal ideal of $\mathcal{O}_{V,v}$.

By Fact 2.4, $\mathfrak{m}_{V,v} = I_V(v)K[V]_{I_V(v)}$.

The next result says that regular functions actually coincide with the polynomial ones.

Proposition 2.6. *Let $f \in K(V)$. Then f is regular if and only if $f \in K[V]$.*

Proof. Clearly, any $f \in K[V]$ is regular. Let $f \in K(V)$ be regular. By Fact 2.4, $f \in \bigcap_{v \in V} K[V]_{I_V(v)}$. However, by Proposition 1.30, the maximal ideals of $K[V]$ correspond to the minimal subvarieties of V, i.e. points, so every maximal ideal $\mathfrak{m} \trianglelefteq K[V]$ is of the form $I_V(v)$ for some $v \in V$. Therefore

$$f \in \bigcap_{\mathfrak{m} \underset{\max}{\trianglelefteq} K[V]} K[V]_{\mathfrak{m}}$$

However, by a known result in ring theory (Problem 2.4) this intersection coincides with $K[V]$. □

We know that any morphism $\Psi : V \to W$ induces a K-algebra homomorphism $\Psi^* : K[W] \to K[V]$ and we get a bijective correspondence. What happens on the level of fields of rational functions? Let us first look at an algebraic fact.

Problem 2.5: Let $\alpha : R_1 \to R_2$ be a homomorphism of domains and $S_1 \subset R_1, S_2 \subset R_2$ be multiplicative subsets. Then α extends to a homomorphism $\beta : (R_1)_{S_1} \to (R_2)_{S_2}$ if and only if $\alpha(S_1) \subseteq S_2$.

Hence $\Psi^* : K[W] \to K[V]$ extends to the fraction fields if and only if $\Psi^*(K[W] \setminus \{0\}) \subseteq K[V] \setminus \{0\}$ which happens if and only if Ψ^* is a monomorphism.

Lemma 2.7. *Let $\Psi : V \to W$ be a morphism. Then Ψ^* is a monomorphism if and only if Ψ is* dominant*, i.e. $\Psi(V)$ is Zariski dense in W.*

Proof. Assume that $\Psi(V)$ is Zariski dense in W and take $f \in K[W]$ such that

$$0 = \Psi^*(f) = f \circ \Psi.$$

This means that $\Psi(V) \subseteq V(F)$ for $F \in K[X_1, \ldots, X_m]$ such that $f = F|_W$. But $\Psi(V)$ is Zariski dense in W and $V(F)$ is Zariski closed, so $W \subseteq V(F)$, hence $0 = F|_W = f$. Assume that $\Psi(V)$ is not Zariski dense in W, so there is a proper Zariski closed $W_0 \subset W$ such that $\Psi(V) \subseteq W_0$. But then there is $F \in K[X_1, \ldots, X_m]$ such that $F|_{W_0} = 0$ and $f := F|_W \neq 0$. Since $F|_{W_0} = 0$ and $\Psi(V) \subseteq W_0$, we get $\Psi^*(f) = 0$, so Ψ^* is not a monomorphism. □

Notation 2.8. The notation $\Phi : V \twoheadrightarrow W$ means that Φ is a dominant morphism from V to W.

Remark 2.9. The notation $V \twoheadrightarrow W$ reminds the notation for an epimorphism (of group or rings). Actually, the dominant morphisms are exactly the epimorphisms in the category of affine algebraic sets and the above lemma is true for arbitrary algebraic sets.

We see that any dominant morphism $\Psi : V \to W$ induces a K-algebra homomorphism of fields $\Psi^* : K(W) \to K(V)$. Actually, Ψ need not to be a morphism to induce such a function.

Definition 2.10. Let $U \subseteq V$ be a non-empty open subset. A function $\Phi : U \to W$ is called a *rational function* between V and W if there are $f_1, \ldots, f_m \in K(V)$ such that

$$U = \operatorname{dom}(f_1) \cap \ldots \cap \operatorname{dom}(f_m),$$

and for all $v \in U$ we have

$$\Phi(v) = (f_1(v), \ldots, f_m(v)).$$

(Note that by Problem 1.12, if we have $U_1, \ldots, U_n$ non-empty subsets of V, then $U_1 \cap \ldots \cap U_n$ is non-empty.) A rational function Φ as above is *dominant*, if $\Phi(U)$ is Zariski dense in W.

Remark 2.11. Formally (and to assure that the statement in Proposition 2.14(2) is true) we need to define rational functions between V and W as equivalence classes of the following relation (on the set of rational functions as in Definition 2.10): $\Phi \sim \Psi$ if and only if there is a non-empty open subset U contained both in the domain of Φ and in the domain of Φ such that:

$$\Phi|_U = \Psi|_U.$$

We want now to compose rational functions. Let us see some examples first.

Example 2.12. Let $V = W = Y = \mathbb{A}^2$, Φ be a rational function between V and W, and Ψ be a rational function between W and Y.

(1) Let Φ be given by (X, X^2) (so it is even a morphism) and Ψ be given by $(0, 1/(Y - X^2))$. Then we can not compose Ψ and Φ, since the image of Ψ has the empty intersection with the domain of Φ.

(2) Let Φ be given by $(1/X, Y^2)$ and Ψ be given by arbitrary rational functions $(F_1/G_1, F_2/G_2)$ (so $G_1, G_2 \neq 0$). Then the following rational functions:

$$G_1\left(1/X, Y^2\right), G_2\left(1/X, Y^2\right)$$

are non-zero (e.g. since Φ is dominant), so we can define the rational function $\Psi \circ \Phi$ as

$$\left(\frac{F_1\left(1/X, Y^2\right)}{G_1\left(1/X, Y^2\right)}, \frac{F_2\left(1/X, Y^2\right)}{G_2\left(1/X, Y^2\right)}\right).$$

We can generalize the second example above to the case of arbitrary rational functions. Let Φ be a rational function between V and W which is dominant and Ψ be a rational function between W and Y. Let Φ be given by $(f_1, \ldots, f_m)$ where $f_1, \ldots, f_m \in K(V)$ and Φ be given by $(g_1, \ldots, g_r)$ where $g_1, \ldots, g_r \in K(W)$. Take $F_1, \ldots, F_r \in K[X_1, \ldots, X_r]$ and $G_1, \ldots, G_r \in K[X_1, \ldots, X_r]$ such that for each j we have $G_j|_W \neq 0$ and

$$g_j = \frac{F_j|_W}{G_j|_W}.$$

Define $\Phi \circ \Psi$ by the following sequence:

$$\left(\frac{F_1(f_1, \ldots, f_m)}{G_1(f_1, \ldots, f_m)}, \ldots, \frac{F_r(f_1, \ldots, f_m)}{G_r(f_1, \ldots, f_m)}\right).$$

As in Example 2.12(2), each $G_j(f_1, \ldots, f_m) \neq 0$, since $G_j|_W \neq 0$ and Φ is dominant. Hence we can compose such rational functions.
Note that $K(V)$ corresponds to rational functions from V to $\mathbb{A}^1$. If we have any $f \in K(W)$, then $f \circ \Psi$ is a rational function from V to $\mathbb{A}^1$ so an element of $K(V)$. Therefore we have a function:

$$\Psi^* : K(W) \to K(V), \quad \Psi^*(f) = f \circ \Psi.$$

We can check (as in the case of morphisms) that Ψ^* is a K-algebra homomorphism.

Notation 2.13. The notation $\Phi : V \dashrightarrow W$ means that Φ is a dominant rational function V to W.

We will state without a proof a result similar to Proposition 1.44 (the proof is similar as well).

Proposition 2.14. (1) *If $\Psi : V \dashrightarrow W$ and $\Phi : W \dashrightarrow Z$, then*

$$(\Phi \circ \Psi)^* = \Psi^* \circ \Phi^*, \quad (\mathrm{id}_V)^* = \mathrm{id}_{K(V)}.$$

(2) *The map $\Psi \mapsto \Psi^*$ is a bijection between the set of dominant rational functions from V to W and the set of K-algebra homomorphisms between $K(W)$ and $K(V)$.*
(3) *For any field extension $K \subseteq L$ such that L is finitely generated (as a field) over K, there is an affine variety V such that*

$$L \cong_K K(V).$$

The above proposition says that the category of affine varieties and dominant rational maps is *antiequivalent* or *dually equivalent* to the category of finitely generated field extensions of K.

2.2. **Smoothness.** We will give an algebraic definition of smoothness. First we need the notion of a partial derivative in a polynomial ring.

Definition 2.15. Let R be a ring and $\partial : R \to R$. The map ∂ is a *derivation* on R if for all $a, b \in R$ we have:

$$\partial(a + b) = \partial(a) + \partial(b), \quad \partial(ab) = b\partial(a) + a\partial(b).$$

Example 2.16. (1) For $R = C^\infty(\mathbb{R})$ we have the standard derivation $\partial = \frac{\partial}{\partial X}$ on R. As we know, we can identify $\mathbb{R}[X]$ with a subring of R and then $\partial|_{\mathbb{R}[X]}$ is a derivation on $\mathbb{R}[X]$.

(2) Let T be an arbitrary ring. We can define a derivation $\partial = \frac{\partial}{\partial X}$ on $T[X]$ by coping the formula for $\partial|_{\mathbb{R}[X]}$ from (1), i.e.

$$\partial(a_0 + a_1X + a_2X^2 + \ldots + a_mX^m) := a_1 + 2a_2X + \ldots + (m-1)a_{m-1}X^{m-1}.$$

It can be easily checked that ∂ is a derivation.

Remark 2.17. Note that if $\mathrm{char}(T) = p > 0$, then there are non-constant polynomials on which ∂ vanishes, e.g. $\partial(X^p) = 0$.

Definition 2.18. For each $i \in \{1, \ldots, n\}$, we have the derivation $\frac{\partial}{\partial X_i}$ on $K[\bar{X}]$ coming from the identification

$$K[\bar{X}] = K[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n][X_i].$$

Example 2.19. Let us consider again $V = V(Y^2 - X^3) \subseteq \mathbb{A}^2$. We intuitively know that $(0,0)$ is a (unique) *singular* point of V. How to see it algebraically? Consider the pair of polynomials

$$\left(\frac{\partial(Y^2 - X^3)}{\partial X}, \frac{\partial(Y^2 - X^3)}{\partial Y}\right) = (-3X^2, 2Y).$$

We can see that for $(a,b) \in V$, this pair of polynomials vanishes on (a,b) if and only if $(a,b) = (0,0)$.

One can wonder what does the condition from the example above has to do with smoothness. To explain this, we will go for a while into the world of differential geometry.

Example 2.20. Let $f : \mathbb{R}^2 \to \mathbb{R}$ be a C^1-function, $V := f^{-1}(0)$ and $(a,b) \in V$. If $\frac{\partial f}{\partial Y}(a,b) \neq 0$, then by the Implicit Function Theorem, there are open neighborhoods

$$a \in U_a \subseteq \mathbb{R}, \quad b \in U_b \subseteq \mathbb{R}$$

and a C^1-function $g : U_a \to U_b$ such that

$$U \cap V = \Gamma_g,$$

where $U = U_a \times U_b$ and Γ_g is the graph of g. Then $U \cap V$ is a *smooth submanifold* of $\mathbb{R}^2$ (as the graph of a smooth function), so (a,b) is a *smooth point* of V. By the Analytic Implicit Function Theorem, the above works for an analytic function $f : \mathbb{C}^2 \to \mathbb{C}$, in particular for polynomial functions. Hence for $V = V(Y^2 - X^3) \subseteq \mathbb{A}^2(\mathbb{C})$, we see that $(0,0)$ is the unique singular (i.e. non-smooth) point of V.

The above examples will motivate the definition of a smooth point on an affine variety. First, we need one more definition.

