A FIRST COURSE IN ALGEBRAIC GEOMETRY

ALEXANDRU BUIUM

Contents

1. Introduction

This is an introduction to graduate algebraic geometry. The only prerequisite is an introductory one year graduate (or even undergraduate) course in Algebra such as Hungerford's or Lang's graduate (or even undergraduate) Algebra books. The course provides a shortcut through the following textbooks:

R.Hartshorne, Algebraic Geometry,
S.Lang, Introduction to Algebraic and Abelian Functions,
D.Mumford: Algebraic Geometry, I: Complex Algebraic Varieties,
J.-P. Serre, Algebraic Groups and Class Fields,
I.R. Shafarevich, Basic Algebraic Geometry, Vol I.

that starts from scratch and ends with the proof of the Riemann-Roch Theorem for curves and its first applications. In the process the basic topics of algebraic geometry are covered such as: projections, blow up, normalization, divisors, differential forms, cohomology, duality.

Geometry comes in essentially two flavors: synthetic geometry and analytic geometry. These two branches closely interact. Synthetic geometry is geometry without coordinates; analytic geometry is geometry with coordinates. Analytic geometry comes in essentially two flavors which, again, interact: differential geometry and algebraic geometry. Differential geometry studies shapes using smooth real functions and its main concepts are metrics and curvature. Algebraic geometry is concerned with the geometry of solution sets of systems of polynomial equations in several variables with coefficients in an arbitrary algebraically closed field k. The simplest non-trivial examples of such objects are 'plane curves'

$$\{(a,b) \in k^2 \mid f(a,b) = 0\}$$

where $f \in k[x,y]$ is a polynomial. This study was initiated by Descartes and Fermat (17th century) and enhanced by the introduction of calculus by Leibniz and Newton, by the work of Euler (especially on elliptic integrals), and by the introduction of projective geometry (18th century). Abel and Riemann made important advances in the 19th century leading to the Riemann-Roch Theorem about spaces of functions on curves with given sets of poles. Futher developments and higher dimensional generalizations of all of this were worked out by the British algebraists (Cayley, Macauley) and by the Italian school (Castelnuovo, Enriques, Severi) in late 19th century. The whole subject was greatly clarified and put on solid algebraic foundations by Dedekind, Hilbert and Emmy Noether around the beginning of the 20th century. By mid 20th century algebraic geometry received a significant impetus from the analytic work of Hodge on harmonic forms which involved the study of certain partial differential equations. All this work was in the case $k = \mathbb{C}$. During the first half of the century (through work of Artin, Hasse, Weil, Zariski, Chevalley, Serre) algebraic geometry was developed over arbitrary fields k, in particular fields of characteristic p; this setting is crucial for applications to the study of congruences in number theory. Over arbitrary fields calculus had to be reinvented; no integration is then available but differentials have an analogue which is sufficient to reconstruct the calculus part of algebraic geometry in this setting (this was seen already in Dedekind). The above algebraic (yet not analytic) developments are reflected in this course at least in the case of curves. A new stage in the development of algebraic geometry (which is not reflected, however, in this course) is Grothendieck's introduction of schemes in mid 20th century which amounts to replacing the field k by an arbitrary ring and 'allowing functions to be nilpotent'. Further paradigms for algebraic geometry were introduced after that including the rigid analytic geometry of Tate (where k is a 'p-adic' field), Arakelov geometry (that combines Grothendieck's framework with complex differential geometry and partial differential equations), and derived algebraic geometry (with its homotopical flavor). Classical algebraic geometry (i.e. the one before Grothendieck) remains, however, the source of most interesting problems in the field.

2. Algebraic preliminaries

We begin by reviewing some basic algebraic notation, terminology, and facts that will be freely used in our course; they are our algebraic prerequisites and are all usually covered by a one year graduate course in Algebra. Here they are:

1) Rings will be usually denoted by $A, B, R, S, ...$; they are commutative with 1. The ring of polynomials in n variables with coefficients in A is denoted by $A[x_1, ..., x_n]$.

2) Ring homomorphisms $f : A \to B$ are assumed to satisfy $f(1) = 1$. Given such a homomorphism we say that B is an A-algebra.

3) The group of invertible elements (units) in a ring A is denoted by $A^\times$.

4) Rings without nilpotents are called reduced.

5) Rings without zero divisors are called integral domains. Rings in which all non-zero elements are invertible are called fields. The characteristic of a field is 0 if the field contains $\mathbb{Q}$ and p is the field contains $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

6) Ideals in a ring A are usually denoted by $\mathfrak{a}, \mathfrak{b}, ...$. Write $a_1 \equiv a_2 \mod \mathfrak{a}$ if $a_1 - a_2 \in \mathfrak{a}$. There is a bijection between the set of ideals in the factor ring $A/\mathfrak{a}$ and the set of ideals in A containing $\mathfrak{a}$.

7) The radical of an ideal $\mathfrak{a} \subset A$ is defined as $\sqrt{\mathfrak{a}} = \{x \in A \mid \exists n,\ x^n \in \mathfrak{a}\}$.

8) Prime ideals in a ring A are usually denoted by $\mathfrak{p}$, $\mathfrak{q}$,... The radical $\sqrt{\mathfrak{a}}$ is the intersection of all prime ideals containing $\mathfrak{a}$. An ideal is called radical if it is equal to its radical. An element $\pi \in A$ is prime if the ideal (π) is prime.

9) Maximal ideals in a ring A are usually denoted by $\mathfrak{m}$, $\mathfrak{n}$,...

10) A principal ideal domain is an integral domain all of whose ideals are principal.

11) Factorial (unique factorization) domains are integral domains in which every non-zero non-invertible element is a product of prime elements. The polynomial ring $k[x_1, ..., x_n]$ over a field k is factorial. Principal ideal domains are factorial.

12) The ring of fractions $S^{-1}A$ of a ring A with respect to a multiplicative subset $S \subset A$ is defined as $S^{-1}A := (A \times S)/\sim$, where $(a, s) \sim (a', s') \Leftrightarrow \exists s'' \in S,\ s''sa' = s''s'a$. If $S = \{f^n \mid n \geq 0\}$ we write $A_f = S^{-1}A$. There is a bijection between the set of prime ideals in $S^{-1}A$ and the set of prime ideals in A disjoint from S.

13) A ring is local if it has a unique maximal ideal. The localization of a ring A at a prime ideal $\mathfrak{p}$ is the ring $A_\mathfrak{p} := (A \backslash \mathfrak{p})^{-1}A$. The fraction field of an integral domain A is the field $Frac(A) := A_{(0)}$. For k a field we let $k(x_1, ..., x_b) = Frac(k[x_1, ..., x_n])$. For $f \in A$ there is an isomorphism $A[x]/(fx - 1) \simeq A_f$ for $f \in A$. Every integral domain is the intersection of all its localizations at the maximal ideals. For a field k we let $k((x)) = Frac(k[[x]]) = k[[x]]_x$ the field of Laurent power series, fraction field of the local ring $k[[x]]$ of power series in one variable x.

14) The Krull dimension of a ring A is the suppremum $\dim(A)$ of all $n \geq 0$ such that there exists a chain $\mathfrak{p}_0 \subset ... \subset \mathfrak{p}_n$ of distinct prime ideals.

15) A-modules are usually denoted by $M, N, ...$ Their module of homomorphisms are denoted by $Hom_A(M, N)$. We assume familiarity with finitely generated modules, submodules, factor modules, kernels, images, and exact sequences of modules. Every A-algebra has a structure of A-module.

16) Modules over a field are called vector spaces. The dual $Hom_k(V, k)$ of a vector space V over a field k is denoted by V°. The (vector space) dimension of V is denoted by $\dim_k(V)$.

17) We assume familiarity with modules of fractions $S^{-1}M$ and localization of modules $M_{\mathfrak{p}}$, product of an ideal with a module $\mathfrak{a}M$, direct sums $\oplus M_i$, direct products $\prod M_i$ of modules and tensor products $M \otimes_A N$. For every A-algebra B, every A-module M and every B-module N one has $Hom_A(M, N) \simeq Hom_B(M \otimes_A B, N)$. One has the formula $\mathfrak{a}(M/N) = (\mathfrak{a}M + N)/N$ for $\mathfrak{a} \subset A$ an ideal and $N \subset M$ a submodule of a module. Also $M \otimes_A (A/\mathfrak{a}) \simeq M/\mathfrak{a}M$ and $M \otimes_A (S^{-1}A) \simeq S^{-1}M$. Also $S^{-1}(M/N) \simeq S^{-1}M/S^{-1}N$ for every submodule N of a module M.

18) The degree of a field extension $K \subset L$ is denoted by $[L : K]$. We assume familiarity with the concept of transcendence basis of a field extension and with the concept of a finitely generated field extension. Every finitely generated field extension L of an algebraically closed field k has a separable transcendence basis, i.e., a transcendence basis $x_1, ..., x_n$ such that L is separable over $k(x_1, ..., x_n)$. The transcendence degree (cardinality of a transcendence basis) of an extension $K \subset L$ is denoted by $\text{tr.deg}(L/K)$.

19) We assume the definition of Galois groups and the Galois correspondence are known. We assume the definitions of trace and norm in a field extension are known. We assume the Theorem of the Primitive Element which says that every finite separable field extension is simple (generated by one element).

20) We assume familiarity with the definition of category, initial elements, final elements, functors, and equivalence of categories. We also assume familiarity with universal properties of various constructions (direct sums, direct products, factors, fractions) and the interpretation of the latter as initial/final objects in appropriate categories.

In what follows we present algebra material that goes beyond our prerequisites described above and will be used in the sequel. We start with the following basic:

Lemma 2.1. *(Nakayama's Lemma) Let A be a local ring with maximal ideal $\mathfrak{m}$ and let M be a finitely generated A-module. Assume $\mathfrak{m}M = M$. Then $M = 0$.*

Proof. Let $x_1, ..., x_n \in M$ generate M. Write $x_i = \sum_j m_{ij} x_j$ with $m_{ij} \in \mathfrak{m}$. Let x be the column vector with entries $x_1, ..., x_n$ and A the matrix with entries $\delta_{ij} - m_{ij}$ where δ_{ij} is the Kronecker symbol, i.e. the identity matrix $I = (\delta_{ij})$. So $Ax = 0$. Let A^* be the adjugate matrix, i.e. $A^*A = \det(A) \cdot I$. We get $A^*Ax = 0$ so $\det(A) \cdot x_i = 0$ for all i. But $\det(A) \in 1 + \mathfrak{m} \subset A^\times$. So $x_i = 0$ for all i. $\square$

Exercise 2.2. Let A be a local ring with maximal ideal $\mathfrak{m}$ and let N be a finitely generated A-module. Let $x_1, ..., x_n \in N$ be such that their images $\overline{x_1}, ..., \overline{x_n}$ in $N/\mathfrak{m}N$ span the k-linear space $N/\mathfrak{m}N$. Then $x_1, ..., x_n \in N$ generated the A-module N. Hint: Apply Nakayama to N/N' where N' is a submodule of N generated by $x_1, ..., x_n$.

Lemma 2.3. *(Chinese Remainder Theorem) Let $\mathfrak{a}_1, ..., \mathfrak{a}_n$ be ideals in a ring A such that $\mathfrak{a}_i + \mathfrak{a}_j = A$ for $i \neq j$. Then the map*

$$A/\mathfrak{a}_1...\mathfrak{a}_n \to A/\mathfrak{a}_1 \times ... \times A/\mathfrak{a}_n, \quad x + \mathfrak{a}_1...\mathfrak{a}_n \mapsto (x + \mathfrak{a}_1, ..., x + \mathfrak{a}_n)$$

is an isomorphism.

Proof. Left to the reader.

Exercise 2.4. Prove the above Lemma.

Definition 2.5.
a) An A-algebra B is called *finite* if B is a finitely generated A-module if there exist $b_1, ..., b_n \in B$ generating B as an A-module $B = Ab_1 + \ldots + Ab_n$
b) An A-algebra B is called *finitely generated* if there exist $b_1, ..., b_n \in B$ such that B is a generated as an A-module by all monomials $b_1^{i_1}...b_n^{i_n}$; write $B = A[b_1, ..., b_n]$.
c) For an A-algebra B element $b \in B$ is called *integral* over A if it is a root of a monic polynomial with coefficients in A. B is called integral over A if all elements of B are integral over A.

Proposition 2.6.
1) An A-algebra B is finite iff if it is finitely generated and integral over A.
2) If B is integral over A and C is integral over B then C integral over A. Same with 'finitely generated' and 'finite' in place of 'integral'.
3) For an A-algebra B the set A'_B of all elements of B that are integral over A is a ring and is called the integral closure of A in B.

Proof. For 1 the only non-obvious fact is that a finite A-algebra B is integral. Let $b_1, ..., b_n$ generate B as an A-module. Let $b \in B$. Write $bb_i = \sum_j a_{ij} b_j$, $a_{ij} \in A$, $D = (b\delta_{ij} - a_{ij})$. By the argument in the proof of Nakayama's Lemma we get $\det(D) = 0$. But $\det(D) = b^n + c_1 b^{n-1} + ... + c_n$, $c_i \in A$. So b is integral over A. Then 2 and 3 follow using 1.

□

Definition 2.7. For an integral domain A its *integral closure* in $Frac(A)$ is denoted by A^{nor}; A is called *integrally closed* (or *normal*) if $A = A^{\text{nor}}$.

Exercise 2.8. Every factorial ring is normal.

Exercise 2.9. If $A \subset B$ is an integral extension of integral domains then A is a field if and only if B is a field.

Exercise 2.10. If $A \to B$ is integral so are $S^{-1}A \to S^{-1}B$ (for $S \subset A$) and $A/\mathfrak{b} \cap A \to B/\mathfrak{b}$ (for $\mathfrak{b} \subset B$).

Exercise 2.11. Let $A \subset B$ be integral.
1) If P is a prime ideal in B then P is maximal iff $P \cap A$ is maximal in A.
2) If $P_1 \subset P_2$ and $P_1 \cap A = P_2 \cap A$ then $P_1 = P_2$.
Hint: use the fact that $A/P \cap A$ is a field if and only if B/P is a field.

Lemma 2.12. *Let $A \subset B$ be an integral extension of rings and $\mathfrak{p}$ a prime ideal in A. Then there exists a prime ideal P in B lying over $\mathfrak{p}$ (i.e. $P \cap A = \mathfrak{p}$).*

Proof. Consider integral extension

$$A_{\mathfrak{p}} \subset B_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1} B.$$

Take a maximal ideal $\mathcal{M}$ in $B_{\mathfrak{p}}$. Then $\mathcal{P} := \mathcal{M} \cap A_{\mathfrak{p}}$ is a maximal ideal by an exercise above. But $A_{\mathfrak{p}}$ is local with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$. So $\mathcal{P} = \mathfrak{p}A_{\mathfrak{p}}$. Then the preimage P of $\mathcal{M}$ in B lies over $\mathfrak{p}$. The finiteness claim follows from the fact that a finite algebra over a field has only finitely many prime ideals (check!). $\square$

Theorem 2.13. *(Going Up Theorem) Let $A \subset B$ be an integral extension of rings, $\mathfrak{p}_1 \subset \mathfrak{p}_2$ prime ideals in A and P_1 a prime ideal in B lying over $\mathfrak{p}_1$. Then there exists a prime ideal P_2 in B with $P_1 \subset P_2$ and P_2 lying over $\mathfrak{p}_2$.*

Proof. Follows from Lemma 2.12 applied to $A/\mathfrak{p}_1 \subset B/P_1$. $\square$

Exercise 2.14. If $A \subset B$ is integral then $\dim(A) = \dim(B)$.

Exercise 2.15. A is normal if and only if $A_{\mathfrak{m}}$ is normal for all maximal ideals.

Theorem 2.16. *(Noether normalization). Let k be a field and $k \subset A$ a finitely generated k-algebra. Then there exists a subring $k \subset R \subset A$ such that A if finite over R and R is k-isomorphic to the ring of polynomials $k[x_1, ..., x_n]$ for some $n \geq 0$.*

Proof We only give the proof in case k is infinite; the case k is finite needs an adjustment of the argument. Induction on the minimum number n of generators. Assume the statement true for at most $n-1$ generators. Let $B = A[b_1, ..., b_n]$. If $b_1, ..., b_n$ are algebraically independent we are done. If not upon renumbering we may assume b_n is algebraic over $A[b_1, ..., b_{n-1}]$, hence b_n is a root of $f(b_1, ..., b_{n-1}, x)$ for some polynomial f in n variables. Let F be the form of highest degree d in f and set $b_i = b_i' + \lambda_i b_n$ for $i = 1, ..., n-1$ where $F(\lambda_1, ..., \lambda_{n-1}, 1) \neq 0$. (For the existence of the λ_i's we use k is infinite.) Then b_n is integral over $k[b_1', ..., b_{n-1}']$. We conclude by induction. $\square$

Corollary 2.17. *For a finitely generated k-algebra A that is an integral domain we have*

$$\dim(A) = \text{tr.deg}(Frac(A)/k).$$

Exercise 2.18. One has

$$\dim(k[x_1, ..., x_n]) = n \quad \text{and} \quad \dim(k[x_1, ..., x_n])/(f) = n - 1$$

for all irreducible polynomial f. Hint: use the statement (and proof) of Noether normalization.

