ALGEBRAIC VARIETIES

LECTURE NOTES

H.A. NIELSEN

DEPARTMENT OF MATHEMATICAL SCIENCES
UNIVERSITY OF AARHUS
2003

Algebraic Varieties

H.A. Nielsen

Contents

Prerequisites

Here is a list of facts to use without notice.

- Basic notions from algebra, such as groups, rings, fields and their homomorphisms.
- Elementary ideal theory and factor rings, prime and maximal ideals.
- Polynomial rings, power series rings and principal ideal domains.
- Integral domains and the construction of fractions.
- The notion of field extensions.
- Linear algebra, bilinear forms, matrices and determinants.

A special choice has been made, that the material is presented without modules. This affects a few standard formulations of popular propositions. More seriously this means that there is neither homological nor sheaf theoretic methods available.
The propositions are stated complete and precise, while the proofs are quite short. No specific references to the literature are given. But lacking details may all be found at appropriate places in the books listed in the bibliography.
The last part is sporadic, informal and only initiates the study of concrete objects. In an elaborate form this should have been included in the ordinary text.

Nielsen, University of Aarhus, Summer 2003

CHAPTER I

Affine rings

All rings are commutative with 1.

1. Hilbert's basis theorem

Definition 1.1. A ring is **noetherian** if every ideal is finitely generated. A factor ring of a noetherian ring is noetherian.

Proposition 1.2. *Let A be a noetherian ring. Any nonempty set of ideals contain members maximal for inclusion. If A is nonzero, then it contains a maximal ideal.*

Proof. If a set of ideals does not contain a maximal member then choose an infinite ascending chain $I_1 \subset I_2 \subset \dots$. The union $\cup I_i$ is finitely generated giving $I_i = I_{i+1}$ for large i. By contradiction maximal members exist. □

Definition 1.3. For an ideal I in a ring A the **radical** is

$$\sqrt{I} = \{a \in A | a^n \in I \text{ for some } n\}$$

A ring is **reduced** if $\sqrt{0} = 0$.

Proposition 1.4. *Let A be a noetherian ring. The radical of an ideal I is the intersection of all prime ideals containing I. High powers of the radical are contained in the ideal itself*

$$(\sqrt{I})^s \subset I$$

Proof. Assume a is not in the radical of I. By 1.2 there is an ideal maximal among the ideals containing I and not containing any power of a. This is a prime ideal excluding a. The inclusion follows as the radical is finitely generated. □

Proposition 1.5. *Let A be a noetherian ring. Then the ring of polynomials $A[T]$ is noetherian.*

Proof. Assume $I \subset A[T]$ to be a not finitely generated ideal. Choose a sequence $f_1, f_2, \dots \in I$ such that

$$f_i = a_i T^{d_i} + \text{ terms of lower degree }, a_i \neq 0$$

and f_{i+1} has lowest degree in $I - (f_1, \dots, f_i)$. The ideal of leading coefficients is finitely generated by $a_1, \dots, a_n$. $a_{n+1} = b_1 a_1 + \dots + b_n a_n$ and $d_1 \leq \dots \leq d_{n+1} = d$ gives

$$f_{n+1} - b_1 T^{d-d_1} f_1 - \dots - b_n T^{d-d_n} f_n$$

in $I - (f_1 \dots, f_n)$ of degree less than d. By contradiction the ideal I is finitely generated. □

Proposition 1.6. *Let $A \subset B$ be a ring extension. Let $J \subset Ac_1 + \dots + Ac_n \subset B$ be a subset satisfying $AJ \subset J$. If A is noetherian, then there are $b_1, \dots, b_m \in J$ such that $J = Ab_1 + \dots + Ab_m$.*

Proof. J is identified with an ideal in a factor ring of $A[T_1, \dots, T_n]$, which is noetherian by 1.5. □

Definition 1.7. Let k be a field. For an ideal I of the ring of polynomials $k[T_1, \dots, T_n]$ the factor ring $k[T_1, \dots, T_n]/I$ is an **affine ring**. A homomorphism of affine rings is the identity on the field k.

Theorem 1.8 (Hilbert's basis theorem)**.** *An affine ring is noetherian.*

Proof. Follows from 1.5. □

Definition 1.9. Let A be an integral domain with fraction field K. For a subset S of A excluding 0 the fractions with denominators a finite product of elements from S is a subring

$$A \subset S^{-1}A \subset K$$

called the **localization**. Contraction of ideals identify prime ideals in $S^{-1}A$ with prime ideals in A excluding S. If $Q \subset S^{-1}A$ and $P = A \cap Q$ then the fraction fields of A/P and $S^{-1}A/Q$ are identified.

Proposition 1.10. *Let A be a noetherian integral domain, then any localization $S^{-1}A$ is noetherian.*
If A is an affine ring and $S = \{s\}$, then the localization

$$S^{-1}A \simeq A[T]/(sT - 1)$$

is affine.

Proof. For an ideal J in $S^{-1}A$ generators of $A \cap J$ will generate J. Affinity follows from 1.5. □

2. Noether's normalization theorem

Definition 2.1. Let B be a ring containing a subring A. An element $b \in B$ is **integral** over A if it is root in a monic polynomial with coefficients in A. By Cramer's rule an element b is integral over A if and only if there are finitely many elements $b_1, \dots, b_n \in B$ such that

$$1, bb_1, \dots, bb_n \in Ab_1 + \cdots + Ab_n$$

The set of elements integral over A is a subring called the **integral closure**. B is **integral** over A if every element in B is integral over A. If A is a field, integral is usually called **algebraic** and a polynomial relation of least degree is called **minimal**. A finitely generated integral extension $A \subset B$ is called **finite**, since there is a finite set $b_1, \dots, b_n \in B$ such that

$$B = Ab_1 + \cdots + Ab_n$$

and conversely an extension satisfying the claim is finite. Clearly, if $A \subset B$ and $B \subset C$ are finite then $A \subset C$ is finite.

Proposition 2.2. *Let K be a field and $p(T)$ a polynomial in $K[T]$. Then there is a finite field extension $K \subset L$ such that $p(T)$ factors in linear factors in $L[T]$.*
If $K \subset L_1$ and $K \subset L_2$ are finite field extensions then there is a finite field extension $K \subset L$ such that $L_1 \cup L_2 \subset L$.

Proof. Assume $p(T)$ irreducible. In $L = K[U]/(p(U))$ the class of U is a root of $p(T)$. □

Definition 2.3. A field K such that any polynomial in $K[T]$ factors in linear factors is called **algebraically closed**. It follows that any field has an algebraic extension field which is algebraically closed.

Proposition 2.4. *Let an integral domain B be integral over a subring A. Then A is a field if and only if B is a field.*

Proof. Let A be a field, a minimal equation for a nonzero $b \in B$

$$b^n + \cdots + a_0 = 0$$

gives

$$b^{-1} = -a_0^{-1}(a_{n-1}b^{n-2} + \cdots + a_1) \in B$$

Let B be a field, an integral equation for the reciprocal of a nonzero $a \in A$

$$a^{-n} + \cdots + a_0 = 0$$

gives

$$a^{-1} = -(a_0 a^{n-1} + \cdots + a_{n-1}) \in A$$

□

Proposition 2.5. *Let K be a finitely generated field over a subfield k. Then there exist a unique number n and a set of elements $t_1, \dots, t_n \in K$ such that the ring $k[t_1, \dots, t_n]$ is a polynomial ring and K is finite over the fraction field $k(t_1, \dots, t_n)$.*

Proof. Let $t_1, t_2, \dots$ be a finite set of generators and $t_1, \dots, t_n$ a maximal subset such that $k[t_1, \dots, t_n]$ is a ring of polynomials. Then K is algebraic over the fraction field $k(t_1, \dots, t_n)$. For another set $u_1, \dots, u_m$ satisfying $k[u_1, \dots, u_m]$ is a ring of polynomials and K is algebraic over the fraction field $k(u_1, \dots, u_m)$ we may assume $n \le m$. For $n = 0$, K is algebraic over k, so $m = 0$. If $0 < n$ then there is a nonzero polynomial $f \in k[T_1, \dots, T_n, U_1]$ such that $f(t_1, \dots, t_n, u_1) = 0$. Since u_1 is not algebraic over k we get after renumbering, that the set $u_1, t_2, \dots, t_n$ satisfy $k[u_1, \dots, t_n]$ is a ring of polynomials and K is algebraic over the fraction field $k(u_1, \dots, t_n)$. Exchanging the field k with $k(u_1)$ gives by induction after n that $n - 1 = m - 1$ and uniqueness follows. □

Definition 2.6. The set of elements in 2.5 is a **transcendence basis** and the number of elements in such a set is the **transcendence degree** denoted

$$\operatorname{trdeg}_k K$$

A set of elements $t_1, \dots, t_n$ generating a polynomial ring is called **algebraically independent** and the extension $k \subset k(t_1, \dots, t_n$ is **pure transcendental**.

Theorem 2.7 (Noether's normalization theorem)**.** *Let k be a field and A an affine ring over k. Assume that A is an integral domain and let K be the fraction field. Then there exist elements $t_1, \dots, t_n \in A$ such that $t_1, \dots, t_n$ is a transcendence basis of K over k, and A is integral over the subring of polynomials $k[t_1, \dots, t_n]$.*

Proof. Let $t_1, \dots, t_n \in A$ be a minimal set such that A is integral over $k[t_1, \dots, t_n]$. If $f \in k[T_1, \dots, T_n]$ is a nonzero polynomial of degree less than d in every variable with $f(t_1, \dots, t_n) = 0$, then the substitutions

$$U_1 = T_1 - T_n^{d^{n-1}}, \dots, U_{n-1} = T_{n-1} - T_n^d$$

give a polynomial

$$f(U_1 + T_n^{d^{n-1}}, \dots, U_{n-1} + T_n^d, T_n) \in k[U_1, \dots, U_{n-1}, T_n]$$

Any monomial $T_1^{d_1} \dots T_n^{d_n}$ gives a monomial in T_n over $k[U_1, \dots, U_{n-1}]$ of unique degree $d_1 d^{n-1} + \cdots + d_n$ as seen by d-adic expansion. This makes t_n integral over $k[u_1, \dots, u_{n-1}]$ and contrasts the minimality of n, showing that $t_1, \dots, t_n$ is a transcendence basis. □

3. Hilbert's Nullstellensatz

Theorem 3.1 (Hilbert's Nullstellensatz)**.** *Let $k \subset K$ be a field extension. If K is an affine ring over k, then K is finite over k.*

Proof. By noetherian normalization 2.7 find $t_1, \ldots, t_n$ such that K is integral over the subring of polynomials $k[t_1, \ldots, t_n]$. By 2.4 $k[t_1, \ldots, t_n]$ is a field. It follows that $n = 0$ and K is algebraic over k. □

Proposition 3.2. *If $\phi : A \to B$ is a homomorphism of affine rings over k and N is a maximal ideal in B, then $\phi^{-1}(N)$ is a maximal ideal in A.*

Proof. By Hilbert's Nullstellensatz $k \to B/N$ is finite. Then the extension $A/\phi^{-1}(N) \subset B/N$ is integral giving maximality by 2.4. □

Theorem 3.3. *Let k be an algebraically closed field. Any maximal ideal of the ring of polynomials $k[T_1, \ldots, T_n]$ has the form*

$$(T_1 - t_1, \ldots, T_n - t_n)$$

for a unique sequence $t_1 \ldots, t_n \in k$.

Proof. An ideal of the given form is maximal. If M is a maximal ideal, then the factor ring

$$k[T_1, \ldots, T_n]/M$$

is an affine field extension of the constants k. Since k is algebraically closed it follows from Hilbert's Nullstellensatz 3.1 that this extension is trivial. There exists unique $t_1, \ldots, t_n \in k$ such that

$$t_i = T_i + M \ , \ i = 1, \ldots, n$$

showing

$$(T_1 - t_1, \ldots, T_n - t_n) \subset M$$

□

Proposition 3.4. *The radical of an ideal in an affine ring is the intersection of maximal ideals.*

Proof. By 1.4 it is enough to show that the zero ideal in an affine integral domain is the intersection of maximal ideals. Let f be nonzero in the affine domain A over k. The affine ring $B = A[T]/(fT - 1)$ is nonzero and therefore contains a maximal ideal N. By 3.1 the field B/N is finite over k and then integral over the domain $A/A \cap N$. By the 2.4 $A \cap N$ is a maximal ideal of A, which by construction avoid f, so the intersection of all maximal ideals is zero. □

Proposition 3.5. *An affine ring A over k is a finite dimensional k-vector space if and only if there are only finitely many maximal ideals $M_1, \ldots, M_r$. In the finite dimensional case all prime ideals are maximal and*

$$0 = M_1^{i_1} \ldots M_r^{i_r} = M_1^{i_1} \cap \cdots \cap M_r^{i_r}$$

$$A \simeq A/M_1^{i_1} \times \cdots \times A/M_r^{i_r}$$

Proof. An integral domain finite dimensional over k is a field so prime ideals are maximal. Since $M_1 \cap \cdots \cap M_j \not\subset M_{j+1}$ there are only finitely many maximal ideals. A high power of the radical $(M_1 \cap \cdots \cap M_r)^s = 0$. Let i_j be given such that $M_j^{i_j} = M_j^{i_j+1}$ and conclude by the Chinese remainder theorem below. □

Proposition 3.6 (Chinese remainder theorem)**.** *Let ideals $I_1, \ldots, I_k$ in a commutative ring A satisfy $I_r + I_s = A$ for $r \neq s$.*

(1) *For $x_1, \ldots, x_k \in A$ there is a $x \in A$, such that $x - x_r \in I_r$ for $r = 1, \ldots, k$*

(2)

$$I_1 \cdots I_k = I_1 \cap \cdots \cap I_k$$

(3) *The product of projections*

$$A/I_1 \cdots I_k \to A/I_1 \times \cdots \times A/I_k$$

is an isomorphism.

Proof. (1)Choose $a_r \in I_1$ and $b_r \in I_r$ such that $a_r + b_r = 1$. The product

$$(a_2 + b_2) \dots (a_k + b_k) = 1 \in I_1 + I_2 \cdots I_k$$

Similarly choose $u_r \in I_r$ and $v_r \in \prod_{s \neq r} I_s$ with $u_r + v_r = 1$. Let $x = x_1 v_1 + \cdots + x_r v_r$. (2) For x in the intersection assume by induction that $x \in I_2 \cdots I_k$. From (1) $x = u_1 x + x v_1$ contained in the product. (3) Subjectivity follows from (1) and the kernel is the intersection. □

4. The polynomial ring is factorial

Definition 4.1. Let A be a unique factorization domain and let $f = a_n T^n + \cdots + a_0$ be a polynomial over A. Then the **content** of f, $c(f)$, is the greatest common divisor of the coefficients $a_0, \dots, a_n$.

Proposition 4.2 (Gauss' lemma)**.** *Let A be a unique factorization domain. For polynomials $f, g \in A[T]$*

$$c(fg) = c(f)c(g)$$

Proof. Assume by cancellation that $c(f), c(g)$ are units in A. For any irreducible $p \in A$ the projections of f, g in $A/(p)[T]$ are nonzero. Since A has unique factorization the ideal (p) is a prime ideal. It follows that the projection of the product fg in $A/(p)[T]$ is also nonzero and therefore p is not a common divisor of the coefficients of the product fg. □

Proposition 4.3. *Let A be a unique factorization domain. Then the ring of polynomials $A[T]$ is a unique factorization domain.*

Proof. Let K be the fraction field of A, then the polynomial ring $K[T]$ is a principal ideal domain. Let $f \in A[T]$ and use unique factorization in $K[T]$ to get $a \in A$ and $p_1, \dots, p_n \in A[T]$, irreducible in $K[T]$, such that

$$af = p_1 \dots p_n$$

Assume by 4.2 that $a = 1$ and $c(p_1), \dots, c(p_n)$ are units in A. Apply 4.2 once more to see that $p_1, \dots, p_n$ are irreducible in $A[T]$. Uniqueness follows by cancellation. □

Theorem 4.4. *Let k be a field. Then the polynomial ring $k[T_1, \dots, T_n]$ is a unique factorization domain.*

Proof. Follows by induction from 4.3. □

Definition 4.5. An integral domain is **normal** if the integral closure in the fraction field is the domain itself. The integral closure in a field extension of the fraction field is a normal ring called the **normal closure**.

Proposition 4.6. *A unique factorization domain is normal.*

Proof. If a fraction $\frac{a}{b}$ satisfies

$$\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + a_0 = 0$$

it follows that any prime divisor in b divides a, so by cancellation b is a unit. □

5. Krull's principal ideal theorem

Proposition 5.1. *Let A be an affine integral domain over a field k with fraction field K. Let P be a prime ideal of A and let $k(P)$ denote the fraction field of A/P. If P is nonzero then*

$$\operatorname{trdeg}_k k(P) < \operatorname{trdeg}_k K$$

Proof. Assume $n = \operatorname{trdeg}_k K$ and let $t_1, \dots, t_n \in A$ project to $\bar{t}_1, \dots, \bar{t}_n \in A/P$. For $t \in P$ nonzero there is an irreducible polynomial $f \in k[T_1, \dots, T_n, T]$ such that

$$f(t_1, \dots, t_n, t) = 0, \text{ in } A$$

This gives

$$f(T_1, \dots, T_n, 0) \neq 0, \text{ in } k[T_1, \dots, T_n]$$
$$f(\bar{t}_1, \dots, \bar{t}_n, 0) = 0, \text{ in } A/P$$

so $\operatorname{trdeg}_k k(P) < n$. □

Proposition 5.2. *Let A be an affine ring over a field k. Then*

(1) *Any prime ideal in A contains a minimal prime ideal.*
(2) *There are only finitely many minimal prime ideals in A.*

Proof. (1) By 5.1 any descending chain of prime ideals will stop. (2) If the set of ideals such that the factor ring have infinitely many minimal prime ideals is nonempty, it contains a maximal member with this property by 1.2. In this factor ring there are only finitely many minimal prime ideals containing a given nonzero ideal. There exist nonzero elements a, b with product $ab = 0$. A minimal prime must contain either a or b so there is only finitely many of these. In conclusion there are only finitely many minimal prime ideals in an affine ring. □

Proposition 5.3. *Let $P_1, \dots, P_r$ be ideals in a ring A with at most 2 not being prime ideals. If an ideal $I \subset P_1 \cup \dots \cup P_r$ then $I \subset P_i$ for some i.*

Proof. Assume by induction on $r > 1$ that I is not contained in any subunion. Then choose

$$a_j \in I \cap P_j - \cup_{i \neq j} P_i$$

giving the element

$$a_r + a_1 \dots a_{r-1}$$

in I but not in any P_i, contradicting the hypothesis. □

Theorem 5.4 (Krull's principal ideal theorem)**.** *Let A be an affine integral domain over a field k with fraction field K. Let P be a prime ideal of A and let $k(P)$ denote the fraction field of A/P. If P is minimal among the prime ideals of A containing a nonzero element $f \in A$ then*

$$\operatorname{trdeg}_k k(P) = \operatorname{trdeg}_k K \ - 1$$

Proof. Let $P_1, \dots, P_s$ be the other minimal primes over f and let $g \in P_1 \dots P_s - P$. After exchanging the ring A with $A[T]/(gT - 1)$ we may assume that P is the only minimal prime over f. By Noether's normalization Theorem 2.7 choose $t_1, \dots, t_n \in A$ such that $k[t_1, \dots, t_n]$ is a polynomial ring and A is integral over this subring. Let

$$f^m + a_{m-1} f^{m-1} + \dots + a_0, \ a_i \in k[t_1, \dots, t_n]$$

be a relation of least degree, then

$$a_0 = -(f^{m-1} + \dots + a_1) f \in P \cap k[t_1, \dots, t_n]$$

If $c \in P \cap k[t_1, \dots, t_n]$ then by 1.4 $c^r = uf$ for some $u \in A$. The $k(t_1, t_2, \dots, t_n)$-linear map $K \to K, x \mapsto c^r x$ has a determinant which factors, $e = \dim_{k(t_1, \dots, t_n)} K$,

$$c^{re} = \det c^r = \det u \det f = \det u \ \pm a_0^{e/m}$$

The least degree relation for u shows $\det u \in A$ so $\det u \in A \cap k(t_1, \dots, t_n) = k[t_1, \dots, t_n]$, since $k[t_1, \dots, t_n]$ is normal by 4.6. This shows that $P \cap k[t_1, \dots, t_n]$ is the unique minimal prime over a_0 in the ring $k[t_1, \dots, t_n]$. Since a polynomial ring is a unique factorization domain the ideal $P \cap k[t_1, \dots, t_n]$ is a principal ideal generated by an irreducible polynomial $d \in P \cap k[t_1, \dots, t_n]$. After renumbering assume that d is a nonconstant polynomial in t_n, then unique factorization gives that the projections of $t_1, \dots, t_{n-1}$ in $k[t_1, \dots, t_n]/(d)$ generate a polynomial ring, so $\operatorname{trdeg}_k k[t_1, \dots, t_n]/(d) \geq n-1$. Together with 5.1 this gives the claim. □

Proposition 5.5. *Let k be a field and A an affine ring over k being an integral domain with fraction field K. Then any chain of prime ideals has the maximal length equal to the transcendence degree of K over k.*

Proof. Follows from Krull's principal ideal theorem 5.4 by induction on $\operatorname{trdeg}_k K$. □

6. Differentials and derivations

Definition 6.1. Let $K \subset L$ be a field extension. An algebraic element $t \in L$ is **separable** over K if the minimal polynomial $f(T)$ for t has no multiple roots, that is the derivative $f'(t) \neq 0$. If every element is separable, the extension is **separable** . If no element outside K is separable, the extension is **purely inseparable**.