Definition 2.21. Let $F_1, \ldots, F_m \in K[\bar{X}]$. The *Jacobian matrix* of $\bar{F} = (F_1, \ldots, F_m)$ is

$$J_{\bar{F}} := \left(\frac{\partial F_i}{\partial X_j}\right)_{i,j} \in M_{m,n}(K[\bar{X}]).$$

If $v \in \mathbb{A}^n$, then $J_{\bar{F}}(v) \in M_{m,n}(K)$.

Problem 2.7: If $G_1, \ldots, G_k \in (F_1, \ldots, F_m)$ and $v \in V(F_1, \ldots, F_m)$, then the rows of $J_{\bar{G}}(v)$ are K-linear combinations of the rows of $J_{\bar{F}}(v)$.

Recall that for $A \in M_{m,n}(K)$ the *rank* of A, denoted $\mathrm{rk}(A)$, is the dimension of the image of A considered as a K-linear map $K^n \to K^m$. It coincides with the maximal number of independent rows of A (and also with the maximal number of independent columns of A).
From Problem 2.7 we immediately get the following fact.

Fact 2.22. *If* $(G_1, \dots, G_k) = I = (F_1, \dots, F_m) \trianglelefteq K[\bar{X}]$ *and* $v \in V(I)$*, then*

$$\mathrm{rk}(J_{\bar{G}}(v)) = \mathrm{rk}(J_{\bar{F}}(v)).$$

Therefore, the rank of such a Jacobian does not depend on the choice of generators.

Now we can finally state the main definition.

Definition 2.23. Let $V \subseteq \mathbb{A}^n$ be an algebraic set, $F_1, \dots, F_m \in I(V)$ be such that $I(V) = (F_1, \dots, F_m)$ and $a \in V$. Let $\bar{F}$ denote the tuple of polynomials $F_1, \dots, F_m$. We say that a is a *non-singular* or a *smooth* point of V if

$$\mathrm{rk}(J_{\bar{F}}(a)) = n - \dim(V).$$

We say that V is a *non-singular variety* or a *smooth variety*, if V is irreducible and all the points of V are smooth.

Note that by Fact 2.22, this definition makes sense, i.e. does not depend on the choice of $F_1, \dots, F_m$. To explain the equality used in the above definition, for a smooth $a \in V$, intuitively, "V around a should infinitesimally look like $J_{\bar{F}}(a)^{-1}(0)$" and we have

$$\dim(J_{\bar{F}}(a)^{-1}(0)) = n - \mathrm{rk}(J_{\bar{F}}(a)),$$

so the rank condition in the above definition makes sense. Also this definition coincides with Example 2.19 and we have the following generalization.

Example 2.24. Let $V = V(F)$ be a plane curve and $(t, s) \in V$. Then $\dim(V) = 1$, so (t, s) is smooth if and only if $\mathrm{rk}(J_F(t, s)) = 1$ which happens if and only if $\frac{\partial f}{\partial X}(t, s) \neq 0$ or $\frac{\partial f}{\partial Y}(t, s) \neq 0$.

Remark 2.25. Assume that $K = \mathbb{C}$ and $V \subseteq \mathbb{A}^n$ is a smooth affine variety. Then it can be proved that V is a complex analytic submanifold of $\mathbb{C}^n$. Thus the analytic and algebraic notions of smoothness coincide.

The following result is shown during the problem session. It allows to skip checking the irreducibility of polynomials.

Fact 2.26. *Let* $F \in K[X, Y]$ *and* $V = V(F) \subseteq \mathbb{A}^2$*. Then:*

1. *If* $F \notin K$*, then* V *is infinite.*
2. *If* $V(F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y})$ *is finite, then* $\sqrt{(F)} = (F)$ *and* $I(V) = (F)$*.*
3. *If* $V(F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y})$ *is empty, then* V *is smooth.*

We will prove a characterization of smoothness in terms of local rings which will be very important in the sequel. Before the statement let us notice that any ideals $I, J \trianglelefteq K[V]$ are also K-vector spaces and if $I \subseteq J$, the quotient J/I is a K-vector space as well (and also a $K[V]$-module). First we prove:

Proposition 2.27. *A point* $a \in V$ *is smooth if and only if*

$$\dim_K(I_V(a)/(I_V(a))^2) = \dim(V).$$

Proof. By applying the translation by a, we can assume that $a = 0 = (0, \dots, 0)$. Let us consider the following map:

$$\Psi : K[\bar{X}] \to K^n, \quad \Psi(F) := \left(\frac{\partial F}{\partial X_1}(0), \dots, \frac{\partial F}{\partial X_n}(0) \right).$$

It is clearly K-linear. Let $I := I(0) \trianglelefteq K[\bar{X}]$. It is easy to check that $\ker(\Psi) \cap I = I^2$ (do at home!). Let $\{e_1, \ldots, e_n\}$ be the standard basis of K^n and pick $i \in \{1, \ldots, n\}$. Then $\Psi(X_i) = e_i$, so $\Psi(I) = K^n$. Therefore

$$I/I^2 \cong K^n \tag{1}$$

(as K-vector spaces).
Let us take $F_1, \ldots, F_m \in I(V)$ such that $I(V) = (F_1, \ldots, F_m)$ and any $F = \sum \alpha_i F_i \in I(V)$. Since $0 \in V$, for each $j \in \{1, \ldots, n\}$ we get by Leibnitz's Rule:

$$\frac{\partial(\alpha_i F_i)}{\partial X_j}(0) = \alpha_i(0)\frac{\partial F_i}{\partial X_j}(0).$$

We obtain:

$$\Psi(F) = \Psi\left(\sum \alpha_i F_i\right) = \sum \alpha_i(0)\Psi(F_i).$$

Since for each i, $\Psi(F_i)$ is the i-th row of $J_{\bar{F}}(0)$, we get:

$$\mathrm{rk}(J_{\bar{F}}(0)) = \dim_K \Psi(I(V)). \tag{2}$$

By (1), we get $\Psi(I(V)) \cong (I(V) + I^2)/I^2$, so by (2) we have:

$$\mathrm{rk}(J_{\bar{F}}(0)) = \dim_K \left((I(V) + I^2)/I^2\right). \tag{3}$$

Consider now the restriction epimorphism $\pi : K[\bar{X}] \to K[V]$. Clearly $\ker(\pi) = I(V)$. We have:

$$I_V(0)/I_V(0)^2 \cong \pi^{-1}(I_V(0))/\pi^{-1}(I_V(0)^2).$$

But $\pi^{-1}(I_V(0)) = I$ and $\pi^{-1}(I_V(0)^2) = I^2 + I(V)$ (check at home!). Hence we get:

$$I_V(0)/I_V(0)^2 \cong I/(I^2 + I(V)) \cong \frac{I/I^2}{(I^2 + I(V))/I^2}. \tag{4}$$

By (1), (3) and (4) we get

$$n = \dim_K(I_V(0)/(I_V(0))^2) + \mathrm{rk}(J_{\bar{F}}(0)).$$

Therefore $\dim_K I_V(0)/(I_V(0))^2 = \dim(V)$ if and only if 0 is a smooth point of V. □

Our statement will follow from the above proposition and the following lemma.

Lemma 2.28. *If V is an affine variety and $a \in V$ then we have:*

$$I_V(a)/(I_V(a))^2 \cong_K \mathfrak{m}_{V,a}/(\mathfrak{m}_{V,a})^2.$$

Proof. Problem 3.3(c) says that for any domain R and any maximal ideal P, we have

$$P/P^2 \cong_{R/P} PR_P/(PR_P)^2.$$

In our case it is enough to take $R = K[V]$ and $P = I_V(a)$, since $\mathfrak{m}_{V,a} = I_V(a)K[V]_{I_V(a)}$ and $K[V]/I_V(a) \cong_K K$. □

Theorem 2.29. *If V is an affine variety and $a \in V$ then a is smooth if and only if*

$$\dim_K(\mathfrak{m}_{V,a}/(\mathfrak{m}_{V,a})^2) = \dim(V).$$

Proof. By Proposition 2.27 and Lemma 2.28. □

Remark 2.30. A Noetherian local ring $(R, \mathfrak{m})$ is called *regular*, if $\dim(R) = \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$. It can be show that for any $a \in V$, we have $\dim(\mathcal{O}_{V,a}) = \dim(V)$. Hence a is a smooth point if and only if $\mathcal{O}_{V,a}$ is regular, so regularity is the exact algebraic counterpart of smoothness.

Remark 2.31. The K-vector space $\mathfrak{m}_{V,a}/(\mathfrak{m}_{V,a})^2$ is called the *cotangent space* (of V at a) and the dual vector space is called the *tangent space* (of V at a). I will tell more about it later in the case of curves.

2.3. **Discrete valuation rings and multiplicities.** In this section we look closer at the local ring of a smooth point of a curve. First we need several algebraic notions.

Definition 2.32. A local ring $(R, \mathfrak{m})$ is a *discrete valuation ring* (DVR), if:

- R is a Noetherian domain,
- R is not a field,
- $\mathfrak{m}$ is principal.

We will need two theorems about local rings, which we leave without proof.

Theorem 2.33 (Nakayama's Lemma)**.** *Let $(R, \mathfrak{m})$ be a local ring and M a finitely generated R-module such that $\mathfrak{m}M = M$. Then $M = \{0\}$.*

Theorem 2.34. *Let $(R, \mathfrak{m})$ be a local Noetherian ring. Then*

$$\bigcap_{n=1}^{\infty} \mathfrak{m}^n = \{0\}.$$

Remark 2.35. Krull's Intersection Theorem is a vast generalization of the above intersection statement. It says that for any Noetherian domain R and any $I \trianglelefteq R$, if $I \neq R$ then

$$\bigcap_{n=1}^{\infty} I^n = \{0\}.$$

Theorem 2.36. *Any DVR is PID.*

Proof. Let $(R, \mathfrak{m})$ be DVR and take any non-zero $I \trianglelefteq R$. Let $t \in \mathfrak{m}$ such that $(t) = \mathfrak{m}$. For any $r \in R$ let

$$A_r := \{n \in \mathbb{N} \ : \ t^n | r\}.$$

If A_r is infinite, then $r \in \bigcap_{n=1}^{\infty} \mathfrak{m}^n$. By Theorem 2.34, $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = \{0\}$, so $r = 0$. Hence for any $r \in R \setminus \{0\}$, there is $n_r := \max(A_r)$. Let us take

$$n := \min\{n_r \mid r \in I \setminus \{0\}\}.$$

We will prove that $I = (t^n)$. Take any $r \in I$. If $r = 0$, then $r \in (t^n)$, so we may assume $r \neq 0$. Since $n_r \geqslant n$, t^n divides r, so $r \in (t^n)$. For the opposite inclusion, take $r \in I$ such that $n_r = n$. Then there is $u \in R$ such that $r = t^n u$. Since $n = n_r$, t does not divide u. Hence $u \in R \setminus \mathfrak{m} = R^*$. Therefore $(r) = (t^n)$, in particular $(t^n) \subseteq I$. □

Remark 2.37. By the proof of Theorem 2.36, if $(R, \mathfrak{m})$ is DVR, then any irreducible element (called here a *uniformizing parameter*) of R generates $\mathfrak{m}$.

Example 2.38. The ring $(K[\![X]\!], (X))$ is DVR and X is a uniformizing parameter.

Let R now be any UFD, $r \in R$ be irreducible (equivalently prime) and $L = R_0$ be the field of fractions of R. We define a function:

$$v_r : L^* \to \mathbb{Z}, \qquad v_r(\alpha) = n, \text{ where } \alpha = r^n \frac{a}{b}, \ a, b \in R, \ r \nmid a, \ r \nmid b.$$

The function v_r is called the *r-adic valuation* on L.

Example 2.39. If $p \in \mathbb{Z}$, then v_p is the (usual) p-adic valuation on $\mathbb{Q}$.

Fact 2.40. *Let R, r, L, v_r be as above. Then for all $\alpha, \beta \in L^*$ we have:*

(1) *if* $\alpha+\beta \in L^*$, *then* $v_r(\alpha+\beta) \geqslant \min\{v_r(\alpha), v_r(\beta)\}$,
(2) $v_r(\alpha\beta) = v_r(\alpha) + v_r(\beta)$,
(3) $v_r(L^*) = \mathbb{Z}$.