Theorem 2.19. *(Hilbert Nullstellensatz) Let k be an algebraically closed field and $\mathfrak{a} \subset A := k[x_1, ..., x_n]$ a radical ideal. Let $f \in A \setminus \mathfrak{a}$. Then there exists $(a_1, ..., a_n) \in k^n$ such that $f(a_1, ..., a_n) \neq 0$ and $g(a_1, ..., a_n) = 0$ for all $g \in \mathfrak{a}$.*

Proof. Consider the finitely generated k-algebra

$$B = (k[x_1, ..., x_n]/\mathfrak{a})_f$$

which is $\neq 0$ so it has a maximal ideal $\mathfrak{m}$. Then $B/\mathfrak{m}$ is a field which by Noether normalization is integral over a polynomial ring C in n variables. So C is a field, so $n = 0$. So B is a finite extension of k so it is equal to k. So there exist $a_i \in k$ whose image in B are the classes of x_i. One checks $a_1, ..., a_n$ have the desired properties. $\square$

Definition 2.20. An A-module is *Noetherian* if every submodule is finitely generated; equivalently if every ascending sequence of submodules $M_1 \subset M_2 \subset M_3 \subset ...$ is stationary, i.e., there exists $n \geq 1$ such that for every $N \geq n$ we have $M_n = M_N$. A ring A is *Noetherian* if it is Noetherian as an A-module, i.e. if every ideal is finitely generated, equivalently if every ascending sequence of ideals $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset ...$ is stationary.

Exercise 2.21. If $M' \subset M$ is a submodule then M is Noetherian if and only if M' and M/M' are Noetherian. In particular if R is Noetherian then every finitely generated A-module is Noetherian.

Theorem 2.22. *(Hilbert Basis Theorem) If A is Noetherian then the polynomial ring $A[x]$ is Noetherian. Hence every finitely generated A-algebra is Noetherian.*

Proof. Let $\mathfrak{b} \subset B = A[x]$ be an ideal. Let $\mathfrak{a}$ be the set of all $a \in A$ such that there exist $c_1, ..., c_n \in A$ with

$$ax^n + c_1x^{n-1} + ... + c_n \in \mathfrak{b}.$$

Then $\mathfrak{a}$ is an ideal in A hence is finitely generated by some elements $a_1, ..., a_m \in \mathfrak{a}$. So there exist polynomials $f_i \in \mathfrak{b}$ such that $f_i(x) = a_i x^{n_i} + ...$ Let N be the maximum of $n_1, ..., n_m$. Let $\mathfrak{b}' \subset \mathfrak{b}$ be the ideal in B generated by $f_1, ..., f_m$ and consider the A-submodule of B generated by $1, x, ..., x^{N-1}$. We claim that

$$\mathfrak{b} = \mathfrak{b}' + (\mathfrak{b} \cap M).$$

This will end the proof because $\mathfrak{b} \cap M$ is an A-submodule of a finitely generated A-module hence is finitely generated by some elements $g_1, ..., g_s$; but then the ideal $\mathfrak{b}$ is generated by $f_1, ..., f_m, g_1, ..., g_s$. To check the claim one checks by induction on d that every polynomial of degree d in $\mathfrak{b}$ belongs to $\mathfrak{b}' + (\mathfrak{b} \cap M)$. Indeed assuming this holds for polynomials of degree at most $d-1$, if f has degree d (which may be assumed to be $\geq N$) then write $f = ax^d + ...$ (so $a \in \mathfrak{a}$), express $a = \alpha_1 a_1 + ... + \alpha_m a_m$, $\alpha_i \in A$, and note that the polynomial

$$g = f - \sum_{i=1}^{m} \alpha_i x^{d-n_i} f_i$$

belongs to $\mathfrak{b}$ and has degree $\leq d-1$. We conclude by the induction hypothesis. $\square$

Theorem 2.23. *(Finiteness of integral closure, I) Let A be a Noetherian normal integral domain, let $K = Frac(A)$, let $K \subset L$ be a finite separable field extension and let $B = A'_L$ be the integral closure of A in L. Then B is a finite A-algebra.*

Proof. We may assume L is Galois over K. Consider the Galois group G, the trace

$$Tr = \sum_{\sigma \in G} \sigma : L \to K,$$

and K-bilinear map $L \times L \to K$ defined by

$$(x, y) \mapsto Tr(xy).$$

Recall that, by separability, this bilinear map is non-degenerate. Also $\sigma(B) \subset B$ for $\sigma \in G$ so $Tr(B) \subset A$. Let $\beta_1, ..., \beta_n \in L$ be a basis of L over K. We may assume $\beta_i =: b_i \in B$ (check!). Let $b_1^*, ..., b^* \in L$ be the dual basis with respect to our bilinear form; hence $Tr(b_i b_j^*) = \delta_{ij}$. Let b be any element in B and write $b = \sum_i c_i b_i^*$ with $c_i \in K$. We have $Tr(bb_j) = \sum_i c_i Tr(b_i^* b_j) = c_j$. So $c_j \in A$. So

B is an A-submodule of the module $\sum_i Ab_i^*$ which is Noetherian. So B is a finitely generated module over A. □

Theorem 2.24. *(Transitivity of Galois groups on fibers) Let $A \subset B$ be an integral extension of integral domains with A normal and assume their extension of fraction fields $K \subset L$ is Galois with Galois group G. Then for each prime ideal $\mathfrak{p}$ in A the group G acts transitively on the set of prime ideals P in B lying over $\mathfrak{p}$.*

Proof. Localizing at $\mathfrak{p}$ we may assume $\mathfrak{p}$ is maximal. Let P_1 and P_2 be prime (hence maximal) ideals in B lying over $\mathfrak{p}$. Let $G = \{\sigma_1, ..., \sigma_n\}$, $\sigma_1 = id$, and assume $\sigma_j P_1 \neq P_2$ for all $j = 1, ..., n$. Then $P_1 + \sigma_j^{-1} P_2 = B$ for all $j = 1, ..., n$. By the Chinese Remainder Theorem there exists $b \in B$ such that $b \equiv 0 \bmod P_1$ and $b \equiv 1 \bmod \sigma_j^{-1} P_2$ for all $j = 1, ..., n$. Let $\beta = \prod_{j=1}^n \sigma_j(b)$. Since β in G-invariant, by Galois theory, it belongs to K. Since β is integral over A and A is normal we get $\beta \in A$. But $\sigma_1 b = b \in P_1$ hence $\beta \in P_1 \cap A = \mathfrak{p}$. On the other hand $\sigma_j(b) \equiv 1 \bmod P_2$ so $\beta \equiv 1 \bmod P_2$ i.e. $\beta - 1 \in P_2$ so $\beta - 1 \in P_2 \cap A = \mathfrak{p}$. So $1 \in \mathfrak{p}$, a contradiction. □

Theorem 2.25. *(Going Down Theorem). Let $A \subset B$ be an integral extension of rings with A normal, $\mathfrak{p}_1 \subset \mathfrak{p}_2$ prime ideals in A and P_2 a prime ideal in B lying over $\mathfrak{p}_2$. Then there exists a prime ideal P_1 in B with $P_1 \subset P_2$ and P_1 lying over $\mathfrak{p}_1$.*

Proof. We only give the proof in case the extension $K \subset L$ of the fraction fields of A and B is Galois. (The proof can be modified to deal with the general case.) There is a prime ideal Q_1 in B lying over $\mathfrak{p}_1$. By the Going Up Theorem there is a prime ideal Q_2 in B containing Q_1 and lying over $\mathfrak{p}_2$. By the Transitivity of Galois on fibers there exists σ in the Galois group of L over K such that $\sigma(Q_2) = P_2$. Set $P_1 = \sigma(Q_1)$. Then P_1 has the desired properties. □

Corollary 2.26. *Let A be a finitely generated algebra over an algebraically closed field k and assume A is an integral domain. Then for all maximal ideals $\mathfrak{m}$ of A we have*

$$\dim(A_{\mathfrak{m}}) = \dim(A).$$

Proof. For $A = k[x_1, ..., x_n]$ a polynomial ring the statement follows from Hilbert's Nullstellensatz because all maximal ideals are of the form $(x_1 - a_1, ..., x_n - a_n)$. In general, by Noether Normalization there is an integral extension $k[x_1, ..., x_n] \subset A$ and we conclude by the Going Down Theorem. □

Theorem 2.27. *(Finiteness of integral closure, II). Let k be a field, A a finitely generated k-algebra which is an integral domain. Then the integral closure A^{nor} of A in $Frac(A)$ is a finite A-algebra.*

Proof. We only give the proof in case k has characteristic zero; for arbitrary characteristic the proof needs an adjustment. By Noether normalization A is finite over a subring C which is a polynomial ring. Since C is factorial it is normal. Let $K = Frac(C)$ and $L = Frac(A)$. The extension $K \subset L$ is finite and separable. By Theorem 2.23 the integral closure D of C in L is a finite C-algebra. But $A^{\text{nor}} \subset D$. So A^{nor} is a finite C-algebra, in particular a finite A-algebra. □

Definition 2.28. A local Noetherian ring A with maximal ideal $\mathfrak{m}$ and residue field $k = A/\mathfrak{m}$ is called *regular* if

$$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \dim(A).$$

Theorem 2.29. *Let A be a local Noetherian integral domain with $\dim(A) = 1$. The following are equivalent.*
1) A is principal.
2) A is factorial.
3) A is normal.
4) A is regular.

Proof. The implications 1 implies 2 implies 3 are true for every ring. Let $\mathfrak{m}$ be the maximal ideal of A. To check 3 implies 4 we need to show $\mathfrak{m}/\mathfrak{m}^2$ is one dimensional (which by Nakayama is the same as $\mathfrak{m}$ principal). Let $0 \neq a \in \mathfrak{m}$. Then $\sqrt{(a)} = \mathfrak{m}$ (recall that the radical of an ideal in any ring is the intersection of all prime ideals containing the ideal). There exists n such that $\mathfrak{m}^n \subset (a) \subset \mathfrak{m}^{n-1}$ (because $\mathfrak{m}$ is finitely generated). Choose $b \in (a) \backslash \mathfrak{m}^{n-1}$ and let $x = a/b \in Frac(A)$. Since $b \notin (a)$ we have $x^{-1} \notin A$. Hence x^{-1} is not integral over A. We claim that $x^{-1}\mathfrak{m} \not\subset \mathfrak{m}$; indeed if the contrary is true then writing $x^{-1}m_i = \sum_j a_{ij}m_j$ for a set of generators m_j of $\mathfrak{m}$, $a_{ij} \in A$, and using an argument similar to the one in the proof of Nakayama's Lemma would imply x^{-1} is integral over A. But $x^{-1}\mathfrak{m} \subset A$ (because $x^{-1}\mathfrak{m} = (b/a)\mathfrak{m}$ and $b\mathfrak{m} \subset \mathfrak{m}^n \subset (a)$) so $x^{-1}\mathfrak{m} = A$ so $\mathfrak{m} = xA$. The implication 4 implies 1 easily follows using Nakayama and is left to the reader. □

Definition 2.30. An A satisfying the conditions in Theorem 2.29 is called a *discrete valuation ring* (DVR). Any generator t of $\mathfrak{m}$ is called a *parameter*.

Any prime element of A is a unit times t (otherwise A would not be local). Since A is factorial every non-zero element of A is a unit times a power of t. Given such an A one can define the 'discrete valuation'

$$v : A \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

by the formula $v(a) = e$ where e is such that $a = ut^e$, u a unit. For $K = Frac(A)$ one extends v to a group homomorphism

$$v : K^\times \to \mathbb{Z}, \quad v(a/b) := v(a) - v(b).$$

Corollary 2.31. *For a Noetherian domain A of dimension 1, A is integrally closed if and only if $A_\mathfrak{m}$ is a DVR for every maximal ideal $\mathfrak{m}$.*

Definition 2.32. A Noetherian integrally closed domain A of dimension 1 is called a *Dedekind* ring.

Exercise 2.33. Every non-zero ideal I in a Dedekind ring A can be written uniquely as a finite product of maximal ideals. Hint: show I is contained in only finitely maximal ideals $P_1, \dots, P_n$. Write $IA_{P_i} = (P_iA_{P_i})^{e_i}$. Prove that $I = P_1^{e_1} \dots P_n^{e_n}$ by showing that this holds after localization at every maximal ideal.

Example 2.34. Let $f \in k[x, y]$ be an irreducible polynomial with $f(0, 0) = 0$. Then the ring

$$A = \left(\frac{k[x, y]}{(f)}\right)_{(x,y)/(f)}$$

is a DVR if and only if not both

$$\frac{\partial f}{\partial x}(0, 0) \text{ and } \frac{\partial f}{\partial y}(0, 0)$$

are zero. Indeed these two elements of k are α and β where

$$f \in \alpha x + \beta y + (x,y)^2.$$

Now if $\mathfrak{m}$ is the maximal ideal of A then we have

$$\mathfrak{m}/\mathfrak{m}^2 \simeq M/M^2$$

where $M = (x,y)/(f)$. We have $M^2 = ((x,y)^2 + (f))/(f)$ hence

$$\begin{array}{rcl} M/M^2 & = & \frac{(x,y)}{(x,y)^2+(f)} \\ & = & \frac{(x,y)}{(x,y)^2+(\alpha x+\beta y)} \\ & = & \frac{(x,y)/(x,y)^2}{((x,y)^2+(\alpha x+\beta y))/(x,y)^2} \\ & = & \frac{kx+ky}{k(\alpha x+\beta y)}. \end{array}$$

The latter has dimension $\neq 1$ if and only if $\alpha = \beta = 0$ and we are done by Theorem 2.29.

Exercise 2.35. Let $A = k[x,y]/(f)$ with f irreducible vanishing at $(0,0)$ and let $M = (x,y)/(f)$. Assume A_M is a DVR.

1) The class of x in A_M is a parameter of A if and only if

$$\frac{\partial f}{\partial y}(0,0) \neq 0.$$

2) The class of y in A_M is a parameter of A if and only if

$$\frac{\partial f}{\partial x}(0,0) \neq 0.$$

Hint: By Nakayama an element in the maximal ideal of a DVR is a parameter if and only if its image modulo the square of the maximal ideal is non-zero.

Lemma 2.36. *Assume A is a DVR, containing a field k, with maximal ideal $\mathfrak{m}$ such that $A/\mathfrak{m} \simeq k$. Then for all $n \geq 1$,*

$$\dim_k(A/\mathfrak{m}^n) = n.$$

In particular for $a \in A$ we have $v(a) = \dim_k(A/(a))$.

Proof. Induction on n. Let t be a parameter. For the induction step one uses the exact sequence

$$0 \to (t^n)/(t^{n+1}) \to A/(t^{n+1}) \to A/(t^n) \to 0$$

and the isomorphism $A/(t) \simeq (t^n)/(t^{n+1})$ given by multiplication by t^n.

□

3. Topological preliminaries

In this section we "review" some basic notions of topology relevant to algebraic geometry (such as irreducibility, Noetherianity, topological dimension). More topological concepts (such as sheaves and cohomology) will be introduced later.

Definition 3.1. A *topological space* is a set X equipped with a set $\mathcal{U}$ of subsets satisfying the following properties:
1) $\emptyset, X \in \mathcal{U}$;
2) If $U, V \in \mathcal{U}$ then $U \cap V \in \mathcal{U}$;
3) If $(U_i)_{i\in I}$ is a family of subsets of X with $U_i \in \mathcal{U}$ for all $i \in I$ then

$$\bigcup_{i\in I} U_i \in \mathcal{U}.$$

The members of $\mathcal{U}$ are called *open*. A subset of X is *closed* if its complement is open. The *closure* of a subset Y of X is the intersection of all closed sets containing Y. A map $f : X \to Y$ between two topological spaces is *continuous* if for every open set $V \subset Y$ the set $f^{-1}(V)$ is open in X. For every subset Y of a topological space X one may consider the topology on Y whose open sets are intersections $Y \cap U$ with U open in X; this topology on Y is called the *induced topology*. A subset Y of a topological space X is *dense* if every non-empty open set of X has a non-empty intersection with Y, equivalently if the closure of Y in X is X.

Exercise 3.2.

1) If Y is a subset of a topological space then the closed sets of Y in the induced topology are the intersections $Z \cap Y$ where Z is closed in X. Hence if T is closed in Y in the induced topology and if $\overline{T}$ is the closure of T in X then $\overline{T} \cap Y = T$.

2) If Y is open in X the open sets of Y in the induced topology are exactly the open sets of X contained in Y.

3) If Y is closed in X the closed sets of Y in the induced topology are exactly the closed sets of X contained in Y.

Definition 3.3. A closed set X in a topological space is called *irreducible* if it cannot be written as a union of two closed sets both strictly contained in X. The *dimension* of a topological space X is the supremum $\dim(X)$ of all $n \geq 0$ such that there exists a sequence $Y_0 \subset Y_1 \subset ... \subset Y_n$ of distinct irreducible closed subsets. A topological space is called a *curve* if it is a finite union of irreducible closed sets of dimension 1; it is called a *surface* if it is a finite union of irreducible closed sets of dimension 2. If $f : X \to Y$ is a continuous map and $P \in Y$ then the *fiber* of f at P is the set $f^{-1}(P)$; it is closed if P is closed.