Definition 6.2. Let $k \subset K$ be a field extension. The space of **k-differentials** of K is the K-vector space

$$\Omega_k(K) = \oplus_{t \in K} K dt / (da, d(u+v) - du - dv, d(uv) - vdu - udv)$$

$a \in k, u, v \in K$ generate the relations.
A k-linear map $D : K \to V$ to a K-vector space V is a **k-derivation** if

$$D(uv) = vD(u) + uD(v), \; u, v \in K$$

The k-linear map $d : K \to \Omega_k(K), \; t \mapsto dt$ is the universal k-derivation on K, that is any derivation $D : K \to V$ is the composite $D = \phi \circ d$ for a unique K-linear map $\phi : \Omega_k(K) \to V$.

Proposition 6.3. *Let $k \subset K \subset L$ be field finitely generated extensions.*

(1) *There is a natural isomorphism of L-vector spaces*

$$\Omega_k(L)/L\Omega_k(K) \simeq \Omega_K(L)$$

(2) *For a finite separable extension $K \subset L$*

$$\dim_L \Omega_k(L) = \dim_K \Omega_k(K)$$

(3) *For a pure transcendental extension $K \subset K(T)$*

$$\dim_{K(T)} \Omega_k(K(T)) = \dim_K \Omega_k(K) + 1$$

(4) *For a finitely generated extension $K \subset L$*

$$\dim_L \Omega_k(L) \geq \dim_K \Omega_k(K) + \operatorname{trdeg}_K L$$

Proof. (2) A derivation $D : K \to K$ has a unique extension to L. □

Theorem 6.4. *A finitely generated field extension $k \subset K$ is finite and separable if and only if*

$$\Omega_k(K) = 0$$

Proof. If $k \subset k(t)$ is finite and t not separable, then the minimal polynomial $f(T)$ has derivative $f'(T) = 0$. There is a well defined nonzero derivation on $k[T]/(f(T)) = k(t)$ given by

$$Dt^i = it^{i-1}$$

In general filter the extension by adding one generator at a time. □

Theorem 6.5. *Let $k \subset K$ be a finitely generated field extension of $\operatorname{trdeg}_k K = n$. Elements $t_1, \dots, t_n \in K$ is a transcendence basis for K over k and $k(t_1, \dots, t_n) \subset K$ is a finite separable extension if and only if*

$$dt_1, \dots, dt_n \in \Omega_k(K)$$

is a K-basis.

Proof. Let $t_1, \dots, t_n \in K$ be a transcendence basis and let $k(t_1, \dots, t_n) \subset K$ be separable. By 6.4 $dt_1, \dots, dt_n$ is a basis.
If $dt_1, \dots, dt_n$ is a basis, then $t_1, \dots, t_n$ is a transcendence basis.
If $k(t_1, \dots, t_n) \subset K$ is not separable then by 6.4 $\Omega_{k(t_1,\dots,t_n)} K \neq 0$ and $dt_1, \dots, dt_n$ will not generate $\Omega_k(K)$, giving a contradiction. □

Definition 6.6. The set of elements $t_1, \dots, t_n$ in 6.5 is called a **separating** transcendence basis . A such exists if and only if

$$\dim_k \Omega_k(K) = \operatorname{trdeg}_k K$$

Proposition 6.7. *Let $k \subset K$ be a finitely generated field extension. If $char(k) = 0$ or k is perfect, i.e. $char(k) = p$ and $k^p = k$ then*

$$\dim_K \Omega_k(K) = \operatorname{trdeg}_k K$$

and there exists a separating transcendence basis $t_1, \dots, t_n \in K$ for K over k.

Proof. If $char(k) = p$ any polynomial in $k[T^p]$ is a p-th power in $k[T]$. □

7. Primitive elements

Theorem 7.1 (Primitive element). *Let $K \subset K(t_1, \dots, t_r)$ be a finite field extension. If $t_2, \dots, t_r$ are separable over K, then there exists a **primitive** element v such that*

$$K(v) = K(t_1, \dots, t_n)$$

Proof. The group of nonzero elements in a finite field is cyclic, so K may be taken infinite. The case $K \subset K(t, u)$, u separable suffices. Let $t_1, \dots, t_m$ and $u_1, \dots, u_n$ be the roots of the minimal polynomials f and g of t and u. Let $s \in K$ be different from the elements

$$\frac{t_i - t_j}{u_k - u_l},\ i \neq j, k \neq l$$

Then $v = t + su$ is a primitive element. u is the only common root in the polynomials

$$g(T),\ f(v - sT) \in K(v)[T]$$

As u is not a multiple root, we get that the greatest common divisor of the polynomials is $T - u \in K(v)[T]$. Therefore $t, u \in K(v)$. □

Theorem 7.2. *Let k be an algebraically closed field and A an affine domain over k with fraction field K. Then there exist a transcendence basis $t_1, \dots, t_n \in A$ for K over k, such that A is integral over the subring of polynomials $k[t_1, \dots, t_n]$ and the field extension*

$$k(t_1, \dots, t_n) \subset K$$

is a finite separable extension.

Proof. Let $t_1, \dots, t_n \in A$ be a transcendence basis from Noether's normalization Theorem 2.7. If $g(t_1, \dots, t_n, t_{n+1}) = 0$ is an irreducible polynomial equation for an element in $t_{n+1} \in K$, then $\partial g / \partial u_i \neq 0$ for some i else p is the characteristic of k and g is a p-power contradicting irreducibility. Renumbering elements and using the substitutions

$$u_i = t_i - t_i^{p^m},\ m >> 0$$

as in the proof of Noether's normalization, give that the extension $k(t_1, \dots, t_n) \subset K$ is separable after finitely many steps, by 7.1. □

Proposition 7.3 (Lüroth)**.** *If $k \subset K \subset k(t)$ is a subextension of $\operatorname{trdeg}_k K = 1$, then there is $u \in K$ such that*

$$K = k(u)$$

Proof. Let

$$f(T, U) = a_n(T)U^n + \cdots + a_1(T)U + a_0(T)$$

be a polynomial in $k[T, U] \cap K[U]$ of least degree in U with t as root. Set

$$u = \frac{a_i(t)}{a_n(t)} \notin k, \ u = \frac{g(T)}{h(T)}|T = t$$

$g(T), h(T)$ with no common factors. Then by Gauss' lemma 4.2

$$h(T)g(U) - g(T)h(U) = f(T, U)q(T, U)$$

By degree considerations it follows that $q(T, U) \in k$ and therefore $\deg g(T) = n$. Then conclude by

$$\dim_{k(u)} k(t) \leq n$$

□

8. Integral extensions of affine domains

Proposition 8.1. *Let A be a normal domain with fraction field K.*

(1) *Let $f, g \in K[T]$ be monic. If $fg \in A[T]$ then $f, g \in A[T]$.*
(2) *If u in some field extension $K \subset L$ is integral over A, the minimal polynomial for u over K is in $A[T]$.*
(3) *$A[T]$ with fraction field $K(T)$ is normal.*

Proof. (1) In an algebraic closure of K the roots of fg are integral over A and therefore also the coefficients of f, g. (3) By 4.6 $K[T]$ is normal. For $P(T) \in K[T]$ integral over $A[T]$ use (1) on $P(T) + T^m$ for large m. □

Proposition 8.2. *Let A be a normal affine domain with fraction field K. Assume $g \in K$ such that*

$$P = \{f \in A | fg \in A\}$$

is a prime ideal and let $k(P)$ denote the fraction field of A/P. Then

$$\operatorname{trdeg}_k k(P) = \operatorname{trdeg}_k K \ - 1$$

Proof. If $gP \subset P$ then g is integral over A and $P = A$ is not a prime ideal. So there exists $t \in P$ such that $tg \in A - P$. In the ring $A[T]/(gtT - 1)$ the induced ideal $P = (t)$, conclude by Krull's principal ideal Theorem 5.4. □

Proposition 8.3. *Let A be a normal domain with fraction field K and let B be the normal closure of A in a finite separable field extension $K \subset L$. Then the extension $A \subset B$ is finite.*

Proof. By 7.1 $L = K(v)$, $v \in B$ with monic minimal polynomial $f(T) \in A[T]$. Let $v = v_1, \ldots, v_n$ be the roots. The square of the van der Monde determinant of these elements $d \neq 0$ in A. So $u_1 = \frac{1}{d}, u_2 = \frac{v}{d}, \ldots, u_n = \frac{v^{n-1}}{d}$ give the statement. □

Theorem 8.4. *Let A be a affine domain over a field k with fraction field K and let B be the normal closure of A in a finite field extension $K \subset L$. Then the extension $A \subset B$ is finite and B is an affine domain over k.*

Proof. Assume by Noether's normalization theorem $A = k[T_1, \ldots, T_n]$ is a polynomial ring. If $K \subset L$ is separable, the conclusion follows from 8.3. If $u \in L$ is not separable over K, then the minimal polynomial has form $f(T^{p^m})$, where p is the characteristic of the ground field k and u^{p^m} is separable over K. Reduce to the separable case by changing to $A = k[T_1^{p^{-m}}, \ldots, T_n^{p^{-m}}]$. □

9. Nakayama's lemma and Krull's intersection theorem

Theorem 9.1 (Nakayama's lemma)**.** *Let $A \subset B$ be a ring extension and let $J = \{b_1, \ldots, b_n\} \subset B$ be a finite set. Assume that $M \subset A$ is an ideal satisfying*

$$MJ = AJ$$

(1) *There is an element $a \in M$ such that $(1 + a)J = 0$.*
(2) *If all elements $1 + a$, $a \in M$ are nonzero divisors on J, then $J = \{0\}$.*

Proof. (1)

$$b_i = \sum_j a_{ij} b_j \ , \ a_{ij} \in M$$

By Cramer's rule

$$(1 - a_i)b_i = 0 \ , \ a_i \in M$$

and

$$1 + a = \Pi_i (1 + a_i)$$

(2) Cancellation give all $b_i = 0$. □

Theorem 9.2 (Krull's intersection theorem)**.** *Let M be an ideal in a noetherian ring A such that the elements $1 + a,\ a \in M$ are nonzero divisors. Then*

$$\bigcap_n M^n = 0$$

Proof. Let $M = (u_1, \ldots, u_m)$. If $b \in M^n$ then

$$b = f_n(u_1, \ldots, u_m)$$

where $f_n \in A[T_1, \ldots, T_m]$ are homogeneous of degree n. By Hilbert's basis theorem, 1.5 there is N such that

$$f_{N+1} = f_1 g_1 + \cdots + f_N g_N$$

where g_n is homogeneous of degree $N - n + 1$. By substitution

$$b = ab \ , \ a \in M$$

giving $b = 0$. □

Proposition 9.3 (Going-up)**.** *Let $A \subset B$ be a finite ring extension and let M be a maximal ideal in A. If B is noetherian there is a maximal ideal N in B contracting $M = A \cap N$.*

Proof. $MB \neq B$ by 9.1. □

Proposition 9.4 (Going-down)**.** *Let $A \subset B$ be a noetherian domain integral over a normal subring. For maximal ideal N in B and a prime ideal $P \subset A \cap N$ in A there is a prime ideal $Q \subset N$ in B contracting $P = A \cap Q$.*

Proof. If

$$st \notin PB, \text{ for all } s \in A - P,\ t \in B - N$$

then choose Q maximal in the set of ideals in B containing PB and not containing any st. Let $K \subset L$ be the fraction fields. Let $st \in PB$ have minimal polynomial over A

$$(st)^n + a_{n-1}(st)^{n-1} + \cdots + a_0 = 0$$

so $a_{n-1}, \ldots, a_0 \in P$. Since A is normal and

$$t^n + \frac{a_{n-1}}{s} t^{n-1} + \cdots + \frac{a_0}{s^n} = 0$$

is the minimal polynomial for t over K it follows that $\frac{a_{n-1}}{s}, \ldots, \frac{a_0}{s^n} \in A$. As $s \notin P$ this gives $t^n \in PB$. So by contradiction $st \notin PB$. □

10. The power series ring

Proposition 10.1. *Let $k[[T_1,\dots,T_n]]$ be the power series ring over a field k. Assume*

$$f(0,\dots,0,T_n) = a_sT_n^s + \dots,\ a_s \neq 0$$

(1) *For any $g \in k[[T_1,\dots,T_n]]$ there are unique $u \in k[[T_1,\dots,T_n]]$ and $b_0,\dots,b_{s-1} \in k[[T_1,\dots,T_{n-1}]]$ such that*

$$g = uf + (b_0 + \dots + b_{s-1}T_n^{s-1})$$

(2) *There are unique unit $u \in k[[T_1,\dots,T_n]]$ and $b_0,\dots,b_{s-1} \in k[[T_1,\dots,T_{n-1}]]$ such that*

$$f = u(b_0 + \dots + b_{s-1}T_n^{s-1} + T_n^s)$$

Proof. (1) Let M be the $k[[T_1,\dots,T_{n-1}]]$-linear map

$$M(\sum a_iT_n^i) = \sum a_{s+i}T_n^i$$

Using $f = (f - M(f)T_n^s) + M(f)T_n^s$, u must satisfy

$$M(g) = M(uf) = M(u(f - M(f)T_n^s)) + uM(f)$$

The linear map

$$uM(f) \mapsto M(u(f - M(f)T_n^s)) + uM(f)$$

is sum of the identity and a linear map with image in the ideal $(T_1,\dots,T_{n-1})$. It is invertible and therefore give the claim. (2) By (1)

$$T_n^s = u^{-1}f - (b_0 + \dots + b_{s-1}T_n^{s-1})$$

□

Proposition 10.2. *The power series ring $k[[T_1,\dots,T_n]]$ over a field k is noetherian.*

Proof. Assume by induction and 1.5 that $k[[T_1,\dots,T_{n-1}]][T_n]$ is noetherian. Let I be an ideal. After a change of variables

$$U_1 = T_1 - T_n^{d^{n-1}},\dots,U_{n-1} = T_{n-1} - T_n^d$$

we may assume $f \in I$ satisfying the hypothesis of 10.1. Any $g \in I$ has a presentation

$$g = uf + b_0 + \dots + b_{s-1}T_n^{s-1}$$

with $b_0 + \dots + b_{s-1}T_n^{s-1} \in I$. By 1.6 the intersection

$$I \cap k[[T_1,\dots,T_{n-1}]] + \dots + k[[T_1,\dots,T_{n-1}]]T_n^{s-1}$$

is generated by finitely many elements. These together with f generates I. □

Theorem 10.3. *Let k be a field. Then the power series ring $k[[T_1,\dots,T_n]]$ is a unique factorization domain.*

Proof. Assume by induction and 4.3 that $k[[T_1,\dots,T_{n-1}]][T_n]$ has unique factorization. By 10.2 there is an irreducible factorization. To see that if an irreducible element $f|gh$ then $f|g$ or $f|h$, make a change of variables

$$U_1 = T_1 - T_n^{d^{n-1}},\dots,U_{n-1} = T_{n-1} - T_n^d$$

such that the product fgh satisfy the hypothesis of 10.1. Then the elements f,g,h are associated to elements in $k[[T_1,\dots,T_{n-1}]][T_n]$ and the result follows from the induction hypothesis. □

CHAPTER II

Algebraic varieties

k is a fixed algebraically closed ground field.

1. Affine space

Definition 1.1. The **affine n-space** $\mathbb{A}^n$ is the coordinate space k^n together with the set of polynomial functions $k[X_1, \ldots, X_n]$. For a set of polynomials S in $k[X_1, \ldots, X_n]$ the subset of $\mathbb{A}^n$ of solutions

$$V(S) = \{x \in \mathbb{A}^n | f(x) = 0, \text{ for all } f \in S\}$$

is a **(closed) affine set**. For any subset X of $\mathbb{A}^n$ the ideal of polynomials vanishing on X is denoted

$$I(X) = \{f \in k[X_1, \ldots, X_n] | f(x) = 0, \text{ for all } x \in X\}$$

If X is an affine set, then the affine ring

$$k[X] = k[X_1, \ldots, X_n]/I(X)$$

is called the **affine coordinate ring** of X.

Proposition 1.2. *Let X be an affine set. The maximal ideals in the affine coordinate ring $k[X]$ are exactly the ideals of the form*

$$(X_1 - x_1, \ldots, X_n - x_n), \ (x_1, \ldots, x_n) \in X$$

Proof. For any $(x_1, \ldots, x_n)$, $I(X) \subseteq (X_1 - x_1, \ldots, X_n - x_n)$ if and only if $f(x_1, \ldots, x_n) = 0$ for all $f \in I(X)$. By Hilbert's Nullstellensatz, I.3.3 this handle all maximal ideals. □

Theorem 1.3. *The ideal of an affine set $V(S)$ is the radical of the ideal generated by S.*

$$I(V(S)) = \{f | f^m \text{ is in the ideal generated by } S\}$$

Proof. $I(V(S))$ is its own radical, so by I.3.4 it is the intersection of all maximal ideals containing it. By 1.2 this is exactly the maximal ideals containing S. □

Definition 1.4. Given an affine set X, an **open** subset is a set of the form $X - Y$, where Y is an affine set in the same affine space. The open subsets give a topology on the set X called the **Zariski topology**. The closed subsets are the affine subsets.