Proof. Let $\alpha = r^n \frac{a}{b}, \beta = r^m \frac{a'}{b'}$, where $a, b, a', b' \in R$, $r \nmid a, b, a', b'$ and (without loss of generality) $n \leqslant m$. Then

$$\alpha + \beta = r^n \left(\frac{a}{b} + r^{m-n} \frac{a'}{b'} \right) = r^n \frac{ab' + r^{m-n} a'b}{bb'}.$$

Since $r \nmid bb'$ and $r^{m-n} \in R$, we get that $v_r(\alpha+\beta) \geqslant n$ proving (1). The item (2) follows immediately from the definition of v_r. For (3), notice that for any $n \in \mathbb{Z}$, we have $v_r(r^n) = n$. □

Remark 2.41. Notice that for any irreducible $r, s \in R$, if $(r) = (s)$, then $v_r = v_s$.

Definition 2.42. Let L be a field. Any function $v : L^* \to \mathbb{Z}$ satisfying $(1) - (3)$ above is called a *discrete valuation* on L. We will skip the word "discrete" in the sequel. (In particular the r-adic valuation is a valuation.) For any valuation $v : L^* \to \mathbb{Z}$ we define:

- $\mathcal{O}_v := \{\alpha \in L^* \mid v(\alpha) \geqslant 0\} \cup \{0\}$ the *valuation ring* of v.
- $\mathfrak{m}_v := \{\alpha \in L^* \mid v(\alpha) > 0\} \cup \{0\}$ the *valuation ideal* of v.

Proposition 2.43. *Let L be a field and $v : L^* \to \mathbb{Z}$ be a* valuation *on L. Then $(\mathcal{O}_v, \mathfrak{m}_v)$ is DVR.*

Proof. From the definition of the valuation it is easy to check that $\mathcal{O}_v$ is a subring of L and that $\mathfrak{m}_v$ is an ideal of $\mathcal{O}_v$. Take any $\alpha \in \mathcal{O}_v \setminus \mathfrak{m}_v$. Then $v(\alpha) = 0$. Since $v : (L^*, \cdot) \to (\mathbb{Z}, +)$ is a group homomorphism, $v(\alpha^{-1}) = 0$, so $\alpha \in (\mathcal{O}_v)^*$. Thus $(\mathcal{O}_v, \mathfrak{m}_v)$ is a local ring. Since v is onto, $\mathfrak{m}_v \neq \{0\}$, so $\mathcal{O}_v$ is not a field. It is enough to check that $\mathcal{O}_v$ is PID. Clearly, $\mathcal{O}_v$ is a domain. Take any non-zero $I \trianglelefteq \mathcal{O}_v$ and $r \in I \setminus \{0\}$ with the minimal $v(r)$. Similarly as in the proof of Theorem 2.36, it can be checked that $I = (r)$. □

Proposition 2.44. *Let $(R, \mathfrak{m})$ be DVR and $r, s \in R$ be uniformizing parameters. Then $v_r = v_s$.*

Proof. By Remark 2.37, $(r) = \mathfrak{m} = (s)$. Hence $v_r = v_s$ (see Remark 2.41). □

We see that each DVR $(R, \mathfrak{m})$ gives a unique valuation v on $L = R_0$. How to describe this valuation? Theorem 2.34 says that

$$\bigcap_{n=1}^{\infty} \mathfrak{m}^n = \{0\}.$$

Hence for any $r \in R$, there is a unique $k \in \mathbb{N}$ such that $r \in \mathfrak{m}^k \setminus \mathfrak{m}^{k+1}$ (we take $\mathfrak{m}^0 = R$). Then (check at home!), $v(r) = k$. We give yet another characterization of the valuation given by a DVR.

Proposition 2.45. *Let $(R, \mathfrak{m})$ be DVR and $r \in R$. Assume that we have a ring extension $K \subseteq R$ such that the composition of the projection map $R \to R/\mathfrak{m}$ with the inclusion $K \subseteq R$ is the identity map* id_K. *Then we have:*

$$v(r) = \dim_{R/\mathfrak{m}}(R/(r)).$$

Proof. Note that $R/\mathfrak{m} = K$. Let a be a uniformizing parameter and $n = v(r)$. Then there is $u \in R^*$ such that $r = ua^n$. Hence $(r) = (a^n) = \mathfrak{m}^n$. We will show inductively that $\dim_{R/\mathfrak{m}}(R/\mathfrak{m}^n) = n$. It is clear for $n = 1$. Recall the notion of a *short exact sequence* of K-vector spaces: the following sequence of K-linear maps of K-vector spaces

$$0 \longrightarrow W \xrightarrow{\alpha} V \xrightarrow{\beta} Z \longrightarrow 0$$

is *exact*, if α is a monomorphism, β is an epimorphism and the kernel of β coincides with the image of α.
Problem 4.1: If a sequence as above is exact, then

$$\dim_K(V) = \dim_K(W) + \dim_K(Z).$$

For any $n \in \mathbb{N}$ we have a short exact sequence of K-vector spaces:

$$0 \to \mathfrak{m}^n/\mathfrak{m}^{n+1} \to R/\mathfrak{m}^{n+1} \to R/\mathfrak{m}^n \to 0.$$

Hence, it is enough (induction) to show that $\dim_{R/\mathfrak{m}}(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = 1$. If $\mathfrak{m}^n = \mathfrak{m}^{n+1}$, then (by Theorem 2.34) $\mathfrak{m}^n = \{0\}$ and $a^n = 0$, but R is a domain, so $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$. Using the assumption that the composition $K \subseteq R \to R/\mathfrak{m}$ coincides with the inclusion identity map, we get that $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is spanned by $a^n + \mathfrak{m}^{n+1}$. Therefore, we get $\dim_{R/\mathfrak{m}}(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = 1$ which we needed to show. □

Theorem 2.46. *Let C be an affine curve and $a \in C$. Then a is smooth if and only if $(\mathcal{O}_{C,a}, \mathfrak{m}_{C,a})$ is DVR.*

Before the proof we will recall.

Theorem 2.47 (a simple form of Nakayama's Lemma)**.** *Let $(R, \mathfrak{m})$ be a Noetherian local ring and $t_1, \ldots, t_m \in \mathfrak{m}$. Then $t_1, \ldots, t_m$ generate $\mathfrak{m}$ (as an ideal) if and only if $t_1 + \mathfrak{m}^2, \ldots, t_m + \mathfrak{m}^2$ generate $\mathfrak{m}/\mathfrak{m}^2$ (as an $R/\mathfrak{m}$-vector space).*

Note that the above statement follows from Nakayama's Lemma, if one takes

$$M := \mathfrak{m}/(t_1, \ldots, t_m).$$

Proof of Theorem 2.46. Since $K[C]$ is a Noetherian domain, any localization of it (as $\mathcal{O}_{C,a}$) is a Noetherian domain as well. Since $\mathfrak{m}_{C,a}$ is non-zero, $\mathcal{O}_{C,a}$ is not a field. By Theorem 2.29, a is smooth if and only

$$\dim_K(\mathfrak{m}_{C,a}/\mathfrak{m}_{C,a}^2) = 1.$$

By a simple form of Nakayama's Lemma above, the latter happens if and only if $\mathfrak{m}_{C,a}$ is principal, i.e. exactly when $(\mathcal{O}_{C,a}, \mathfrak{m}_{C,a})$ is DVR. □

Definition 2.48. Let C be an affine curve and $a \in C$ be a smooth point.

(1) Any uniformizing parameter $f \in \mathcal{O}_{C,a}$ is called a *local parameter* for C at a.
(2) The unique valuation on $K(C)$ given by the DVR $(\mathcal{O}_{C,a}, \mathfrak{m}_{C,a})$ (note that $K(C)$ is the fraction field of $\mathcal{O}_{C,a}$) is denoted ord_a.
(3) For $f \in K(C) \setminus \{0\}$ and $n \in \mathbb{N}_{>0}$:
   - if $\mathrm{ord}_a(f) = n$, we say that f *has a zero at a of order n*,
   - if $\mathrm{ord}_a(f) = -n$, we say that f *has a pole at a of order n*.

Problem 3.6: Let C be an affine curve, $a \in C$ be a smooth point and $f \in K(C)$. Then f is a local parameter for C at a if and only if f has a zero at a of order 1.

Example 2.49. Let $C = \mathbb{A}^1$ and take $0 \in C$. Then $K[C] = K[X]$, $K(C) = K(X)$ and $I_C(0) = (X)$. Therefore

$$\mathcal{O}_{C,0} = K[X]_{(X)} = \{F/G \mid F, G \in K[X],\ G(0) \neq 0\}.$$

The valuation ord_0 on $K(X)$ is clearly the X-adic valuation v_X. Then for any $\alpha = F/G \in K(X) \setminus \{0\}$ if F and G has no common prime divisors, then α has a zero at 0 of order n if and only if 0 is a root of F of multiplicity n. Thus the notion of order generalizes (from $\mathbb{A}^1$ to arbitrary affine curves) the notion of the multiplicity of a root. The rational function α has a pole at 0 of order n if and only if 0 is a root of G of multiplicity n.

Example 2.50. Let $C = V(Y^2 - X^3)$ and take $a = (0, 0) \in C$. We know that a is not a smooth point of C, we will see that $(\mathcal{O}_{C,a}, \mathfrak{m}_{C,a})$ is not DVR. Firstly, notice that

$$K[C] \cong K[X, Y]/(Y^2 - X^3) \cong K[X^2, X^3].$$

Then we have

$$\mathcal{O}_{C,a} = \{F/G \mid F, G \in K[X^2, X^3],\ G(a) \neq 0\}.$$
$$\mathfrak{m}_{C,a} = \{F/G \mid F, G \in K[X^2, X^3],\ G(a) \neq 0, F(a) = 0\}.$$

Then $\mathfrak{m}_{C,a} = (X^2, X^3)$, but it can be shown that $\mathfrak{m}_{C,a}$ is not principal. So $(\mathcal{O}_{C,a}, \mathfrak{m}_{C,a})$ is not DVR.

Let C be an affine curve, $a \in C$ a smooth point and $f \in K[C]$. By 2.45, we know that $\mathrm{ord}_a(f) = \dim_K(\mathcal{O}_{C,a}/f\mathcal{O}_{C,a})$. One can wonder what happens when we skip the localization and just compute $\dim_K(K[C]/fK[C])$. But if we take e.g. $C = \mathbb{A}^1$ and $f = F \in K[X]$, then we have

$$\dim_K(K[X]/(F)) = \deg(F),$$

which is not much related to the order of F at a point of $\mathbb{A}^1$. There is a relation though which we will explore in the sequel (it may be considered as a baby version of Bézout's Theorem):

$$\dim_K(K[X]/(F)) = \sum_{a \in V(F)} \mathrm{ord}_a(F).$$

Let us look at one more example.

Example 2.51. Consider two plane curves:

$$C_1 := V(Y), \quad C_2 := V(Y - X^3 - X^2)$$

and the point $0 \in C_1 \cap C_2$. It is easy to see that

$$\mathrm{ord}_0(Y|_{C_2}) = 2 = \mathrm{ord}_0((Y - X^3 - X^2)|_{C_1}).$$

Can this quantity be expressed in a way independent of the choice of the local ring $\mathcal{O}_{C_1,0}$ or $\mathcal{O}_{C_2,0}$? We need an algebraic fact.