Exercise 3.4.

1) A topological space is irreducible if and only if the intersection of any two non-empty open sets is non-empty. So every non-empty open set of an irreducible space is dense.

2) If X is an irreducible topological space and U is a non-empty open set then $\dim(U) = \dim(X)$.

Definition 3.5. A toplogical space is called *Noetherian* if every descending sequence $Y_0 \supset Y_1 \supset Y_2 \supset ...$ of closed sets is stationary (i.e. there exists n such for every $m \geq n$ we have $Y_m = Y_n$.)

Exercise 3.6.

1) In a Noetherian topological space every non-empty set of closed sets has a minimum element.

2) In a Noetherian topological space every closed set is a finite union of irreducible closed sets. Hint: consider the set Σ of all closed sets that are not finite unions of

irreducible closed sets, assume Σ is non-empty, take a minimal element in Σ, and derive a contradiction.

3) Call a decomposition $X = X_1 \cup ... \cup X_c$ of a closed set into irreducible closed sets non-redundant if $X_i \not\subset X_j$ for $i \neq j$. In a Noetherian topological space every two non-redundant decompositions of a closed set into finite unions of irreducible closed sets must coincide. (The irreducible closed sets in a decomposition of X are called the irreducible components of X).

4. Algebraic sets in $\mathbb{A}^n$

For the remainder of this course, k denotes an algebraically closed field of arbitrary characteristic.

Definition 4.1. The *affine space* n-space is the set $\mathbb{A}^n = k^n$.

Consider the polynomial ring. $A = k[y_1, ..., y_n]$. For every subset $X \subset \mathbb{A}^n$ let $I(X) \subset A$ be the ideal of all polynomials $f \in A$ such that $f(P) = 0$ for all $P \in X$; it is a radical ideal. For every subset $T \subset A$ let $Z(T) \subset \mathbb{A}^n$ be the set of all $P \in \mathbb{A}^n$ such that $f(P) = 0$ for all $f \in T$; so if $\mathfrak{a}$ is the ideal generated by T then $Z(T) = Z(\mathfrak{a}) = Z(\sqrt{\mathfrak{a}})$. The set $Z(T)$ is referred to as the set of zeroes of T. We refer to $y_1, ..., y_n$ as (affine) coordinates of $\mathbb{A}^n$; note that y_i define functions $y_i : \mathbb{A}^n \to k$.

Definition 4.2. A subset of $\mathbb{A}^n$ is called *algebraic* if it is of the form $Z(T)$ for some $T \subset A$.

Exercise 4.3. The algebraic sets in $\mathbb{A}^n$ are the closed sets of a topology on $\mathbb{A}^n$ (called the Zariski topology). Hint: $Z(\cup T_i) = \cap Z(T_i)$, $Z(T_1 T_2) = Z(T_1) \cup Z(T_2)$.

Exercise 4.4. (For the reader familiar with topology)

1) The above topology is not Hausdorff. However all points are closed sets.

2) The Zariski topology on $\mathbb{A}^2 = \mathbb{A}^1 \times \mathbb{A}^1$ is not the product of the Zariski topologies on the two factors.

For $X \subset \mathbb{A}^n$ a closed set the ring $A(X) = A/I(X)$ is called the affine coordinate ring of X. It is a reduced finitely generated k-algebra. The Hilbert Nullstellensatz implies:

Corollary 4.5. *The maps $X \mapsto I(X)$ and $\mathfrak{a} \mapsto Z(\mathfrak{a})$ between the set of all closed sets of $\mathbb{A}^n$ and the set of all radical ideals of A are inverse to each other. We have X irreducible if and only if $I(X)$ is a prime ideal. We have* $\dim(X) = \dim(A(X))$.

Remark 4.6. By the above Corollary the map from X to the set of maximal ideals of $A(X)$ given by $P \mapsto \mathfrak{m}(P) = I(P)/I(X)$ is a bijection.

Remark 4.7. By Nullstellensatz $\mathbb{A}^n$ with the Zariski topology is Noetherian. Hence so is every closed subset of $\mathbb{A}^n$.

Definition 4.8. For $f \in A = k[y_1, ..., y_n]$ and $P = (a_1, ..., a_n) \in Z(f)$ we define the *linear part* of f at P to be

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

For an algebraic set $X \subset \mathbb{A}^n$ write $I(X) = (f_1, ..., f_n)$ and define the (affine) *tangent space* to X at P to be the algebraic set

$$T_P X := Z(\ell_P(f_1), ..., \ell_P(f_n)) \subset \mathbb{A}^n. \tag{4.1}$$

Note (check!) that the affine tangent space depends only on X (and not on the choice of the equations f_i) and is the translation of a linear subspace of $\mathbb{A}^n$ by the vector P. On the other hand let

$$\mathfrak{m} = \mathfrak{m}(P) = \frac{I(P)}{I(X)} = \frac{(x_1 - a_1, ..., x_n - a_n)}{(f_1, ..., f_n)}$$

and define the (abstract) tangent space to X at P to be the k-linear space dual to $\mathfrak{m}/\mathfrak{m}^2$, i.e.,

$$T'_P X = \left(\mathfrak{m}/\mathfrak{m}^2\right)^\circ := Hom_k(\mathfrak{m}/\mathfrak{m}^2, k) \tag{4.2}$$

Exercise 4.9. We have a natural k-linear isomorophism

$$\mathfrak{m}/\mathfrak{m}^2 \simeq \frac{k(x_1 - a_1) + ... + k(x_n - a_n)}{k\ell_P(f_1) + ... + k\ell_P(f_n)}$$

and an induced bijection

$$T'_P X \to T_P X, \quad \varphi \mapsto (\varphi(x_1 - a_1) + a_1, ..., \varphi(x_n - a_n) + a_n), \quad \varphi : \mathfrak{m}/\mathfrak{m}^2 \to k.$$

We will identify, whenever useful, the spaces $T_P X$ and $T'_P X$ above via the above bijection and we refer to either of them as the tangent space to X at P.

Definition 4.10. A *linear* algebraic set in $\mathbb{A}^n$ is a set of the form $Z(h_1, ..., h_m)$ where h_i are polynomials of degree 1. A linear algebraic set of dimension 1 is called a *line*; one of dimension 2 is called a *plane*. We say 3 points are *collinear* if they lie on a line.

Exercise 4.11. Prove that for every two distinct points $P, Q \in \mathbb{A}^n$ there is exactly one line passing through them (usually denoted by L_{PQ}). Prove that two distinct lines in $\mathbb{A}^2$ either meet in one point or they do not meet (in which case we say they are parallel). Prove that through any 3 non-collinear points in $\mathbb{A}^n$ there is exactly one plane containing them. Prove that if two planes in $\mathbb{A}^n$ meet and don't coincide then they meet in a line.

Exercise 4.12. (Desargues' Theorem) Let $A_1, A_2, A_3, A'_1, A'_2, A'_3$ be distinct points in the affine plane $\mathbb{A}^2$. Also for all $i \neq j$ assume A_iA_j and $A'_iA'_j$ are not parallel and let P_{ij} be their intersection. Assume the 3 lines $L_{A_1A'_1}, L_{A_2A'_2}, L_{A_3A'_3}$ have a point in common. Then prove that the points P_{12}, P_{13}, P_{23} are collinear.

Hint: Consider the projection $\mathbb{A}^3 \to \mathbb{A}^2$, $(x, y, z) \mapsto (x, y)$ and show that lines project onto lines or points. Next show that configuration of points $A_i, A'_i \in \mathbb{A}^2$ can be realized as the projection of a similar configuration of points $B_i, B'_i \in \mathbb{A}^3$ not contained in a plane. (Identifying $\mathbb{A}^2$ with the set of points in space with zero third coordinate we take $B_i = A_i$, $B'_i = A'_i$ for $i = 1, 2$, we let B_3 have a nonzero third coordinate, and then we choose B'_3 such that the lines $L_{B_1B'_1}, L_{B_2B'_2}, L_{B_3B'_3}$ have a point in common.) Then prove "Desargues' Theorem in Space" (by noting that if Q_{ij} is the intersection of $L_{B_iB_j}$ with $L_{B'_iB'_j}$ then Q_{ij} is in the plane containing B_1, B_2, B_3 and also in the plane containing B'_1, B'_2, B'_3; hence Q_{ij} is in the intersection of these planes which is a line). Finally deduce the original plane Desargues by projection.

5. Algebraic sets in $\mathbb{P}^n$

Definition 5.1. The *projective n-space* is the set

$$\mathbb{P}^n := \frac{k^{n+1} \setminus \{0\}}{\sim}$$

where $v \sim w$ if $\exists \lambda \in k^\times$ such that $w = \lambda v$. The class in $\mathbb{P}^n$ of a point $(a_1, ..., a_n) \in k^{n+1}$ is denoted by

$$(a_1 : ... : a_n) \in \mathbb{P}^n.$$

Exercise 5.2. Prove that $\mathbb{P}^n$ is in a natural bijection with the set of all 1-dimensional vector subspaces of k^{n+1}.

Consider the ring of polynomials

$$S = k[x_0, ..., x_n] = \bigoplus S_d$$

where S_d is the k-vector space of homogeneous polynomials of degree d (i.e. polynomials all of whose monomials have degree d). For $F \in S_d$ we have

$$f(\lambda a_1, ..., \lambda a_n) = \lambda^d f(a_1, ..., a_n)$$

hence if two points of $k^{n+1} \setminus \{0\}$ are equivalent then F vanishes at one of the points if and only F vanishes at the other point. For $P = (a_1 : ... : a_n)$ we write $F(P) = 0$ if and only if $F(a_1, .., a_n) = 0$. Set

$$S^h := \bigcup_{d \geq 0} S_d$$

the set of homogeneous polynomials. For every subset $X \subset \mathbb{P}^n$ let $I(X) \subset S$ be the ideal generated by all polynomials $F \in S^h$ such that $F(P) = 0$ for all $P \in X$; it is a radical homogeneous ideal. (An ideal in S is called homogeneous if it is generated by homogeneous polynomials.) For every subset $T \subset S^h$ let $Z(T) \subset \mathbb{P}^n$ be the set of all $P \in \mathbb{P}^n$ such that $F(P) = 0$ for all $F \in T$. We refer to $x_0, ..., x_n$ as (projective) coordinates of $\mathbb{P}^n$; note that x_i do not define functions $\mathbb{P}^n \to k$.

Definition 5.3. A subset of $\mathbb{P}^n$ is called *algebraic* if it is of the form $Z(T)$ for some $T \subset S^h$.

Exercise 5.4. The algebraic sets in $\mathbb{P}^n$ are the closed sets of a topology on $\mathbb{P}^n$ (called the Zariski topology).

For $X \subset \mathbb{P}^n$ closed set $S(X) = A/I(X)$ (called the homogeneous coordinate ring of X). The ideal $(x_0, ..., x_n) \subset S$ is called the irrelevant ideal. The Hilbert Nullstellensatz implies:

Corollary 5.5. *The maps $X \mapsto I(X)$ and $\mathfrak{a} \mapsto Z(\mathfrak{a})$ between the set of all closed sets of $\mathbb{P}^n$ and the set of all non-irrelevant radical homogeneous ideals of S are inverse to each other. We have X irreducible if and only if $I(X)$ is a prime ideal.*

Definition 5.6. A *linear* subspace in $\mathbb{P}^n$ is a closed set of the form $Z(L_1, ..., L_s)$ where $L_i \in S_1$ are linearly independent linear forms. If $s = 1$ the linear subspace is called a hyperplane. If $s = n$ the linear subspace is called a *line*. If $s = n - 1$ the linear subspace is called a *plane*. A *hypersurface* in $\mathbb{P}^n$ of degree d is a closed set of the form $H = Z(F)$ with $F \in S_d$, F without multiple factors. A hypersurface of degree 2 is called a *quadric*. (In case $n = 2$ quadrics are called *conics*.) A hypersurface of degree 3 is called a *cubic*. Similarly one defines *quartics, quintics, sextics*, etc. One says 3 points in $\mathbb{P}^n$ are *collinear* if they lie on a line.

Consider the following maps (called homogenizing and dehomogenizing maps)

$$A \to S^h \setminus x_0 S^h, \quad f(y_1, ..., y_n) \mapsto f^h := x_0^{\deg(f)} f(\frac{x_1}{x_0}, ... \frac{x_n}{x_0}),$$

$$S^h \setminus x_0 S^h \to A, \quad F(x_0, ..., x_n) \mapsto F^{h^{-1}} := F(1, y_1, ..., y_n).$$

Exercise 5.7. The above maps are inverse to each other:

$$(f^h)^{h^{-1}} = f, \quad (F^{h^{-1}})^h = F.$$

Exercise 5.8. The map $\varphi_0 : \mathbb{P}^n \setminus Z(x_0) \to \mathbb{A}^n$ given by

$$\varphi_0(a_0 : ... : a_n) = (a_1/a_0, ..., a_n/a_0)$$

is a homeomorphism. Hint: $\varphi^{-1}(Z(T)) = Z(T^h) \setminus Z(x_0)$ and $\varphi(Z(\mathfrak{T}) \setminus Z(x_0)) = Z(\mathfrak{T}^{h^{-1}})$. More generally a similar result holds for the maps

$$\varphi_i : \mathbb{P}^n \setminus Z(x_i) \to \mathbb{A}^n$$

given by

$$\varphi_i(a_0 : ... : a_n) = (a_0/a_i, ..., \widehat{a_i/a_i}, ... a_n/a_i).$$

We usually identify $\varphi^{-1}(\mathbb{A}^n)$ with $\mathbb{P}^n \setminus Z(x_i)$.

Exercise 5.9. If $f \in A = k[y_1, ..., y_n]$ is an irreducible polynomial then the Zariski closure of $Z(f)$ in $\mathbb{P}^n$ is $Z(f^h)$. Hint: $Z(f^h)$ is irreducible (because f irreducible implies f^h irreducible) and it contains $Z(h)$ as an open set; but every open set in an irreducible topological space is dense.

We identify in what follows $A = k[y_1, ..., y_n]$ with the subring $k[x_1/x_0, ..., x_n/x_0]$ of the fraction field of S via the map $y_i \mapsto x_i/x_0$; under this identification if $f \in A$ has degree d then

$$f = f^h/x_0^d.$$

We identify $\mathbb{A}^n$ with a subset of $\mathbb{P}^n$ via φ_0. For every ideal $I \subset S$ we define

$$I_{(x_0)} = \{F/x_0^d \mid d \geq 0, \ F \in S_d\}.$$

In particular $S_{(x_0)} = k[x_1/x_0, ..., x_n/x_0]$.

Proposition 5.10. *For every closed subset $X \subset \mathbb{P}^n$ we have*

$$I(X \cap \mathbb{A}^n) = I(X)_{(x_0)}.$$

Proof. The inclusion $\supset$ is clear. For $\subset$ let $f \in I(X \cap \mathbb{A}^n)$ have degree d. Then f vanishes on X. Hence $F := f^h$ vanishes on $X \cap \mathbb{A}^n$. Hence $x_0 F$ vanishes on X. Now

$$f = F/x_0^d = x_0 F/x_0^{d+1} \in I(X)_{(x_0)}.$$

$\square$

Exercise 5.11. (Desargues Theorem in $\mathbb{P}^2$). Let $A_1, A_2, A_3, A'_1, A'_2, A'_3$ be distinct points in $\mathbb{P}^2$. For all $i \neq j$ assume $A_i A_j$ and $A'_i A'_j$ intersect in one point P_{ij}. Assume the 3 lines $L_{A_1 A'_1}, L_{A_2 A'_2}, L_{A_3 A'_3}$ have a point in common. Prove that the points P_{12}, P_{13}, P_{23} are collinear.

Exercise 5.12. (Conic through 5 points). Prove that if 5 points are given in $\mathbb{P}^2$ such that no 4 of them are collinear then there exists a unique conic passing through these given 5 points. If no 3 of the 5 points are collinear then the unique conic is irreducible.

Hint: Consider the vector space of all homogeneous polynomials of degree 2 that vanish on a set S of points. Next note that if one adds a point to S the dimension of this space either stays the same or drops by one. Since the space of all polynomials of degree 2 has dimension 6 it is enough to show that for $r \leq 5$ the space of polynomials that vanish at $r-1$ of the r points is strictly bigger than the space of polynomials that vanish at all r points. For $r=5$, for instance, this is done as follows. Let $P_1, ..., P_5$ be our points and let L_{ij} be the line that passes through P_i and P_j. If neither L_{12} nor L_{34} passes through P_5 the quadric $L_{12} \cup L_{34}$ will not pass through P_5. Assume now that one of the lines L_{12} or L_{34}, for instance L_{12} passes through P_5. Then one checks that none of the lines L_{13} or L_{24} passes through P_5. (Indeed if L_{13} passes through P_5 then L_{12} and L_{13} have 2 points P_1, P_5 in common so they coincide, so P_1, P_2, P_3, P_5 lie on a line, a contradiction; on the other hand if L_{24} passes through P_5 then L_{12} and L_{24} have 2 points P_2, P_5 in common, hence they coincide, hence P_1, P_2, P_4, P_5 line on a line, a contradiction.) So the quadric $L_{13} \cup L_{24}$ does not pass through P_5. The irreducibility part is easy.