Definition 1.5. Let U be an open subset of an affine set X, a function $f : U \to k$ is **regular at** $u \in U$, if there exist elements $g, h \in k[X]$ such that $h(u) \neq 0$ and $f(v) = g(v)/h(v)$ for all $v \in U - V(h)$. f is **regular** if it is regular at every $u \in U$. The regular functions on U give a ring denoted

$$\Gamma(U)$$

Proposition 1.6. *Let $X \subset \mathbb{A}^n$ be an affine set. The ring of regular functions is the affine coordinate ring*

$$\Gamma(X) = k[X]$$

Proof. If $f = g_x/h_x$ is regular at every $x \in X$, then by Hilbert's basis theorem I.1.8 the ideal generated by the denominators h_x is finitely generated by $h_1, \dots, h_m$ and $fh_1^2 = g_1h_1, \dots, fh_m^2 = g_mh_m$. Since $h_x(x) \neq 0$, by 1.2 the ideal $(h_1, \dots, h_m)$ is the whole ring, so $1 = a_1h_1^2 + \cdots + a_mh_m^2$ for some $a_1, \dots, a_m$. This gives $f = a_1g_1h_1 + \cdots + a_mg_mh_m \in k[X]$. □

2. Projective space

Definition 2.1. The **projective n-space** $\mathbb{P}^n$ is the coordinate space $k^{n+1} - \{0\}$ modulo the equivalence relation

$$(x_0, \dots, x_n) \sim (\lambda x_0, \dots, \lambda x_n),\ \lambda \in k - \{0\}$$

together with the set of homogeneous polynomial functions $k[X_0, \dots, X_n]$. For a set of homogeneous polynomials of positive degree S in $k[X_0, \dots, X_n]$ the subset of $\mathbb{P}^n$ of solutions

$$V(S) = \{x \in \mathbb{P}^n | f(x) = 0, \text{ for all } f \in S\}$$

is a **(closed) projective set**. For any subset X of $\mathbb{P}^n$ the homogeneous ideal of polynomials vanishing on X is denoted

$$I(X) = \{f \in k[X_0, \dots, X_n] | \deg f > 0,\ f(x) = 0, \text{ for all } x \in X\}$$

If X is a projective set, then the graded affine ring

$$k[X] = k[X_0, \dots, X_n]/I(X)$$

is called the **homogeneous coordinate ring** of X.

Proposition 2.2. *Let X be a projective set. Then X is empty if and only if the ideal*

$$I(X) = (X_0, \dots, X_n)$$

Proof. $X \subset \mathbb{P}^n$ is empty if and only if the affine set $V(I(X)) = \{0\} \subset \mathbb{A}^{n+1}$. So the statement follows from 1.2. □

Theorem 2.3. *The homogeneous ideal of a projective set $V(S)$ is*

$$I(V(S)) = \{f | f^m \textit{ is in the ideal generated by } S\}$$

Proof. Follows from 1.3 applied to the affine set $V(S) \subset \mathbb{A}^{n+1}$. □

Definition 2.4. Given a projective set X, an **open** subset is a set of the form $X - Y$, where Y is a projective set in the same projective space. The open subsets give a topology on the set X called the **Zariski topology**. The closed subsets are the projective subsets.

Definition 2.5. Let U be an open subset of an projective set X, a function $f : U \to k$ is **called regular at** $u \in U$, if there exist homogeneous elements $g, h \in k[X]$ of the same degree such that $h(u) \neq 0$ and $f(v) = g(v)/h(v)$ for all $v \in U - V(h)$. f is **regular** if it is regular at every $u \in U$. The regular functions on U give a ring denoted

$$\Gamma(U)$$

Proposition 2.6. *Let $X \subset \mathbb{P}^n$ be a projective set. The ring of regular functions is a finite product of copies of the field k*

$$\Gamma(X) = k \times \cdots \times k$$

Proof. See 3.10 below. □

3. Varieties

Definition 3.1. An **(algebraic) variety** is an open subset of either an affine set or a projective set together with the Zariski topology and the rings of regular functions. An **affine** variety is a full affine set and a **projective** variety is a full projective set.
An **(algebraic) morphism** of varieties is a map $f : X \to Y$ transforming by composition regular functions on Y to regular functions on X. That is

(1) f is continuous.
(2) For an open subset of V of Y and a regular function $g : V \to k$ the composite $g \circ f : f^{-1}(V) \to k$ is a regular function.

Definition 3.2. A nonempty closed subset of a variety is **irreducible** if it is not the union of two smaller closed subsets. A nonempty open subset of an irreducible variety is a dense subset and an irreducible variety. The closure of an irreducible subvariety is irreducible. Maximal closed irreducible subsets are called **irreducible components**.

Proposition 3.3. *Let X be a variety.*

(1) *Any nonempty set of closed subsets contain minimal elements.*
(2) *There is a decomposition*
$$X = X_1 \cup \cdots \cup X_s$$
into irreducible components, unique up to order.

Proof. (1) A variety is of the form $V(I) - V(J),\ J \subset I$, so closed subsets correspond to ideals between I, J in a noetherian ring. Such a set contains maximal elements giving minimal closed subsets. (2) If there is a subset which is not a finite union of irreducible subsets, then by (1) there is a minimal such. This is union of two smaller sets each then being a finite union of irreducible subset giving a contradiction. If Y is in a decomposition then for some i, j $X_i \subset Y$ and $Y \subset X_j$ giving uniqueness. □

Proposition 3.4. *An affine or projective variety X is irreducible if and only if the ideal $I(X)$ is a prime ideal. The irreducible components of X correspond to the minimal prime ideals containing $I(X)$.*

Proof. If the product of two ideals is contained in a prime ideal, then one of the ideals is contained in the prime ideal. This fact gives the statement. □

Proposition 3.5. *Let X be a variety. Morphisms $X \to \mathbb{A}^1$ are exactly the regular functions on X.*

Proof. Let $f \in \Gamma(X)$, it suffices to show that the subset $f^{-1}(0)$ is closed. If $f(x) = g(x)/h(x) = 0$ then $V(g) \cap X$ is a closed subset, and the intersection of all these is $f^{-1}(0)$. □

Proposition 3.6. *Assume $Y \subseteq \mathbb{A}^n$. A morphism $f : X \to Y$ is given by regular functions $f_1, \dots, f_n \in \Gamma(X)$*
$$f(x) = (f_1(x), \dots, f_n(x))$$
If Y is an affine variety, this gives a ring homomorphism
$$f^* : k[Y] \to \Gamma(X),\ Y_j \mapsto f_j$$
and $f \mapsto f^*$ maps morphisms bijectively onto ring homomorphisms.

Proof. Follows from 3.5 and 1.6. □

Proposition 3.7. *Let $U_i = \mathbb{P}^n - V(X_i)$. The map*
$$U_i \to \mathbb{A}^n,\ (x_0, \dots, x_i, \dots, x_n) \mapsto (\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i})$$

is an isomorphism.
$U_0, \ldots, U_n$ *give an open covering of the projective space* $\mathbb{P}^n$ *by copies of the affine space* $\mathbb{A}^n$.

Proof. The map is clearly bijective transforming closed subsets to closed subsets, so it is a homeomorphism. If $i = 0$, a fraction of polynomials $g(x_1, \ldots, x_n)/h(x_1, \ldots, x_n)$ with $\deg g = e,\ \deg h = f$ give a fraction of homogeneous polynomials

$$\frac{x_0^{e+f} g(x_1/x_0, \ldots, x_n/x_0)}{x_0^{e+f} h(x_1/x_0, \ldots, x_n/x_0)}$$

of the same degree $e + f$. So the map is an isomorphism. □

Proposition 3.8. *A variety is isomorphic to an open subset of a projective set.*

Proof. By 3.7 an affine set $X \subset \mathbb{A}^n$ is isomorphic to an open subset of the closure of the image in $\mathbb{P}^n$. □

Proposition 3.9. *Assume* $Y \subseteq \mathbb{P}^n$. *A morphism* $f : X \to Y$ *is a map given by an open covering* $U_1, \ldots, U_s$ *of* X *and regular functions* $f_{i0}, \ldots, f_{in} \in \Gamma(U_i)$

$$f(x) = (f_{i0}(x), \ldots, f_{in}(x)),\ x \in U_i$$

satisfying

$$f_{ik}(x) f_{jl}(x) - f_{il}(x) f_{jk}(x),\ x \in U_i \cap U_j$$

Proof. 3.6 and 3.7 and two homogeneous coordinates $(f_{i0}, \ldots, f_{in})$ and $(f_{j0}, \ldots, f_{jn})$ are proportional if and only if they satisfy the relation in the statement. □

Proposition 3.10. *Let* $X \subset \mathbb{P}^n$ *be an irreducible projective variety. A regular function is constant, that is the ring of regular functions* $\Gamma(X) = k$.

Proof. Let X have homogeneous coordinate ring $k[X] = k[X_0, \ldots, X_n]/I$ and let $f : X \to k$ be a regular function. By 3.7 and 3.5 there are homogeneous polynomials g_i such that $f = g_i/X_i^{d_i}$ on $X \cap U_i$. It follows for big d that the homogeneous part $f\, k[X]_d \subset k[X]_d$ and therefore $f^m\ k[X]_d \subset k[X]_d$ for all m. $(x, y) = (x, f(x))$ are solutions to a set of equations

$$Y^m X_i^d - g_{im}(X_0, \ldots, X_n) = 0$$

The space of homogeneous forms of degree d is finite dimensional,

$$g_{im} = a_0 g_{i0} + \cdots + a_{m-1} g_{i\,m-1},\ a_j \in k$$

giving

$$Y^m X_i^d = (a_0 + \cdots + a_{m-1} Y^{m-1}) X_i^d$$

Now use that a polynomial has only finitely many roots and conclude that f is constant. □

Proposition 3.11. *Let* $X \subseteq \mathbb{A}^n$ *be an affine variety and* f *a regular function. The open subset* $X_f = X - V(f)$ *is isomorphic to the affine variety* $V(I, fX_{n+1} - 1) \subseteq A^{n+1}$ *by the morphism*

$$(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_n, 1/f(x_1, \ldots, x_n))$$

Proof. By 3.5 this is a morphism and the projection $(x_1 \ldots, x_{n+1}) \mapsto (x_1 \ldots, x_n)$ is the inverse. □

Proposition 3.12. *A variety has a basis for the Zariski topology consisting of open subsets isomorphic to affine sets.*

Proof. 3.11 gives the affine case and 3.7 makes the reduction to the affine case. □

4. Product of varieties

Proposition 4.1. *The Segre map*

$$\mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{mn+m+n}$$

$$((x_0,\dots,x_m),(y_0,\dots,y_n)) \mapsto (z_{ij}) = (x_0y_0,\dots,x_0y_n,\dots,x_my_n)$$

is injective. The image is the projective variety

$$V(\{z_{ik}z_{jl} - z_{il}z_{jk} | i \neq j, k \neq l\})$$

A subset $Z \subset \mathbb{P}^m \times \mathbb{P}^n$ maps to a closed subset of $\mathbb{P}^{mn+m+n}$ if it is the set of solutions to polynomials $F(X_0,\dots,X_m,Y_0,\dots,Y_n)$ homogeneous in the X_i's and Y_j's.

Proof. The matrix identity

$$\begin{pmatrix} x_0y_0 & \dots & x_0y_n \\ & \vdots & \\ x_my_0 & \dots & x_my_n \end{pmatrix} = \begin{pmatrix} x_0 \\ \vdots \\ x_m \end{pmatrix} \begin{pmatrix} y_0 & \dots & y_n \end{pmatrix}$$

shows that the lefthanded side has rank 1. The image is given by equations

$$z_{ik}z_{jl} - z_{il}z_{jk} = 0$$

The projection of a matrix onto a nonzero column is the inverse map. If the degree in X_i's is d and Y_j's is e and $e > d$, then the polynomial F is replaced by the $m+1$ homogeneous polynomials

$$FX_0^{e-d},\dots,FX_m^{e-d}$$

of degree e in both set of variables and therefore coming from homogeneous polynomials in the variables $Z_{ij} = X_iY_j$. □

Definition 4.2. Let varieties $X,\ Y$ be given as open subsets of projective sets in $\mathbb{P}^m,\ \mathbb{P}^n$. By the image of the Segre map a variety in $\mathbb{P}^{mn+m+n}$ is defined and called the **product** denoted by $X \times Y$. $\mathbb{A}^m \times \mathbb{A}^n$ is isomorphic to $\mathbb{A}^{m+n}$. If $X,\ Y$ are affine then $X \times Y$ is affine. If $X,\ Y$ are projective then $X \times Y$ is projective.

Proposition 4.3. *The product $X \times Y$ satisfy*

(1) *The projections $p : X \times Y \to X,\ q : X \times Y \to Y$ are morphisms.*
(2) *For any pair of morphisms $g : Z \to X,\ h : Z \to Y$ there exist a unique morphism $f : Z \to X \times Y$ such that $g = p \circ f,\ h = q \circ h$.*

Proof. To prove the maps being morphisms the varieties X, Y can be assumed affine. The result follows from 3.6. □

Proposition 4.4. *The product of irreducible varieties is an irreducible variety.*

Proof. If $X \times Y = Z_1 \cup Z_2$ then the sets

$$X_i = \{x \in X | x \times Y \subset Z_i\}$$

give a decomposition $X = X_1 \cup X_2$. The set

$$X_i = \bigcap_{y \in Y} \{x | (x,y) \in Z_i\}$$

is closed. □

Proposition 4.5. *The graph of a morphism $f : X \to Y$ is a closed subset of $X \times Y$.*

Proof. It suffices to prove that the diagonal $\mathbb{A}^n \subset \mathbb{A}^n \times \mathbb{A}^n$ is closed. This is given by linear equations. □

Theorem 4.6. *Let X be a projective variety and Y any variety. For any closed subset $Z \subset X \times Y$ the projection $p(Z) \subset Y$ is a closed subset.*

Proof. It is enough to treat the case $p : \mathbb{P}^n \times \mathbb{A}^m \to \mathbb{A}^m$. A closed subset Z is the zero's of a finite number of polynomials

$$f_i(X_0, \dots, X_n, Y_1, \dots, Y_m) = 0,\ i = 1, \dots, r$$

homogeneous in the X_j's of degree d_i. For $y \in \mathbb{A}^m$

$$y \notin p(Z) \text{ if and only if } (X_0, \dots, X_n)^s \subset (f_i(X, y)),\ s >> 0$$

The linear map

$$\oplus_i k[X]_{s-d_i} \to k[X]_s,\ (g_i(X)) \to \sum_i g_i(X) f_i(X, y)$$

is surjective when a maximal minor is nonzero, so the set of $y \notin p(Z)$ is open. □

Proposition 4.7.

(1) *The image of a projective variety is a projective variety.*
(2) *A morphism from an irreducible projective variety to an affine variety is constant.*
(3) *A variety which is both affine and projective is a finite set of points.*

Proof. (1) 4.5, 4.6. (2) A coordinate function has closed irreducible image in $\mathbb{A}^1$ and it cannot be surjective because $\mathbb{A}^1$ is open in $\mathbb{P}^1$ then contradicting 4.6. □

Proposition 4.8. *The **Veronese morphism** of degree d is the map sending homogeneous coordinates to monomials of degree d*

$$\mathbb{P}^n \to \mathbb{P}^{\binom{n+d}{d}-1}$$

$$(x_0, \dots, x_n) \mapsto (\dots, y_{i_0 \dots i_n}, \dots) = (x_0^d, x_0^{d-1} x_1, \dots, x_n^d)$$

This is an isomorphism onto the image which is a closed subvariety.
If $F \in k[X_0, \dots, X_n]$ is a nonzero homogeneous form, then the open subset $\mathbb{P}^n - V(F)$ is mapped isomorphically to an affine subvariety of $\mathbb{A}^{\binom{n+d}{d}-1}$.

Proof. Projecting onto the next $n+1$ coordinates starting at a pure d-power

$$(\dots, y_{i_0 \dots i_n}, \dots) \mapsto (x_0, \dots, x_n) = (y_{\dots d \dots}, \dots, y_{\dots d-1\,0 \dots 0\,1 \dots})$$

is an inverse. By 4.7 the map transports closed sets to closed sets so it is an isomorphism. The image of $V(F)$ is represented by the intersection of the hyperplane given by the linear form with coefficients from the monomials in F, so the complement is in a complement of a hyperplane which is affine. □

5. Rational functions

Definition 5.1. Let X be an irreducible variety. Define an equivalence relation on the set of all regular functions by

$$(f : U \to k) \sim (g : V \to k) \text{ if } f = g \text{ on } U \cap V$$

The equivalence classes give a field extension $k(X)$ of k called the **field of rational functions**. It depends only on a nonempty open subset.

Proposition 5.2. *Let X be an irreducible affine variety. The field of rational functions $k(X)$ is the field of fractions of the ring of regular functions $k[X]$.*

Proof. Follows from 1.6. □

Proposition 5.3. *Let X be an irreducible projective variety. The field of rational functions $k(X)$ is the subfield of fractions $\frac{f}{g}$, f, g homogeneous of the same degree. For any nonzero form t of degree 1 the ring $k(X)[t, t^{-1}]$ is the ring consisting of all homogeneous fractions of any degree.*

Proof. Assume by coordinate change $t = X_0$. □

Proposition 5.4. *For an irreducible variety X the field of rational functions $k(X)$ is a finitely generated field extension of k.*

Proof. As the field of rational functions only depend on an open subset, this follows from 5.2. □

6. Dimension of varieties

Definition 6.1. The **dimension** of an irreducible variety X is

$$\dim X = \operatorname{trdeg}_k k(X)$$

A nonempty open subset U of X has dimension $\dim U = \dim X$.

Proposition 6.2. *If $Y \subset X$ is an irreducible closed proper subset of an irreducible variety, then*

$$\dim Y < \dim X$$

Proof. The varieties can be assumed affine. Then this follows from I.5.1. □

Theorem 6.3. *If $f \in \Gamma(X)$ is a nonzero regular function on an irreducible variety and Y is an irreducible component of the* ***hypersurface*** *$V(f)$, then*

$$\dim Y = \dim X \ - 1$$

Proof. I.5.4. □

Proposition 6.4. *The length of a maximal chain of irreducible closed subsets of an irreducible variety X is $\dim X$, i.e.*

$$\emptyset \neq Y_1 \subset \cdots \subset Y_{\dim X} = X$$

Y_i irreducible closed and the chain cannot be refined.

Proof. Let $U \subset X$ be an open affine and $f \in k[U]$ not constant. Then set $Y_{\dim X - 1}$ to be a component of the closure of $V(f)$ in X. By 6.3 $\dim Y_{\dim X-1} = \dim X - 1$. Finish by induction. □

Proposition 6.5. *If $f_1, \dots, f_r \in \Gamma(X)$ and Y is an irreducible component of $V(f_1, \dots, f_r)$, then*

$$\dim Y \geq \dim X \ - r$$

Proof. Let Z be a component of $V(f_1, \dots, f_{r-1})$ containing Y. If f_r is nonzero on Z, $\dim Y = \dim Z - 1$, 6.3. □

Proposition 6.6. *Let $X \subset \mathbb{P}^n$ be an irreducible projective variety and let $F_1, \dots, F_r$ be homogeneous forms. If $r \leq \dim X$, then*

$$V(F_1, \dots, F_r) \cap X \neq \emptyset$$

and for Y an irreducible component of $V(F_1, \dots, F_r) \cap X$

$$\dim Y \geq \dim X \ - r$$

Proof. In $\mathbb{A}^{n+1}$, $0 \in V((F_1, \dots, F_r) + I(X))$ so there is a nonempty component Z of dimension

$$\dim Z \geq \dim X + 1 - r \geq 1$$

giving $V(F_1, \dots, F_r) \cap X \neq \emptyset$. □

Proposition 6.7. *Let $X \subset \mathbb{P}^n$ be an irreducible projective variety. Then there are $L_0, \dots, L_{\dim X}$ linear homogeneous forms such that*

$$V(L_0, \dots, L_{\dim X}) \cap X = \emptyset$$

Proof. 6.6. □

Proposition 6.8.