Problem 4.2: Let R be a domain and $P \subseteq I \subseteq Q$ a chain of ideals of R such that P and Q are prime. Then we have:

$$\frac{R_Q}{IR_Q} \cong \frac{(R/P)_{Q/P}}{I/P(R/P)_{Q/P}}.$$

Applying to $R = K[X, Y]$, $P = (Y)$, $I = (Y, Y - X^3 - X^2)$, $Q = (X, Y)$ we get

$$\mathcal{O}_{C_1,0}/((Y - X^3 - X^2)|_{C_1}) \cong K[X, Y]_{(X,Y)}/(Y, Y - X^3 - X^2).$$

Similarly for R, Q, I as above and $P = (Y - X^3 - X^2)$ we get

$$\mathcal{O}_{C_2,0}/(Y|_{C_2}) \cong K[X,Y]_{(X,Y)}/(Y, Y - X^3 - X^2).$$

We will study the numbers of the form

$$\dim_K(K[X,Y]_{(X,Y)}/(Y, Y - X^3 - X^2)).$$

Let us fix $F, G \in K[X,Y]$ and $a = (x,y) \in \mathbb{A}^2$ and define

$$\mathcal{O} := K[X,Y]_{(X-x,Y-y)} = K[X,Y]_{I(a)} = \mathcal{O}_{\mathbb{A}^2,a}.$$

Definition 2.52. We define the *intersection number* of F and G at a as

$$I(a, F \cap G) := \dim_K(\mathcal{O}/(F,G)\mathcal{O}).$$

Before calculating intersection numbers we need several properties of them.

(1) It is easy to see that the intersection number $I(a, F \cap G)$ depends only on the ideals $(F), (G)$. Therefore for plane curves C_1, C_2 we can define the intersection number of C_1 and C_2 at a as

$$I(a, C_1 \cap C_2) := I(a, F \cap G)$$

for any F, G such that $(F) = I(C_1)$ and $(G) = I(C_2)$. It is important that in the general definition of the intersection number we can go beyond the case of affine curves (i.e. irreducible polynomials) to include also possible "multiplicities" of plane curves.

(2) Directly from the definition it follows that

$$I(a, F \cap G) = I(a, G \cap F).$$

(3) Since $(F,G)\mathcal{O} \neq \mathcal{O}$ if and only if $(F,G) \subseteq I(a)$ which happens if and only if $F(a) = 0 = G(a)$, we get

$$I(a, F \cap G) > 0 \quad \Leftrightarrow \quad a \in V(F,G).$$

(4) The notion of the intersection number is reasonable only if this number is finite. It is easy to find examples when it is not, e.g. $I(0, X \cap X) = \infty$. In this example the intersection (of $V(X)$ with $V(X)$) itself is infinite. It turns out it is always the reason of the infinite intersection number, since we have the following property.

$$|V(F,G)| < \infty \quad \Rightarrow \quad I(a, F \cap G) < \infty.$$

Proof. Let $V(F,G) = \{a_1, \ldots, a_k\}$, where $a = a_1$. By Hilbert's Nullstellensatz (and Chinese Remainder Theorem), we have the equality of ideals in $K[X,Y]$:

$$\sqrt{(F,G)} = I(\{a_1, \ldots, a_k\}) = I(a_1) \cap \ldots \cap I(a_k) = I(a_1) \cdot \ldots \cdot I(a_k).$$

By Problem 4.3, there is $m \in \mathbb{N}$ such that

$$(F,G) \supseteq (I(a_1) \cdot \ldots \cdot I(a_k))^m = I(a_1)^m \cdot \ldots \cdot I(a_k)^m.$$

Therefore there is an epimorphism:

$$R := \frac{\mathcal{O}}{(I(a_1)^m \ldots I(a_k)^m)\mathcal{O}} \to \frac{\mathcal{O}}{(F,G)\mathcal{O}},$$

so it is enough to show that $\dim_K(R)$ is finite. However, for all $i > 1$ we have $I(a_i)\mathcal{O} = \mathcal{O}$. Assume for convenience that $a_1 = (0,0)$. Then we have

$$\mathcal{O}/(I(a_1)^m \ldots I(a_k)^m)\mathcal{O} = \mathcal{O}/(I((0,0))^m)\mathcal{O} = \mathcal{O}/(I((0,0))\mathcal{O})^m.$$

Similarly, as in Problem 3.3(c) we have:

$$\mathcal{O}/(I((0,0))\mathcal{O})^m \cong K[X,Y]/(X,Y)^m$$

and it is easy to compute that

$$\dim_K(K[X,Y]/(X,Y)^m) = \frac{m(m+1)}{2} < \infty,$$

which finishes the proof. □

From now we will assume (explicitly or implicitly) that $V(F,G)$ is finite.

(5) If F is irreducible and $a \in V(F)$ is smooth then (see Example 2.51)

$$I(a, F \cap G) = \mathrm{ord}_a(G|_{V(F)}).$$

Proof. We have

$$I(a, F \cap G) = \dim_K(K[X,Y]_{I(a)}/(F,G)K[X,Y]_{I(a)}).$$

By 2.45, we have

$$\mathrm{ord}_a(G|_{V(F)}) = \dim_K(\mathcal{O}_{V(F),a}/G|_{V(F)}\mathcal{O}_{V(F),a}).$$

If we apply Problem 4.2 for $R = K[X,Y]$, $P = (F)$, $I = (F,G)$ and $Q = I(a)$ we get an isomorphism

$$K[X,Y]_{I(a)}/(F,G)K[X,Y]_{I(a)} \cong \mathcal{O}_{V(F),a}/G|_{V(F)}\mathcal{O}_{V(F),a},$$

similarly as in Example 2.51. □

Example 2.53. Let

$$L_X := V(Y), L_Y := V(X), C_1 := V(Y^2 - X^3), C_2 := V(Y - X^3).$$

Using Property (5) above we compute:

$$I(0, L_X \cap C_1) = \mathrm{ord}_0((Y^2 - X^3)|_{L_X}) = 3,$$
$$I(0, L_Y \cap C_1) = \mathrm{ord}_0((Y^2 - X^3)|_{L_Y}) = 2,$$
$$I(0, L_X \cap C_2) = \mathrm{ord}_0((Y - X^3)|_{L_X}) = 3,$$
$$I(0, L_Y \cap C_2) = \mathrm{ord}_0((Y - X^3)|_{L_Y}) = 1.$$

We see that in the examples above, a line is tangent to a curve if and only if the intersection number is greater than 1. We take it as the definition.

Definition 2.54. Let C be a plane curve and $a \in \mathbb{A}^2$.

- A subset $L \subseteq \mathbb{A}^2$ is called a *line* if there are $\alpha, \beta, \gamma \in K$ such that $L = V(\alpha X + \beta Y + \gamma)$ and $(\alpha, \beta) \neq (0,0)$.
- A line $L \subseteq \mathbb{A}^2$ is *tangent* to C at a if $I(a, L \cap C) > 1$.
- The *tangent space* to C at a, denoted T_aC, is the union of all the tangent lines to C at a.

Let us assume for simplicity that $a = 0 = (0,0) \in C$ and let $I(C) = (F)$.

Problem 4.4(a) $T_0(C) = V\left(\frac{\partial F}{\partial X}(0)X + \frac{\partial F}{\partial Y}(0)Y\right)$.

As promised, we are going to see now how to understand the K-vector space $\mathfrak{m}_{C,0}/(\mathfrak{m}_{C,0})^2$ as $(T_0C)^*$: the *cotangent space* to C at 0, i.e. the dual space to T_0C (that is the space of K-linear maps from T_0C to K).
We a have a K-bilinear map:

$$K^2 \times K[X,Y] \ni ((x,y), F) \mapsto \frac{\partial F}{\partial X}(0)x + \frac{\partial F}{\partial Y}(0)y \in K.$$

(The element $\frac{\partial F}{\partial X}(0)x+\frac{\partial F}{\partial Y}(0)y$ is actually the *directional derivative* of f along the vector (x,y) at 0.) By Problem 4.4(a), $T_0C \times I(C)$ is mapped to 0 hence we get a K-bilinear map:

$$T_0C \times K[C] \ni (h,f) \mapsto \Psi(h,f) \in K.$$

For any $F, G \in I(0)$ we have

$$\frac{\partial(FG)}{\partial X}(0) = 0, \quad \frac{\partial(FG)}{\partial Y}(0) = 0,$$

hence we get a K-bilinear map:

$$T_0C \times I_C(0)/(I_C(0))^2 \ni (h,f) \mapsto \Phi(h,f) \in K.$$

Problem 4.4(c) The last K-bilinear map is non-degenerate.

Therefore we get

$$(T_0C)^* \cong I_C(0)/(I_C(0))^2.$$

We recall now an isomorphism of K-vector spaces (Problem 3.3(c))

$$I_C(0)/(I_C(0))^2 \cong \mathfrak{m}_{C,0}/(\mathfrak{m}_{C,0})^2,$$

which finally gives our desired isomorphism

$$(T_0C)^* \cong \mathfrak{m}_{C,0}/(\mathfrak{m}_{C,0})^2.$$

Let $F, G, H \in K[X,Y]$. We will need more properties of the intersection numbers.

(6) $I(a, F \cap G) = I(a, F \cap (G + HF))$.

Proof. Clearly $(F,G) = (F, G+HF)$. □

(7) $I(a, F \cap GH) = I(a, F \cap G) + I(a, F \cap H)$.

Proof. We have a short exact sequence of K-vector spaces

$$0 \to (F,G)/(F,GH) \to \mathcal{O}/(F,GH) \to \mathcal{O}/(F,G) \to 0.$$

We will show that there is an isomorphism of K-vector spaces

$$\mathcal{O}/(F,H) \cong (F,G)/(F,GH),$$

which will be enough by Problem 4.1 and the definition of intersection number. For $z \in \mathcal{O}$ let $\bar{z}$ denote the coset of z in the appropriate quotient ring which will be clear from the context. We define

$$\alpha : \mathcal{O}/(F,H) \to (F,G)/(F,GH), \quad \alpha(\bar{z}) := \overline{zG}.$$

It is easy to check that α is well-defined and K-linear (do at home!). It is also onto, since for any $f, g \in \mathcal{O}$ we have clearly

$$fF + gG \equiv gG \mod (F, GH).$$

It remains to check (the most difficult part) that α is a monomorphism.
Take $z \in \mathcal{O}$ such that $\overline{Gz} = 0$. We aim to show that $\bar{z} = 0$, i.e. we need to find $b, d \in \mathcal{O}$ such that $z = bH + dF$. Since $\overline{Gz} = 0$, there are $u, v \in \mathcal{O}$ such that we have the following equality in the ring $\mathcal{O}$:

$$Gz = uF + vGH.$$

Take $S \in K[X,Y]$ such that $S(a) \neq 0$ and all the

$$A := Su, \ B := Sv, \ C := Sz$$

belong to $K[X,Y]$ (this is possible since $\mathcal{O} = K[X,Y]_{I(a)}$). Then we have an equality in the ring $K[X,Y]$:

$$AF = SuF = SGz - SvGH = G(C - BH).$$

Since $V(F,G)$ is finite, F and G have no common prime factors in $K[X,Y]$. But then F divides $C - BH$ in $K[X,Y]$, i.e. there is $D \in K[X,Y]$ such that $C - BH = DF$. Take finally

$$b := B/S \in \mathcal{O}, \quad d := D/S \in \mathcal{O}.$$

We have $z = bH + dF$ as we wanted. □

Example 2.55. We compute two intersection numbers:

$$\begin{aligned} I(0,(Y^2 - X^3) \cap (Y^2 - X^3 - X^2)) &= I(0,(Y^2 - X^3) \cap X^2) \\ &= 2I(0,(Y^2 - X^3) \cap X) \\ &= 4 \end{aligned}$$

$$\begin{aligned} & I(0,(Y^2 - X^3) \cap (Y^4 + X^4 - X^2)) \\ = \; & I(0,(Y^2 - X^3) \cap (Y^4 + X^4 - X^2 - Y^2(Y^2 - X^3))) \\ = \; & I(0,(Y^2 - X^3) \cap (X^4 - X^2 + Y^2X^3)) \\ = \; & I(0,(Y^2 - X^3) \cap X^2) + I(0,(Y^2 - X^3) \cap (X^2 - 1 + Y^2X)) \\ = \; & 2I(0,(Y^2 - X^3) \cap X) + 0 \\ = \; & 4 \end{aligned}$$

We usually consider the localization of a *domain* R with respect to a multiplicative subset S. Not much changes if we drop the domain assumption. One needs to be careful about the equivalence relation:

$$\frac{r_1}{s_1} = \frac{r_2}{s_2} \iff (\exists s_3 \in S)(s_3(s_1r_2 - s_2r_1) = 0).$$

The only difference is that the natural map $R \to R_S$ need not to be one-to-one, the kernel consists of elements $r \in R$ such that for some $s \in S$ we have $rs = 0$. Also a generalization of Problem 4.2 holds, where P can be taken as an arbitrary ideal.
We will need a lemma about such localizations. Recall that $e \in R$ is *idempotent*, if $e^2 = e$. If e is idempotent, then the ideal eR is a ring with the unity e.