Exercise 5.13. (Three Cubics Theorem) Prove that if two distinct cubics in $\mathbb{P}^2$ meet in 9 distinct points such that no 4 of the 9 points lie on a line and no 7 of the 9 points lie on a conic then every cubic that passes through 8 of the 9 points must pass through the 9th point as well.

Hint: First show that if $r \leq 8$ and r points are given then the vector space of homogeneous polynomials of degree 3 vanishing at these points is strictly smaller than the vector space of homogeneous polynomials of degree 3 vanishing at $r-1$ of the r points. (In order to find, for instance, a cubic passing through $P_1, ..., P_7$ but not through P_8 one considers the cubics $C_i = Q_{1234i} \cup L_{jk}$, $\{i, j, k\} = \{5, 6, 7\}$, where Q_{1234i} is the unique conic passing through P_1, P_2, P_3, P_4, P_i and L_{jk} is the unique line through P_j and P_k. Assume C_5, C_6, C_7 all pass through P_8 and derive a contradiction as follows. Note that P_8 cannot lie on 2 of the 3 lines L_{jk} because this would force us to have 4 collinear points. So we may assume P_8 does not lie on either of the lines L_{57}, L_{67}. Hence P_8 lies on both Q_{12345} and Q_{12346}. So these conics have 5 points in common so they coincide. So this conic contains 7 points, a contradiction.) Once this is proved let $P_1, ..., P_9$ be the points of intersection of the cubics with equations F and G. We know that the space of homogeneous polynomials of degree 3 vanishing at $P_1, ..., P_8$ has dimension 2 and contains F and G. So every polynomial in this space is a linear combination of F and G, hence will vanish at P_9.

Exercise 5.14. (Pascal's Theorem) Let $P_1, P_2, P_3, Q_1, Q_2, Q_3$ be distinct points on a conic C in $\mathbb{P}^2$. Let A_1 be the intersection of the lines $L_{P_2Q_3}$ with $L_{P_3Q_2}$, and define A_2, A_3 similarly. Prove that A_1, A_2, A_3 are collinear.

Hint: The cubics

$$L_{Q_1P_2} \cup L_{Q_2P_3} \cup L_{Q_3P_1} \quad \text{and} \quad L_{P_1Q_2} \cup L_{P_2Q_3} \cup L_{P_3Q_1}$$

pass through all of the following 9 points:

$$P_1, P_2, P_3, Q_1, Q_2, Q_3, A_1, A_2, A_3.$$

On the other hand the cubic $C \cup L_{A_2A_3}$ passes through all these points except possibly A_1. Then by the Three Cubics Theorem $C \cup L_{A_2A_3}$ passes through A_1. Hence $L_{A_2A_3}$ passes through A_1.

Exercise 5.15. (Pappus' Theorem) Let L and M be two distinct lines in $\mathbb{P}^2$, let P_1, P_2, P_3 be distinct points on L and let Q_1, Q_2, Q_3 be distinct points on M. Let A_1 be the intersection of the lines $L_{P_2Q_3}$ and $L_{P_3Q_2}$ and define A_2, A_3 similarly. Prove that A_1, A_2, A_3 are collinear.

Hint: Use Pascal's Theorem.

6. Algebraic sets in products

Consider the ring

$$R = k[y_1, ..., y_m, x_0, ..., x_n] = \bigoplus_{d \geq 0} R_d$$

where R_d are the A-modules generated by all monomials in $y_1, ..., y_m$ of degree d and set $R^h = \cup R_d$. For every subset $T \subset R^h$ let $Z(T) \subset \mathbb{A}^m \times \mathbb{P}^n$ be the set of all $(P, Q) \in \mathbb{A}^m \times \mathbb{P}^n$ such that $F(P, Q) = 0$ for all $F \in T$.

Definition 6.1. A subset of $\mathbb{A}^m \times \mathbb{P}^n$ is called *algebraic* if it is of the form $Z(T)$ for some $T \subset R^h$.

Exercise 6.2. The algebraic sets in $\mathbb{P}^n$ are the closed sets of a topology on $\mathbb{A}^m \times \mathbb{P}^n$ (called the Zariski topology). The maps $id \times \varphi_i : \mathbb{A}^m \times (\mathbb{P}^n \setminus Z(x_i)) \to \mathbb{A}^{m+n}$ are homeomeorphisms.

Remark 6.3. (For the reader familiar with topology) The above topology on $\mathbb{A}^m \times \mathbb{P}^n$ is not the product topology!

Exercise 6.4. Let $\mathbb{A}^2$ have coordinates y_1 and y_2 and consider $Y = Z(y_1y_2 - 1) \subset \mathbb{A}^2$ and the first projection $f : \mathbb{A}^2 \to \mathbb{A}^1$. Prove that $f(Y) = \mathbb{A}^1 \setminus \{0\}$. In particular $f(Y)$ is not closed.

By contrast we have:

Theorem 6.5. *(Elimination Theorem) Let $Y \subset \mathbb{A}^m \times \mathbb{P}^n$ be a closed set and let $f : \mathbb{A}^m \times \mathbb{P}^n \to \mathbb{A}^n$ be the first projection. Then $f(Y)$ is closed.*

Proof. Let $I = I(X) \subset S := k[y, x]$, $A = k[y]$, $U_i = \mathbb{P}^n \setminus Z(x_i)$. Then, as in the case $m = 0$,

$$I(Y \cap (\mathbb{A}^m \times U_i)) = I(Y)_{(x_i)} \subset R_{(x_i)}.$$

Let $P \in \mathbb{A}^m \setminus f(Y)$. We will show that there is an open set $V \subset \mathbb{A}^m$ containing P and disjoint from $f(Y)$. Let $\mathfrak{m} = \mathfrak{m}_P \subset A$ be the maximal ideal corresponding to P, so $\mathfrak{m} = I(P)$. Hence no maximal ideal of $R_{(x_i)}$ containing $I_{(x_i)}$ contains $\mathfrak{m}$ (because otherwise there would be a point in Y lying over P). Hence

$$\mathfrak{m}R_{(x_i)} + I_{(x_i)} = R_{(x_i)}$$

One easily gets that there exists N_i such that for all i we have

$$x_i^{N_i} = \sum_j m_{ij} F_{ij} + G_i$$

with $m_{ij} \in \mathfrak{m}$, $F_{ij} \in R_{N_i}$, $G_i \in I_{N_i}$. Taking $N = \sum N_i$ we get

$$R_N \subset \mathfrak{m}R_N + I_N \subset R_N$$

hence $\mathfrak{m}R_N + I_N = R_N$ hence

$$\mathfrak{m}(R_N/I_N) = R_N/I_N$$

hence

$$\mathfrak{m}(R_N/I_N)_{\mathfrak{m}} = (R_N/I_N)_{\mathfrak{m}}$$

hence by Nakayama

$$(R_N/I_N)_{\mathfrak{m}} = 0$$

so there exists $g \in A \setminus \mathfrak{m}$ such that $gR_N \subset I_N$ so $x_i^N g \in I_N$ so $g \in I_{(x_i)}$ so every maximal ideal of $R_{(x_i)}$ containing $I_{(x_i)}$ must contain g so every point of $Y \cap (\mathbb{A}^m \times U_i)$ lies over a point in $Z(g)$ hence $f(Y) \subset Z(g)$. Also since $g \in A \setminus \mathfrak{m}$ we have $P \notin Z(g)$. Hence

$$P \in \mathbb{A}^n \setminus Z(g) \subset \mathbb{A}^n \setminus f(Y).$$

□

Example 6.6. A "familiar" example of the above theorem is the following. Consider $\mathbb{A}^{n^2}$ with coordinates $(y_{ij})_{i,j \in \{1,...,n\}}$ and let $\mathbb{P}^{n-1}$ have coordinates $x_1, ..., x_n$. Let

$$Y := Z(\sum_j y_{1j}x_j, ..., \sum_j y_{nj}x_j) \subset \mathbb{A}^{n^2} \times \mathbb{P}^{n-1}$$

and let

$$f : \mathbb{A}^{n^2} \times \mathbb{P}^{n-1} \to \mathbb{A}^{n^2}$$

be the first projection. Then

$$f(Y) = Z(\det(y_{ij})).$$

Consider now the ring

$$B = k[u_0, ..., u_m, v_0, ..., v_n] = \bigoplus_{d,e \geq 0} B_{d,e}$$

where $B_{d,e}$ is the k-linear span of all monomials that degree d in the u's and degree e in the v's. Let $B^h = \cup B_{d,e}$. For every subset $T \subset B^h$ let $Z(T) \subset \mathbb{P}^m \times \mathbb{P}^n$ be the set of all $(P, Q) \in \mathbb{P}^m \times \mathbb{P}^n$ such that $F(P, Q) = 0$ for all $F \in T$.

Definition 6.7. A subset of $\mathbb{P}^m \times \mathbb{P}^n$ is called *algebraic* if it is of the form $Z(T)$ for some $T \subset B^h$.

Exercise 6.8. The algebraic sets in $\mathbb{P}^m \times \mathbb{P}^n$ are the closed sets of a topology on $\mathbb{P}^m \times \mathbb{P}^n$ (called the Zariski topology). The maps

$$\varphi_j \times \varphi_i : (\mathbb{P}^m \setminus Z(x_j)) \times (\mathbb{P}^n \setminus Z(x_i)) \to \mathbb{A}^{m+n}$$

are homeomeorphisms. (Again, the above topology on $\mathbb{P}^m \times \mathbb{P}^n$ is not the product topology!)

Exercise 6.9. If $X \subset \mathbb{P}^m$ and $Y \subset \mathbb{P}^n$ are closed then $X \times Y$ is closed in $\mathbb{P}^m \times \mathbb{P}^n$. Same if one or boith projective spaces are replaced by affine spaces.

Exercise 6.10. Let $X \subset \mathbb{P}^n$ be closed. Then the 'diagonal'

$$\{(P, Q) \in X \times X \mid P = Q\}$$

is closed in $X \times X$. Same for the projective space replaced by an affine space.

Exercise 6.11. View $\mathbb{P}^N = \mathbb{P}^{(m+1)(n+1)-1}$ with projective coordinates (w_{ij}) where $i = 0, ..., m$, $j = 0, ..., n$. Consider the Segre map

$$s : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^N,$$

$$((a_0 : ... : a_m), (b_0 : ... : b_n)) \mapsto (..., a_i b_j, ...)$$

Prove that this map is injective, its image is closed, and the map is a homeomorphism onto its image. Hint: the image is $Z(\{w_{ij}w_{kl} - w_{il}w_{kj}\})$.

Exercise 6.12. Let $n = m = 1$ in the previous exercise. Then the image of the Segre map is a quadric in $\mathbb{P}^3$ and for all $P \in \mathbb{P}^1$ the images of $\{P\} \times \mathbb{P}^1$ and $\mathbb{P}^1 \times \{P\}$ are lines in $\mathbb{P}^3$.

Exercise 6.13. Consider the Veronese map

$$v_{m,d} : \mathbb{P}^m \to \mathbb{P}^N, \quad (a_0 : ... : a_m) \mapsto (... : a_0^{i_0} ... a_n^{i_n} : ...)$$

where $i_0, ..., i_n$ range through the set of all tuples of non-negative numbers such that $i_0 + ... + i_n = d$. Prove that this map is injective, its image is closed, and the map is a homeomorphism onto its image.

Exercise 6.14. The image of $v_{1,2}$ is a quadric in $\mathbb{P}^2$.

Exercise 6.15. Identify $\mathbb{P}^n$ with set of all 1-dimensional linear subspaces $L \subset \mathbb{A}^{n+1}$. Then the set

$$X := \{(P, L) \in \mathbb{A}^{n+1} \times \mathbb{P}^n \mid P \in L\}$$

is closed in $\mathbb{A}^{n+1}$. Show that the fibers of the projection $X \to \mathbb{P}^n$ are homeomorphic to $\mathbb{A}^1$. Show that the fibers of the projection $X \to \mathbb{A}^{n+1}$ at points $\neq 0$ consist of one point. Show that the fiber of the projection $X \to \mathbb{A}^{n+1}$ at 0 is homeomorphic to $\mathbb{P}^n$. X is called the blow up of $\mathbb{A}^{n+1}$ at 0. Hint: $X = Z(\{x_i y_j - x_j y_i\})$.

Exercise 6.16. Let $\check{\mathbb{P}}^n$ be the set of all hyperplanes $Z(\sum_{i=0}^n a_i x_i)$ in $\mathbb{P}^n$. Identify $\check{\mathbb{P}}^n$ with $\mathbb{P}^n$ by

$$Z(\sum_{i=0}^n a_i x_i) \mapsto (a_0 : ... : a_n).$$

Then the 'incidence' set

$$X = \{(P, H) \in \mathbb{P}^n \times \check{\mathbb{P}}^n \mid P \in H\}$$

is closed in $\mathbb{P}^n \times \check{\mathbb{P}}^n$. Show that the fibers of both projections

$$X \to \mathbb{P}^n, \quad X \to \check{\mathbb{P}}^n$$

are homeomorphic to $\mathbb{P}^{n-1}$. Hint: $X = Z(\sum_{i=0}^n u_i x_i)$ where u_i are the projective coordinates in $\check{\mathbb{P}}^n$.

7. Varieties

Definition 7.1. Let X be a topological space and k a field. For every open set $U \subset X$ denote by $Fun(U, k)$ the ring of all functions $U \to k$. A *sheaf of (k-valued) functions* on X is a rule $\mathcal{O}$ that attaches to each open set $U \subset X$ a subring $k \subset \mathcal{O}(U) \subset Fun(U, k)$ with the following properties

1) for every open sets $V \subset U$ if $f \in \mathcal{O}(U)$ then $f_{|V} \in \mathcal{O}(V)$;

2) for every open set U and every open cover $U = \cup_i U_i$ if $f \in Fun(U, k)$ has the property that $f_{|U_i} \in \mathcal{O}(U_i)$ for all i then $f \in \mathcal{O}(U)$.

Here if $f : U \to k$ is a function and $V \subset U$ we denote by $f_{|V} : V \to k$ the restriction of f to V.

Later we will need a more general notion of sheaf.

Definition 7.2. For a sheaf of functions $\mathcal{O}$ on X one defines the *stalk* of $\mathcal{O}$ (or the ring of germs) at a point $P \in X$ to be the ring

$$\mathcal{O}_P := \{(U, f) \mid P \in U,\ f \in \mathcal{O}(U)\}/\sim$$

where $(U, f) \sim (V, g)$ if and only if there exists an open set $P \in W \subset U \cap V$ such that $f_{|W} = g_{|W}$. If in addition X is irreducible one defines the ring

$$K(X) = \{(U, f) \mid U \neq \emptyset,\ f \in \mathcal{O}(U)\}/\sim$$

where $(U, f) \sim (V, g)$ if and only if there exists a non-empty open set $W \subset U \cap V$ such that $f_{|W} = g_{|W}$.

Definition 7.3. One defines a *classical ringed space* over a field k to be a pair $(X, \mathcal{O}_X)$ consisting of a topological space X and sheaf of functions $\mathcal{O}_X$ on it. A morphism of classical ringed spaces $(X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is a continuous map $f : X \to Y$ such that for every open set $V \subset Y$ and every $g \in \mathcal{O}(V)$ the composition $f^*(g) := g \circ f : f^{-1}(V) \to V \to k$ belongs to $\mathcal{O}(f^{-1}(V))$. We obtain a category called the category of classical ringed spaces.

Remark 7.4. The terminology of "classical ringed space" is not standard! There is a standard notion of "ringed space," not to be discussed here, and our "classical ringed spaces" are examples of "ringed spaces." Topological manifolds, smooth manifolds, complex analytic manifolds, and the algebraic varieties of "classical" algebraic geometry can all be introduced as special cases of "classical ringed spaces." On the other hand Grothendieck's schemes (which are the main objects of "non-classical" algebraic geometry) do not fit into the paradigm of "classical ringed spaces" but rather require the more general paradigm of "ringed spaces."

Remark 7.5. For a morphism $f : X \to Y$ of classical ringed spaces we have ring homomorphisms

$$f^* : \mathcal{O}(V) \to \mathcal{O}(f^{-1}(V)), \quad f^* : \mathcal{O}_{f(P)} \to \mathcal{O}_P, \quad P \in X.$$

If X, Y are irreducible and $f(X)$ is dense in Y we have an induced morphism

$$f^* : K(Y) \to K(X).$$

An open set U of a classical ringed space $(X, \mathcal{O}_X)$ has a naturally induced structure of classical ringed space $(U, \mathcal{O}_U)$: one sets $\mathcal{O}_U(V) = \mathcal{O}_X(V)$ for every open set $V \subset U$.