(1) *Let* $Y \subset X \subset \mathbb{A}^n$ *be irreducible closed subvarieties with* $r = \dim X - \dim Y$. *Then there exist* $f_1, \dots, f_r \in \Gamma(X)$ *such that and* Y *is an irreducible component of* $V(f_1, \dots, f_r) \cap X$.

(2) *Let* $Y \subset X \subset \mathbb{P}^n$ *be irreducible closed subvarieties with* $r = \dim X - \dim Y$. *Then there exist* $F_1, \dots, F_r$ *homogeneous forms such that and* Y *is an irreducible component of* $V(F_1, \dots, F_r) \cap X$.

Proof. $f_1 \in I(Y) - I(X)$. Let $Z_1, \dots, Z_s$ be the components of $V(f_1, \dots, f_{i-1}) \cap X$, $f_i \in I(Y) - I(Z_1) \cup \dots \cup I(Z_s)$, then $\dim Z = \dim X - i$ for any component Z of $V(f_1, \dots, f_i)$. □

Proposition 6.9. *Let* X, Y *be irreducible. Then*

$$\dim X \times Y = \dim X + \dim Y$$

Proof. A combined chain of irreducible give $\dim X \times Y \geq \dim X + \dim Y$. Assume X, Y affine and by 6.8 there are $f_1, \dots, f_{\dim X} \in k[X]$ such that $\{x\}$ is a component of $V(f_1, \dots, f_{\dim X})$. By 6.5 $\dim Y \geq \dim X \times Y - \dim X$. □

Proposition 6.10.

(1) *Let* $X \subset \mathbb{A}^n$ *be irreducible closed subvariety with* $\dim X = n - 1$. *Then there exists a polynomial* f *such that*

$$X = V(f),\ I(X) = (f)$$

(2) *Let* $X \subset \mathbb{P}^n$ *be irreducible closed subvariety with* $\dim X = n - 1$. *Then there exists a homogeneous form* F *such that*

$$X = V(F),\ I(X) = (F)$$

Proof. Unique factorization, I.4.4, gives that prime ideals minimal over a polynomial are principal. □

Proposition 6.11.

(1) *Let* $X, Y \subset \mathbb{A}^n$ *be irreducible closed subvarieties. If* Z *is an irreducible component of* $X \cap Y$, *then*

$$\dim Z \geq \dim X + \dim Y - n$$

(2) *Let* $X, Y \subset \mathbb{P}^n$ *be irreducible closed subvarieties. If* Z *is an irreducible component of* $X \cap Y$, *then*

$$\dim Z \geq \dim X + \dim Y - n$$

If $\dim X + \dim Y \geq n$ *then* $X \cap Y \neq \emptyset$.

Proof. (1) $X \cap Y = X \times Y \cap$ (diagonal in$\mathbb{A}^n \times A^n$), $X \cap Y = X \times Y \cap V(X_1 - Y_1, \dots, x_n - Y_n)$ and 6.5. (2) There is a component W of the nonempty closed subset $V(I(X) + I(Y)) \subset \mathbb{A}^{n+1}$. By (1) $\dim W \geq \dim X + 1 + \dim Y + 1 - (n + 1) \geq 1$ giving $X \cap Y \neq \emptyset$. □

7. Finite morphisms

Definition 7.1. A morphism $f : X \to Y$ is called **finite** if for every $y \in Y$ there is an open affine subset $y \in V \subset Y$ such that $f^{-1}(V)$ is affine and the ring extension $f^*(k[V]) \subset k[f^{-1}(V)]$ is finite.

Proposition 7.2. *Let* $f : X \to Y$ *be a finite morphism. If* Y *is affine, then* X *is affine and the extension* $f^*(k[Y]) \subset k[X]$ *is finite.*

Proof. Let $g_j \in k[Y]$ be a finite set of elements such that $\cup Y_{g_j} = Y$, $X_{g_j \circ f}$ are affine and $f^*(k[Y_{g_j}]) \subset k[X_{g_j \circ f}]$ are integral. $\Gamma(X) \to \prod k[X_{g_j \circ f}]$ is injective so $\Gamma(X)$ is integral over $f^*(K[Y])$ and becomes an affine ring. The affine variety with coordinate ring $\Gamma(X)$ is isomorphic to X. □

Proposition 7.3. *Let $f : X \to Y$ be a finite morphism.*

(1) *$f^{-1}(y)$ is a finite set for each $y \in Y$.*
(2) *Let $Z \subset X$ be a closed subset, then $f(Z) \subset Y$ is a closed subset.*

Proof. Assume X, Y affine. (1) $f^{-1}(y)$ corresponds to the maximal ideals in the ring $k[X]/f^*(m_y)k[X]$ which is has finite dimension over k. (2) Assume $Z = X$. If $y \in Y - f(X)$ then $f^*(m_y)k[X] = k[X]$ so by Nakayama's lemma, I.9.1 there is $g \in k[Y]$ with $g(y) \neq 0$ and $Y_g \cap f(X) = \emptyset$. □

Proposition 7.4. *Let X be an irreducible variety of dimension n.*

(1) *If X is affine, then there is a separable surjective finite morphism*
$$f : X \to \mathbb{A}^n$$
(2) *If X is projective, then there is a (separable??) surjective finite morphism*
$$f : X \to \mathbb{P}^n$$

Proof. I.7.2 and 7.3. □

Proposition 7.5. *Let $X \subset \mathbb{P}^n$ be an irreducible projective variety and $L_0, \ldots, L_{\dim X}$ linear homogeneous forms such that $V(L_0, \ldots, L_{\dim X}) \cap X = \emptyset$, then*
$$X \to \mathbb{P}^{\dim X},\ x \mapsto (L_0(x), \ldots, L_{\dim X}(x))$$
is a finite surjective morphism.

Proof. 6.7. □

Definition 7.6. A morphism $f : X \to Y$ is called **dominant** if the image is dense $\overline{f(X)} = Y$.

Proposition 7.7. *Let $f : X \to Y$ be a dominant morphism of irreducible varieties.*

(1) *There is a field extension $f^*(k(Y)) \subset k(X)$.*
(2) $\dim X \geq \dim Y$.
(3) *$f(X)$ contains a nonempty open subset of Y.*

Proof. (3) Assume X, Y affine, $r = \dim X - \dim Y$ and choose by Noether's normalization theorem, I.2.7, $t_1, \ldots, t_r \in k[X]$ algebraically independent over $f^*(k(Y))$. Clearing denominators in the minimal polynomials for a finite set of generators of $k[X]$ over $f^*(k[Y])$ gives a nonconstant $g \in k[Y]$ such that $k[X_{g \circ f}]$ is integral over $f^*(k[Y_g])[t_1, \ldots, t_r]$. This gives a finite morphism $X_{g \circ f} \to Y_g \times \mathbb{A}^r$ which by 7.3 is surjective, so $Y_g \subset f(X)$. □

Theorem 7.8. *Let $f : X \to Y$ be a dominant morphism of irreducible varieties.*

(1) *Let $W \subset Y$ be a closed irreducible subset of Y and let $Z \subset X$ be an irreducible component of $f^{-1}(W)$ with $\overline{f(Z)} = W$, then*
$$\dim Z \geq \dim W + (\dim X - \dim Y)$$
(2) *There is a nonempty subset $V \subset f(X)$ open in Y such that for W, Z as in (1) satisfying $W \cap V \neq \emptyset$, $Z \cap f^{-1}(V) \neq \emptyset$*
$$\dim Z = \dim W + (\dim X - \dim Y)$$

Proof. Assume X, Y affine. (1) W is a component of $V(f_1, \dots, f_{\dim Y - \dim W})$ by 6.8, so

$$\dim Z \geq \dim X - (\dim Y - \dim W)$$

(2) By the proof of 7.7 there is an open subset $V \subset Y$ and finite surjective morphism $f^{-1}(V) \to V \times \mathbb{A}^{\dim X - \dim Y}$. It follows that $\dim Z \leq \dim W + (\dim X - \dim Y)$. □

8. Fibre of morphisms

Proposition 8.1. *Let $f : X \to Y$ be a dominant morphism of irreducible varieties.*

(1) *Let $y \in Y$ and let $Z \subset X$ be a irreducible component of the fibre $f^{-1}(y)$, then*

$$\dim Z \geq \dim X - \dim Y$$

(2) *There is a nonempty subset $V \subset f(X)$ open in Y such that for each $y \in V$ and Z as in (1)*

$$\dim Z = \dim X - \dim Y$$

Proof. 7.8. □

Proposition 8.2. *Let $f : X \to Y$ be a dominant morphism of irreducible varieties. For every nonnegative integer n the set*

$$\{x \in X \mid \dim Z \geq n \textit{ for some component } Z \textit{ of } f^{-1}(f(x))\}$$

is a closed subset of X.

Proof. 8.1 gives an open subset $V \subset Y$ such that for $x \in X - f^{-1}(V)$ all components of $f^{-1}(f(x))$ have dimension $\dim X - \dim Y$. Induction on $\dim Y$ give the statement for $f_| : Z \to W$, where W is a component of $Y - V$ and Z a component of $f^{-1}(W)$. □

Proposition 8.3. *Let $f : X \to Y$ be a surjective morphism $f(X) = Y$ of projective varieties with Y and $f^{-1}(y)$, $y \in Y$ all irreducible. If the dimension $\dim f^{-1}(y)$ is constant then X is irreducible.*

Proof. There is a component Z of X such that $f(Z) = Y$. Now use 8.2 to get $X = Z$. □

Proposition 8.4. *Let $f : X \times Y \to Z$ be a morphism. Assume X is irreducible projective and Y irreducible. If there exists $y' \in Y$ such that $X \times \{y'\} \subset f^{-1}(f(y'))$ then*

$$X \times \{y\} \subset f^{-1}(f(y)), \ \ y \in Y$$

Proof. X is projective so the projection of the graph of f onto $Y \times Z$ is a closed subvariety W by 4.6. Let $x' \in X$ be fixed. The projection $p : W \to Y$ is surjective with fibre $p^{-1}(y') = (y', f(x', y'))$ so $\dim W = \dim Y$ by 8.1. The graph of $Y \to Z$, $y \mapsto f(x', y)$ is a closed subvariety of W isomorphic to Y and thereby equal to W giving $f(x, y) = f(x', y)$. □

Definition 8.5. Let U_i be open and Z_i closed subsets of X. The finite union

$$U_1 \cap Z_1 \cup \cdots \cup U_r \cap Z_r$$

is called **constructible**.

Proposition 8.6 (Chevalley)**.** *Let $f : X \to Y$ be a morphism and $W \subset X$ a constructible subset. The image $f(W) \subset Y$ is constructible.*

Proof. Assume $W = X$ and by induction on $\dim Y$ assume f dominant. By 7.8 reduce to a component of $Y - V$ and use induction. □

Proposition 8.7. *Let $X \subset Y$ be a constructible subset. The following conditions are equivalent.*

(1) *$X \subset Y$ is open.*
(2) *If $W \subset Y$ is an irreducible closed subset with $X \cap W \neq \emptyset$, then $\overline{X \cap W} = W$.*

Proof. 8.6. □

Proposition 8.8. *Let $f : X \to Y$ be a morphism. The following conditions are equivalent.*

(1) *For any open $U \subset X$ the image $f(U) \subset Y$ is open.*
(1) *If $W \subset Y$ is an irreducible closed subset with $f(X) \cap W \neq \emptyset$ and $Z \subset f^{-1}(W)$ an irreducible component, then $\overline{f(Z)} = W$.*

Proof. 8.6. □

Proposition 8.9. *Let $U \subset X \times Y$ be an open subset. The projections $p(U) \subset X$, $q(U) \subset Y$ are open.*

Proof. 8.6. □

Definition 8.10. A dominant morphism $f : X \to Y$ with $f^*(k(Y)) = k(X)$ is called a **birational** isomorphism.

Proposition 8.11. *Let $f : X \to Y$ be a birational isomorphism. There is a nonempty open subset $V \subset Y$ such that $f : f^{-1}(V) \to V$ is an isomorphism.*

Proof. Assume Y affine and let $U \subset X$ be an open affine. If Z is a component of $X - U$ then $\dim \overline{f(Z)} < \dim Y$, so there is $h \in k[Y]$ such that $f^{-1}(Y_g) \subset U$, so assume also X affine. Clearing denominators in a set of generators of $k[X]$ over $k[Y]$ gives the result. □

9. Local ring and tangent space

Definition 9.1. Let X be a variety. For $x \in X$ the **local ring** $O_{X,x}$ (or O_x) at x is defined to be the ring of equivalence classes of regular functions at x

$$(f : U \to k) \sim (g : V \to k) \text{ if } f_{|W} = g_{|W}$$

where $W \subset U \cap V$ are open sets containing x.
The local ring depends only on an open neighborhood of the point.

Proposition 9.2.

(1) *For affine space*

$$O_{\mathbb{A}^n,x} = \{\frac{f}{g} \in k(X_1, \dots, X_n) | g(x) \neq 0\}$$

(2) *If $X \subset \mathbb{A}^n$ is an affine variety, then*

$$O_{X,x} = O_{\mathbb{A}^n,x}/I(X)O_{\mathbb{A}^n,x}$$

(3) *$O_{X,x}$ is a noetherian ring with exactly one maximal ideal m_x and*

$$O_{X,x}/m_x \simeq k$$

Proof. (1) A fraction of fractions is a fraction. (2) The righthand side maps surjectively to the lefthanded side. If a fraction f/g gives the 0 function, it is 0 in an open affine set $X - V(h)$ so $hf = 0$ on X, that is $f/g \in IO_{\mathbb{A}^n,x}$. (3) $f : U \to k$ is in m_x if $f(x) = 0$ and if $f(x) \neq 0$ it is invertible in $O_{X,x}$. □

Proposition 9.3. *The local ring O_x is an integral domain if and only if $x \in X$ is lying on exactly one irreducible component.*

Proof. Let $X = X_1 \cup \dots \cup X_s$ be the irreducible components.

$$U = X_1 - X_2 \cup \dots \cup X_s$$

is an open irreducible subset of X. If $x \in U$ then O_x is an integral domain. If $x \in X_1 \cap X_2$ and for simplicity $s = 2$ choose $f_i \in I(X_i) - I(X_j)$. Then $f_1, f_2 \neq 0$ and $f_1 f_2 = 0$ in O_x. □

Proposition 9.4. *Assume X to be irreducible.*

(1) *$O_{X,x}$ is an integral domain and the field of fractions is the field of rational functions $k(X)$.*
(2) *If $U \subset X$ is an open subset, then*

$$\Gamma(U) = \bigcap_{x \in U} O_{X,x}$$

Proof. (2) An element of the intersection give for every $x \in U$ a value $f(x) \in k$. □

Definition 9.5. Let $X = V(I) \subset \mathbb{A}^n$ be an affine set. For $x \in X$ and $f \in I$ the differential

$$df = \sum_1^n \frac{\partial f}{\partial X_i}(x)(X_i - x_i)$$

is a linear polynomial in $k[X_1, \dots, X_n]$. The **(embedded) tangent space** to X at x is the affine linear subspace

$$T_x X = V(\{df | f \in I\})$$

Let $X = V(I) \subset \mathbb{P}^n$ be a projective set. For $x \in X$ and $F \in I$ homogeneous the differential

$$dF = \sum_0^n \frac{\partial f}{\partial X_i}(x) X_i$$

is a homogeneous polynomial in $k[X_0, \dots, X_n]$. The **projective (embedded) tangent space** to X at x is the projective linear subspace

$$T_x X = V(\{dF | F \in I\})$$

By Euler's formula $\sum_0^n \frac{\partial f}{\partial X_i} X_i = \deg(F)\, F$ it follows that the restriction of the projective tangent space to an open affine coordinate space in $\mathbb{P}^n$ is identified with the affine tangent space.

Proposition 9.6. *Let $m_x \subset O_{X,x}$ be the maximal ideal in the local ring at x. The tangent space is the k-linear dual to the vector space m_x/m_x^2*

Proof. Let $h \in m_x,\ y \in T_x X$ then $dh(y) \in k$ gives a nondegenerate pairing

$$m_x/m_x^2 \times T_x X \to k$$

Assume $X \subset \mathbb{A}^n$ and $x = 0$ so m_x is generated by $X_1, \dots, X_n$. If $dh(y) = 0$ for all y then h is represented by a polynomial with zero constant and linear term, so $h \in m_x^2$. □

Definition 9.7. Let X be a variety, the **tangent space** $T_x X$ is independent of an open affine neighborhood and identified with the linear dual of m_x/m_x^2.
Let $f : X \to Y$ be a morphism of varieties. For $y = f(x)$ transport of regular functions give a ring homomorphism

$$f^* : O_{Y,y} \to O_{X,x},\ f^*(m_y) \subset m_x$$

and an induced map linear map

$$f^*(x) : m_y/m_y^2 \to m_x/m_x^2$$

The linear dual map

$$df(x) : T_x X \to T_y Y$$

is called the **differential** at x.
These constructions respect composition, so an isomorphism give isomorphic tangent spaces.
If $p : X \times Y \to X,\ q : X \times Y \to Y$ are the projections, then

$$(dp(x,y), dq(x,y)) : T_{(x,y)} X \times Y \to T_x X \times T_y Y$$

is an isomorphism.

Proposition 9.8. *Let $x \in X,\ y \in Y$ be points on varieties. If $\phi : O_{Y,y} \to O_{X,x},\ \phi(m_y) \subset m_x$ is a ring homomorphism, then there are open neighborhoods $x \in U \subset X,\ y \in V \subset Y$ and a morphism $f : U \to V$ such that $f^* = \phi : O_{Y,y} \to O_{X,x}$. If ϕ is an isomorphism, then f also can be chosen to be an isomorphism.*

Proof. Assume $X \subset \mathbb{A}^m, Y \subset \mathbb{A}^n$ affine and x, y the 0 points. Then

$$\phi(T_j) = \sum_1^m \frac{f_i}{g_i} S_i,\ f_i, g_i \in k[X]$$

Let $U = X - V(g_1 \dots g_m)$. □

Proposition 9.9. *Let $f : X \to Y$ be an injective morphism such that the differential $df(x)$ is injective for all points $x \in X$. If one of the following conditions are satisfied*

(1) *X is projective.*
(2) *f is finite.*

then $f : X \to f(X)$ is an isomorphism.

Proof. Let $y = f(x)$

$$f^*(x) : m_y/m_y^2 \to m_x/m_x^2$$

is surjective, so by Nakayama's lemma I.9.1

$$f^* : O_{Y,y} \to O_{X,x}$$

is surjective for all x. Assume X, Y affine and let J be the kernel of $f^* : k[Y] \to k[X]$. This gives $k[Y]/J \simeq k[X]$. □

Proposition 9.10. *Let X be irreducible of $\dim X = n$. Then there is a nonempty open subset $U \subseteq X$ which is isomorphic to an open subset of an irreducible hypersurface in $\mathbb{A}^{n+1}$.*

Proof. Assume X affine and find I.7.2 regular functions $f_1, \dots, f_n$ such that $k[X]$ is integral over the polynomial ring $k[f_1, \dots, f_n]$ and $k(f_1, \dots, f_n) \subset k(X)$ is separable. The rest follows from the primitive element theorem I.7.1. □

Proposition 9.11. *Let X be an irreducible variety. Then for $x \in X$*

$$\dim T_x X \geq \dim X$$

Proof. 3.12 reduces to an affine variety $X = V(f_1, \dots, f_m) \subset \mathbb{A}^n$. The subset of points x where

$$\dim T_x X = \min\{\dim T_z X | z \in X\}$$

is given by nonvanishing minors of the Jacobi matrix $\big(\partial f_i/\partial X_j\big)$ and is therefore open. By 9.10 it is assumed $m = 1$, so the result follows from 6.3. □

10. Nonsingular varieties

Definition 10.1. An irreducible variety X is **nonsingular,(smooth, regular)** at x if $\dim T_x X = \dim X$ else **singular, (nonsmooth,nonregular)**. If all points are nonsingular then X is nonsingular.
$x \in X,\ y \in Y$ are nonsingular if and only if $(x, y) \in X \times Y$ is nonsingular.