Lemma 2.56. *Assume R is a ring, $P \trianglelefteq R$ is prime and $e \in R \setminus P$ is idempotent which is divisible by each element of $R \setminus P$. Then the natural map $\phi : R \to R_P$ induces an isomorphism of rings $eR \cong R_P$ (preserving the unit elements).*

Before the proof, let us see what happens when $e = 1$. Then the assumption says that any element of $R \setminus P$ divides 1, i.e. $R \setminus P = R^*$. But this exactly means that (R,P) is local, hence $R \to R_P$ is an isomorphism.

Proof of Lemma 2.56. Since $\phi(e) \in (R_P)^*$ ($e \in R \setminus P$) and $\phi(e)$ is idempotent, $\phi(e) = 1$. Thus the unit elements are preserved by $\phi|_{eR}$. Take any $r \in R$ and assume that $\phi(re) = 0$. Thus there is $s \in R \setminus P$ such that $res = 0$. But s divides e, so there is $s' \in R$ such that $ss' = e$. We have:

$$re = ree = ress' = 0.$$

Hence the kernel of $\phi|_{eR}$ is trivial.
Take any $f/g \in R_P$ and $g' \in R$ such that $gg' = e$. Then we have

$$\phi(efg') = \phi(e)\phi(fg') = \phi(fg') = \frac{fg'}{1} = \frac{f}{g},$$

so $\phi|_{eR}$ is onto. □

We will use this lemma to prove a generalization of the "baby version of Bézout's Theorem":

$$\dim_K(K[X]/(F)) = \sum_{a \in V(F)} \mathrm{ord}_a(F),$$

which will be very important in the proof of the actual Bézout's Theorem.

Proposition 2.57. *Assume that $V := V(F, G)$ is finite. Then:*

$$\dim_K(K[X, Y]/(F, G)) = \sum_{a \in V} I(a, F \cap G).$$

Proof. It will follow from a more general fact. Assume $I \trianglelefteq K[\bar{X}]$ is such that $V(I) = \{a_1, \ldots, a_m\}$ is finite. We will show

$$(*) \qquad K[\bar{X}]/I \cong_K K[\bar{X}]_{I(a_1)}/IK[\bar{X}]_{I(a_1)} \times \ldots \times K[\bar{X}]_{I(a_m)}/IK[\bar{X}]_{I(a_m)}$$

Note that:

$$I(a, F \cap G) := \dim_K(K[X, Y]_{I(a)}/(F, G)K[X, Y]_{I(a)}).$$

Hence indeed proving $(*)$ is enough (taking $I = (F, G)$ and $\bar{X} = (X, Y)$).
Let $R := K[\bar{X}]/I$ and $\mathfrak{m}_i := I(a_i)/I \trianglelefteq R$. Then (by the more general version of Problem 4.2 for $P = I$ and $Q = I(a_i)$) the right-hand side in $(*)$ is isomorphic to

$$R_{\mathfrak{m}_1} \times \ldots \times R_{\mathfrak{m}_m},$$

and we have to show that this product ring is isomorphic to R.
For each $i \in \{1, \ldots, m\}$, we will find an idempotent $e_i \in R$ such that $\sum e_i = 1$ and e_i satisfies Lemma 2.56 for $P = \mathfrak{m}_i$. It will be enough, since by a general result about product rings we have then:

$$R \cong e_1R \times \ldots \times e_mR.$$

and by Lemma 2.56, $e_iR \cong R_{\mathfrak{m}_i}$.
By Hilbert's Nullstellensatz, $\sqrt{I} = I(a_1) \ldots I(a_m)$ and by Problem 4.3, there is $d \in \mathbb{N}$ such that

$$I(a_1)^d \ldots I(a_m)^d \subseteq I.$$

For any i, take $F_i \in K[\bar{X}]$ such that $F_i(a_i) = 1$ and for $j \neq i$, $F_i(a_j) = 0$. We define

$$E_i := 1 - (1 - F_i^d)^d, \quad e_i := E_i + I.$$

This is a good choice, we skip a computational argument, which can be found on pages 56-57 of Fulton.
Add from lecture notes!! □

3. Projective varieties

Let us take $F, G \in K[X, Y]$. Bézout's theorem should say that if the number of the intersection points of $V(F)$ and $V(G)$ is finite, then this number (counted with multiplicities) equals the product of the degrees of F and G. Such a statement clearly fails inside $\mathbb{A}^2$, since two disjoint parallel lines do not intersect. Therefore we have to improve the ambient space $\mathbb{A}^2$. It turns out that we just need to make sure that all the lines intersect.

3.1. **Projective space.** The projective plane should coincide with the affine plane expanded by the set of extra points where parallel lines would intersect. We call them "points at infinity". We just add one such a point for each equivalence class of parallel lines. Clearly, each such a class has a natural representative: the line going through zero. Thus our first approximation of projective plane is affine plane enlarged with the set of all 1-dimensional K-linear subspaces of K^2.

Definition 3.1. Let $n \in \mathbb{N}$. *Projective n-th space* over K, denoted $\mathbb{P}^n(K)$ or $\mathbb{P}^n$, is defined as the set of all 1-dimensional K-subspaces (i.e. lines passing through zero) of K^{n+1}.

We will see that for $n = 2$ this definition coincides with the intuitive description above. We need to check whether "$\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$", since the points at infinity correspond now exactly to $\mathbb{P}^1$. To do that we need to understand how to consider $\mathbb{A}^2$ as a subset of $\mathbb{P}^2$ and $\mathbb{P}^1$ as a subset of $\mathbb{P}^2$. Let $L \in \mathbb{P}^n$. For each $a \in L \setminus \{0\}$, we have $L = \operatorname{span}_K(a)$. For any $(a_1, \ldots, a_{n+1}) \in \mathbb{A}^{n+1} \setminus \{(0, \ldots, 0)\}$ we define:

$$[a_1 : \ldots : a_{n+1}] := \operatorname{span}_K\{(a_1, \ldots, a_{n+1})\} \in \mathbb{P}^n.$$

If $x = [a_1 : \ldots : a_{n+1}] \in \mathbb{P}^n$, then $a_1, \ldots, a_{n+1}$ are called the *projective* or *homogenous* coordinates of x. For any

$$(a_1, \ldots, a_{n+1}), (b_1, \ldots, b_{n+1}) \in \mathbb{A}^{n+1} \setminus \{(0, \ldots, 0)\},$$

we clearly have

$$(*) \qquad [a_1 : \ldots : a_{n+1}] = [b_1 : \ldots : b_{n+1}] \;\Leftrightarrow\; \exists \lambda \in K \; \forall i \leqslant n+1 \; \lambda a_i = b_i$$

Let $i \in \{1, \ldots, n+1\}$. We define:

$$\psi_i : \mathbb{A}^n \to \mathbb{P}^n, \quad \psi_i(a_1, \ldots, a_n) := [a_1 : \ldots : a_{i-1} : 1 : a_i : \ldots : a_n].$$

Let $U_i \subseteq \mathbb{P}^n$ denote the image of ψ_i. By $(*)$ we have:

$$U_i = \{[a_1 : \ldots : a_{n+1}] \in \mathbb{P}^n \mid a_i = 1\} = \{[a_1 : \ldots : a_{n+1}] \in \mathbb{P}^n \mid a_i \neq 0\}.$$

Again by $(*)$, ψ_i is a bijection between $\mathbb{A}^n$ and U_i, allowing us to regard $\mathbb{A}^n$ as a subset of $\mathbb{P}^n$.
For $n > 0$, we have also a one-to-one function

$$\pi_i : \mathbb{P}^{n-1} \to \mathbb{P}^n, \quad \pi_i([a_1 : \ldots : a_n]) := [a_1 : \ldots : a_{i-1} : 0 : a_i : \ldots : a_n]$$

(note that by $(*)$, π_i is well defined and indeed one-to-one). It is easy to see that

$$\pi_i(\mathbb{P}^{n-1}) = \mathbb{P}^n \setminus U_i,$$

hence we get our desired equality "$\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}$".
We usually concentrate on $i = n + 1$ and write $\mathbb{A}^n \subset \mathbb{P}^n$ identifying $\mathbb{A}^n$ with U_{n+1}. Using this convention, for $W \subseteq \mathbb{P}^n$ we often write $W \cap \mathbb{A}^n$ and denote

$$H_\infty := \pi_{n+1}(\mathbb{P}^{n-1}) \subset \mathbb{P}^n$$

(the "hyperplane at infinity").

Example 3.2. (1) $\mathbb{P}^0$ is just a point.
(2) $\mathbb{P}^1 = \{[x:1] \mid x \in K\} \cup \{[1:0]\}$ and $H_\infty = \{[1:0]\}$ (just one point at infinity).
(3) $\mathbb{P}^2 = \{[x:y:1] \mid x \in K\} \cup \{[x:y:0] \mid (x,y) \in \mathbb{A}^2 \setminus \{0\}\}$ (the projective line at infinity).

Remark 3.3. We know that $\mathbb{P}^1 = U_1 \cup U_2$, and that

$$\psi_1 : \mathbb{A}^1 \to U_1, \quad \psi_2 : \mathbb{A}^1 \to U_2$$

are bijections. Hence $\mathbb{P}^1$ may be understood as two copies of $\mathbb{A}^1$ "glued" along certain subsets of $\mathbb{A}^1$. Let us first see these subsets and then the gluing map.
These subsets are $\psi_i^{-1}(U_1 \cap U_2)$ for $i = 1, 2$. Clearly

$$U_1 \cap U_2 = \{[a:b] \in \mathbb{P}^1 \mid a \neq 0, b \neq 0\}.$$

Then we have

$$\psi_1^{-1}(U_1 \cap U_2) = \mathbb{A}^1 \setminus \{0\} = \psi_2^{-1}(U_1 \cap U_2).$$

For $a, b \in \mathbb{A}^1 \setminus \{0\}$, we "glue" a with b if and only if $\psi_1(a) = \psi_2(b)$. The latter happens if and only if $[1:a] = [b:1]$, which is equivalent (by the formula $(*)$ above) to $b = a^{-1}$. Therefore, $\mathbb{P}^1$ may be understood as two copies of $\mathbb{A}^1$ "glued" along $\mathbb{A}^1 \setminus \{0\}$ and the gluing map is

$$\mathbb{A}^1 \setminus \{0\} \ni a \mapsto a^{-1} \in \mathbb{A}^1 \setminus \{0\}.$$

Note that this map is a rational map on $\mathbb{A}^1$.
In a similar way, $\mathbb{P}^n$ may be understood as $n+1$ copies of $\mathbb{A}^n$ glued along certain open subsets of $\mathbb{A}^n$ using certain rational maps on $\mathbb{A}^n$. Such a gluing process leads to the general definition of an *algebraic variety*, but we do not go into this direction here.

We want to do algebraic geometry inside projective space in a similar way as we were doing it inside affine space. In particular, we need the notion of a projective algebraic set. The problem is that for $x \in \mathbb{P}^n$ and $F \in K[X_1, \ldots, X_{n+1}]$, we can not apply F to x in a meaningful way. We need to consider a special type of polynomials.

Definition 3.4. Let $d, k, d_1, \ldots, d_k \in \mathbb{N}, a \in K$ and $H \in K[X_1, \ldots, X_k]$.