Definition 7.6. Let X be a closed set in $\mathbb{A}^n$ (or $\mathbb{P}^n$ or $\mathbb{A}^m \times \mathbb{P}^n$ or $\mathbb{P}^m \times \mathbb{P}^n$). Define a sheaf of functions on X as follows. Let $V \subset X$ be open. A function $f : V \to k$ is regular at P if there exists an open set $P \in W \subset V$ and $g, h \in A$ (or S_d or R_d or $B_{d,e}$) such that $g(Q) \neq 0$ for all $Q \in W$ and such that $f(Q) = g(Q)/h(Q)$ for all $Q \in W$. Let $\mathcal{O}_Y(V)$ be the ring of all functions $f : V \to k$ that are regular at all points $P \in V$. Clearly this defines a sheaf of functions, $\mathcal{O}_X$ on X hence a structure of classical ringed space on X, and hence on every open set of X.

Definition 7.7. A *variety* (over k) is a classical ringed space X such that every point $P \in X$ has an open neighborhood U which is isomorphic as a classical ringed space to a closed set in $\mathbb{A}^n$ for some n.

Remark 7.8. Note that, in the above definition, one requires that that every point $P \in X$ has an open neighborhood U which is isomorphic to a **closed** (rather then **open**!) set in $\mathbb{A}^n$. This is in deep contrast with the definitions of topological, smooth or analytic manifolds based on classical ringed spaces! We will not further comment of this discrepancy here.

Exercise 7.9. The maps $\varphi : \mathbb{P}^n \setminus Z(x_i) \to \mathbb{A}^n$ are isomorophism of classical ringed spaces. So every closed set in $\mathbb{P}^n$ is a variety. Same for $\mathbb{A}^m \times \mathbb{P}^n$ or $\mathbb{P}^m \times \mathbb{P}^n$.

Exercise 7.10.

1) Let $X = Z(f_1, ..., f_m) \subset \mathbb{A}^n$ and $f \in A = k[y_1, ..., y_n]$. Then

$$X_f := X \setminus Z(f)$$

is isomorphic as a classical ringed space to

$$Z(f_1, ..., f_n, y_{n+1}f - 1) \subset \mathbb{A}^{n+1}.$$

2) X_f above is a variety.
3) Every open set of a variety is a variety (which we call an open subvariety).
4) Every closed set of a variety is a variety (which we call an closed subvariety)

Definition 7.11. The category of varieties has as its objects the varieties and as its morphisms the morphisms of classical ringed spaces. A morphism of varieties is also called a *regular map*. A variety is called *affine* if it is isomorphic to a closed set in $\mathbb{A}^n$. A variety is called *projective* if it is isomorphic to a closed set in $\mathbb{P}^n$. A variety is called *quasi-affine* (resp. *quasi-projective*) if it is isomorphic to an open subset of an affine (or projective) variety.

So every affine variety is quasi-projective, every quasi-affine variety is quasi-projective and every projective variety is quasi-projective. Every quasi-affine variety is affine. Clearly every quasi-projective variety is a Noetherian topological space.

Exercise 7.12.

1) Let $f_1, ..., f_m \in k[x_1, ..., x_n]$ be arbitrary polynomials. Then the map

$$\mathbb{A}^n \to \mathbb{A}^m,$$

$$(a_1, ..., a_n) \mapsto (f_1(a_1, ..., a_n), ..., f_m(a_1, ..., a_n))$$

is regular.

2) Let $F_0, ..., F_m \in k[x_0, ..., x_n]$ be arbitrary homogeneous polynomials of the same degree. Then the map

$$\mathbb{P}^n \setminus Z(F_0, ..., F_m) \to \mathbb{P}^m,$$

$$(a_0 : ... : a_n) \mapsto (F_0(a_0 : ... : a_n) : ... : F_m(a_0 : ... : a_n))$$

is regular.

Remark 7.13.

1) Every regular function $f \in \mathcal{O}(X)$ induces (and is induced by) a morphism (still denoted by) $f : X \to \mathbb{A}^1$.

2) The stalks $\mathcal{O}_P = \mathcal{O}_{X,P}$ of a variety are local rings with maximal ideals

$$\mathfrak{m}_P = \{f \in \mathcal{O}_P \mid f(P) = 0\}.$$

3) One has $\mathcal{O}_P/\mathfrak{m}_P \simeq k$.

4) If X is irreducible then $K(X)$ is a field (called the field of rational functions) and

$$\dim(X) = \dim(\mathcal{O}_P) = \text{tr.deg}(K(X)/k), \quad \forall P \in X.$$

Definition 7.14. For a variety X and $P \in X$ the *tangent space* to X at P is the k-linear space

$$T_P X = (\mathfrak{m}_P/\mathfrak{m}_P^2)^\circ := Hom_k(\mathfrak{m}_P/\mathfrak{m}_P^2, k).$$

If X is a closed set in $\mathbb{A}^n$ this definition agrees with the definition of the (abstract) tangent space given previously; this follows from assertion 2 in Theorem 7.19 below.

Note that if $f : X \to Y$ is a morphism of varieties then for all $P \in X$ we have an induced k-linear map

$$T_P f : T_P X \to T_{f(P)} Y$$

called the tangent map at P.

Definition 7.15. A point P of a variety X is called *non-singular* if $\mathcal{O}_P$ is regular, i.e.,

$$\dim_k(\mathfrak{m}_P/\mathfrak{m}_P^2) = \dim(\mathcal{O}_P).$$

Equivalently

$$\dim_k T_P X = \dim(X).$$

A variety is *non-singular* if all points are non-singular.

Remark 7.16. A curve is non-singular if and only if all local rings $\mathcal{O}_P$ are DVR's.

Exercise 7.17. A plane curve $Z(f) \subset \mathbb{A}^2$ (where $f = f(x, y)$ is irreducible) is non-singular if and only if the ideal

$$\left(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right)$$

is the whole ring $k[x, y]$.

Remark 7.18.

1) The Segre maps are morphisms of varieties that are isomorphisms onto their images and so are the Veronese maps.

2) The product of two varieties has a natural structure of variety.

3) Projection maps from products of varieties to their factors are morphisms of varieties.

4) Products of affine varieties are affine. Products of projective varieties are projective (use Segre maps). Products of quasi-projective varieties are quasi-projective.

5) The complement of a hypersurface in projective space is affine (use the Veronese map).

Theorem 7.19. *Let $X \subset \mathbb{A}^n$ be a closed subvariety. Then the following hold:*

1) $\mathcal{O}_P = A(X)_{\mathfrak{m}(P)}$ for $\mathfrak{m}(P) = I(P)/I(X)$.

2) $\mathfrak{m}_P = \mathfrak{m}(P)A_{\mathfrak{m}(P)}$ hence $\mathfrak{m}_P/\mathfrak{m}_P^2 = \mathfrak{m}(P)/\mathfrak{m}(P)^2$.

3) $\mathcal{O}(X) = A(X)$.

4) $K(X) \simeq Frac(A(X))$.

Proof. The natural map $A(X) \to \mathcal{O}(X)$ is clearly injective; we view this map as an inclusion. By the definition of regular functions the maps $A(X)_{\mathfrak{m}(P)} \to \mathcal{O}_P$ are correctly defined and bijective. We proved assertion 1. Also, in $K(X)$, we have the following ionclusions of subsets of $K(X)$:

$$A(X) \subset \mathcal{O}(X) \subset \bigcap_{P \in X} \mathcal{O}_P = \bigcap_{\mathfrak{m} \text{ maximal}} A(X)_{\mathfrak{m}} = A(X).$$

This proves assertion 3. The rest of the assertions are trivial. □

Assertions 1-3 also hold without the assumption that X is irreducible.

Exercise 7.20. With the notation in Exercise 7.10 we have $\mathcal{O}(X_f) = \mathcal{O}(X)_f$. Hint: use the isomorphism $A[y]/(fy-1) \simeq A_f$ valid for every ring A and every $f \in A$.

Theorem 7.21. *The functor $X \mapsto \mathcal{O}(X)$ is an equivalence between the category of affine varieties and the category of reduced finitely generated k-algebras.*

Proof. One needs a functor in the opposite direction such that the composition of the two functors in each direction are isomorphic to the identity. The functor in the opposite direction is defined by taking any reduced finitely generated k-algebra A, choosing an arbitrary surjective homomorphism $k[y_1, ..., y_n] \to A$, letting $\mathfrak{a}$ be the kernel of this homomorphism and attaching to A the affine variety $Z(\mathfrak{a})$. For an morphism $u : A \to B$ one gets an induced homomorphism

$$u' : k[y_1, ..., y_n]/\mathfrak{a} \simeq A \xrightarrow{u} B \simeq k[z_1, ..., z_m]/\mathfrak{b}$$

which can be lifted (non-uniquely) to a homomorphism

$$u'' : k[y_1, ..., y_n] \to k[z_1, ..., z_m], \quad y_i \mapsto f_i(z_1, ..., z_m).$$

Then the map

$$\mathbb{A}^m \to \mathbb{A}^n, \quad P = (a_1, ..., a_m) \mapsto (f_1(P), ..., f_n(P))$$

induces a morphism of varieties $Z(\mathfrak{a}) \to Z(\mathfrak{b})$ which is independent of the lifting u'' of u'. One checks that this functor has the desired property. □

Exercise 7.22. Let $f : X \to Y$ be a morphism of closed subvarieties of affine some affine spaces.

1) If $P \in Y$ then $\mathcal{O}(f^{-1}(P)) = A(X)/\sqrt{\mathfrak{m}(P)A(X)}$.

2) If $Z \subset Y$ is the Zariski closure of $f(X)$ then $\mathcal{O}(Z) = A(Y)/\mathfrak{a}$, where $\mathfrak{a}$ is the kernel of the homomorphism $A(Y) \to A(X)$.

Example 7.23. The quasi-affine variety $\mathbb{A}^2 \setminus \{0\}$ is not affine. Indeed assume it is and we will get a contradiction. Consider the inclusion $\mathbb{A}^2 \setminus \{0\} \to \mathbb{A}^2$ and the induced homomorphism

$$k[x,y] = A(\mathbb{A}^2) = \mathcal{O}(\mathbb{A}^2) \subset \mathcal{O}(\mathbb{A}^2 \setminus \{0\}) \subset \mathcal{O}(\mathbb{A}^2 \setminus Z(x)) \cap \mathcal{O}(\mathbb{A}^2 \setminus Z(y)) =$$

$$= k[x,y]_x \cap k[x,y]_y = k[x,y]$$

hence

$$\mathcal{O}(\mathbb{A}^2) \subset \mathcal{O}(\mathbb{A}^2 \setminus \{0\})$$

is an isomorphism hence, by the equivalence of categories, $\mathbb{A}^2 \setminus \{0\} \to \mathbb{A}^2$ is an isomorophism; but the latter is not surjective, contradiction.

8. Morphisms

Definition 8.1. A morphism of irreducible varieties is called *dominant* if it has dense image.

Theorem 8.2. *(Chevalley's Theorem) For every dominant morphism of irreducible varieties $f : X \to Y$ the image $f(X)$ contains a non-empty open set of Y.*

Proof. We may assume X and Y are affine (check!). Set $A = \mathcal{O}(Y)$ and $B = \mathcal{O}(X)$. So A and B are integral domains. From the fact that $f(X)$ is dense in Y it follows that the induced homomorphism $A \to B$ is injective (check!). We view the latter as an inclusion. Since B is a finitely generated A-algebra there exist a surjective homomorphism $A[x_1, ..., x_n] \to B$, $x_i \mapsto b_i$. We may assume there exists m such that $b_1, ..., b_m$ are algebraically independent (i.e. the induced homomorphism $A[x_1, ..., x_m] \to B$ is an isomorphism which we view as an equality) and that $b_{m+1}, ..., b_n$ are algebraic over $A[x_1, ..., x_m]$ (check!). Then for each $i = m + 1, ..., n$ the element b_i is a root of a polynomial

$$\Phi_i(t) = F_{i0}(x_1, ..., x_m)t^{n_i} + F_{i1}(x_1, ..., x_m)t^{n_i-1} + ... + F_{in_i}(x_1, ..., x_m)$$

with $F_{ij} \in A[x_1, ..., x_m]$. Let

$$F = \prod_{i=1}^{m} F_{i0}.$$

Then the extension

$$A[x_1, ..., x_m]_F \subset B_F$$

is finite because each b_i with $i = m+1, ..., n$ is integral over $A[x_1, ..., x_m]_F$ (check!). By Lemma 2.12 every maximal ideal of $A[x_1, ..., x_m]_F$ has a maximal ideal in B_F lying above. On the other hand if s is a non-zero coefficient of F then every maximal ideal $\mathfrak{m}$ in A not containing s has the maximal ideal $\mathfrak{m}[x_1, ..., x_m]_F$ of $A[x_1, ..., x_m]_F$ lying above it. This shows that the open set $Y \setminus Z(s)$ is contained in $f(X)$. $\square$

Definition 8.3. A morphism of varieties $f : X \to Y$ is called *finite* if for every point $P \in Y$ there is an affine open set $P \in V \subset Y$ such that $f^{-1}(V)$ is affine and the algebra

$$\mathcal{O}(V) \to \mathcal{O}(f^{-1}(V))$$

is finite.

Remark 8.4. Let us say that a morphism of varieties $f : X \to Y$ is *finite in the strong sense* if for every affine open set $V \subset Y$ we have that $f^{-1}(V)$ is affine and the algebra

$$\mathcal{O}(V) \to \mathcal{O}(f^{-1}(V))$$

is finite. Clearly a composition of finite morphisms in the strong sense is finite in the strong sense. It is actually a theorem that every finite morphism is finite in the strong sense. We omit the proof of this theorem. Note that, by the theorem just referred to, a composition of finite morphisms is finite. We will not need this in what follows; the compositions of finite morphisms to be considered in what follows can be checked directly to be finite.

Definition 8.5. A morphism is *quasi-finite* if all fibers are finite.

By Lemma 2.12 we get

Corollary 8.6. *If $f : X \to Y$ is a finite morphism then it is quasi-finite and has a closed image. In particular a finite dominant morphism is surjective.*

Definition 8.7. The *degree* $\deg(f)$ of a finite dominant morphism of irreducible varieties $f : X \to Y$ is the degree of the field extension $[K(X) : K(Y)]$ where $K(Y)$ is viewed as a subfield of $K(X)$ via the embedding $f^* : K(Y) \to K(X)$.

Definition 8.8. Let $Z = Z(L_0, ..., L_s)$ be a linear subspace of $\mathbb{P}^n$ where $L_0, ..., L_s$ are linear forms. The morphism

$$\pi : \mathbb{P}^n \setminus Z \to \mathbb{P}^s,\ \pi(P) = (L_0(P) : ... : L_s(P))$$

is called the *projection* from Z.

Remark 8.9. Every projection as above is a composition of projection from points. For the projection from a point the inverse image of the complement of a hyperplane is the complement of a hyperplane.

Theorem 8.10. *Assume the situation in the above Definition and let $X \subset \mathbb{P}^n$ be a closed subvariety such that $X \cap Z = \emptyset$. Then the induced morphism $\pi : X \to \mathbb{P}^s$ (called again the projection from Z) is finite.*

Proof. It is enough to check that if Z is a point and V is the complement of a hyperplane then $\pi^{-1}(V)$ (which is X minus a hyperplane) has the property that

$$\mathcal{O}(V) \to \mathcal{O}(\pi^{-1}(V))$$

is finite. We may assume $Z = Z(x_1, ..., x_n)$ hence

$$\pi(a_0 : a_1 : ... : a_n) = (a_1 : ... : a_n).$$

Let $x_1, ..., x_n$ be the projective coordinates on $\mathbb{P}^{n-1}$ and let $V_i = \mathbb{P}^{n-1} \setminus Z(x_i)$ for $i = 1, ..., n$. Then $\pi^{-1}(V_i) = X \setminus Z(x_i)$ which is affine. We are left to prove that the algebra map

$$A(V_i) = k[x_1, ..., x_n]_{(x_i)} \to A(X \setminus Z(x_i)) = k[x_0, ..., x_n]_{(x_i)}/I(X)_{(x_i)}$$

is finite. But since $(1 : 0... : 0) \notin X$ there exists a homogeneous $F \in I(X)$ of some degree d such that x_0^d appears in F. Hence $I(X)_{(x_i)}$ contains a monic polynomial in x_0/x_i with coefficients in $k[x_1, ..., x_n]_{(x_i)}$ and the finiteness of the algebra map above follows. □

Corollary 8.11. *(Projective Noether Normalization) For every projective irreducible variety X of dimension d there is a finite surjective morphism $X \to \mathbb{P}^d$.*

Proof. If $X \subset \mathbb{P}^n$ is not the whole of $\mathbb{P}^n$ let $Y \subset \mathbb{P}^{n-1}$ be the image of X under the projection from a point in $\mathbb{P}^n \setminus X$. If Y is not the whole of $\mathbb{P}^{n-1}$ consider a further projection, etc. This process will stop. □

Exercise 8.12. Let $Z = \{P\}$ where $O = (1 : 0 : ... : 0) \in \mathbb{P}^n$ and identify $\mathbb{P}^{n-1}$ with $Z(x_0) \subset \mathbb{P}^n$. Also take $L_0 = x_1, ..., L_{n-1} = x_n$. Show that under this identification the projection $\pi : \mathbb{P}^n \setminus \{O\} \to \mathbb{P}^{n-1} = Z(x_0)$ can be described as follows: for all $Q \in \mathbb{P}^n \setminus \{O\}$ the point $\pi(Q) \in Z(x_0)$ is the unique point of intersection of $Z(x_0)$ with the line L_{OQ} passing through O and Q. Hint: the points O, Q and $\pi(Q)$ lie on a line because the $3 \times (n+1)$ matrix whose rows are their coordinates has rank 2.