Theorem 10.2. *Let X be an irreducible variety.*

(1) *The set of nonsingular points is a nonempty open subset.*
(2) *If Y is an irreducible component of the singular points in X, then*

$$\dim Y < \dim X$$

Proof. (1) By 9.10 it is assumed that $X = V(f)$ for some $f \in k[X_1, \dots, X_{n+1}]$. Then in characteristic 0 some $\partial f/\partial X_i \neq 0$. In characteristic p if all $\partial f/\partial X_i = 0$ there is g, $g^{p^m} = f$ with some $\partial g/\partial X_i \neq 0$. In both cases the set of nonsingular points is nonempty. (2) 6.2. □

Theorem 10.3. *Let $x \in X$ be a nonsingular point in an irreducible variety. The local ring at x, O_x is a unique factorization domain.*

Proof. Let the regular functions in an open affine neighborhood of x, $t_1, \dots, t_n$ give a basis over k of the space m_x/m_x^2. The Taylor-expansion define compatible ring isomorphisms

$$O_x/m_x^s \simeq k[t_1, \dots, t_n]/(t_1, \dots, t_n)^s$$

giving an identification

$$O_x \subset k[[t_1, \dots, t_n]]$$

by Krull's intersection Theorem, I.9.2.
If $f, g \in O_x$ is such that the fraction $\frac{g}{f} \in k[[t_1, \dots, t_n]]$ then by Krull's theorem

$$gO_x = \bigcap_x gO_x + m_x^n$$

so $\frac{g}{f} \in O_x$.
By 9.2 it remains to show that if an irreducible element $f|gh$ in O_x then $f|g$ or $f|h$. By I.10.3 there is a factorization $g = fg'$ in $k[[t_1, \dots, t_n]]$ giving a factorization in O_x by the result above. □

Proposition 10.4. *Let X be a nonsingular irreducible variety and let $Y \subset X$ be an irreducible closed subvariety. If $\dim Y = \dim X - 1$, then for any $y \in Y$ there is an open affine $U \subset X$, $y \in U$ and $f \in k[U]$ such that $I(Y \cap U) = (f)$ in $k[U]$.*

Proof. 10.3 give that a prime ideal in $O_{X,y}$ minimal over a nonzero element is principal. □

Proposition 10.5. *Let X be a nonsingular irreducible variety and let Y be a projective variety. Assume $f : U \to Y$ is a morphism defined on a maximal open subset $U \subset X$. Then for a component Z of $X - U$*

$$\dim Z \leq \dim X - 2$$

Proof. If $\dim Z = \dim X - 1$ then by 10.4 there is an open affine neighborhood U of any $z \in Z$ such that $I(U \cap Z) = (h)$. If $Y \subset \mathbb{P}^n$ then the morphism hf extends f. □

Proposition 10.6. *Let X be a nonsingular irreducible projective variety. If $\dim X = n$ then X is isomorphic to a closed subvariety of $\mathbb{P}^{2n+1}$.*

Proof. Let $X \subset \mathbb{P}^N$ and consider the closed subset $X_1 \subset \mathbb{P}^N$ consisting of all projective lines through two points of X and the closed subset $X_2 \subset \mathbb{P}^N$ consisting of all embedded projective tangent lines through points of X. Then $\dim X_1 \leq 2n + 1$ and $\dim X_2 \leq 2n$. If $N > 2n + 1$ then $y \in \mathbb{P}^N - (X_1 \cup X_2)$ give a projection $X \to \mathbb{P}^{N-1}$ which by 9.9 is an isomorphism onto a closed subvariety. □

Proposition 10.7. *Let $x \in X$ be a nonsingular point of an irreducible variety of dimension n. Then there is an open neighborhood U of x which is isomorphic to an open subset of a closed hypersurface in $\mathbb{A}^{n+1}$.*

Proof. ??? Local version of the proof of 10.6. □

Proposition 10.8. *Let X be an nonsingular irreducible variety, and let $Y, Z \subset X$ be irreducible closed subvarieties. If W is an irreducible component of $Y \cap Z$, then*

$$\dim W \geq \dim Y + \dim Z - \dim X$$

Proof. $Y \cap Z = Y \times Z \cap$ diagonal in X and 6.5. □

11. Normal varieties

Definition 11.1. An irreducible variety X is **normal** at x if the local ring O_x is normal. If normality hold at all points then X is normal.
If $x \in X, y \in Y$ are normal then $(x, y) \in X \times Y$ is normal.

Proposition 11.2. *A nonsingular variety is normal.*

Proof. 10.3. □

Proposition 11.3. *Let X be a normal irreducible variety and let $Y \subset X$ be a irreducible closed subvariety. If $\dim Y = \dim X - 1$, then there is an open affine $U \subset X,\ Y \cap U \neq \emptyset$ and $f \in k[U]$ such that $I(Y \cap U) = (f)$ in $k[U]$.*

Proof. Assume X affine and $I(Y) \subset k[X]$ the unique prime ideal minimal over $g \neq 0$. Then there is a minimal n such that $I(Y)^n \subset (g)$. Choose $h \in I(Y)^{n-1} - (g)$, then $hI(Y) \subset (g)$. If $hI(Y) \subset gI(Y)$, then $\frac{h}{g}$ is integral over the normal domain $k[X]$, so the contradiction $h \in (g)$. Therefore choose $f \in I(Y)$ such that $hf \in hI(Y) - gI(Y)$ then $hf = gs,\ s \in k[X] - I(Y)$. In the ring $k[X][s^{-1}]$, $I(Y) = (f)$. □

Proposition 11.4. *Let X be a normal irreducible variety and let Y be a component of the closed set of singular points in X. Then*

$$\dim Y \leq \dim X - 2$$

Proof. If $\dim Y = \dim X - 1$, $I(Y) = (f)$ by 11.3. By 10.2 there is $y \in Y$ such that $\dim T_y Y = \dim Y$. Now $m_{Y,y} = m_{X,y}/fO_{X,y}$ so $\dim T_y X \leq \dim Y + 1 = \dim X$ and y is nonsingular on X. □

Proposition 11.5. *Let X be a normal irreducible variety and let $f : U \to k$ be a regular function on an open subset $U \subset X$. If for every component Z of $X - U$*

$$\dim Z \leq \dim X - 2$$

then f is the restriction to U of a regular function on X.

Proof. Assume X affine and $f \notin k[X]$. $k[X]$ is noetherian so choose the ideal $P = \{g \in k[X] | ghf \in k[X]\}$ maximal in the family over $h \in k[X],\ hf \notin k[X]$. P is a prime ideal and by construction f is not regular at $x \in X - V(P)$. $V(P)$ is a component of $X - U$ and by I.8.2 $\dim V(P) = \dim X - 1$. □

Proposition 11.6. *Let $f : X \to Y$ be a finite surjective morphism of irreducible varieties.*

(1) *If Y is normal and $f(x) \in W \subset Y$ is closed irreducible, then there is an irreducible component $x \in Z \subset f^{-1}(W)$ such that $\overline{f(Z)} = W$.*
(2) *If Y is normal then for every open subset $U \subset X$, f(U) is open in Y. For each $y \in Y$ the number of points in the fibre*
$$|f^{-1}(y)| \leq \dim_{k(Y)} k(X)$$
(3) *If the extension $f^*(k(Y)) \subset k(X)$ is separable then there is a nonempty open subset V of Y such that for each $y \in Y$ the number of points in the fibre*
$$|f^{-1}(y)| = \dim_{k(Y)} k(X)$$

Proof. Assume X, Y affine. (2) Let $g \in k[X]$, $y \in f(X_g)$. The minimal polynomial for g over $f^*(K(Y))$ come from $T^r + T^{r-1}a_1 + \cdots + a_r \in k[Y][T]$ since the ring $k[Y]$ is normal, 10.3. The morphism $X \to Y \times \mathbb{A}, x \mapsto (f(x), g(x))$ is then finite and therefore surjective by 7.3. If $a_i(y) \neq 0$ then $Y_{a_i} \subset f(X_g)$ and $f(X_g)$ is open. If g have distinct values at points in $f^{-1}(y)$, then $T^r + T^{r-1}a_1(y) + \cdots + a_r(y)$ has at least $|f^{-1}(y)|$ roots,

$$|f^{-1}(y)| \leq r \leq \dim_{k(Y)} k(X)$$

(3) By 10.2 assume Y nonsingular and $k[X]$ is generated over $f^*(k[Y])$ by a separable polynomial. In that case

$$|f^{-1}(y)| = \dim_{k(Y)} k(X)$$

for all $y \in Y$. □

Definition 11.7. Let Y be an irreducible variety and $k(Y) \subset K$ a finite field extension. A **normalization** of Y in K is a normal irreducible variety X and a finite surjective morphism $\pi : X \to Y$ such that the extension $\pi^*(k(Y) \subset k(X)$ is isomorphic to the given extension. If $k(Y) = K$ this is the normalization.

Proposition 11.8. *Let Y be an irreducible variety and $k(Y) \subset K$ a finite field extension.*

(1) *There is a up to isomorphism unique normalization $\pi : X \to Y$ of Y in K.*
(2) *If Y is affine, then X is affine.*
(3) *If Y is projective, then X is projective.*

Proof. (2) $k[X]$ is the normalization of $k[Y]$ in K I.8.4. (3) Let A be the integral closure of $k[Y]$ in $K(t)$ for some form t of degree one, 5.3. A is a graded ring finitely generated over k. There is a d such that the subring $A_0 \oplus A_d \oplus A_{2d} \oplus \dots$ is generated by elements of 'degree one'. The projective variety with this homogeneous coordinate ring is the normalization. □

Proposition 11.9. *Let Y an irreducible variety. The set of points where Y is normal is a nonempty open subset.*

Proof. The normalization $f : X \to Y$ gives the open subset $y \in V \subset Y$ where $|f^{-1}(y)| = 1$. □

Proposition 11.10. *Let X be a normal irreducible projective variety. If $\dim X = n$ then X is isomorphic to the normalization of a closed hypersurface $V(F) \subset \mathbb{P}^{n+1}$.*

Proof. Assume $X \subset \mathbb{P}^N$ and let $L_0, \dots, L_{n+1}$ be linear forms such that $X \cap V(L_0, \dots, L_{n+1}) = \emptyset$, then the projection $X \to \mathbb{P}^{n+1}$ is finite with image $V(F)$. Conclude by X is normal. □

12. Flat morphisms

Definition 12.1. An morphism $f : X \to Y$ is **flat** at $x \in X$ if the local ring O_x is flat over $O_{f(x)}$. If f is flat for all points then f is a flat morphism.
If $V \subset Y$ is open or closed then the restriction $f : f^{-1}(V) \to V$ is flat. The projection $X \times Y \to X$ is flat. A morphism to a point is flat.

Proposition 12.2. *Let $f : X \to Y$ be a flat morphism of irreducible varieties. If $Z \subset f^{-1}(y)$ is an irreducible component, then*

$$\dim Z = \dim X - \dim Y$$

Proof. 10.3. □

Proposition 12.3. *Let $f : X \to Y$ be a flat morphism. Assume Y is irreducible and n is a fixed number. The following are equivalent.*

(1) *Any irreducible component $Z \subset X$ has*

$$\dim Z = \dim Y + n$$

(2) *If $W \subset Y$ is irreducible and $Z \subset f^{-1}(W)$ is an irreducible component, then*

$$\dim Z = \dim W + n$$

(3) *If $Z \subset f^{-1}(y)$ is an irreducible component, then*

$$\dim Z = n$$

Proof. 10.3. □

Proposition 12.4. *Let $f : X \to Y$ be a flat morphism. For any open $U \subset X$ the image $f(U) \subset Y$ is open.*

Proof. 10.3. □

Proposition 12.5. *Let $f : X \to Y$ be a flat morphism with Y irreducible. Then there is a nonempty open subset $V \subset Y$ such that the restriction $f : f^{-1}(V) \to V$ is flat.*

Proof. 10.3. □

Proposition 12.6. *Let $f : X \to Y$ be a flat and finite morphism with Y irreducible. Then for any nonempty open subset affine $V \subset Y$ the extension*

$$f^*(k[V]) \subset k[f^{-1}(V)]$$

is free.

Proof. 10.3. □

Proposition 12.7. *Let $f : X \to Y$ be a finite morphism with Y irreducible. The following are equivalent.*

(1) *f is flat.*
(2) *The rank*

$$\dim_k O_x / f^*(m_y)$$

is independent of points $y = f(x)$.

Proof. 10.3. □

CHAPTER III

Algebraic curves

In this note a **curve** is an irreducible nonsingular projective variety of dimension 1 over a fixed algebraically closed ground field k.
The general theory for nonsingular and normal varieties, chapter II, section 9-11, provides several useful facts.

(1) The normalization of an irreducible projective variety of dimension 1 is a curve, II.11.8, II.11.4.
(2) A morphism $U \to Y$ from an open subset of a curve X to a projective variety extends to a morphism $X \to Y$, II.10.5.
(3) A nonconstant morphism $f : X \to Y$ of curves is surjective and characterized by the finite field extension $f^* : k(Y) \to k(X)$, II.9.8.
(4) By normalization any finitely generated field K of $\mathrm{trdeg}_k K = 1$ is the field of rational functions $K \simeq k(X)$ for a curve X unique up to isomorphism.
(5) A curve X admits a finite morphism $X \to \mathbb{P}^1$.
(6) Also any curve is isomorphic to a curve in $\mathbb{P}^3$, II.10.6.

The theory of curves is therefore equivalent to the theory of finitely generated field extensions of transcendence degree one over a fixed algebraically closed field.

1. Local ring

Let x be a point on a curve X. The local ring O_x is identified with a subring of the field of rational functions $k(X)$. The maximal ideal is denoted m_x and $k = O_x/m_x$.

Proposition 1.1. *Let x be a point on a curve X. The maximal ideal in the local ring O_x is principal and any nonzero ideal is a power of the maximal ideal. The local ring is a principal ideal domain.*

Proof. Let $t \in m_x$ give a generator of m_x/m_x^2. By I.9.1 $m_x = (t)$. By I.9.2 $\cap_n (t^n) = 0$, so for $0 \neq f \in O_x$ there is n such that $f \in (t^n) - (t^{n+1})$. Since any ideal is finitely generated it follows that a nonzero ideal is of the form (t^n). □

Definition 1.2. A function t giving a generator of m_x is a **local parameter** at x. A nonzero $f \in k(X)$ has a unique representation $f = ut^i$ where u is a unit in O_x and $i \in \mathbb{Z}$. The integer exponent is independent of the choice of local parameter t. This defines

$$v_x : k(X)^* \to \mathbb{Z},\ f \mapsto i$$

the **valuation** at x, satisfying

(1) $v_x(f) = 0$ if $f \in k^*$.
(2) $v_x(fg) = v_x(f) + v_x(g)$
(3) $v_x(f + g) \geq \min(v_x(f), v_x(g))$

x is a **zero** of f if $v_x(f) > 0$ and a **pole** if $v_x(f) < 0$.
A surjective map $k(X)^* \to \mathbb{Z}$ satisfying (1)-(3) is a **valuation** on the field.

Proposition 1.3. *Let x be a point on a curve X. The local ring is*

$$O_x = \{f \in k(X) | f = 0 \textit{ or } v_x(f) \geq 0\}$$

The maximal ideal is

$$m_x = \{f \in k(X) | f = 0 \textit{ or } v_x(f) \geq 1\}$$

Proof. Property (1)-(3) in 1.2. □

Proposition 1.4. *Let X be a curve. The map*

$$x \to v_x$$

defines a bijection between the points of X and the set of valuations on the field $k(X)$.

Proof. Let $x, y \in X$ have $v_x = v_y$ and choose an open affine set containing x, y. From $m_x = m_y$ it follows that $I(x) = I(y)$ and therefore $x = y$ showing injectivity. Let v be a valuation and assume $X \subset \mathbb{P}^n$ such that all $X_i \notin I(X)$ and $v(X_i/X_0) \geq 0$. Let $k[x_1, \ldots, x_n]$ be the coordinate ring of $X \cap \mathbb{P}^n - V(X_0)$, note that $\{f | v(f) > 0\}$ is a maximal ideal and get a point $(a_1, \ldots, a_n)$ such that $v(x_i - a_i) > 0$ for all i. Then $v(f) \geq 0$ for all $f \in O_{X,a}$. It follows that $v = v_a$. □

Proposition 1.5. *Let X be a curve.*

(1) *For a rational function $f \in k(X)^*$ there is at most finitely many points with $v_x(f) \neq 0$.*
(2) *For finitely many points $x_1, \ldots, x_s \in X$ and integers $n_1, \ldots, n_s$ there exists a rational function $f \in k(X)$ with*

$$v_{x_i}(f) = n_i, \; i = 1, \ldots, s$$

Proof. (1) $\{x | v_x(f) \neq 0\}$ is a closed subset. (2) Let U be an open affine subset containing $x_1, \ldots, x_s$ and let $m_1, \ldots, m_s \subset k[U]$ be corresponding maximal ideals. Choose $f_i \in m_i - m_i^2 \cup \cup_{j \neq i} m_j$ and set $f = \prod_i f_i^{n_i}$. □

2. Divisor

Definition 2.1. A **divisor** on a curve X is a finite formal sum

$$D = \sum_i n_i x_i$$

where $x_i \in X$ and $n_i \in \mathbb{Z}$. This is an element in the **divisor group** $\mathrm{Div}(X)$ being the free Abelian group on the points of X. The **degree** is $\deg(D) = \sum_i n_i$ and this is an additive map $\mathrm{Div}(X) \to \mathbb{Z}$. D is **effective** if $n_i \geq 0$ for all i. There is an ordering $D \geq D'$ if $D - D'$ is effective.

Proposition 2.2. *There is an additive map*

$$\mathrm{div} : k(X)^* \to \mathrm{Div}(X), \; \mathrm{div}(f) = \sum_x v_x(f) \, x$$

satisfying

$$\mathrm{div}(f) = 0 \textit{ if and only if } f \in k^*$$

Proof. Well defined by 1.5. If $\mathrm{div}(f) = 0$ then $f \in \Gamma(X)$ and therefore constant by II.3.10. □

Definition 2.3. A divisor $D' = D + \mathrm{div}(g)$ is **equivalent** to D, $D' \sim D$.