- If $H = aX_1^{d_1} \cdot \ldots \cdot X_k^{d_k}$ is a monomial, then the *degree* of H is $d_1 + \ldots + d_k$.
- We call H a *homogenous polynomial of degree* d if H is a sum of monomials of degree d.

Problem 5.3: A non-zero polynomial H is homogenous of degree d if and only if for all $\lambda \in K$ we have

$$H(\lambda X_1, \ldots, \lambda X_k) = \lambda^d H$$

(equality of polynomials).

By Problem 5.3, if $F \in K[X_1, \ldots, X_{n+1}]$ is a homogenous polynomial of degree d, then for any $a \in \mathbb{A}^{n+1}$ and $\lambda \in K$ we have $F(\lambda a) = \lambda^d F(a)$. We still can not apply F to $x \in \mathbb{P}^n$, but we can at least define what does it mean "$F(x) = 0$", since $F(a) = 0$ if and only if for any $\lambda \in K \setminus \{0\}$, we have $F(\lambda a) = 0$.

Definition 3.5. A subset $V \subseteq \mathbb{P}^n$ is called a *projective algebraic set*, if there are homogenous polynomials $F_1, \ldots, F_k \in K[X_1, \ldots, X_{n+1}]$ such that

$$V = \{x \in \mathbb{P}^n \mid F_1(x) = 0, \ldots, F_k(x) = 0\}.$$

Definition 3.6. A subset $V \subseteq \mathbb{P}^2$ is called a *line in* $\mathbb{P}^2$ if there is $(\alpha, \beta, \gamma) \in K^3 \setminus \{(0,0,0)\}$ such that

$$V = \{[a : b : c] \in \mathbb{P}^2 \mid \alpha a + \beta b + \gamma c = 0\}.$$

Problem 5.2: Any two lines in $\mathbb{P}^2$ have non-empty intersection.

Example 3.7. Let $V = V(F) \subseteq \mathbb{A}^2$, where $F = Y^2 - X^3 - X$. Let us consider the homogenous polynomial $F^* = Y^2Z - X^3 - XZ^2$ and the projective algebraic set

$$V^* := \{x \in \mathbb{P}^2 \mid F^*(x) = 0\}.$$

It is easy to see that for any $a \in \mathbb{A}^2$, we have $a \in V$ if and only if $\psi_3(a) \in V^*$. Therefore we have (recall our convention):

$$V = V^* \cap \mathbb{A}^2.$$

Let us see the "points at infinity" of V, i.e. the intersection of V^* with the line at infinity H_∞. For any $x \in H_\infty$, we have $F^*(x) = 0$ if and only if $x = [0 : 1 : 0]$. Therefore

$$V^* = V \cup \{[0 : 1 : 0]\},$$

and $[0 : 1 : 0]$ is the unique point at infinity of V.

For any $F \in K[X_1, \ldots, X_n]$, we want to find an appropriate homogenous polynomial $F^* \in K[X_1, \ldots, X_{n+1}]$ as in the example above. Intuitively, we need to make F homogenous using the variable X_{n+1} in the most economic way. There is a unique $d \in \mathbb{N}$ and unique $F_0, \ldots, F_d \in K[X_1, \ldots, X_n]$ such that $F = F_0 + \ldots + F_d$, $F_d \neq 0$ and for each $i \leqslant d$, F_i is a homogenous polynomial of degree i or $F_i = 0$. Define

$$F^* := \sum_{i=0}^{d} X_{n+1}^{d-i} F_i.$$

Clearly, F^* is a homogenous polynomial of degree d called the *homogenization* of F (with respect to X_{n+1}).

Problem 5.4: For F and d as above, we have:

$$F^* = X_{n+1}^d F\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right).$$

Note that we can homogenize F with respect to any variable, the simplest way is to change a bit the formula from Problem 5.4. The *homogenization* of F with respect to X_i is

$$X_i^d F\left(\frac{X_1}{X_i}, \ldots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \ldots, \frac{X_{n+1}}{X_i}\right).$$

Let us fix $n \in \mathbb{N}$ and $i \in \{1, \ldots, n+1\}$. We list several facts without proofs:

(1) Projective algebraic subsets of $\mathbb{P}^n$ are closed sets of certain topology on $\mathbb{P}^n$ called again the *Zariski topology*.
(2) The set $\mathbb{P}^n$ together with the Zariski topology is again a Noetherian topological space. By the general definitions and results about Noetherian topological spaces from Section 1, we get the notions of dimension of projective algebraic set and irreducible components of projective algebraic sets.

(3) Take any homogenous polynomials $F_1, \ldots, F_k \in K[X_1, \ldots, X_{n+1}]$ and let
$$V := \{x \in \mathbb{P}^n \mid F_1(x) = 0, \ldots, F_k(x) = 0\}.$$
Then we have:
$$\psi_i^{-1}(V) = V(F_1|_{X_i=1}, \ldots, F_k|_{X_i=1}),$$
where for any $H \in K[X_1, \ldots, X_{n+1}]$, we define $H|_{X_i=1}$ as the polynomial in n variables obtained from H by plugging $X_i = 1$. Such a polynomial is called the *dehomogenization* of H with respect to X_i.
In particular, the set $\psi^{-1}(V)$ is Zariski closed in $\mathbb{A}^n$, hence the function ψ_i is continuous.

(4) Take any $H_1, \ldots, H_l \in K[X_1, \ldots, X_n]$ and let
$$W = V(H_1, \ldots, H_l) \subseteq \mathbb{A}^n.$$
For each $j \leqslant l$, let $\widetilde{H}_j$ be the homogenization of H_j with respect to X_i and define:
$$V := \{x \in \mathbb{P}^n \mid \widetilde{H}_1(x) = 0, \ldots, \widetilde{H}_l(x) = 0\}.$$
If $i = n + 1$, then we denote V by W^* and call $W^* \cap H_\infty$ the set of *points at infinity* of W. We have
$$V \cap U_i = \psi_i(W)$$
In particular (using also (3) above), ψ_i is a homeomorphism between $\mathbb{A}^n$ and U_i. Thus $\mathbb{P}^n$ has an open cover of $n+1$ sets such that each such set is homeomorphic to $\mathbb{A}^n$.

(5) Assume $V \subseteq \mathbb{A}^n$ is Zariski closed. We have:
- V^* coincides with the Zariski closure of V in $\mathbb{P}^n$;
- $\dim(V) = \dim(V^*)$;
- V is irreducible if and only if V^* is irreducible (Problem 1.2).

(6) If $W \subseteq \mathbb{P}^n$ is an irreducible projective algebraic set and $W \cap U_i$ is non-empty, then W coincides with the Zariski closure of $W \cap U_i$ in $\mathbb{P}^n$.

Example 3.8. Consider the *projective Fermat curve*
$$V := \left\{[a : b : c] \in \mathbb{P}^2 \mid a^3 + b^3 + c^3 = 0\right\},$$
and let $F := X^3 + Y^3 + Z^3$. Then $V \cap \mathbb{A}^2$ (remember our convention!) is given by the dehomogenization of F with respect to Z (see (3) above), i.e.
$$V \cap \mathbb{A}^2 = V(X^3 + Y^3 + 1) \subseteq \mathbb{A}^2.$$

Definition 3.9.
- A *projective variety* is an irreducible projective algebraic set.
- A *projective curve* is a projective variety of dimension 1.
- A *projective plane curve* is a projective curve, which is a subset of $\mathbb{P}^2$.

Remark 3.10. Let V be a projective plane curve. It can be shown that
- There is an irreducible homogenous polynomial $F \in K[X, Y, Z]$ such that
$$V = \{x \in \mathbb{P}^2 \mid F(x) = 0\}.$$
- For any F_1, F_2 as above (i.e. giving the same projective plane curve V), there is $\lambda \in K \setminus \{0\}$ such that $F_2 = \lambda F_1$.

Hence we can define the *degree* of V as the degree of F as above.

Definition 3.11. Let $V \subseteq \mathbb{P}^n$ be a projective variety and $x \in V$.

- The point x is a *smooth* point of V, if there is $i \leqslant n+1$ such that $x \in U_i$ and $\psi_i^{-1}(x)$ is a smooth point of the affine variety $\psi_i^{-1}(V)$.
- The point x is a *singular* point of V, if v is not a smooth point of V.
- The projective variety V is *smooth* if for all $x \in V$, x is a smooth point of V.

Remark 3.12. It can be shown that in the above definition "there is i" can be replaced with "for all i".
There is also an equivalent definition of smoothness not using the embeddings ψ_i, but an appropriately defined local ring $\mathcal{O}_{V,x}$.

Example 3.13. Let $W = V(Y - X^2) \subseteq \mathbb{A}^2$. We will check whether W^* is smooth. Since W is smooth, it is enough to check whether the points at infinity of W are smooth, i.e. whether "W is smooth at infinity". Let us take $[a : b : 0] \in H_\infty$, a point at infinity of $\mathbb{A}^2$. We will check when $[a : b : 0]$ is a point at infinity of W.
The homogenization of $Y - X^2$ is $YZ - X^2$, so $[a : b : 0]$ is a point at infinity of W if and only if

$$b \cdot 0 - a^2 = 0.$$

Thus $[0 : 1 : 0]$ is a unique point at infinity of W. Clearly $[0 : 1 : 0] \in U_2$. To see whether $[0 : 1 : 0]$ is a smooth point of W^*, we should check whether $\psi_2^{-1}([0 : 1 : 0])$ is a smooth point of the affine variety $\psi_2^{-1}(W^*)$. Clearly, $\psi_2^{-1}([0 : 1 : 0]) = (0, 0)$. By the property (4) above, $\psi_2^{-1}(W^*)$ is the set of zeroes of the dehomogenization of $YZ - X^2$ with respect to Y (the second variable). Hence

$$\psi_2^{-1}(W^*) = V(Z - X^2) \subseteq \mathbb{A}^2.$$

We get a parabola again which is smooth, so $[0 : 1 : 0]$ is a smooth point of W^*, and W^* is smooth (i.e. W is "smooth at infinity").

Example 3.14. Let $W = V(Y - X^3) \subseteq \mathbb{A}^2$. We will check whether W^* is smooth. Again, since W is smooth, we just need to check whether W is smooth at infinity. The homogenization of $Y - X^3$ is $YZ^2 - X^3$. By a similar computation as in the previous example, $[0 : 1 : 0]$ is a unique point at infinity of W. Again, $\psi_2^{-1}([0 : 1 : 0]) = (0, 0)$ and $\psi_2^{-1}(W^*)$ is the set of zeroes of the dehomogenization of $YZ^2 - X^3$ with respect to Y. Hence

$$\psi_2^{-1}(W^*) = V(Z^2 - X^3).$$

However, we know that $(0, 0)$ is a singular point of $V(Z^2 - X^3)$, hence W is not smooth at infinity (W is singular at infinity).

3.2. **Bézout's Theorem.** We need to define the intersection number of two "curves with possible multiplicities" in $\mathbb{P}^2$. As in the affine case, we will define the intersection number of two polynomials (in this case homogenous ones) at a point of projective plane.

Definition 3.15. Let $x \in \mathbb{P}^2$ and $F, H, G \in K[X_1, X_2, X_3]$ be homogenous polynomials.

- Let $i \in \{1, 2, 3\}$ be such that $x \in U_i$. We define the *intersection number* as
$$I(x, F \cap H) := I(\psi_i^{-1}(x), (F|_{X_i=1}) \cap (H|_{X_i=1})).$$
- If F and H are irreducible and $V, W \subset \mathbb{P}^2$ are projective plane curves such that
$$V = \{x \in \mathbb{P}^2 \mid F(x) = 0\}, \quad W = \{x \in \mathbb{P}^2 \mid H(x) = 0\},$$
then we define:
$$I(x, V \cap G) := I(x, F \cap G).$$
$$I(x, V \cap W) := I(x, F \cap H).$$

Remark 3.16. It can (and should) be shown that the above definition does not depend on the choice of i. By Remark 3.10, the second part does not depend on the choice of F and H.