Exercise 8.13. Let $v_{1,3} : \mathbb{P}^1 \to \mathbb{P}^3$ be the Veronese map and $X = v_{1,3}(\mathbb{P}^1)$.

1) Find the equation of $\pi(X)$ in $\mathbb{P}^2$ where $\pi : X \to \mathbb{P}^2$ is the projection from the point $(0 : 1 : 0 : 0)$.

2) Find the equation of the Zariski closure of $\pi(X)$ in $\mathbb{P}^2$ where $\pi : X \setminus \{O\} \to \mathbb{P}^2$ is the projection from the point $(1 : 0 : 0 : 0) \in X$.

Definition 8.14. A variety X is *separated* if its diagonal $\{(P, P) \in X \times X \mid P \in X\}$ is closed in $X \times X$.

Exercise 8.15. Every quasi-projective variety is separated. Hint: use the fact that the diagonal of $\mathbb{P}^n$ is closed.

Definition 8.16. A variety X is *complete* if for every variety Y and every closed set $Z \subset Y \times X$ if $\pi : Y \times X \to Y$ denotes the first projection then $\pi(Z)$ is closed in Y.

Exercise 8.17. Every projective variety is complete. Hint: use the Elimination Theorem.

Exercise 8.18. Every closed subvariety of a complete variety is complete.

Exercise 8.19. If $f : X \to Y$ is a morphism of varieties with X complete then for all closed subsets Z of X the set $f(Z)$ is closed in Y. Hint: f is the composition of the morphism $f \times id : X \to Y \times X$ with the second projection. Then note that $f \times id$ induces an isomorphism between its source and its image.

We have the following analogue of Liouville's Theorem in complex analysis saying that any holomorphic map on the Riemann sphere is a constant.

Theorem 8.20. *(Analogue of Liouville's Theorem) If X is complete and irreducible then $\mathcal{O}(X) = k$.*

Proof. Let $f \in \mathcal{O}(X)$ and view it as a morphism $f : X \to \mathbb{A}^1$. Consider the composition

$$g : X \xrightarrow{f} \mathbb{A}^1 \subset \mathbb{P}^1.$$

Since X is complete and irreducible $g(X)$ is closed and irreducible in $\mathbb{P}^1$. So $g(X)$ is either a point or the whole of $\mathbb{P}^1$. The second alternative cannot occur because $g(X) \subset \mathbb{A}^1$. $\square$

Corollary 8.21. *If X is both complete and affine and if X is connected then X is a point.*

Proof. By Liouville $\mathcal{O}(X) = k$. If P is a point $\mathcal{O}(P) = k$. Since X and P are affine with isomorphic rings of regular functions we get $X \simeq P$. $\square$

Exercise 8.22. Let X be a closed subvariety of $\mathbb{P}^n$ of dimension ≥ 1 and let H be a hypersurface in $\mathbb{P}^n$. Then $X \cap H \neq \emptyset$. Hint: If the intersection is empty then the connected components of the intersection are affine and projective so they are points, a contradiction.

Definition 8.23. Let X and Y be irreducible varieties. A *rational map* is an element of the set

$$Rat(X, Y) := \{(U, f) \mid \emptyset \neq U \subset X \text{ open}, \quad f : U \to Y \text{ a morphism}\}/\sim$$

where $(U, f) \sim (V, g)$ if there exists an open $\emptyset \neq W \subset U \cap V$ such that $f_{|W} = g_{|W}$. The class of a pair (U, f) is denoted by $f : X \cdot\cdot \to Y$. (In particular $K(X) =$

$Rat(X, \mathbb{A}^1) = Rat(X, \mathbb{P}^1)$.) A morphism $f : X \to Y$ will be identified with the rational map defined by (X, f). (If $(X, g) \sim (X, g)$ then $f = g$; check!) A rational map is *dominant* if it represented by some (U, f) with f dominant. One can define naturally (check!) the composition of two dominant rational maps which is again a dominant rational map. A rational map $f : X \cdot\cdot \to Y$ is called *birational* if it dominant and there exists a dominant rational map $g : Y \cdot\cdot \to X$ such that $f \circ g = id$, $g \circ f = id$.

Exercise 8.24. If X is the blow up of $\mathbb{A}^{n+1}$ at 0 (cf. Exercise 6.15) then the morphism $X \to \mathbb{A}^{n+1}$ in loc.cit. is a birational morphism.

Exercise 8.25. The category C whose objects are irreducible varieties and whose morphisms are dominant rational maps is equivalent to the category of fields that are finitely generated over k. (An isomorphism in C is called a birational isomorphism.) In particular X and Y are birationally isomorphic if and only if the fields $K(X)$ and $K(Y)$ are k-isomorphic.

Exercise 8.26. Every irreducible variety is birationally isomorphic to a hypersurface in some projective space. Hint: Every finitely generated field extension of k is a separable finite extension of a field of rational functions in several variables; then use the Theorem of the primitive element (which says that every separable finite extension of fields can be generated by one element).

We have the following deep result (which we will not need and we will not prove):

Theorem 8.27. *(Hironaka Desingularization Theorem) Let Y be an irreducible projective variety over a field k of characteristic zero. Then there exists a non-singular projective variety X and a morphism $X \to Y$ which is birational and dominant.*

The above is not known for k of positive characteristic.

9. Normalization

Definition 9.1. An irreducible variety X is *normal* if all local rings $\mathcal{O}_{X,P}$ are normal. By a *normalization* of a variety Y we understand a normal variety X equipped with a finite birational morphism $X \to Y$.

Remark 9.2. A curve is normal if and only if it is non-singular.

Theorem 9.3. *Every affine variety has a normalization which is affine.*

Proof. Let Y be an affine variety and $A = \mathcal{O}(Y)$. Let A^{nor} be the normalization of A which is known to be finite over A, in particular finitely generated over k. By the equivalence of categories between affine varieties and finitely generated reduced k-algebras A^{nor} corresponds to a variety X (which is then normal) and the inclusion $A \subset A^{\text{nor}}$ corresponds to a morphism $X \to Y$ (which is finite and birational). $\square$

Theorem 9.4. *Every projective variety has a normalization which is projective.*

Sketch of proof. Consider the projective coordinate ring $C = S(Y)$ of a projective variety $Y \subset \mathbb{P}^n$. One has a decomposition (grading)

$$C = \bigoplus_{d=0}^{\infty} C_d, \quad C_d C_e \subset C_{d+e}$$

induced by that of the ring of polynomials. Let $C^h = \bigcup_{d=0}^{\infty} C_d$. Let $\Sigma = C^h \setminus \{0\}$ and consider the ring of fractions $D = \Sigma^{-1}C$. One checks that one has an induced decomposition (grading)

$$D = \bigoplus_{d=-\infty}^{\infty} D_d, \quad D_d D_e \subset D_{d+e}.$$

Let

$$D_{\geq 0} := \bigoplus_{d=0}^{\infty} D_d$$

and let E be the integral closure of C in $D_{\geq 0}$. Then E is finite over C, hence finitely generated over k. One checks that one has an induced decomposition (grading)

$$E = \bigoplus_{d=0}^{\infty} E_d, \quad E_d E_e \subset E_{d+e}.$$

Then one checks that there exists an integer s such that

$$F := \bigoplus_{d=0}^{\infty} E_{ds}$$

is generated as a k-algebra by finitely many elements $f_0, ..., f_m \in E_s$. Consider the surjective ring homomorphism

$$k[x_0, ..., x_m] \to F, \quad x_i \mapsto f_i.$$

Then the kernel $\mathfrak{a}$ of this homomorphism is generated by homogeneous polynomials. We let $X = Z(\mathfrak{a}) \subset \mathbb{P}^m$. One checks that X is a normal variety equipped with a finite birational morphism to Y. $\square$

Theorem 9.5. *If X is a non-sigular curve then every rational map from X to a projective variety Y extends to a regular map $X \to Y$.*

Proof. We may assume $Y = \mathbb{P}^n$. Then the rational map is given on an open say U of X by

$$P \mapsto f(P) = (f_0(P) : \ldots : f_n(P))$$

where $f_i \in K(X)$. Let $Q \in X$. Since $\mathcal{O}_Q$ is a discrete valuation ring with maximal $\mathfrak{m}_Q = (t_Q)$ there exists $e \in \mathbb{Z}$ such that $g_i := t_Q^e f_i$ are all in $\mathcal{O}_Q$ and not all are in $\mathfrak{m}_Q$. Then f can be extended on a neighborhood of Q by the formula

$$P \mapsto (g_0(P) : ... : g_n(P)).$$

$\square$

Exercise 9.6. Show by an example that in the above Theorem one cannot drop the assumption that Y be projective.

Theorem 9.7. *Every non-constant morphism of non-singular projective curves is finite.*

Proof. We will prove an a priori stronger result namely that every non-constant morphism of non-singular projective curves is finite in the strong sense. Consider such a morphism $f : X \to Y$. Let $V \subset Y$ be affine and $A = \mathcal{O}(V)$. Let B be the integral closure of A in $K(X)$ and let U be an affine variety with $\mathcal{O}(U) = B$. Since $K(U) = K(X)$ there is a birational map $\varphi : U \cdot\cdot\to X$. By Theorem 9.5 φ is a regular map. It is sufficient to check that $f^{-1}(V) = \varphi(U)$. Assume this is false and let $Q_0 \in f^{-1}(V) \setminus \varphi(U)$, $P_0 = f(Q_0) \in V$, $f^{-1}(P_0) = \{Q_0, ..., Q_r, Q_{r+1}, ..., Q_n\}$ with $Q_0, ..., Q_r \notin U$ and $Q_{r+1}, ..., Q_n \in U$. There exists $w \in K(X)$ such that

$$w \notin \mathcal{O}_{Q_0}, \quad w \in \mathcal{O}_{Q_{r+1}} \cap ... \cap \mathcal{O}_{Q_n}.$$

(Indeed one can choose hyperplanes in the projective space where X sits, given by linear forms $H_0, ..., H_n$ such that each of them passes exactly through one of the points $Q_0, ..., Q_n$ respectively. Then one can take w to be the restriction to X of the function $\frac{H_1 ... H_n}{H_0^n}$.) Let $R_0, ..., R_s \in U$ be the points where $w : U \cdots \to k$ is not defined; so $f(R_i) \neq P_0$ for all i. Then, by an argument using hyperplanes as above, one can find $v \in \mathcal{O}(V)$ such that

$$v \in \mathcal{O}_{P_0}^{\times}, \quad u := vw \in \mathcal{O}(U) = B.$$

Since B is integral over A one has

$$u^n + a_1 u^{n-1} + ... + a_n = 0$$

for some $a_1, ..., a_n \in A$. So

$$u = -a_1 - a_2 u^{-1} - ... - a_n u^{-n+1}.$$

But $u \notin \mathcal{O}_{Q_0}$ while $-a_1 - a_2 u^{-1} - ... - a_n u^{-n+1} \in \mathcal{O}_{Q_0}$ because $u^{-1} \in \mathcal{O}_{Q_0}$, a contradiction. □

Exercise 9.8. Show by an example that in the above Theorem one cannot replace the word ‘projective’ by the word ‘affine’.

Corollary 9.9. *Every birational morphism of non-singular projective curves is an isomorphism.*

Proof. Every such morphism is finite hence a normalization hence an isomorphism. □

Exercise 9.10. Find an isomorphism between the projective line $\mathbb{P}^1$ and the quadric $Z(x_0^2 + x_1^2 + x_2^2) \subset \mathbb{P}^2$.

Corollary 9.11. *Every two birationally equivalent non-singular projective curves are isomorphic.*

Proof. Clear from the above corollary. □

10. Divisors on curves

Definition 10.1. By a *divisor* on a curve X we mean an element

$$D = \sum_{P \in X} n_P P$$

of the free abelian group generated by X. (So $n_P \in \mathbb{Z}$ and $n_P = 0$ for all except finitely many $P \in X$.) Set $\deg(D) = \sum n_P$ and let $Div(X)$ be the group of divisors. Write $D \geq 0$ if all $n_P \geq 0$. Define the *support* of D to be the finite set

$$Supp(D) = \{P \in X \mid n_P \neq 0\} \subset X.$$

Write $D = D_+ - D_-$ where $D_+, D_- \geq 0$ and D_+, D_- have disjoint supports.

Recall that for X a non-singular curve and $P \in X$ we have a discrete valuation homomorphism $v_P : K(X) \to \mathbb{Z}$ defined by $v_P(ut_P^e) = e$ for $u \in \mathcal{O}_P^\times$ and t_P a parameter at P, i.e., generator of the maximal ideal $\mathfrak{m}_P$ of $\mathcal{O}_P$.

Let $X \subset \mathbb{P}^n$ and $H = Z(F)$ be a hypersurface of degree N, F without multiple factors, hence F has degree N. Assume $X \not\subset H$. We define a divisor $X \cdot H \in Div(X)$ as follows. If $P \notin X \cap H$ set $(X \cdot H)_P = 0$. Otherwise let i be such that the i-th coordinate of P is $\neq 0$, consider the restriction to X, $f = (F/x_i^N)_{|X} \in \mathcal{O}_P$, of F/x_i^N, and let

$$(X \cdot H)_P = v_P(f) = \dim_k(\mathcal{O}_P/(f)).$$

Then set

$$X \cdot H = \sum (X \cdot H)_P P.$$

Clearly $Supp(X \cdot H) = X \cap H$. If H is a hyperplane call $X \cdot H$ the hyperplane section corresponding to X.

Example 10.2. Let $X = Z(\Phi) \subset \mathbb{P}^2$ be a curve with Φ irreducible of degree d and write

$$\Phi(x_0, x_1, x_2) = x_0 N(x_0, x_1, x_2) + M(x_1, x_2)$$

with N and M homogeneous of degrees $d-1$ and d respectively. Let $P = (0 : 0 : 1) \in X$ and $m(y) = M(y, 1)$; hence $m(0) = 0$. Let $H = Z(x_0)$. We claim that $(X \cdot H)_P$ equals the multiplicity e of 0 as a root of m i.e. s is such that $h(y) = y^e m_1(y)$ with $m_1(0) \neq 0$. Indeed let

$$\varphi(y_0, y_1) = \Phi(y_0, y_1, 1) = y_0 n(y_0, y_1) + m(y_1).$$

Then we have

$$\mathcal{O}_P/(y_0) = \left(\frac{k[y_0, y_1]}{(\varphi, y_0)}\right)_{(y_0,y_1)} = \left(\frac{k[y_0, y_1]}{(m(y_1), y_0)}\right)_{(y_0,y_1)} = \left(\frac{k[y_1]}{(m(y_1))}\right)_{(y_1)} = \frac{k[y_1]}{(y_1^e)}.$$

The latter has dimension e which proves our claim.

Remark 10.3. A computation similar to the one in the above example shows that if X, H are both non-singular curves in $\mathbb{P}^2$ then

$$(X \cdot H)_P = (H \cdot X)_P.$$

If in addition $H = Z(L)$ is a line (hence $L = \sum_{i=0}^2 a_i x_i$ is a linear form) and $X = Z(\Phi)$ then in order to compute the divisor $X \cdot H$ one considers the system

$$\Phi(x_0, x_1, x_2) = L(x_0, x_1, x_2) = 0.$$

One solves the system by solving $L = 0$ for one of the variables, say x_0, and substituting the value of x_0 into Φ. One gets an equation

$$\Psi(x_1, x_2) = 0.$$

One solves the latter by writing

$$\Psi(x_1, x_2) = \prod_i (c_i x_1 - b_i x_2)^{n_i}$$

where the factors are relatively prime. Then one finds a_i from the equation

$$L(a_i, b_i, c_i) = 0$$

Setting $P_i = (a_i : b_i : c_i)$ one concludes that

$$X \cdot H = \sum_i n_i P_i.$$

Exercise 10.4. Prove that if $X = Z(\Phi) \subset \mathbb{P}^2$ is a curve with Φ irreducible of degree d then every hyperplane section of X has degree d.

Exercise 10.5. Compute the divisor $X \cdot H$ for $X = Z(x_0^3 + x_1^3 + x_2^3) \subset \mathbb{P}^2$ and $H = Z(x_0) \subset \mathbb{P}^2$.

Exercise 10.6. Compute the divisor $X \cdot H$ for $X = Z(x_0 x_2^2 - x_1^3 + x_0^3) \subset \mathbb{P}^2$ and $H = Z(x_0) \subset \mathbb{P}^2$.