Definition 2.4. For a divisor D the k-vector space

$$L(D) = \{f \in k(X) | f = 0 \text{ or } \mathrm{div}(f) \geq -D\}$$

is the **linear series**. The dimension is denoted

$$l(D) = \dim_k L(D)$$

Proposition 2.5. *For divisors $D, D' \in \mathrm{Div}(X)$*

(1) *If* $D \geq D'$ *then* $L(D') \subseteq L(D)$ *and* $\dim_k L(D)/L(D') \leq \deg(D - D')$.
(2) $L(0) = k$ *and if* $D < 0$ *then* $L(D) = 0$.
(3) $l(D)$ *is finite.*
(4) *If* $D = \sum n_i x_i$ *then* $l(D) \leq \sum_{n_i > 0} n_i + 1$.
(5) *If* $D \sim D'$ *then* $l(D) = l(D')$

Proof. (1) Assume $D = \sum n_x x = D' + x$ and let t be a local parameter at x. Then $L(D')$ is the kernel of the linear map

$$L(D) \to k, f \mapsto (t^{n_x} f)(x)$$

(2) If $D < 0$ then there is a zero. (3)-(4) Use (1) and (2). (5) If $D + \operatorname{div}(g) = D'$ then $L(D') \simeq L(D),\ f \mapsto fg$. □

3. Riemann's Theorem

Definition 3.1. For a divisor $D = \sum n_x\, x$ the k-vector space

$$\Lambda(D) = \{\lambda : X \to k(X) | \lambda(x) = 0 \text{ or } v_x(\lambda(x)) \geq -n_x, \text{ for all } x\}$$

is the **adele series**. The union

$$\Lambda(X) = \bigcup_D \Lambda(D)$$

contains $k(X)$ as constant maps such that

$$L(D) = \Lambda(D) \cap k(X)$$

Proposition 3.2. *For divisors* $D \geq D'$

(1) $\Lambda(D') \subseteq \Lambda(D)$ *and*

$$\dim_k \Lambda(D)/\Lambda(D') = \deg(D - D')$$

(2) $l(D) - l(D') =$

$$\deg(D) - \deg(D') - \dim_k \Lambda(D) + k(X)/\Lambda(D') + k(X)$$

Proof. (1) Let $n_x \geq n'_x$ and t a local parameter at x, then $t^{-n_x}, \ldots, t^{-n'_x - 1}$ give a basis over k at x. (2) Noether's isomorphism and (1). □

Proposition 3.3. *Let* $f \in k(X)^*$ *be a nonzero rational function.*

(1) *If* f *is nonconstant*

$$\sum_{v_x(f)>0} v_x(f) = \dim_{k(f)} k(X)$$

(2) $\deg(\operatorname{div}(f)) = 0$.
(3) *If* $D \sim D'$ *then* $\deg(D) = \deg(D')$.
(4) *If* $\deg(D) < 0$ *then* $l(D) = 0$.

Proof. Let $x_1, \ldots, x_s$ be the points where $v_x(f) > 0$. By 1.5 choose f_i such that $v_{x_i}(f_i) = 1$ and $v_{x_j}(f_i) >> 0,\ j \neq i$, then

$$f_1^{-1}, \ldots, f_1^{-v_{x_1}(f)}, \ldots, f_s^{-1}, \ldots, f_s^{-v_{x_s}(f)}$$

are linear independent over $k(f)$ giving

$$\sum_{v_x(f)>0} v_x(f) \leq \dim_{k(f)} k(X)$$

Let $D = \sum_{v_x(f)>0} v_x(f) x$. If $g \in k(X)$ is integral over $k[f^{-1}]$ then $v_x(g) \geq 0$ if $x \neq x_i$, all i. There exist a positive m_0, $g \in L(m_0 D)$ and for $m \geq m_0$

$$g, gf^{-1}, \ldots, gf^{-m+m_0} \in L(mD)$$

Applying this to a basis of $k(X)$ over $k(f)$ integral over $k[f^{-1}]$ give

$$l(mD) \geq (m - m_0 + 1)\dim_{k(f)} k(X)$$

From 3.2 we then get

$$\begin{aligned} m \sum_{v_x(f)>0} v_x(f) \quad &\geq \quad -1 + \dim_k \Lambda(mD) + k(X)/\Lambda(0) + k(X) \\ &\quad +(m - m_0 + 1)\dim_{k(f)} k(X) \end{aligned}$$

for $m >> 0$. In the limit

$$\sum_{v_x(f)>0} v_x(f) \geq \dim_{k(f)} k(X)$$

□

Theorem 3.4 (Riemann)**.** *The set*

$$\{\deg(D) + 1 - l(D) | D \in \mathrm{Div}(X)\}$$

is bounded above.

Proof. Let $f \in k(X)$ be nonconstant and set $D = \sum_{v_x(f)>0} v_x(f)x$. From 3.3 and its proof follows

$$(m_0 - 1)\deg(D) \geq \dim_k \Lambda(mD) + k(X)/\Lambda(0) + k(X)$$

giving the right hand side is a positive constant for large m, so

$$\deg(mD) + 1 - l(mD)$$

is a positive constant for large m.
It suffices to treat a divisor $D' \geq 0$. For $m >> 0$, $l(mD - D') > 0$ so choose $0 \neq h \in L(mD - D')$ and get $mD \geq D' - \mathrm{div}(h)$ for $m >> 0$. The boundary for mD gives the statement. □

Definition 3.5. The maximal number of the set above is the **genus** of X and denoted by $g = g_X$. Note that $g \geq 0$.

Proposition 3.6.

(1) *For any divisor* D, $l(D) \geq \deg(D) + 1 - g$.
(2) *Let* D_0 *be a divisor giving* $g = \deg(D_0) + 1 - l(D_0)$.
If $\deg(D) \geq \deg(D_0) + g$ *then* $l(D) = \deg(D) + 1 - g$.

Proof. 3.4 and 2.5. □

Theorem 3.7. *For any divisor* D *on a curve* X

(1) $\Lambda(X)/\Lambda(D) + k(X)$ *has finite dimension over* k.
(2) $l(D) - \dim_k \Lambda(X)/\Lambda(D) + k(X) = \deg(D) + 1 - g$.

Proof. 3.4 and 2.5. □

4. Rational differential and canonical divisor

Definition 4.1. Let X be a curve. The space of **rational differentials** on X is the $k(X)$-vector space

$$\Omega(X) = \oplus_{f \in k(X)} k(X)df/(da, d(g+h) - dg - dh, d(gh) - hdg - gdh)$$

$a \in k, g, h \in k(X)$ generate the relations.
The k-linear map $d : k(X) \to \Omega(X),\ f \mapsto df$ is the universal k-derivation on $k(X)$, that is any derivation is the composite of d and a $k(X)$-linear map.

Theorem 4.2. *The dimension of differentials*

$$\dim_{k(X)} \Omega(X) = 1$$

Any function $t \in k(X)$ such that $k(t) \subset k(X)$ is finite separable gives a basis dt for $\Omega(X)$. If t is a local parameter at x, then dt is a basis.

Proof. By I.7.2 we may assume t transcendental over k and $k(t) \subset k(X)$ finite separable generated by u.
So $k(X) = k(t)[u]/(g)$ with $\frac{\partial g}{\partial u} \neq 0$. By implicit differentiation

$$du = -\frac{\frac{\partial g}{\partial t}}{\frac{\partial g}{\partial u}} dt$$

so dt is a generator and moreover

$$f \mapsto \frac{\partial f}{\partial t} - \frac{\frac{\partial g}{\partial t}}{\frac{\partial g}{\partial u}} \frac{\partial f}{\partial u}$$

is a nonzero derivation, so dt is a basis.
Let $x \in U = V(f_1, \dots, f_m) \subset \mathbb{A}^n$ be an open affine neighborhood.

$$\operatorname{rank}_k \big(\frac{\partial f_i}{\partial X_j}(x)\big) = n - 1$$

so for a local parameter t

$$dt = \sum_j \frac{\partial t}{\partial X_j} dX_j$$

must be nonzero. □

Definition 4.3. Let X be a curve. A nonzero rational differential $\omega \in \Omega(X)$ has a presentation $f dt$ where t is a local parameter at x. Define the **order** at x

$$v_x(\omega) = v_x(f)$$

independent of presentation and define a **canonical divisor**

$$\operatorname{div}(\omega) = \sum v_x(\omega) x$$

The sum is finite since $t - t(y)$ is a local parameter at y in an open neighborhood of x. All these divisors are equivalent and any choice is denoted $K = K_X$. For a divisor D there is a k-vector space

$$\Omega(D) = \{\omega \in \Omega(X) | \operatorname{div}(\omega) \geq D\}$$

Proposition 4.4 (Serre duality)**.** *Let $K = \operatorname{div}(\omega)$ be a canonical divisor. The linear map*

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

is an isomorphism.

Proof. 4.2. □

Definition 4.5. Let x be a point on a curve X. A local parameter t at x define compatible ring isomorphisms

$$O_x / m_x^n \simeq k[t]/(t^n)$$

giving a "Laurent series" embedding

$$L_t : k(X) \to k((t))$$

into the fraction field of the power series ring. Remark that

$$v_x(f) = \min\{r | a_r \neq 0,\ L_t f = \Sigma_n a_n t^n\}$$

and

$$O_x = k(X) \cap k[[t]]$$

In the basis dt a rational differential $\omega = f dt \in \Omega(X)$ has a presentation

$$L_t\omega = L_t f\, dt$$

satisfying

$$L_t df = \frac{d}{dt} L_t f\ dt = \Sigma_n n a_n t^{n-1} dt,\ L_t f = \Sigma_n a_n t^n$$

Define the **residue**

$$R_x(\omega) = a_{-1}$$

well defined by the following proposition.

Proposition 4.6. *The definition of residue is independent of the choice of local parameter t at x.*

Proof. Let t, u be local parameters and R_t, R_u the residue maps. Assume $f, g \in k(X)$, then the claim is

$$R_u(L_u g df) = R_t(L_t g df)$$

By the chain rule and additivity this reduces to

$$R_u(u^n du) = R_t(u(t)^n \frac{du}{dt}(t) dt)$$

for all integers n and $u(t) = t + a_2 t^2 + \dots$.

$$R_t(\frac{1}{t}(1 + a_2 t + \dots)^{-1}(1 + 2a_2 t + \dots) dt) = 1$$

shows the claim for $-1 \le n$. If the characteristic of k is 0 the formula

$$u(t)^n \frac{du}{dt}(t) = \frac{1}{n+1} \frac{du^{n+1}}{dt}(t)$$

gives the result for $n < -1$. Since the claim is a formal algebraic identity this suffices. □

Theorem 4.7. *Let ω be a rational differential. The sum of residues vanishes*

$$\sum_x R_x(\omega) = 0$$

Proof. If $X = \mathbb{P}^1,\ k(X) = k(t)$ then expansion in partial fractions reduces to the case

$$\omega = t^n dt = -(\frac{1}{t})^{-n-2} d\frac{1}{t}$$

For $n = -1$

$$R_{(0,1)}(t^{-1} dt) = 1,\ R_{(1,0)}(-(\frac{1}{t})^{-1} d\frac{1}{t}) = -1$$

give the formula. In general choose by I.7.2 a finite surjective separable morphism $\pi : X \to \mathbb{P}^1$, identifying $\pi^* : k(t)[u]/(g(u)) \simeq k(X)$ with $g(u)$ separable of degree n. For $x \in \mathbb{P}^1$, $\pi^{-1}(x) = \{x_1, \dots, x_r\}$ with local parameters t at x and t_i at x_i. By 3.3

$$\sum_i v_{x_i}(\pi^*(t)) = n$$

Laurent series

$$L_t : k(\mathbb{P}^1) \to k((t)),\ L_{t_i} : k(X) \to k((t_i))$$
$$L_{t_i}(\pi^*(t)) = t_i^{v_{x_i}(\pi^*(t))} + \dots$$

give field extensions

$$k((t)) \subset k((t_i)) \text{ of dimension } v_{x_i}(\pi^*(t))$$

By counting dimensions

$$k((t))[u]/(g(u)) \simeq k((t_1)) \times \cdots \times k((t_r))$$

so the trace map decomposes

$$Tr_{k(X)/k(t)} = \sum_i Tr_{k((t_i))/k((t))}$$

By the $\mathbb{P}^1$-case it is enough to show

$$\sum_i R_{x_i}(f d\pi^*(t)) = R_x(Tr_{k(X)/k(t)}(f)dt)$$

which amounts to the local result

$$R_s(s^m \frac{dt}{ds}(s)ds) = R_t(Tr_{k((s))/k((t))}(s^m)dt)$$

where $t = s^q + \dots$ determines the extension $k((t)) \subset k((s))$. Since the claim is a formal algebraic identity the case where the characteristic of k is 0 suffices. In this case assume by change of coordinates that $t = s^q$. The computations

$$s^m \frac{dt}{ds}(s) = qs^{m+q-1}$$

$$Tr_{k((s))/k((t))}(s^m) = \begin{cases} 0 & , \quad m \neq pq \\ qt^{m/q} & , \quad m = pq \end{cases}$$

give the result. □

Theorem 4.8. *The bilinear pairing*

$$\Omega(D) \times \Lambda(X)/\Lambda(D) + k(X) \to k$$

$$< \omega, \lambda >= \sum_x R_x(\lambda(x)\omega)$$

is nondegenerate and

$$\dim_k \Omega(D) = \dim_k \Lambda(X)/\Lambda(D) + k(X)$$

Proof. By 4.7 the pairing is well defined. If $< \omega, \lambda >= 0$ for all $\lambda \in \Lambda(X)$ then $\omega = 0$. Let $D = \sum n_x x$. If $\lambda \notin \Lambda(D) + k(X)$ then $v_x(\lambda(x)) < -n_x$ for some x. After chancing λ with a constant adele, let t be a local parameter at x chosen by 1.5 such that

$$v_y(t)(v_x(\lambda(x)) - 1) + v_y(\lambda(y)) \geq 0$$

for $y \neq x$, then

$$< t^{v_x(\lambda(x))-1}dt, \lambda >= R_x(t^{v_x(\lambda(x))-1}\lambda(x)dt) \neq 0$$

□

5. Riemann-Roch Theorem

Theorem 5.1 (Riemann-Roch)**.** *Let K be a canonical divisor on a curve X of genus g. Then for any divisor D*

$$l(D) - l(K - D) = \deg(D) + 1 - g$$

Proof. By 4.8

$$\dim_k \Omega(D) = \dim_k \Lambda(X)/\Lambda(D) + k(X)$$

3.7 and the isomorphism $L(K - D) \simeq \Omega(D)$ from 4.4. give the equality. □

Proposition 5.2. *Let X be a curve of genus g, K a canonical divisor and D any divisor.*

1. $\deg(K) = 2g - 2$.
2. $l(K) = g$.
3. *If* $\deg(D) \geq 2g - 1$ *then* $l(D) = \deg(D) + 1 - g$.
4. *If* $\deg(D) = 2g - 2$ *and* $l(D) = g$ *then* $D = K + \mathrm{div}(g)$.

Proof. 5.1. □

Proposition 5.3 (Clifford). *If D is a divisor with $l(D) > 0$ and $l(K-D) > 0$ then*

$$l(D) \leq 1 + \frac{1}{2}\deg(D)$$

Proof. By the hypothesis assume $D \geq 0$ and $K - D \geq 0$ and such that $l(D-x) < l(D)$ for all x. $h \in L(D) - \cup_x L(D-x)$ union over x with $K - D - x \geq 0$ gives an injective map

$$L(K-D)/L(0) \to L(K)/L(D),\ f \mapsto hf$$

Then by Riemann-Roch Theorem 5.1

$$\begin{aligned} l(D) &\leq 1 + l(K) - l(D) - \deg(K) + \deg(D) - 1 + g \\ &= -l(D) + 2 + \deg(D) \end{aligned}$$

□

Proposition 5.4. *If $n \geq 2g$ then for every $x \in X$ there is $f \in k(X)$ with "pole of order n at x", that is*

$$v_x(f) = -n,\ v_y(f) \geq 0, y \neq x$$

Proof. $f \in L(nx) - L((n-1)x)$ by 5.2. □

6. Zeuthen-Hurwitz formula

Let $f : X \to Y$ be a nonconstant morphism of curves.

Definition 6.1. f is surjective and by composition there is defined a finite field extension $k(Y) \subseteq k(X)$. The **degree** of f is

$$\deg(f) = \dim_{k(Y)} k(X)$$

For $x \in X$ the **ramification** is

$$e_x = v_x(f^*(u))$$

where u is a local parameter at $f(x)$. A point x with $e_x > 1$ is a **ramification** point of f.

Proposition 6.2. *For $y \in Y$*

$$\sum_{x \in f^{-1}(y)} e_x = \deg(f)$$

There are only finitely many ramification points, that is $e_x = 1$ except for finitely many $x \in X$.

Proof. For $Y = \mathbb{P}^1$ this is 3.3.
In general choose by 5.4 $h \in L(ny)$ such that $v_y(h) = -n,\ v_z(h) \geq 0, z \neq y$. This gives a morphism $h : Y \to \mathbb{P}^1$. The claim for $h, h \circ f$ gives the claim for f. II.11.6 give $e_x = 1$ except for finitely many x. □

Theorem 6.3 (Zeuthen-Hurwitz). *Let $f : X \to Y$ be a nonconstant morphism and assume that field extension $k(Y) \subset k(X)$ is separable and that the characteristic of the ground field k do not divide any ramification index e_x. Let g_X, g_Y denote the genus, then*

$$2g_X - 2 = \deg(f)\,(2g_Y - 2) + \sum_x (e_x - 1)$$

Proof. Let dh be a nonzero differential on Y, then by separability $df^*(h)$ is a nonzero differential on X. Let $f(x) = y$. If $v_y(h) \neq 0$ then by separability and the condition on e_x, $v_y(dh) = v_y(h) - 1$ and $v_x(df^*(h)) = e_x v_y(h) - 1$, otherwise all are zero. Therefore

$$\begin{aligned} 2g_X - 2 &= \sum_x v_x(df^*(h)) \\ &= \sum_y \sum_{x \in f^{-1}(y)} (e_x v_y(h) - 1) \\ &= \sum_y (v_y(h) - 1) \sum_{x \in f^{-1}(y)} e_x + \sum_x (e_x - 1) \end{aligned}$$

and then

$$\begin{aligned} 2g_X - 2 &= \sum_y v_y(dh) \deg(f) + \sum_x (e_x - 1) \\ &= \deg(f)(2g_Y - 2) + \sum_x (e_x - 1) \end{aligned}$$

□

Definition 6.4. A curve X of genus $g \geq 2$ is **hyperelliptic** if there is a separable morphism $f : X \to \mathbb{P}^1$ of $\deg(f) = 2$. The involution on the field extension $k(\mathbb{P}^1) \subset k(X)$ gives an involution $\tau : X \to X$ commuting with f, $f \circ \tau = f$.

Proposition 6.5. *Assume that the characteristic of* k *is not* 2*.*

(1) *A curve of genus* $g = 2$ *is hyperelliptic.*
(2) *A hyperelliptic curve has exactly* $2g + 2$ *ramification points.*

Proof. (1) Choose a canonical divisor $K \geq 0$. $f \in L(K) - L(0)$ gives $f : X \to \mathbb{P}^1$ of degree 2. (2) Let $f : X \to \mathbb{P}^1$ be of degree 2. By 6.3

$$\sum (e_x - 1) = 2g + 2, \quad \sum_{x \in f^{-1}(y)} e_x = \deg(f) = 2$$

give the number of ramification points. □

7. Plane curves

Let $X = V(F) \subset \mathbb{P}^2$ be a plane curve with $F \in k[X, Y, Z]$ irreducible homogeneous of degree n.

Definition 7.1. Let $G \in k[X, Y, Z]$ be a homogeneous form of degree m and not divisible by F. Then $V(F) \cap V(G) = \{x_1, \ldots, x_s\}$. Let $L \in k[X, Y, Z]$ be a linear form such that $V(L) \cap \{x_1, \ldots, x_s\} = \emptyset$ and define a divisor

$$\operatorname{div}(G) = \sum_i v_{x_i}\left(\frac{G}{L^m}\right) x_i$$

independent of L. This satisfies the product rule

$$\operatorname{div}(GH) = \operatorname{div}(G) + \operatorname{div}(H)$$

and therefore defines a divisor

$$\operatorname{div}\left(\frac{G}{H}\right) = \operatorname{div}(G) - \operatorname{div}(H)$$

also satisfying the product rule.