Example 3.17. Consider affine plane curves

$$C_1 := V(Y^2 - X^3), \quad C_2 := V(Y - X^3).$$

We will find all the intersection points of C_1^* and C_2^* and count their multiplicities. We start with the intersection points of C_1 and C_2. Since C_2 is smooth, for any $x \in C_2$ we have

$$I(x, C_1 \cap C_2) = \mathrm{ord}_x((Y^2 - X^3)|_{C_2}).$$

We know that $K[C_2] \cong K[X]$ and under this isomorphism we have:

$$(Y^2 - X^3)|_{C_2} \mapsto (X^3)^2 - X^3 = X^3(X^3 - 1).$$

Hence (we know it already) $I((0,0), C_1 \cap C_2) = 3$. To compute the other intersection points, we need to consider two cases.

Case 1 $\mathrm{char}(K) \neq 3$
Since $\mathrm{char}(K) \neq 3$ and K is algebraically closed, there is a primitive third root of unity in K, let us call it ε. Then we have

$$X^3(X^3 - 1) = X^3(X - 1)(X - \varepsilon)(X - \varepsilon^2)$$

and

$$C_1 \cap C_2 = \{(0,0), (1,1), (\varepsilon, 1), (\varepsilon^2, 1)\}.$$

Since

$$\mathcal{O}_{C_2,(1,1)} \cong K[X]_{(X-1)}, \quad \mathcal{O}_{C_2,(\varepsilon,1)} \cong K[X]_{(X-\varepsilon)}, \quad \mathcal{O}_{C_2,(\varepsilon^2,1)} \cong K[X]_{(X-\varepsilon^2)}$$

we get

$$I((1,1), C_1 \cap C_2) = 1, \quad I((\varepsilon, 1), C_1 \cap C_2) = 1, \quad I((\varepsilon^2, 1), C_1 \cap C_2) = 1.$$

Case 2 $\mathrm{char}(K) = 3$
We have

$$X^3(X^3 - 1) = X^3(X - 1)^3, \quad C_1 \cap C_2 = \{(0,0), (1,1)\}.$$

Therefore we get

$$I((1,1), C_1 \cap C_2) = 3.$$

Let us look now at the intersection points at infinity. The homogenizations of our polynomials are

$$Y^2Z - X^3, \quad YZ^2 - X^3.$$

Looking at their projective zero sets, we see that:

$$C_1^* = C_1 \cup \{[0:1:0]\}, \quad C_2^* = C_2 \cup \{[0:1:0]\}.$$

To compute $I([0:1:0], C_1^* \cap C_2^*)$, we need to take the dehomogenizations with respect to Y: $Z - X^3, Z^2 - X^3$. Quite accidentally, this homogenization/dehomogenization process switches the polynomials and we get:

$$I([0:1:0], C_1^* \cap C_2^*) = I((0,0), (Z - X^3) \cap (Z^2 - X^3)) = 3.$$

The total number of intersection points (counted with multiplicities) in the above example is 9 regardless of the characteristic of K. Note that 9 is the product of the degrees of the curves. Bézout's theorem is a generalization of this observation.

Theorem 3.18. *Let $F, H \in K[X, Y, Z]$ be homogenous polynomials such that the set*

$$V := \{x \in \mathbb{P}^2 \mid F(x) = 0,\ H(x) = 0\}$$

is finite. Then we have:

$$\sum_{x \in V} I(x, F \cap H) = \deg(F) \cdot \deg(H).$$

We do not have enough time to give the full proof of Bézout's Theorem.

Outline of the proof. Steps 1 and 2 reduce the problem to the affine case. Step 3 is the most difficult one.

Step 1 There is a line L in $\mathbb{P}^2$ such that $L \cap V = \emptyset$.

Let

$$V = \{[a_1 : b_1 : c_1], \ldots, [a_m : b_m : c_m]\}.$$

We are looking for $(\alpha, \beta, \gamma) \in K^3 \setminus \{0\}$ such that for all $i \leqslant m$ we have

$$\alpha a_i + \beta b_i + \gamma c_i \neq 0.$$

Let L_i be the line in $\mathbb{P}^2$ given by (a_1, b_1, c_1). In other words, we are looking for

$$[\alpha : \beta : \gamma] \in \mathbb{P}^2 \setminus (L_1 \cup \ldots \cup L_m),$$

i.e. we want to show that $\mathbb{P}^2 \neq L_1 \cup \ldots \cup L_m$. Assume that $\mathbb{P}^2 = L_1 \cup \ldots \cup L_m$ and we will reach a contradiction. It is easy to see that the intersection with of a line in $\mathbb{P}^2$ with any $\mathbb{A}^2$ (remember our convention again!) is a line in $\mathbb{A}^2$, so we get that $\mathbb{A}^2$ is a finite finite union of lines. This is impossible over an infinite field (find an argument!).

Step 2 Without loss of generality we may assume $L = H_\infty$.

Let L be the line from Step 1. We need to apply an appropriate "projective change of coordinates" to move L to the line at infinity H_∞. The group $\mathrm{GL}_3(K)$ acts on K^3 mapping lines to lines, so this action induces an action on $\mathbb{P}^2$. Since $\mathrm{GL}_3(K)$ acts transitively on planes (i.e. 2-dimensional subspaces) in K^3, it acts transitively on lines in $\mathbb{P}^2$. In particular, there is $\phi \in \mathrm{GL}_3(K)$ such that $\phi(L) = H_\infty$. Now we need to believe that this action ("projective change of coordinates") does not change the intersection numbers.

Step 3 The proof is reduced to showing the following property of affine plane curves (with possible multiplicities):

Let $F_*, H_* \in K[X, Y]$ be the dehomogenizations of F, H with respect to Z. By Step 2, $V(F_*)$ and $V(H_*)$ have no common points at infinity. Then:

$$\sum_{x \in V(F_*, H_*)} I(x, F_* \cap H_*) = \deg(F) \cdot \deg(H).$$

This is "affine Bézout's Theorem". Note that obvious counterexamples (like parallel lines) do not apply here, since there is always a common point at infinity in such a case. By Proposition 2.57, we have

$$\sum_{x \in V(F_*, H_*)} I(x, F_* \cap H_*) = \dim_K K[X, Y]/(F_*, H_*).$$

So we need to show

$$(\dagger) \qquad \dim_K K[X, Y]/(F_*, H_*) = \deg(F) \cdot \deg(H).$$

It is clearly a statement about polynomials F_*, H_* in variables X, Y only, but the proof still uses the homogenous polynomials F, H in variables X, Y, Z. This is the most difficult part of the proof, we just give the main ingredients. Let $d \in \mathbb{N}$ and

- $R := K[X, Y, Z]$;
- $\Gamma := K[X, Y, Z]/(F, H)$;
- $\pi : R \to \Gamma$ be the quotient map;
- R_d be the K-subspace of R consisting of homogeneous polynomials of degree d;
- $\Gamma_d := \pi(R_d)$;
- $\Gamma_* := K[X, Y]/(F_*, H_*)$;
- $n := \deg(F),\ m := \deg(H)$.

The aim is to show that for $d \geqslant n + m$ we have

$$\dim_K \Gamma_* = \dim_K \Gamma_d = mn,$$

which clearly gives (†). This goes again in three steps.

(1) For $d \geqslant n + m$, we have $\dim_K \Gamma_d = mn$.

This is computational and not very difficult. There is an exact sequence of K-vector spaces

$$0 \to R_{d-m-n} \to R_{d-m} \times R_{d-n} \to R_d \to \Gamma_d \to 0,$$

which gives $\dim_K(\Gamma_d)$ by a kind of "exclusion-inclusion" principle, since for any $l \in \mathbb{N}$, we have $\dim_K R_l = \frac{(l+1)(l+2)}{2}$.

(2) Define

$$\alpha : \Gamma \to \Gamma, \quad \alpha(w) = \pi(Z)w.$$

Then α is one-to-one.

This requires also some computations and the fact that we do not have intersection points at infinity is used here.

(3) Let us fix $d \geqslant n+m$ and take $A_1, \ldots, A_{mn} \in R_d$ such that $\{\pi(A_1), \ldots, \pi(A_{mn})\}$ is a basis of Γ_d (Step 1). For any $i \leqslant mn$, let A_{i*} denote the dehomogenization of A_i with respect to Z and a_i the image of A_{i*} in Γ_*. Then $\{a_1, \ldots, a_{mn}\}$ is a basis of Γ_*.

This is the most complicated part. From Step 2 and Step 1 we know that for each $r \in \mathbb{N}$, the set $\{\pi(Z^r A_1), \ldots, \pi(Z^r A_{mn})\}$ is a basis of Γ_{d+r}. This fact together with some computations and properties of homogenization/dehomogenization process give that $\{a_1, \ldots, a_{mn}\}$ is a basis of Γ_*

By (3), we get that $\dim_K(\Gamma_*) = mn$, which finishes the proof. □

Remark 3.19. The "projective change of coordinates" appearing in Step 2 above make sense for any $n \in \mathbb{N}$ and gives a transitive action of $\mathrm{GL}_{n+1}(K)$ on $\mathbb{P}^n$. Note that the subgroup of scalar matrices coincides with the kernel of this actions. However, the subgroup of scalar matrices is also the center of $\mathrm{GL}_{n+1}(K)$ hence we get an action of

$$\mathrm{PGL}_{n+1}(K) := \mathrm{GL}_{n+1}(K)/Z(\mathrm{GL}_{n+1}(K))$$

on $\mathbb{P}^n$. After an appropriate definition of a morphism between projective varieties, it can be shown that $\mathrm{PGL}_n(K)$ is exactly the group of automorphisms of $\mathbb{P}^n$ hence the name *Projective General Linear* group.

Let V be a plane projective curve.

Definition 3.20. The group of *divisors* on V, denoted $\mathrm{Div}(V)$, is the free Abelian group with basis V.

Let $F \in K[X,Y,Z]$ a homogenous polynomial such that the set

$$\{x \in V \mid F(x) = 0\}$$

is finite. We define the *intersection divisor* as:

$$V \cdot F := \sum_{x \in V} I(x, V \cap F) \cdot x \in \mathrm{Div}(V).$$

This is a good way to formalize the intuitive notion of the "intersection of two curves with counted multiplicities". Again, if F is irreducible and $W = \{x \in \mathbb{P}^2 | F(x) = 0\}$, then we define

$$V \cdot W = V \cdot F \in \mathrm{Div}(V).$$

Example 3.21. Let C_1, C_2 be as in Example 3.17. If $\mathrm{char}(K) \neq 3$, then we have

$$C_1^* \cdot C_2^* = 3(0,0) + 1(1,1) + 1(\varepsilon, 1) + 1(\varepsilon^2, 1) + 3[0:1:0].$$

If $\mathrm{char}(K) = 3$, then we have

$$C_1^* \cdot C_2^* = 3(0,0) + 3(1,1) + 3[0:1:0].$$

Definition 3.22. If $D = n_1 x_1 + \ldots + n_m x_m \in \mathrm{Div}(V)$, then the *degree* of D, denoted $\deg(D)$, is the sum:

$$\deg(D) = n_1 + \ldots + n_m.$$

Note that in the above example $\deg(C_1^* \cdot C_2^*) = 9$ regardless of the characteristic of K. Bézout's Theorem implies that if V is plane projective curve, then we have:

$$\deg(V \cdot F) = \deg(V) \deg(F).$$

3.3. **Elliptic curves.** Our definition of elliptic curves is quite a restrictive one.

Definition 3.23. An *elliptic curve* is a pair (C, O) such that C is smooth projective plane curve of degree 3 and $O \in C$.

Let us fix an elliptic curve (C, O). Our aim is to show that there is a natural commutative group structure on C such that O becomes the neutral element. Recall that for $F \in K[X,Y,Z]$, a homogenous polynomial such that the set

$$\{x \in C \mid F(x) = 0\}$$

is finite, we define the intersection divisor as:

$$C \cdot F := \sum_{x \in C} I(x, C \cap F) \cdot x \in \mathrm{Div}(C).$$

By Bézout's theorem, we have $\deg(C \cdot F) = 3 \deg(F)$.
We need to collect a few facts about lines in $\mathbb{P}^2$. Let $i \in \{1,2,3\}$.