If $f : X \to Y$ is a non-constant morphism of non-singular projective curves one can define a morphism of abelian groups $f^* : Div(Y) \to Div(X)$ as follows. Let $Q \in Y$. Then set

$$f^*Q = \sum_{f(P)=Q} v_P(f^* t_Q) P$$

and extend this definition by linearity. Here $f^* : \mathcal{O}_Q \to \mathcal{O}_P$ is induced by f.

For X a non-singular projective curve define the group homomorphism $div : K(X)^\times \to Div(X)$,

$$div(f) := \sum_{P \in X} v_P(f) P.$$

We have $Ker(div) = k^\times$. Set $P(X) = Im(div)$ and $Cl(X) = Div(X)/P(X)$. The elements of $P(X)$ are called principal divisors. The group $Cl(X)$ is called the divisor class group. For $D \in Cl(X)$ we denote by $cl(D)$ the class of D in $Cl(X)$. For $D_1, D_2 \in Div(X)$ we write $D_1 \sim D_2$ if $D_1 - D_2 \in P(X)$ and we say D_1 and D_2 are linearly equivalent.

Exercise 10.7. For $f : X \to Y$ a non-constant morphism of non-singular projective curves and all $g \in Div(Y)$ we have

$$f^*(div(g)) = div(f^*(g)).$$

As a consequence we have an induced homomorphism $f^* : Cl(Y) \to Cl(X)$.

Proposition 10.8. *For $X \subset \mathbb{P}^n$ a nonsingular curve and H_1, H_2 two hypersurfaces of the same degree, not containing X we have $X \cdot H_1 \sim X \cdot H_2$.*

Proof. One checks that if $H_i = Z(F_i)$ then $X \cdot H_1 - X \cdot H_2 = div((F_1/F_2)_{|X})$. $\square$

Proposition 10.9. *For $f : X \to Y$ a non-constant morphism of non-singular projective curves and all $D \in Div(Y)$ we have*

$$\deg(f^*D) = (\deg f)(\deg D).$$

Proof. We may assume D is one point Q and we need to show that

$$\deg(f^*Q) = \deg(f).$$

We may replace X, Y by affine curves with a finite morphism f between them. Let $A = \mathcal{O}(Y)$ and $B = \mathcal{O}(X)$ and $f^{-1}(Q) = \{P_1, ..., P_r\}$. Let $\mathfrak{m} \subset A$ and $\mathfrak{n}_i \subset B$ be the maximal ideals corresponding to Q and P_i. Let t_Q and t_{P_i} be parameters at the corresponding points. Let $v_{P_i}(t_Q) = e_i$ so $f^*Q = \sum_i e_i P_i$. Then the inclusion $\mathfrak{m}B \subset \mathfrak{n}_1^{e_1} ... \mathfrak{n}_r^{e_r}$ is an equality because it is an equality after localization at every maximal ideal of B. Since $A_\mathfrak{m}$ is a DVR hence principal it follows that $B_\mathfrak{m} := (A \setminus \mathfrak{m})^{-1} B$ is a free $A_\mathfrak{m}$-module and its rank is clearly equal to the degree $\deg(f)$. Hence $B_\mathfrak{m}/\mathfrak{m}B_\mathfrak{m}$ is a free $k = A_\mathfrak{m}/\mathfrak{m}$-vector space of dimension equal to the degree $\deg(f)$. Also we have

$$B/\mathfrak{n}_i^{e_i} = B_{\mathfrak{n}_i}/\mathfrak{n}_i^{e_i} B_{\mathfrak{n}_i} = \mathcal{O}_{P_i}/(t_{P_i}^{e_i}).$$

Using the Chinese Remainder Theorem and Lemma 2.36 we have

$$\begin{aligned}\deg(f) &= \dim_k(B_{\mathfrak{m}}/\mathfrak{m}B_{\mathfrak{m}}) \\ &= \dim_k(B/\mathfrak{m}B) \\ &= \dim_k(\textstyle\prod_i B/\mathfrak{n}_i^{e_i}) \\ &= \textstyle\sum_i e_i \\ &= \deg(f^*Q).\end{aligned}$$

□

Proposition 10.10. *If X is a non-singular projective curve and $D_1 \sim D_2$ are two linearly equivalent divisors. The* $\deg(D_1) = \deg(D_2)$.

Hence we have an induced homomorphism $\deg : Cl(X) \to \mathbb{Z}$. We denote by $Cl^0(X)$ the kernel of this homomorphism. This group is referred to as the group of divisor classes of degree 0.

Proof. Let $D_1 - D_2 = div(g)$. View g as a rational map $g : X \cdots \to k = \mathbb{A}^1$. By Theorem 9.5 g extends to a morphism $g : X \to \mathbb{P}^1$ and one checks that

$$div(g) = g^*(0 - \infty)$$

By Proposition 10.9 we get

$$\deg(div(g)) = (\deg g)(\deg(0 - \infty)) = 0.$$

□

By Propositions 10.8 and 10.10 we get

Corollary 10.11. *For $X \subset \mathbb{P}^n$ a nonsingular curve and H_1, H_2 two hypersurfaces of the same degree, not containing X we have* $\deg(X \cdot H_1) = \deg(X \cdot H_2)$.

Definition 10.12. For $X \subset \mathbb{P}^n$ a nonsingular curve define the *degree* of X in $\mathbb{P}^n$ as

$$\deg(X) = \deg(X \cdot H)$$

where H is any hyperplane not containing X. (The definition is correct due to Corollary 10.11 and coincides with the usual definition of degree of a curve in the plane due to Exercise 10.4.)

Note that if two curves in two projective spaces are isomorphic their respective degrees are not necessarily equal.

Exercise 10.13. Give an example when this happens. Hint: Think of a line and a quadric.

Theorem 10.14. *(Bezout) For $X \subset \mathbb{P}^n$ a nonsingular curve of degree d_1 and H hypersurface of degree d_2 not containing X we have*

$$\deg(X \cdot H) = d_1 d_2.$$

Proof. If H' is a union of d_2 distinct hyperplanes H_i we have $X \cdot H \sim X \cdot H'$ so the degrees of the two divisors are equal. But one can check using the definitions that

$$\deg(X \cdot H') = \sum \deg(X \cdot H_i)$$

which concludes the proof. □

Exercise 10.15. Let $f : \mathbb{P}^1 \to \mathbb{P}^{n+1}$ be the Veronese embedding given by all the monomials of degree n in 2 variables. Find the degree of $f(\mathbb{P}^1) \subset \mathbb{P}^n$.

Theorem 10.16. *The following are equivalent for a non-singular projective curve:*
1) $X \simeq \mathbb{P}^1$.
2) $X \sim \mathbb{P}^1$.
3) $Cl^0(X) = 0$.
4) For all points P and Q in X we have $P \sim Q$.
5) There exist two distinct points P and Q in X such that $P \sim Q$.

If the above hold we say X is rational.

Proof. 1 is equivalent to 2 by Theorem 9.9. 2 implies 3 imples 4 implies 5 are trivial. Assume 5. Let $P - Q = div(f)$ and view f as a morphism $X \to \mathbb{P}^1$. It is sufficient to show $\deg(f) = 1$; cf. Theorem 9.9. But

$$1 = \deg f^*0 = (\deg(f))(\deg 0) = \deg(f).$$

□

11. Plane curves

Let $F \in k[x_0, x_1, x_2]$ be irreducible, homogeneous, of degree d; call $X = Z(F) \subset \mathbb{P}^2$ a (projective) irreducible plane curve of degree d. By a plane curve of degree d we mean the union of distinct irreducible curves whose degrees sum up to d. Lines are curves of degree 1. Conics are curves of degree 2; so they are either irreducible or unions of 2 lines. Cubics are curves of degree 3; so they are either irreducible or unions of an irreducible conic and a line or unions of 3 lines.

If P, Q are two distinct points in the projective plane we usually denote by L_{PQ} the unique line that passes through P and Q.

Recall a point P on an irreducible curve X is called non-singular if $\mathcal{O}_P$ is a DVR, equivalently $\dim_k \mathfrak{m}_P/\mathfrak{m}_P^2 = 1$. If this is so let t_P be a parameter of $\mathcal{O}_P$ i.e., a generator of $\mathfrak{m}_P$. Call $Sing(X)$ the set of singular points of X.

Exercise 11.1.
1) Prove the following formula of Euler for a homogeneous polynomial F of degree d:

$$d \cdot F = x_0 \frac{\partial F}{\partial x_0} + x_1 \frac{\partial F}{\partial x_1} + x_2 \frac{\partial F}{\partial x_2}$$

2) Prove that

$$Sing(X) = Z(F, \frac{\partial F}{\partial x_0}, \frac{\partial F}{\partial x_1}, \frac{\partial F}{\partial x_2}).$$

So if the degree of F is not divisible by the characteristic of k then

$$Sing(X) = Z(\frac{\partial F}{\partial x_0}, \frac{\partial F}{\partial x_1}, \frac{\partial F}{\partial x_2}).$$

In particular a conic is irreducible if and only if it is non-singular.

Let $PGL_{n+1}(k) = GL_{n+1}(k)/\text{Center}$. This group acts on $\mathbb{P}^n$ by linear transformations. Two curves X and Y in $\mathbb{P}^n$ are called projectively equivalent if there is a $\sigma \in PGL_{n+1}(k)$ such that $\sigma(X) = Y$; two such curves are then isomorphic as varieties.

Exercise 11.2. The automorphism group of $\mathbb{P}^1$ is $PGL_2(k)$.

One can show that the automorphism group of $\mathbb{P}^n$ is $PGL_{n+1}(k)$. We will not need this.

Exercise 11.3. Prove that:

1) Every two lines in $\mathbb{P}^2$ are projectively equivalent.

2) Every two non-singular conics in $\mathbb{P}^2$ are projectively equivalent (Sylvester's Theorem).

3) Every non-singular conic is isomorphic to a line but not projectively equivalent to a line.

Definition 11.4. For a plane curve $X \subset \mathbb{P}^2$ and $P \in X \setminus Sing(X)$ the *(projective) tangent line* to X at P is the line

$$\overline{T_P X} := Z\left(\frac{\partial F}{\partial x_0}(P)x_0 + \frac{\partial F}{\partial x_1}(P)x_1 + \frac{\partial F}{\partial x_2}(P)x_2\right) \subset \mathbb{P}^2$$

(Then $\overline{T_P X}$ passes through P by Euler's formula!) A line in $\mathbb{P}^2$ is *tangent* to X at P if it is the tangent line to X at P.

Exercise 11.5.

1) For $i = 0, 1, 2$, upon identifying $\mathbb{P}^2 \setminus Z(x_i) \simeq \mathbb{A}^2$ we have

$$\overline{T_P X} \cap \mathbb{A}^2 = T_P(X \cap \mathbb{A}^2)$$

for $P \in X \cap \mathbb{A}^2$. Equivalently, the Zariski closure of $T_P(X \cap \mathbb{A}^2)$ in $\mathbb{P}^2$ is $\overline{T_P X}$.

2) A line L in $\mathbb{P}^2$ is tangent to X at a non-singular point $P \in X$ if and only if $(X \cdot L)_P \geq 2$.

Exercise 11.6. Let k have characteristic $\neq 2, 3$ and let $a, b \in k$ with $4a^3 + 27b^2 \neq 0$. The cubic

$$E_{a,b} := Z(x_0 x_2^2 - x_1^3 - a x_0^2 x_1 - b x_0^3) \subset \mathbb{P}^2$$

is non-singular. Hint: Set $\varphi(x) = x^3 + ax + b$ and use the fact that $4a^3 + 27b^2$ is in the ideal $(\varphi, d\varphi/dx) \subset k[x]$; to check the latter use the Euclid division algorithm to compute the gcd of φ and $d\varphi/dx$.

Proposition 11.7. *The cubic $E_{a,b}$ is not rational.*

Proof. Assume the cubic is rational. Then the cubic minus its intersection with $Z(x_0)$ is easily seen to be isomorophic to $\mathbb{P}^1$ minus a finite set. The latter has a ring of regular functions which is factorial (UFD). So it is enough to show that the ring

$$A := \frac{k[x, y]}{(y^2 - x^3 - ax - b)}$$

is not factorial. This is an easy exercise in algebra; one can use the natural norm map $N : A \to k[x]$ induced by the norm $N : Frac(A) \to k(x)$ in the corresponding field extension. $\square$

Theorem 11.8. *Consider the cubic $X = E_{a,b}$ and a point $P_0 \in X$. Then the map*

$$X \to Cl^0(X), \quad P \mapsto cl(P - P_0)$$

is a bijection.

Proof. The map is injective because if not we would get $P \sim Q$ for two distinct P, Q in X. By Theorem 10.16 X would be rational which contradicts Proposition 11.7. To prove surjectivity we proceed in several steps.

Step 1. Given $P, Q \in X$ there exists $S \in X$ such that $P + Q \sim P_0 + S$.

Indeed let L_{PQ} be either the line through P and Q (if they are distinct) or the tangent line to X at P (if $P = Q$) and write

$$X \cdot L_{PQ} = P + Q + R$$

Similarly let L_{P_0R} be the line through P_0 and R or the tangent respectively and write

$$X \cdot L_{P_0R} = P_0 + R + S.$$

We conclude by the fact that $X \cdot L_{PQ} \sim X \cdot L_{P_0R}$.

Step 2. For every divisor $D \geq 0$ there exist $k \geq 0$ and $P \in X$ such that $D \sim kP_0 + P$.

This follows from Step 1 by induction

Step 3. For every divisor D with $\deg(D) = 0$ there exist $P, Q \in X$ such that $D \sim P - Q$.

This follows directly from Step 2.

Step 4. For every $P, Q \in X$ there exists $R \in X$ such that $P - Q \sim R - P_0$.

This follows from Step 1 applied to P, P_0, Q in place of P, Q, P_0.

The Theorem follows now from Steps 3 and 4. $\square$

Remark 11.9. It is useful to draw pictures illustrating Steps 1 and 4.

By an algebraic group we mean a variety G which is also a group such that the multiplication map $G \times G \to G$ and the inverse map $G \to G$ are regular maps.

Exercise 11.10. Check that the following are algebraic groups:
1) $\mathbb{A}^1$ with the addition.
2) $\mathbb{G}_m := \mathbb{A}^1 \setminus \{0\}$ with multiplication.
3) $GL_n := GL_n(k)$ with multiplication of matrices.

Theorem 11.11. *Consider on the cubic $X = E_{a,b}$ the group structure induced from that on $Cl^0(X)$ via the bijection $X \to Cl^0(X)$ in Theorem 11.8, where $\{P_0\} = E_{a,b} \cap Z(x_0)$. Then X is an algebraic group.*

Proof. One computes the group law using 'analytic geometry' and one discovers that the formulae giving addition and inversion on X are regular functions. See Exercise 11.12 below for details. $\square$

A deep theorem in algebraic geometry, generalizing Theorem 11.11, states that for every non-singular projective curve X and every point $P_0 \in X$ there exists a projective variety $Jac(X)$ (unique up to isomorphism, called the Jacobian of X) and a bijection $\sigma : Cl^0(X) \simeq Jac(X)$ such that $Jac(X)$ equipped with the group structure induced from $Cl^0(X)$ via σ is an algebraic group and such that the composition of σ with the map of sets

$$X \to Cl^0(X), \quad P \mapsto cl(P - P_0)$$

is a morphism of varieties

$$\alpha := \alpha_{P_0} : X \to Jac(X).$$

The morphism α is called the Abel-Jacobi map. If k is complex field the map α is related to the theory of 'Abelian integrals' due to Abel, Riemann, and Jacobi. The above will not be discussed in this course.

Going back to the context of Theorem 11.11, in order to avoid confusion between addition in the group $Div(X)$ and addition in the group X we denote by $P[+]Q \in X$ the result of the addition of the points $P, Q \in X$ in the group structure of X and by $P + Q \in Div(X)$ the result of the addition of the points P and Q in the group $Div(X)$. Therefore we have

$$P[+]Q = S \quad \Leftrightarrow \quad P - P_0 + Q - P_0 \sim S - P_0 \quad \Leftrightarrow \quad P + Q \sim S + P_0.$$

We claim that to find S one lets R to be the third point of intersection of L_{PQ} with X, i.e.,

$$X \cdot L_{PQ} = P + Q + R$$

and then S will be the third point of intersection of L_{P_0S} with X, i.e.

$$X \cdot L_{P_0R} = P_0 + R + S;$$

for from the last 2 equations one gets

$$P + Q + R \sim P_0 + R + S$$

from which one gets

$$P + Q \sim P_0 + S.$$

Exercise 11.12. Let $\mathbb{A}^2 = \mathbb{P}^2 \setminus Z(x_0)$ and for every $x_1, y_1 \in k$ let us call $(x_1, -y_1)$ the symmetric of (x_1, y_1) with respect to the x-axis. Let $X = E_{a,b}$ and let

$$U := X \cap \mathbb{A}^2 = Z(y^2 - (x^3 + ax + b))$$

and let $P_1[+]P_2 = S$ for points $P_1, P_2 \in U$.

1) If P_1 and P_2 are symmetric with respect to the x-axis then $S = P_0$. Hint: show that $X \cdot L_{P_1P_2} = P_1 + P_2 + P_0$ and $X \cdot L_{P_0P_0} = 3P_0$.