Proposition 7.2 (Bezout)**.**

(1) $\operatorname{div}(G) \geq 0$.
(2) $\deg(\operatorname{div}(G)) = mn$.

Proof. (2) Assume by change of coordinates and product rule that $G = Z$. Then use 3.3. □

Proposition 7.3. *The genus of X is*

$$g = \frac{1}{2}(n-1)(n-2)$$

Proof. Assume $X \cap V(Y,Z) = \emptyset$. For a fraction $\frac{H}{K}$ of homogeneous forms of degree d such that $\operatorname{div}(\frac{H}{K}) \geq -\operatorname{div}(Z^m)$

$$v_x(\frac{HZ^m}{Y^{m+d}}) \geq v_x(\frac{K}{Y^d})$$

for all x. This gives forms G, E such that

$$HZ^m = GK + EF$$

It follows that the linear map

$$k[X,Y,Z]_m \to L(\operatorname{div}(Z^m)),\ G \mapsto \frac{G}{Z^m}$$

is surjective and the linear map

$$k[X,Y,Z]_{m-n} \to k[X,Y,Z]_m,\ H \mapsto H \cdot F$$

for large m is an isomorphism onto the kernel of the map above. This gives for large m

$$l(\operatorname{div}(Z^m)) = \binom{m+2}{2} - \binom{m-n+2}{2} = mn + \frac{3n-n^2}{2}$$

Then by 3.6

$$g = \deg(Z^m) + 1 - l(\operatorname{div}(Z^m)) = mn + 1 - (mn + \frac{3n-n^2}{2}) = \frac{1}{2}(n-1)(n-2)$$

□

8. Morphisms to projective space

Definition 8.1. Let D be a divisor on X. A basis $f_0, \dots, f_n$ of $L(D)$ give a morphism

$$\phi(x) = (f_0(x), \dots, f_n(x)) : X \to \mathbb{P}^n$$

depending on the basis up to an isomorphism of $\mathbb{P}^n$.

Proposition 8.2. *Assume $D \geq 0$ and let $\phi : X \to \mathbb{P}^n$ be given above. If*

$$l(D - x - y) = l(D) - 2 \text{ for all } x \neq y$$

then ϕ is injective. If the condition also holds for $x = y$ then

$$\phi : X \to \phi(X)$$

is an isomorphism.

Proof. Let $D = \sum n_z z$ with $n_x = n_y = 0$ and assume $v_x(f_0) = 0$ and $v_y(f_0) = 1$. Then

$$\phi(x) = (1, \dots) \neq (0, \dots) = \phi(y)$$

Next assume $v_x(f_1) = 1$ and let $(Y_0, \dots)$ be coordinates in $\mathbb{P}^n$. Then

$$\phi^*(\frac{Y_1}{Y_0}) = \frac{f_1}{f_0}$$

is a local parameter at x giving injectivity of the differential $d\phi(x) : T_x X \to T_{\phi(x)}\mathbb{P}^n$. Conclude by II.9.9. □

Proposition 8.3. *Assume $D \geq 0$ and let $\phi : X \to \mathbb{P}^n$ be given above.*

(1) *If $\deg(D) \geq 2g + 1$ then $\phi : X \to \phi(X)$ is an isomorphism.*
(2) *If genus $g = 0$ and $D = x$ then $\phi : X \to \phi(X) = \mathbb{P}^1$ is an isomorphism.*

(3) *If genus* $g = 1$ *and* $D = 3x$ *then* $\phi : X \to \phi(X) \subset \mathbb{P}^2$ *is an isomorphism.*
(4) *If genus* $g \geq 2$ *and* $D = 3K$ *then* $\phi : X \to \phi(X) \subset \mathbb{P}^{5g-5}$ *is an isomorphism.*
(5) *If genus* $g > 2$ *and* $D = K$ *then* $\phi : X \to \mathbb{P}^{g-1}$ *is injective and if* X *is not hyperelliptic then* $\phi : X \to \phi(X) \subset \mathbb{P}^{g-1}$ *is an isomorphism.*

Proof. Riemann-Roch Theorem 5.1. 5.2. □

9. Weierstrass points

Definition 9.1. n is a **gap number** at x if $l(nx) = l((n-1)x)$, that is if there exists no rational function f such that $v_x(f) = -n, v_y(f) \geq 0,\ y \neq x$ or there exists a rational differential ω such that $v_x(\omega) = n-1, v_y(\omega) \geq 0,\ y \neq x$.

Proposition 9.2. *At a given* x *there are exactly* g *gap numbers*

$$1 = i_1 < \cdots < i_g \leq 2g - 1$$

Proof. By 5.2

$$1 = l(0) \leq \cdots \leq l((2g-1)x) = g$$
$$l(nx) \leq l((n-1)x) + 1, \text{ with equality if } n \geq 2g$$

□

Definition 9.3. x is a **Weierstrass point** if some gap number $i_j \neq j$, that is the sequence of gap numbers is not

$$1 < \cdots < g$$

By the Riemann-Roch Theorem x is a Weierstrass point exactly if $l(gx) > 1$ or if $l(K - gx) = \dim \Omega(gx) > 0$.

Proposition 9.4. *On a curve of genus* $g = 0, 1$ *there are no Weierstrass points. On a hyperelliptic curve of genus* g *the* $2g + 2$ *ramification points are the Weierstrass points.*

Proof. 6.3. □

Theorem 9.5. *If the characteristic of* k *is* 0 *then there are only finitely many Weierstrass point on a given curve* X*. If the genus* $g \geq 2$ *and the curve is not hyperelliptic then there are at least* $2g + 3$ *Weierstrass points.*

Proof. If u is a nonconstant rational function there is a basis
$f_1 du, \ldots, f_g du$ for $\Omega(0)$ such that $v_x(f_j du) = i_j(x) - 1$ for every gap number $i_j(x)$ at x. Let t be a local parameter at x, then $f_j du = f_j \frac{du}{dt} dt$ so a local calculation gives

$$v_x(\det\big(\frac{d^{i-1} f_j}{du^{i-1}}\big)) = \sum (i_j - j) - \frac{1}{2} g(g+1) v_x(du)$$

Summing over all points x give

$$\sum_{x,j} (i_j(x) - j) = (g-1)g(g+1)$$

The claim now follows. □

10. Automorphisms

Proposition 10.1. *A nontrivial automorphism of a curve of genus* g *has at most* $2g + 2$ *fixed points.*

Proof. Choose $f \in k(X)$ with $g + 1$ poles disjoint from the fixed points of an automorphism σ.Then $f - f \circ \sigma$ has $2g + 2$ poles and therefore at most this number of zero's. □

Theorem 10.2 (Hurwitz). *Assume the characteristic of* k *is* 0*. For a curve* X *of genus* $g \geq 2$ *the group of automorphisms* $\mathrm{Aut}(X)$ *is a finite group and the order is bounded*

$$|\mathrm{Aut}(X)| \leq 84(g-1)$$

Proof. If X is not hyperelliptic then an automorphism is determined by the permutation of the more than $2g + 2$ Weierstrass points. If $f : X \to \mathbb{P}^1$ is hyperelliptic then an automorphism commutes with the involution τ and therefore induces an automorphism of $\mathbb{P}^1$ which permute the images of the $2g + 2 > 5$ ramification points. In all cases $\mathrm{Aut}(X)$ is finite.

Let $|\,\mathrm{Aut}(X)| = n$ and choose by normalization a curve Y together with a morphism $f : X \to Y$ of $\deg(f) = n$ identifying $f^*(k(Y)) = k(X)^{\mathrm{Aut}(X)}$ as the fixed field. By the Zeuthen-Hurwitz formula

$$\frac{2g-2}{n} = 2g_Y - 2 + \sum_y (1 - \frac{1}{r_y})$$

giving

$$\frac{2g-2}{n} \geq -2 + (1 - \frac{1}{2}) + (1 - \frac{1}{3}) + (1 - \frac{1}{7}) = \frac{1}{42}$$

□

Examples and comments

k is a fixed algebraically closed ground field of characteristic 0 when necessary.

1. Non affine variety

1.1. The open subset $\mathbb{A}^1 - \{0\}$ of $\mathbb{A}^1$ is a variety isomorphic to the affine variety $V(Y_1Y_2 - 1) \subset \mathbb{A}^2$. The isomorphism is given by

$$x_1 \mapsto (y_1, y_2) = (x_1, \frac{1}{x_1})$$

$$(y_1, y_2) \mapsto x_1 = y_1$$

The coordinate ring

$$k[\mathbb{A}^1 - \{0\}] \simeq k[X_1, X_1^{-1}]$$

1.2. The open subset $\mathbb{A}^n - V(X_n)$ of $\mathbb{A}^n$ is a variety isomorphic to the affine variety $V(Y_nY_{n+1} - 1) \subset \mathbb{A}^{n+1}$. The isomorphism is given by

$$x \mapsto y = (x, \frac{1}{x_n})$$

$$y \mapsto x = (y_1, \ldots, y_n)$$

The coordinate ring

$$k[\mathbb{A}^n - V(X_n)] \simeq k[X_1, \ldots, X_n, X_n^{-1}]$$

1.3. The open subset $U = \mathbb{A}^2 - \{(0,0)\}$ of $\mathbb{A}^2$ is a variety not isomorphic to any affine variety.
The inclusion gives an injective ring homomorphism

$$k[X_1, X_2] \to \Gamma(U)$$

A regular function $f : U \to k$ has representations

$$f = \frac{P(X_1, X_2)}{X_1^d} \ , \ x \in \mathbb{A}^2 - V(X_1)$$

$$f = \frac{Q(X_1, X_2)}{X_2^d} \ , \ x \in \mathbb{A}^2 - V(X_2)$$

giving

$$P(X_1, X_2)X_2^d = Q(X_1, X_2)X_1^d \ , \ (x, y) \in \mathbb{A}^2 - V(X_1X_2)$$

By irreducibility of $\mathbb{A}^2$ and unique factorization in the polynomial ring it follows that the ring homomorphism above is surjective. If U is isomorphic to an affine variety, then the ring isomorphism above is an isomorphism of coordinate rings contradicting that the inclusion $U \subset \mathbb{A}^2$ is not an isomorphism.

2. Bijective morphism

2.1. The morphism

$$\mathbb{A}^1 \to \mathbb{A}^2,\ x \mapsto y = (x_1^2, x_1^3)$$

is a bijection onto the affine variety $V(Y_1^3 - Y_2^2) \subset \mathbb{A}^2$. The induced ring homomorphism of coordinate rings

$$k[Y_1, Y_2]/(Y_1^3 - Y_2^2) \to k[X_1]$$

is not surjective, so the morphism above is not an isomorphism.
Moreover the varieties $\mathbb{A}^1$ and $V(Y_1^3 - Y_2^2)$ are not isomorphic by any morphism, since the ring $k[X_1^2, X_1^3]$ is not normal.

2.2. The morphism

$$\mathbb{P}^1 \to \mathbb{P}^2,\ x \mapsto y = (x_0^2, x_0x_1, x_1^2)$$

is an isomorphism onto the projective variety $V(Y_0Y_2 - Y_1^2) \subset \mathbb{P}^2$.
The inverse morphism is given by

$$y \mapsto x = \begin{cases} (y_0, y_1) & , \quad y_0 \neq 0 \\ (y_1, y_2) & , \quad y_2 \neq 0 \end{cases}$$

The homogeneous coordinate rings

$$k[X_0, X_1] \text{ and } k[Y_0, Y_1, Y_2]/(Y_0Y_2 - Y_1^2)$$

are not isomorphic as graded rings.

2.3. The morphism

$$\mathbb{P}^1 \to \mathbb{P}^2,\ x \mapsto y = (x_0^3, x_0x_1^2, x_1^3)$$

is a homeomorphism onto the projective variety $V(Y_0Y_2^2 - Y_1^3) \subset \mathbb{P}^2$. But it is not an isomorphism.

3. Finite morphism

3.1. The inclusion

$$\mathbb{A}^1 - \{0\} \subset \mathbb{A}^1$$

is not a finite morphism.

3.2. The morphism

$$\mathbb{A}^1 - \{0\} \to \mathbb{A}^1,\ x \mapsto x + \frac{1}{x}$$

is a finite surjective morphism. The corresponding ring extension is

$$k[X + \frac{1}{X}] \subset k[X, \frac{1}{X}]$$

If $U = X + \frac{1}{X}$ then

$$X^2 - UX + 1 = 0,\ \left(\frac{1}{X}\right)^2 - U\frac{1}{X} + 1 = 0$$

3.3. The morphism

$$\mathbb{A}^1 \to \mathbb{P}^1,\ x \mapsto y = (x_1^2 - 1, x_1)$$

is a finite surjective morphism. Extend to

$$\mathbb{P}^1 \to \mathbb{P}^1,\ x \mapsto y = (x_1^2 - x_0^2, x_0x_1)$$

3.4. The composite morphism

$$\mathbb{A}^1 - \{0\} \to \mathbb{P}^1,\ x \mapsto y = (x_1^2 + \frac{1}{x_1^2} + 1, x_1 + \frac{1}{x_1})$$

is a surjective morphism.

4. Constructible set

4.1. The morphism

$$\mathbb{A}^2 \to \mathbb{A}^2,\ x \mapsto y = (x_1 x_2, x_2)$$

has a constructible image

$$Y = (\mathbb{A}^2 - V(Y_2)) \cup \{(0,0)\}$$

which is not a variety in $\mathbb{A}^2$.
The closure of Y is $\mathbb{A}^2$. If Y is open then $\{0\} \subset \mathbb{A}^1$ is open, contradicting irreducibility of $\mathbb{A}^1$.

4.2. Let W be a constructible set in a variety X. If the closure $\overline{W}$ is irreducible then there is a subset $U \subset W$ being open in $\overline{W}$.

$$W = U_1 \cap Z_1 \cup \cdots \cup U_s \cap Z_s$$

so for some i, $\overline{W} \subset Z_i$.
In general W contains a subset dense in $\overline{W}$.

5. Connected variety

5.1. An affine variety X is connected if and only if $0, 1$ are the only idempotent elements in the coordinate ring $k[X]$.
If $e \neq 0, 1$ is idempotent then

$$X = V(e) \cup V(1-e),\ V(e) \cap V(1-e) = \emptyset$$

If

$$X = V(I) \cup V(J),\ V(I) \cap V(J) = \emptyset$$

then conclusion by Chinese remainder theorem.

5.2. The affine variety $V(X_1 X_2) \subset \mathbb{A}^2$ is connected but not irreducible.

6. Morphism of projective space

6.1. The projection

$$p : \mathbb{A}^{n+1} - \{0\} \to \mathbb{P}^n,\ x \mapsto y$$

is locally of the form

$$p^{-1}(U_i) \simeq \mathbb{A}^n \times (\mathbb{A}^1 - \{0\})$$
$$x \mapsto (y, u) = (\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}, x_i)$$
$$(y, u) \mapsto x = (uy_1, \ldots, u, \ldots, uy_n)$$

For an irreducible variety X in $\mathbb{P}^n$ $p^{-1}(X)$ is irreducible and

$$\dim p^{-1}(X) = \dim X + 1$$

6.2. A morphism $f : \mathbb{P}^m \to \mathbb{P}^n$ is constant if $m > n$.
$Y = f(\mathbb{P}^m) \subset \mathbb{P}^n$ is irreducible and closed. Assume

$$n > r = n - \dim Y \geq 0$$

Choose linear forms $L_0, \ldots, L_r \in k[\mathbb{P}^n]$ such that $Y \cap V(L_0, \ldots, L_r) = \emptyset$. The inverse image $f^{-1}(V(L_i)) \neq \emptyset$ and any component Z has dimension $\dim Z \geq m - 1$. Since

$$f^{-1}(V(L_0)) \cap \cdots \cap f^{-1}(V(L_r)) = \emptyset$$

it follows that

$$m \leq r + 1 \leq n$$

6.3. Projection from a point

$$p : \mathbb{P}^n - \{(0, \dots, 0, 1)\} \to \mathbb{P}^{n-1},\ x \mapsto y = (x_0, \dots, x_{n-1})$$

gives a finite morphism from a projective variety $X \subset \mathbb{P}^n$ not containing the point $(0, \dots, 0, 1)$. $p^{-1}(\mathbb{P}^{n-1} - V(Y_i)) = \mathbb{P}^n - V(X_i)$ is affine. Let $F(X_0, \dots, X_n) \in I(X)$ be such that $F(0, \dots, 0, 1) \neq 0$. Then

$$k[\frac{y_0}{y_i}, \dots, \frac{y_{n-1}}{y_i}] \to k[\frac{x_0}{x_i}, \dots, \frac{x_{n-1}}{x_i}]/(F(\frac{x_0}{x_i}, \dots, \frac{x_{n-1}}{x_i}))$$

is finite and maps onto $k[X - V(X_i)]$.

6.4. An automorphism of the projective line is linear

$$f : \mathbb{P}^1 \to \mathbb{P}^1,\ x \mapsto y = (a_0x_0 + b_0x_1, a_1x_0 + b_1x_1)$$

with $a_0b_1 - a_1b_0 \neq 0$.
Remark that

$$f(1, 0) = (a_0, a_1), f(0, 1) = (b_0, b_1), f(1, 1) = (a_0 + b_0, a_1 + b_1)$$

For a given automorphism g and the distinct points $g(1, 0) = (a_0, a_1), g(0, 1) = (b_0, b_1), g = (1, 1) = (c_0, c_1) \in \mathbb{P}^1$ there is a choice of $a_0, a_1, b_0, b_1 \in k$ such that $(c_0, c_1) = (a_0 + b_0, a_1 + b_1)$. The composite $f^{-1} \circ g$ induces an isomorphism of $\mathbb{A}^1 = \mathbb{P}^1 - \{(0, 1)\}$ being the identity.

7. Big fibre

7.1. The morphism

$$f : \mathbb{A}^2 \to \mathbb{A}^2,\ x \mapsto y = (x_1x_2, x_2)$$

has image

$$Y = (\mathbb{A}^2 - V(Y_2)) \cup \{(0, 0)\}$$

and therefore dominating. The fibres are

$$f^{-1}(y) = \begin{cases} V(X_2) & , \quad y = (0, 0) \\ (\frac{y_1}{y_2}, y_2) & , \quad y_2 \neq 0 \end{cases}$$

7.2. The closure of the graph of the projection

$$\mathbb{A}^{n+1} - \{0\} \to \mathbb{P}^n,\ x \mapsto y$$

$$Z = V(\{X_iY_j - X_jY_i | i \neq j\}) \subset \mathbb{A}^{n+1} \times \mathbb{P}^n$$

is the blowup of 0 in $\mathbb{A}^{n+1}$. The projection $p : Z \to \mathbb{A}^{n+1}$ is a finite surjective map with fibres

$$p^{-1}(x) = \begin{cases} \{0\} \times \mathbb{P}^n & , \quad x = 0 \\ (x, x) & , \quad x \neq 0 \end{cases}$$

8. Big tangent space

8.1. The morphism

$$f : \mathbb{A}^1 \to \mathbb{A}^n,\ x \mapsto y = (x_1^{n+1}, \dots, x_n^{2n})$$

has closed image Y. The tangent space is

$$T_0Y = k^n$$

8.2. The curve Y is not isomorphic to a curve in any $\mathbb{A}^m$ for $m < n$.

9. Algebraic group

9.1. A group G which is an algebraic variety such that composition $G \times G \to G$ and inversion $G \to G$ are morphisms is called an algebraic group. There are many popular examples

- $\mathbb{A}^n$ with addition
- $\mathbb{A}^1 - \{0\}$ with multiplication
- The group of invertible matrices with matrix multiplication

9.2. The connected component G_e containing the unit is irreducible and again an algebraic group.
Let $G_1 \dots G_s$ be multiplication of the irreducible components containing e. The image contains all G_i so $s = 1$ and G_1 is a subgroup. The cosets xG is an irreducible component containing x, so there are only finitely many cosets. These being disjoint gives $G_e = G_1$.