(1) If L is a line in $\mathbb{P}^2$, then $\psi_i^{-1}(L)$ is a line in $\mathbb{A}^2$ (or the empty set).
(2) If L is a line in $\mathbb{A}^2$, then the Zariski closure of $\psi_i(L)$ in $\mathbb{P}^2$ is a line in $\mathbb{P}^2$.
(3) Using (1), we see that for any distinct $x, y \in \mathbb{P}^2$, there is a unique line in $\mathbb{P}^2$ through x and y.
(4) Take $x \in C \cap \psi_i(\mathbb{A}^2)$. We define $T_x C$, the tangent line to C at x in $\mathbb{P}^2$, as the Zariski closure of $\psi_i(T_{\psi_i^{-1}(x)} \psi_i^{-1}(C))$ (as usual, one has to show that it does not depend on the choice of i).

(5) For $x \in C$ and a line L in $\mathbb{P}^2$, as in the affine case we have

$$L = T_x C \iff I(x, C \cap L) > 1.$$

Lemma 3.24. *For any $x, y \in C$ there is a unique line L in $\mathbb{P}^2$ and a unique $z \in C$ such that*

$$C \cdot L = x + y + z.$$

(Note that this is an equality in $\mathrm{Div}(C)$*, so x, y, z need not be distinct.)*

Proof. For any line L in $\mathbb{P}^2$, the intersection $C \cap L$ is finite (since C is not a line itself), hence we can consider the intersection divisor $C \cdot L$. We consider two cases.

Case 1 $x \neq y$.
By (3), there is a unique line L in $\mathbb{P}^2$ passing through x and y. By Property (3) of the intersection number, $C \cdot L = x + y + D$, where D is a *positive* divisor, i.e. all the integer coefficients in D are non-negative. By Bézout's theorem, $\deg(C \cdot L) = 3$. Therefore, there is a unique $z \in C$ such that $D = z$ and $C \cdot L = x + y + z$.

Case 2 $x = y$.
Let L be a line in $\mathbb{P}^2$. By (5), there is $z \in C$ such that $C \cdot L = 2x + z$ if and only if $L = T_x C$. Hence L and $z \in C$ are unique. □

Using the above lemma we can define a binary operation $\varphi : C \times C$ such that $\varphi(x, y) = z$ if and only if there is a line L in $\mathbb{P}^2$ such that

$$C \cdot L = x + y + z.$$

Since addition in $\mathrm{Div}(C)$ is commutative, we get the following.

Lemma 3.25. *For $x, y, z \in C$ we have $\varphi(x, y) = \varphi(y, x)$ and*

$$\varphi(x, y) = z \iff \varphi(y, z) = x \iff \varphi(z, x) = y.$$

Unfortunately, φ is not a group operation, it is easy to see there is no neutral element. We need to correct φ using our choice of $O \in C$ (it was first done by Weil in 1920's). Let us define:

$$x \oplus y := \varphi(O, \varphi(x, y)).$$

The definition of $\oplus$ depends on O, but we still write $\oplus$ rather than $\oplus_O$.

Theorem 3.26. *The structure $(C, \oplus, O)$ is a commutative group.*

Proof. By Lemma 3.25, $\oplus$ is commutative.
Let us take $x \in C$ and $y := \varphi(x, O)$. By Lemma 3.25, $\varphi(O, y) = x$. Therefore:

$$x \oplus O = \varphi(O, \varphi(x, O)) = \varphi(O, y) = x,$$

hence O is the neutral element of $\oplus$.
Let $z := \varphi(O, O)$ and $x' := \varphi(x, z)$. By Lemma 3.25 again, we have:

$$x \oplus x' = \varphi(O, \varphi(x, x')) = \varphi(O, z) = O.$$

Therefore, x' is the inverse of x.
Proving associativity of $\oplus$ is more difficult. We will return to it after some preparations. □

Definition 3.27. Let $D, D' \in \mathrm{Div}(C)$ and

$$D = \sum_{P \in C} n_P P, \qquad D' = \sum_{P \in C} n'_P P.$$

We write $D \leqslant D'$, if for each $P \in C$, we have $n_P \leqslant n'_p$.

We need a theorem which is an easy consequence of Max Noether's (Emma Noether's father) "$AF + BG$ theorem". The proof is done in the problem session.

Theorem 3.28. *Let $F, G \in K[X, Y, Z]$ be homogenous such that each of them has finitely many zeroes on C and for each $x \in C$ we have*

$$I(x, C \cap F) \geqslant I(x, C \cap G).$$

Then there is a homogenous polynomial $H \in K[X, Y, Z]$ such that

$$C \cdot F = C \cdot G + C \cdot H.$$

Remark 3.29. In terms of intersection divisors, one can write the assumption in the above theorem as $C \cdot F \geqslant C \cdot G$.

Lemma 3.30. *For F and G as above we have:*

$$C \cdot (FG) = C \cdot F + C \cdot G.$$

Proof. Let us take $x \in C$ and assume for simplicity that $x \in \mathbb{A}^2$. Let C_* denote $C \cap \mathbb{A}^2$ and for any $H \in K[X, Y, Z]$, let $H_* = H|_{Z=1}$. Note that $(FG)_* = F_* G_*$. By properties of the valuation ord_x we have:

$$\begin{aligned} I(x, C \cap (FG)) &= \mathrm{ord}_x((FG)_*|_{C_*}) \\ &= \mathrm{ord}_x((F_* G_*)|_{C_*}) \\ &= \mathrm{ord}_x((F_*|_{C_*})(G_*|_{C_*})) \\ &= \mathrm{ord}_x(F_*|_{C_*}) + \mathrm{ord}_x(G_*|_{C_*}) \\ &= I(x, C \cap F) + I(x, C \cap G). \end{aligned}$$

Hence $C \cdot (FG) = C \cdot F + C \cdot G$. □

Proposition 3.31. *Take homogenous polynomials F, G as above of degree 3, and $x_1, \ldots, x_8, y, z \in C$ such that*

$$C \cdot F = x_1 + \ldots + x_8 + y,$$

$$C \cdot G = x_1 + \ldots + x_8 + z.$$

Then $y = z$.

Proof. Let L be a line in $\mathbb{P}^2$ passing through y and H be the linear homogenous polynomial defining L. Then

$$C \cdot L = y + r + s$$

for some $r, s \in C$. By Lemma 3.30, we have

$$C \cdot (GH) = C \cdot G + C \cdot H = x_1 + \ldots + x_8 + z + y + r + s = C \cdot F + z + r + s.$$

In particular, $C \cdot (GH) \geqslant C \cdot F$. By Theorem 3.28, there is a homogenous $T \in K[X, Y, Z]$ such that

$$C \cdot (GH) = C \cdot F + C \cdot T.$$

Since $\deg(C \cdot (GH)) = 12$ and $\deg(C \cdot F) = 9$, we get $\deg(C \cdot T) = 3$. By Bézout's theorem, $\deg(T) = 1$, so T defines a line L' in $\mathbb{P}^2$. Therefore we have

$$C \cdot L = r + s + y, \quad C \cdot L' = C \cdot T = r + s + z.$$

By Lemma 3.24, $y = z$. □

Proof of the associativity of $\oplus$. Let us take

$$x, y, z \in C; \quad \text{lines } L_1, L_2, L_3, M_1, M_2, M_3 \text{ in } \mathbb{P}^2; \quad s, s', u, u', t', t'' \in C$$

such that:

$$C \cdot L_1 = x + y + s', \ C \cdot L_2 = s + z + t', \ C \cdot M_1 = O + s + s' \tag{1}$$

$$C \cdot L_3 = O + u + u', \ C \cdot M_2 = y + z + u', \ C \cdot M_3 = x + u + t'' \tag{2}$$

Then (1) implies that

$$(x \oplus y) \oplus z = s \oplus z = \varphi(O, t'),$$

and (2) implies that

$$x \oplus (y \oplus z) = x \oplus u = \varphi(O, t'').$$

Hence it is enough to show that $t' = t''$. For any $i \in \{1, 2, 3\}$, let F_i be the homogenous polynomial of degree 1 defining L_i and G_i be the homogenous polynomial of degree 1 defining M_i. Let $F := F_1F_2F_3$ and $G := G_1G_2G_3$. By Lemma 3.30, we have

$$C \cdot F = C \cdot L_1 + C \cdot L_2 + C \cdot L_3 = x + y + s' + s + z + t' + O + u + u',$$

$$C \cdot G = C \cdot M_1 + C \cdot M_2 + C \cdot M_3 = O + s + s' + y + z + u' + x + u + t''.$$

From Proposition 3.31, we get $t' = t''$. □

It can be shown that for two different choices $O_1, O_2 \in C$, there is an isomorphism of groups

$$(C, \oplus, O_1) \cong (C, \oplus, O_2),$$

which is given by rational functions. Hence the choice of $O \in C$ does not matter much. However, some choices make computations easier. We need one more definition.

Definition 3.32. A point $x \in C$ is called an *inflection point*, if

$$I(x, C \cap T_xC) > 2.$$

The definition above makes sense for an arbitrary plane (projective or affine) smooth curve. In the case of the elliptic curve C, for $x \in C$ the following are equivalent:

- x is an inflection point,
- $I(x, C \cap T_xC) = 3$,
- $\varphi(x, x) = x$.

Note that if $O \in C$ is an inflection point, then the procedure of finding the inverse elements is easier, since in such a case we get:

$$\ominus x = \varphi(x, \varphi(O, O)) = \varphi(x, O).$$

(We use the notation $\ominus x$ for the inverse element to x in the elliptic curve C.)
We state another fact without a proof.

Proposition 3.33. *If* $\operatorname{char}(K) \neq 3$*, then there are* 9 *inflection points on* C.

We choose $O \in C$ as an inflection point. By a projective change of coordinates in $\mathbb{P}^2$ (which moves C!), we can also assume that O is a point at infinity and that the tangent line to C at O is the line at infinity H_∞. This choice implies that O is the *unique* point at infinity of C, since

$$I(O, C \cap H_\infty) = I(O, C \cap T_OC) = 3.$$

We finish the lecture by analyzing the points of order 2 and 3 on C. Let $x \in C$.

Points of order 2 **on** C

Clearly, the order of x is at most 2 if and only if

$$O = x \oplus x = \varphi(O, \varphi(x, x)).$$

The equality above holds if and only if there is a line L in $\mathbb{P}^2$ such that

$$C \cdot L = O + O + \varphi(x, x).$$

Hence L as above must be the tangent line to C at O. Since O is the inflection point, $\varphi(x, x) = O$. Therefore, the order of x is at most 2 if and only if $\varphi(x, x) = O$. From the picture we can "see" that there are 4 such points (to be precise, if $\mathrm{char}(K) \neq 2$).

Points of order 3 **on** C

the order of x is 1 or 3 if and only if

$$\ominus x = x \oplus x = \varphi(O, \varphi(x, x)) = \ominus\varphi(x, x)$$

which happens if and only if $\varphi(x, x) = x$, i.e. when x is an inflection point. We know that there are 9 such points (if $\mathrm{char}(K) \neq 3$).

Remark 3.34. If $K = \mathbb{C}$, then $\mathbb{P}^2(\mathbb{C})$ is also a compact differential manifold of (real) dimension 4. Then C is a smooth submanifold of $\mathbb{P}^2(\mathbb{C})$ of (real) dimension 2. Since the group operation on C is actually given by rational functions which are smooth, C has also a structure of a Lie group. So C is a compact commutative Lie group of (real) dimension 2. From the classification of commutative Lie groups, we see that C is isomorphic to $S^1 \times S^1$ as a Lie group. This coincides with our computations above, since the group of 2-torsion of $S^1 \times S^1$ has 4 elements and the group of 3-torsion of $S^1 \times S^1$ has 9 elements.