9.3. If $f : G \to H$ is a homomorphism of algebraic groups, then the image $f(G)$ is a closed subgroup of H.
By constructibility let $V \subset f(G)$ be non-empty and dense in $\overline{f(G)}$. For $y \in \overline{f(G)}$ $V \cap yV^{-1} \neq \emptyset$ so

$$\overline{f(G)} \subset f(G)f(G) = f(G)$$

9.4. If an algebraic group G is projective, then G is an Abelian group.
The commutator morphism

$$f : G \times G \to G,\ (x, y) \mapsto xyx^{-1}y^{-1}$$

satisfy $f(G \times e) = e$ and therefore constant.

10. Projective line

10.1. Let $\mathbb{P}^1 = U_0 \cup \{\infty = (0, 1)\}$. The morphism $\mathbb{A}^1 \to \mathbb{P}^1,\ x \mapsto y = (1, x_1)$ identifies $k(X_1) = k(\frac{Y_1}{Y_0})$.

$$X_1 - x_1 = \frac{y_0 Y_1 - y_1 Y_0}{y_0 Y_0}$$

is a local parameter at $x = (1, x_1) = (y_0, y_1)$.

$$\frac{1}{X_1} = \frac{Y_0}{Y_1}$$

is a local parameter at $\infty = (0, 1)$.

10.2. The differential $dX_1 \neq 0$ in $\Omega(\mathbb{P}^1)$.

$$dX_1 = d(X_1 - x_1) \Rightarrow v_y(dX_1) = 0,\ y \in U_0$$

$$dX_1 = -\left(\frac{1}{X_1}\right)^{-2} d\frac{1}{X_1} \Rightarrow v_\infty(dX_1) = -2$$

A canonical divisor is

$$K_{\mathbb{P}^1} = -2 \cdot \infty$$

10.3. Calculate

$$v_x(X_1 - x_1) = \begin{cases} 0 & , \quad x \neq x_1 \\ 1 & , \quad x = x_1 \\ -1 & , \quad x = \infty \end{cases}$$

giving

$$\operatorname{div}(X_1 - x_1) = 1 \cdot x_1 - 1 \cdot \infty$$

For

$$f = (X_1 - x_{11})^{m_1} \dots (X_1 - x_{1s})^{m_s}$$

the divisor

$$\operatorname{div}(f) = m_1 \cdot x_{11} + \cdots + m_s \cdot x_{1s} - (m_1 + \cdots + m_s) \cdot \infty$$

10.4. Calculate for $n \geq 0$

$$L(n \cdot \infty) = \{f | \operatorname{div}(f) \geq -n \cdot \infty\} = Span(1, X_1, \ldots, X_n)$$

giving

$$l(n \cdot \infty) = n + 1$$

Conclude that the genus

$$g_{\mathbb{P}^1} = 0$$

10.5. For a general divisor D on $\mathbb{P}^1$ the Riemann-Roch theorem states

$$l(D) - l(-2 \cdot \infty - D) = \deg D + 1$$

11. Conic

11.1. A plane curve given by a homogeneous form F of degree 2 is a conic. Let $char(k) \neq 2$, then by change of coordinates

$$F = aX_0^2 + bX_1^2 + cX_2^2$$

and

$$dF = 2aX_0 dX_0 + 2bX_1 dX_1 + 2cX_2 dX_2$$

Necessary and sufficient for $V(F) \subset \mathbb{P}^2$ to be nonsingular and irreducible is $abc \neq 0$.

11.2. By further change of coordinates

$$F = X_0^2 + X_1^2 + X_2^2 = (X_0 - \sqrt{-1}X_2)(X_0 + \sqrt{-1}X_2) + X_1^2$$

The morphism $\mathbb{P}^1 \to \mathbb{P}^2$

$$(y_0, y_1) \mapsto (x_0, x_1, x_2) = (\frac{1}{2}(y_0^2 + y_2^2), y_0 y_2, \frac{1}{2\sqrt{-1}}(y_0^2 - y_2^2))$$

is an isomorphism $\mathbb{P}^1 \simeq V(F)$.

12. Elliptic curve

12.1. A curve X of genus 1 is called an elliptic curve. The canonical divisor K has

$$\deg K = 0,\ l(K) = 1$$

so $K \sim 0$. The Riemann-Roch theorem gives

$$l(D) - l(-D) = \deg D$$

for any divisor D.

12.2. Let $\operatorname{Div}_0(X)$ be the subgroup of divisors of degree 0. Fix a point x_0 on X. The map

$$\phi : X \to \operatorname{Div}_0(X)/\operatorname{div}(k(X)^*),\ x \mapsto x - x_0$$

is a bijection.

12.3. The map

$$\begin{array}{ccc} X \times X & \to & X \\ (x_1, x_2) & \mapsto & \phi^{-1}(x_1 - x_0 + x_2 - x_0) \end{array}$$

defines a structure of abelian algebraic group on X with zero x_0.

12.4. Assume $char(k) \neq 2, 3$. A plane curve given by a homogeneous form F of degree 3 is an elliptic curve. By change of coordinates

$$F = X_1^3 + aX_0^2X_1 + bX_0^3 - X_0X_2^2$$

and

$$dF = (2aX_0X_1 + 3bX_0^2 - X_2^2)dX_0 + (3X_1^2 + aX_0^2)dX_1 + (-2X_0X_2)dX_2$$

Necessary and sufficient for $V(F) \subset \mathbb{P}^2$ to be nonsingular and irreducible is

$$16a^3 + 27b^2 \neq 0$$

13. Morphism of a cubic curve

13.1. The variety $X \subset \mathbb{P}^2$ given by the equation

$$X_0^3 - X_0X_2^2 - X_1^2X_2 = 0$$

intersects the hyperplanes

$$X \cap V(X_0) = \{(0,1,0), (0,0,1)\}$$
$$X \cap V(X_1) = \{(0,0,1), (1,0,1), (1,0,-1)\}$$
$$X \cap V(X_2) = \{(0,1,0)\}$$

and therefore covered by the affine pieces

$$X_1 \neq 0,\ X_0^3 - X_0X_2 - X_2 = 0$$
$$X_0X_2 \neq 0,\ X_0^3 - X_0 - X_1^2 = 0$$

A morphism $f : X \to X$ is given by

$$f(\frac{x_0}{x_1}, \frac{x_2}{x_1}) = (-\frac{x_0}{x_1}\frac{x_2}{x_1}, -\frac{x_2}{x_1}, \frac{x_0}{x_1}\frac{x_0}{x_1})$$
$$f(\frac{x_0}{x_2}, \frac{x_1}{x_2}) = (-\frac{x_0}{x_2}, -\frac{x_1}{x_2}, \frac{x_0}{x_2}\frac{x_0}{x_2})$$

This is an isomorphism, the inverse being f itself.

14. Hyperelliptic curve

14.1. Assume $char(k) = 0$. An affine variety in $\mathbb{A}^2$ is given by the affine equation

$$X_2^2 = g(X_1) = (X_1 - a_1)\dots(X_1 - a_n)$$

where $n \geq 5$ is odd and $a_1, \dots, a_n$ are all nonzero and different. The projective closure by $X_1 = \frac{Y_1}{Y_0}, X_2 = \frac{Y_2}{Y_0}$ is given by the homogeneous form

$$F = Y_0^{n-2}Y_2^2 - (Y_1 - a_1Y_0)\dots(Y_1 - a_nY_0)$$

The differential has components

$$\frac{\partial F}{\partial Y_0} = (n-2)Y_0^{n-3}Y_2^2 - \frac{\partial F}{\partial Y_0}\left(Y_0^n g\left(\frac{Y_1}{Y_0}\right)\right)$$
$$\frac{\partial F}{\partial Y_1} = -Y_0^{n-1}g'\left(\frac{Y_1}{Y_0}\right)$$
$$\frac{\partial F}{\partial Y_2} = 2Y_0^{n-2}Y_2$$

This shows that the projective closure has a singular point at $(0,0,1)$. The normalization Y is a hyperelliptic curve.

14.2. Let $f : Y \to \mathbb{P}^1$ be the extension to the normalization of the projection from $(0,0,1), (y_0, y_1, y_2) \mapsto (y_0, y_1)$, $V(F) - (0,0,1) \to \mathbb{P}^1$. f has degree 2 and gives the field extension

$$k(X_1) \subset k(X_1)[X_2]/(X_2^2 - g(X_1))$$

14.3. $f : Y \to \mathbb{P}^1$ is clearly ramified over the n points $(1, a_1), \ldots, (1, a_n)$. If f were not ramified at $z \in f^{-1}(0, 1)$ then $v_z(X_1) = -1$ and

$$2v_z(X_2) = v_z(g(X_1)) = -n$$

As n is odd, f is ramified over $(0, 1)$ as well. The ramification is 2 so the Zeuthen-Hurwitz formula gives

$$2g - 2 = 2(-2) + (n + 1),\ g = \frac{n-1}{2}$$

15. Fermat curve

15.1. Assume $char(k) = 0$. A plane curve given by a homogeneous form

$$F = Y_0^n + Y_1^n + Y_2^n$$

is a Fermat curve.

$$dF = (nY_0^{n-1}, nY_1^{n-1}, nY_2^{n-1})$$

so $V(F) \subset \mathbb{P}^2$ is nonsingular and irreducible.

15.2. Let $X_1 = \frac{Y_1}{Y_0}, X_2 = \frac{Y_2}{Y_0}$ be the affine coordinates on $\mathbb{P}^2 - V(Y_0)$ satisfying

$$X_1^n + X_2^n = -1$$

The differential $\omega = dX_1$ is treated by the relation

$$X_1^{n-1} dX_1 + X_2^{n-1} dX_2 = 0$$

In a point $x = (x_1, x_2), x_2 \neq 0$, a local parameter is $X_1 - x_1$ giving $v_x(\omega) = 0$. If $x_2 = 0$ then X_2 is a local parameter at the n points $x = (\zeta_i, 0)$ running through $\sqrt[n]{-1}$. The relation above gives $v_x(\omega) = n - 1$.

15.3. Let $X_0 = \frac{Y_0}{Y_1}, X_2 = \frac{Y_2}{Y_1}$ be the affine coordinates on $\mathbb{P}^2 - V(Y_1)$ and get the relation

$$dX_1 = -X_0^{-2} dX_0$$

In a point $x = (0, \zeta_i)$ a local parameter is X_0 giving $v_x(\omega) = -2$.

15.4. A canonical divisor is

$$\operatorname{div} d\omega = \sum_i (n-1) \cdot (1, \zeta_i, 0) - 2 \cdot (0, 1, \zeta_i)$$

The degree is

$$n(n-3) = 2g - 2$$

confirming the genus formula

$$g = \frac{(n-1)(n-2)}{2}$$

16. Genus formula

16.1. Let a plane curve X be given by a homogeneous form F of degree n. Assume after change of coordinates that $(0, 0, 1) \notin X$ and only simple tangents through $(0, 0, 1)$. The tangents points is the intersection of X and $V(\frac{\partial F}{\partial X_2})$. By Bezout's theorem the number is $n(n-1)$. Apply Zeuthen-Hurwitz formula to the projection from $(0, 0, 1)$ of X to get

$$2g - 2 = n(-2) + n(n-1)$$

giving

$$g = \frac{(n-1)(n-2)}{2}$$

16.2. Let a plane curve X be given by a homogeneous form F of degree n. Assume after change of coordinates that

$$(1,0,0) \notin X \cap V(X_2) = \{x_1, \dots, x_n\}$$

and $\frac{X_2}{X_1}$ is a local parameter at $\{x_1, \dots, x_n\}$. $U_0 = \frac{X_0}{X_2}$, $U_1 = \frac{X_1}{X_2}$ satisfy the equation $F(U_0, U_1, 1) = 0$. A canonical divisor is given by the differential

$$\omega = \frac{dU_0}{\frac{\partial F}{\partial U_1}} = -\frac{dU_1}{\frac{\partial F}{\partial U_0}}$$

Calculate

$$v_{x_i}(\omega) = n - 3$$

and

$$\deg(\operatorname{div}\omega) = n(n-3) = 2g - 2$$

giving

$$g = \frac{(n-1)(n-2)}{2}$$

17. Automorphism

17.1. The Fermat curve X given by

$$X_0^4 + X_1^4 + X_2^4 = 0$$

has genus $g = 3$ and a canonical divisor of $\deg K = 4$ and $l(K) = 3$.

17.2. Permutation of coordinates define 6 automorphisms of X. Multiplication of a coordinate with a fourth root of unit define 16 automorphisms. All together

$$96 = |\operatorname{Aut}(X)| \leq 84(g-1) = 168$$

17.3. The curve given by

$$X_0^3 X_1 + X_1^3 X_2 + X_0 X_2^3 = 0$$

has genus $g = 3$ and

$$|\operatorname{Aut}(X)| = 84(g-1) = 168$$

18. Grassmann variety

18.1. The set of linear subspaces of fixed dimension m in $\mathbb{P}^n$ is bijectively described by a projective subset of $\mathbb{P}^{\binom{n+1}{m+1}-1}$ called the Grassmann variety $\mathbb{G}^{n,m}$.

18.2. Choose a basis of the $m+1$ dimensional subspace of k^{n+1} as row vectors, giving a $(m+1) \times (n+1)$-matrix. For $m+1$ columns with indexes $0 \leq j_0 < \cdots < j_m \leq n+1$ let the $(m+1)$-minor give the Plücker coordinates

$$(y_{j_0 \dots j_m}) \in \mathbb{P}^{\binom{n+1}{m+1}-1}$$

A change of basis multiply all minors with the determinant of the base change matrix.

18.3. The Grassmann variety is the projective subset given by the Plücker relations homogeneous of degree 2. Let $0 \leq j_0, \dots, j_m \leq n+1$ be indices. If some are equal then put $y_{j_0 \dots j_m} = 0$. Otherwise let σ be the permutation giving ordering $j_{\sigma(0)} < \cdots < j_{\sigma(m)}$ and put $y_{j_0 \dots j_m} = \operatorname{sign}(\sigma) y_{j_{\sigma(0)} \dots j_{\sigma(m)}}$. The relations are then

$$y_{i_0 \dots i_m} y_{j_0 \dots j_m} = \sum_r y_{i_0 \dots j_r \dots i_m} y_{j_0 \dots i_s \dots j_m}$$

for all indices and $0 \leq s \leq m$.

18.4. Lines in $\mathbb{P}^3, n = 3, m = 1$ give one nontrivial relation

$$y_{01}y_{23} - y_{02}y_{13} + y_{03}y_{12} = 0$$

defining $\mathbb{G}^{3,1}$ as a hypersurface in $\mathbb{P}^5$.

18.5. By Gauss elimination the Grassmann variety is covered by open affine spaces $\mathbb{A}^{(m+1)(n-m)}$. It follows that $\mathbb{G}^{n,m}$ is an irreducible nonsingular projective variety of dimension

$$\dim \mathbb{G}^{n,m} = (m+1)(n-m)$$

19. Secant and tangent variety

19.1. Let $X \subset \mathbb{P}^N$ be a nonsingular projective variety of dimension n. Let $W \subset \mathbb{P}^N \times \mathbb{P}^N \times \mathbb{P}^N$ be points on lines

$$W = \{(x, y, z) | z \text{ on the line through } x, y\}$$

Let $\Delta_X \subset X \times X$ be the diagonal. Consider projections

$$\phi : (X \times X \times \mathbb{P}^N - \Delta X \times \mathbb{P}^N) \cap W \to \mathbb{P}^N$$

$$\pi : (X \times X \times \mathbb{P}^N - \Delta X \times \mathbb{P}^N) \cap W \to \mathbb{X} \times X$$

The image $Im(\phi) \subset \mathbb{P}^N$ is the secant variety. By the fibre dimension formula

$$\dim Im(\phi) \leq \dim X \times X + \dim \pi^{-1}(x, y) = 2n + 1$$

19.2. Let $X \subset \mathbb{P}^N$ be a nonsingular projective variety of dimension n. Let $W \subset X \times \mathbb{P}^N$ be points on tangent lines

$$W = \{(x, y) | y \in T_x X\}$$

Consider projections

$$\phi : W \to \mathbb{P}^N$$

$$\pi : W \to X$$

The image $Im(\phi) \subset \mathbb{P}^N$ is the tangent variety. By the fibre dimension formula

$$\dim Im(\phi) \leq \dim X + \dim \pi^{-1}(x) = 2n$$

20. Determinantal variety

20.1. Let $\{X_{ij}\}$ be a $m \times n$-matrix of indeterminates. The affine subvariety of $\mathbb{A}^{mn}$ given by

$$V(r - \text{minors of } \{X_{ij}\})$$

is of dimension $mn - (m - r + 1)(n - r + 1)$.

20.2. The determinantal variety is normal. If $m, n \geq r > 1$ then 0 is a singular point.

21. Jacobian question

21.1. Assume $char(k) = 0$ and let

$$f : \mathbb{A}^n \to \mathbb{A}^n$$

be a morphism with Jacobian determinant

$$J_f = \det \left\{ \frac{\partial f_i}{\partial X_j} \right\} \in k^*$$

Is f an isomorphism?

21.2. The question is unanswered even in case

$$f : \mathbb{C}^2 \to \mathbb{C}^2$$

Bibliography

A. Altman and S. Kleiman, *Introduction to Grothendieck duality theory*, Springer-Verlag 1970.
M. Atiyah and I. Macdonald, *An introduction to commutative algebra*, Addison-Wesley 1969.
N. Bourbaki, *Algébre commutative*, Hermann-Masson 1961-.
H. Cartan and S. Eilenberg, *Homological algebra*, Princeton 1956.
J. Dieudonné, *Cours de géométrie algébrique*, Presses Universitaires de France 1974.
D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer-Verlag 1996.
W. Fulton, *Algebraic curves*, Benjamin inc. 1969.
W. Fulton, *Intercection theory*, Springer-Verlag 1984.
A. Grothendieck, *Sur quelques points d'algégre homologique*, Tôhoku Math, Journ., 9, 1957.
A. Grothendieck, *Eléments de géométrie algébrique*, IHES 1960-67.
A. Grothendieck, *Séminaire de géométrie algébrique*, IHES 1960-67.
R. Hartshorne, *Residues and duality*, Springer-Verlag 1966.
R. Hartshorne, *Algebraic geometry*, Springer-Verlag 1977.
B. Iversen, *Generic local structure in commutative algebra*, Springer-Verlag 1974.
B. Iversen, *Cohomology of sheaves*, Springer-Verlag 1986.
E. Kunz, *Introduction to commutative algebra*, Birkhäuser 1980.
S. Lang, *Algebra*, Addison-Wesley 1965.
H. Matsumura, *Commutative algebra*, Benjamin inc. 1970.
J. Milne, *http://www.jmilne.org*.
D. Mumford, *Introduction to algebraic geometry*, Red and 1 inch thick.
D. Mumford, *Algebraic geometry I, complex projective varieties*, Springer-Verlag 1976.
C. Peskine, *An algebraic introduction to complex projective geometry*, Cambridge University Press 1997.
M. Nagata, *Local rings*, Interscience Publ. 1962.
J-P. Serre, *Algébre locale - multiplicités*, Springer-Verlag 1965.
J-P. Serre, *Faisceaux algébrique cohérents*, Ann. of Math., 61, 1955.
I. Shafarevich, *Basic algebraic geometry*, Springer-Verlag 1974.
O. Zariski and P. Samuel, *Commutative algebra*, van Nostran 1958-60.