2) Assume P_1 and P_2 are not symmetric with respect to the x-axis. Let L_{12} be the line through P_1 and P_2 (or the tangent line at P_1 if $P_1 = P_2$) and let P_3 be the third point of intersection of L_{12} with X. Then $P_1[+]P_2$ is the symmetric of P_3 with respect to the x-axis. Hint: this follows directly from 1).

3) For the situation in 2) find the affine coordinates of $P_1[+]P_2$ above as regular functions of the coordinates of P_1 and P_2. (This plus a similar computation in $\mathbb{P}^2 \setminus Z(x_1)$ and $\mathbb{P}^2 \setminus Z(x_2)$ proves Theorem 11.11.)

Here is a hint (essentially a solution) for Part 3. By Part 2, for $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in U$ with $(x_2, y_2) \neq (x_1, -y_1)$, we have

$$(x_1, y_1)[+](x_2, y_2) = (x_3, -y_3)$$

where $P_3 = (x_3, y_3)$ is the third point of intersection of E with the line L_{12} passing through (x_1, y_1) and (x_2, y_2) (or tangent to at P_1 if $P_1 = P_2$). If $(x_1, y_1) \neq (x_2, y_2)$ then L_{12} is by definition the set

$$L_{12} = Z(y - y_1 - m(x - x_1))$$

where

$$m = (y_2 - y_1)(x_2 - x_1)^{-1}.$$

If $(x_1, y_1) = (x_2, y_2)$ then $y_1 \neq 0$ and one needs to replace m in the above definition of L_{12} by the 'slope of the tangent'

$$m = (3x_1^2 + a)(2y_1)^{-1}.$$

We find (x_3, y_3) by solving the system consisting of the equations defining U and L_{12}: replacing y in $y^2 = x^3 + ax + b$ by $y_1 + m(x - x_1)$ we get a cubic equation in x:

$$(y_1 + m(x - x_1))^2 = x^3 + ax + b$$

which can be rewritten as

$$x^3 - m^2x^2 + ... = 0.$$

But x_1, x_2 are known to be roots of this equation. So x_3 is the third root hence

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = y_1 + m(x_3 - x_1).$$

The expressions of x_3 and y_3 are rational functions of x_1, y_1, x_2, y_2. They are in fact regular functions. To check this it is enough to check m is a regular function of these coordinates. But the rational function m is regular at every point (x_1, y_1, x_2, y_2) for which $y_1 \neq -y_2$ (and its value is given by the expression of m as a slope of a tangent if $x_1 = x_2$) because

$$\begin{aligned} m &= \tfrac{y_1 - y_2}{x_1 - x_2} \\ &= \tfrac{y_1^2 - y_2^2}{(x_1 - x_2)(y_1 + y_2)} \\ &= \tfrac{x_1^3 + ax_1 + b - x_2^3 - ax_2 - b}{(x_1 - x_2)(y_1 + y_2)} \\ &= \tfrac{x_1^2 + x_1x_2 + x_2^2 + a}{y_1 + y_2}. \end{aligned}$$

Exercise 11.13. Use the Three Cubics Theorem to give an alternative proof of the associativity of the chord-tangent operation on a cubic.

Hint: Let E be the elliptic curve and Q, P, R points on it different from P_0. Let

$$L_{PQ} \cap E = \{P, Q, U\}$$
$$L_{P_0U} \cap E = \{P_0, U, V\}$$
$$L_{VR} \cap E = \{V, R, W\}$$
$$L_{PR} \cap E = \{P, R, X\}$$
$$L_{P_0X} \cap E = \{P_0, X, Y\}.$$

Note that

$$Q[+]P = V, \quad V[+]R = W', \quad P[+]R = Y.$$

We want to show that

$$(Q[+]P)[+]R = Q[+](P[+]R).$$

This is equivalent to

$$V[+]R = Q[+]Y$$

i.e., that

$$W' = Q[+]Y$$

i.e., that Q, Y, W are collinear. Now the two cubics

$$E \quad \text{and} \quad L_{PQ} \cup L_{WR} \cup L_{YX}$$

both pass through the 9 points

$$P, Q, R, U, V, W, X, Y, P_0.$$

On the other hand the cubic

$$\Gamma = L_{UV} \cup L_{PR} \cup L_{QY}$$

passes through all 9 points except W. By the Three Cubics Theorem we get that Γ passes through W hence L_{QY} passes through W. The above argument only applies when one avoids the corresponding "degeneracies," e.g., tangencies or cases where 4 of the 8 points in question (the 9 points above except W) lie on a line or 7 of the points in question lie on a conic. To conclude that associativity holds in the "degenerate" cases as well one needs to use the fact that two morphisms of algebraic varieties that coincide on an open set must coincide.

12. Space curves

Generalizing the case $n = 2$, the projective tangent space $\overline{T_P X} \subset \mathbb{P}^n$ to a closed subvariety $X \subset \mathbb{P}^n$ at a point $P \in X$ is defined as follows. If $I(X) = (F_1, ..., F_m)$ then one defines the linear subspace

$$\overline{T_P X} = Z(L_P(F_1), ..., L_P(F_m)) \subset \mathbb{P}^n,$$

where

$$L_P(F_j) := \sum_{i=1}^{n} \frac{\partial F_j}{\partial x_i}(P) \cdot x_i, \quad j = 1, ..., m.$$

As in Exercise 11.5, upon identifying $\mathbb{P}^n \setminus Z(x_i) \simeq \mathbb{A}^n$, we have

$$\overline{T_P X} \cap \mathbb{A}^n = T_P(X \cap \mathbb{A}^n)$$

for all $P \in X \cap \mathbb{A}^n$. Equivalently, the Zariski closure of $T_P(X \cap \mathbb{A}^n)$ in $\mathbb{P}^n$ is $\overline{T_P X}$.

In particular if X is a non-singular curve then $\overline{T_P X}$ is a line in $\mathbb{P}^n$.

Proposition 12.1. *Let $X \subset \mathbb{P}^n$ be a non-singular projective curve and $O \in X$. By Theorem 9.5 the projection $\pi : X \setminus \{O\} \to \mathbb{P}^{n-1}$ extends to a morphism $\pi : X \to \mathbb{P}^{n-1}$. Say $O = (1 : 0 : ...0)$, $\pi(a_0 : ... : a_n) = (a_1 : ... : a_n)$ and identify $\mathbb{P}^{n-1}$ with $Z(x_0)$. Then $\pi(O)$ is the unique intersection of $Z(x_0)$ with the tangent line $\overline{T_O X}$.*

Proof. For simplicity we give the proof only in case $n = 2$; the general case is proved similarly. Let $U := X \setminus Z(x_0) = Z(f) \subset \mathbb{A}^2$ with $f \in k[x, y]$ irreducible ($x = y_1, y = y_2$). The morphism $\pi : X \setminus \{O\} \to \mathbb{P}^1$ induces an algebra homomophisms

$$k[x_1/x_2] \to (k[x, y]/(f))_y, \quad x_1/x_2 \mapsto x/y,$$

$$k[x_2/x_1] \to (k[x, y]/(f))_x, \quad x_2/x_1 \mapsto y/x.$$

Since $A = (k[x,y]/(f))_{(x,y)}$ is a DVR either x/y or y/x is in A. Assume $x/y \in A$ and write $x = gy$ with $g \in A$. Also write $f = \alpha x + \beta y + h$ with $\alpha, \beta \in k$ and $h \in (x,y)^2$. Hence $T_O X = Z(\alpha x + \beta y)$ and therefore $\overline{T_O X} = Z(\alpha x_1 + \beta x_2)$ so

$$\overline{T_O X} \cap Z(x_0) = \{(0 : -\beta : \alpha)\}.$$

We have $x/y \in (k[x,y]/(f))_s$ for some $s \in k[x,y] \setminus (x,y)$. The ring homomorphism

$$k[x_1/x_2] \to (k[x,y]/(f))_s, \quad x_1/x_2 \mapsto g$$

induces a morphism

$$\pi' : U \setminus Z(s) \to \mathbb{A}^1 \subset \mathbb{P}^1$$

which extends the projection π. We claim $\alpha \neq 0$ and $\pi'(O) = -\beta/\alpha$; this easily implies the conclusion of the Proposition. To check the claim note that, denoting by hats the classes of polynomials in A we have

$$0 = \widehat{f} = \alpha\widehat{x} + \beta\widehat{y} + \widehat{h} = \widehat{y}(\alpha\widehat{g} + \widehat{\beta}) + \widehat{h}.$$

We have $v_O(\widehat{h}) \geq 2$ and $v_O(\widehat{y}) = 1$ which implies $v_O(\alpha\widehat{g} + \widehat{\beta}) \geq 1$, hence $\alpha \neq 0$ and $g(0,0) = -\beta/\alpha$. This ends the proof of the claim. □

Proposition 12.2. *Let $\pi : \mathbb{P}^n \setminus \{O\} \to \mathbb{P}^{n-1}$ be the projection from a point O. Let $X \subset \mathbb{P}^n$ be a non-singular curve not passing through O and let $P \in X$. Then the tangent map $T_P\pi : T_P X \to T_P \mathbb{P}^{n-1}$ is injective if and only if the projective tangent line $\overline{T_P X}$ does not pass through O.*

Proof. A local computation with flavor similar to that of the proof of Proposition 12.1. □

Remark 12.3. It is useful to draw a picture illustrating the above Proposition.

Proposition 12.4. *Let $f : X \to Y$ be a finite morphism of varieties which is injective and such that for all $P \in X$ the tangent map $T_P f : T_P X \to T_{f(P)} Y$ is injective. Then f is an embedding (by which we mean induces an isomorphism $X \to f(X)$).*

Proof. One may assume Y (and hence X) is affine. Let $A = \mathcal{O}(Y)$ and $B = \mathcal{O}(X)$. It is enough to check that $A \to B$ is surjective. It is then enough to show that for every maximal ideal $\mathfrak{m}$ of A the map $A_\mathfrak{m} \to B_\mathfrak{m}$ is surjective. The maximal ideals of $B_\mathfrak{m}$ are in bijection with the points in X lying above the point in Y corresponding to $\mathfrak{m}$. So $B_\mathfrak{m}$ has only one maximal ideal (it is local with maximal ideal M) and finite over $A_\mathfrak{m}$. Since the map $\mathfrak{m}/\mathfrak{m}^2 \to M/M^2$ is surjective it follows by Nakayama's Lemma for the $B_\mathfrak{m}$-module M that $\mathfrak{m}B_\mathfrak{m} = M$. Again by Nakayama's Lemma for the $A_\mathfrak{m}$-module $B_\mathfrak{m}$ since 1 generates the $A_\mathfrak{m}$-module $k = B_\mathfrak{m}/M = B_\mathfrak{m}/\mathfrak{m}B_\mathfrak{m}$ it follows that 1 generates the $A_\mathfrak{m}$-module $B_\mathfrak{m}$ and we are done. □.

Corollary 12.5. *If X is a non-singular projective curve then X is isomorphic to a curve in $\mathbb{P}^3$.*

Proof. Start with $X \subset \mathbb{P}^n$ with $n \geq 4$. One can show that the closure S of the union of all lines passing through at least 2 points of X has dimension at most 3. Similarly the closure T of the union of all projective tangent lines at points of X has dimension at most 2. So there is a point $O \in \mathbb{P}^n$ not on S or T. By Propositions 12.2 and 12.4 the projection from O induces an isomorphism between X and a curve in $\mathbb{P}^{n-1}$. We conclude by induction. □

Remark 12.6. Not all non-singular projective curves are isomorphic to curves in $\mathbb{P}^2$ i.e., to plane curves!

Proposition 12.7. *Let $X \subset \mathbb{P}^n$ be a non-singular projective curve and let $\pi : X \to Y = f(X) \subset \mathbb{P}^{n-1}$ be the projection from a point outside X. Assume Y is non-singular. Prove that*

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

Proof. One may assume $P = (1 : 0 : \ldots : 0)$. By Proposition 10.9 it is enough to show that if $H = Z(x_0) \subset \mathbb{P}^{n-1}$ and $\mathcal{H} = Z(x_0) \subset \mathbb{P}^n$ then $f^*(Y \cdot H) = \mathcal{H} \cdot X$. This can be checked by directly using the definitions. □

13. Differentials

Let A be a ring, B an A-algebra, and M a B-module.

Definition 13.1. An A-*derivation* from B to M is an A-module homomorphism $d : B \to M$, $b \mapsto db$, satisfying the Leibniz rule:

$$d(b_1 b_2) = b_1 db_2 + b_2 db_1, \quad b_1, b_2 \in B.$$

Denote by $Der_A(B, M)$ the B-module of A-derivations from B to M.

Definition 13.2. Let B' be a set equipped with a bijection $B \to B'$, $b \mapsto b'$. The B-module $\Omega_{B/A}$ (called the module of *Kähler differentials*) is the module E/F where E is the free B-module generated by the set B' and F is the B-submodule generated by elements of E of the form

$$(b_1 + b_2)' - b_1' - b_2', \quad (b_1 b_2)' - b_1 b_2' - b_2 b_1' \quad \text{and} \quad a',$$

where $b_1, b_2 \in B$, $a \in A$.

Then we have an A-derivation $d : B \to \Omega_{B/A}$,

$$b \mapsto db := b' + F$$

We have the following universal property:

Proposition 13.3. *The map*

$$Hom_B(\Omega_{B/A}, M) \to Der_A(B, M), \quad f \mapsto f \circ d$$

is an isomorphism.

Proof. Left to the reader. □

Remark 13.4. For ring homomorphisms $A \to B \to C$ we have a naturally induced B-module homomorphism

$$\Omega_{B/A} \to \Omega_{C/A}.$$

Exercise 13.5. For S a multiplicative subset in B we have

$$\Omega_{S^{-1}B/A} \simeq S^{-1}\Omega_{B/A}.$$

Hint: use the universal property of Ω in Proposition 13.3.

Exercise 13.6. $\Omega_{A[x_1,\ldots,x_n]/A}$ is a free $A[x_1, \ldots, x_n]$-module with basis $dx_1, \ldots, dx_n$. Hint: use the universal property of Ω in Proposition 13.3

Exercise 13.7. If $A \to B \to C$ are ring homomorphisms then there is a natural exact sequence of C-modules

$$\Omega_{B/A} \otimes_B C \to \Omega_{C/A} \to \Omega_{C/B} \to 0$$

Hint: use the universal property of Ω.

Proposition 13.8. *If I is an ideal in B and $C = B/I$ then we have a natural exact sequence*

$$I/I^2 \xrightarrow{d} \Omega_{B/A} \otimes_B C \to \Omega_{C/A} \to 0.$$

Proof. Recall $\Omega_{B/A} \otimes_B C = \frac{\Omega_{B/A}}{I\Omega_{B/A}}$. Then one proves that the module

$$\frac{\Omega_{B/A}}{dI + I\Omega_{B/A}}$$

has the same universal property as $\Omega_{C/A}$. □

Proposition 13.9. *Let K be a finitely generated extension of an algebraically closed field k with separable transcendence basis $x_1, ..., x_n$ (i.e., K is separable over $L := k(x_1, ..., x_n)$). Then $dx_1, ..., dx_n$ is a basis of the K-vector space $\Omega_{K/k}$.*

Proof. By the Theorem of the Primitive Element

$$K = L[x]/(f)$$

for some polynomial f. Then use the previous Proposition and Exercises plus the fact that $df = f'(x)dx$ where f' is the usual derivative of f. □

Proposition 13.10. *Let X be a variety, $P \in X$, and $\mathfrak{m}_P$ the maximal ideal of $\mathcal{O}_P$. Then the map*

$$\frac{\mathfrak{m}_P}{\mathfrak{m}_P^2} \to \frac{\Omega_{\mathcal{O}_P/k}}{\mathfrak{m}_P\Omega_{\mathcal{O}_P/k}}$$

is an isomorphism. So we have an induced isomorphism

$$T_P X := \left(\frac{\mathfrak{m}_P}{\mathfrak{m}_P^2}\right)^\circ = Hom_k\left(\frac{\mathfrak{m}_P}{\mathfrak{m}_P^2}, k\right) \simeq Der_{\mathcal{O}_P}(\mathcal{O}_P, k).$$

Proof. By Proposition 13.8 this map is surjective. To prove injectivity it is enough to prove that the dual map

$$Hom_k(\frac{\Omega_{\mathcal{O}_P/k}}{\mathfrak{m}_P\Omega_{\mathcal{O}_P/k}}, k) \to Hom_k(\frac{\mathfrak{m}_P}{\mathfrak{m}_P^2}, k)$$

is surjective. But

$$Hom_k(\frac{\Omega_{\mathcal{O}_P/k}}{\mathfrak{m}_P\Omega_{\mathcal{O}_P/k}}, k) = Hom_{\mathcal{O}_P}(\Omega_{\mathcal{O}_P/k}, k) = Der_{\mathcal{O}_P}(\mathcal{O}_P.k)$$

So we have to show that every k-linear map $\varphi : \frac{\mathfrak{m}_P}{\mathfrak{m}_P^2} \to k$ comes from a derivation $D : \mathcal{O}_P \to k$. Define

$$Df = \varphi(f - f(P) + \mathfrak{m}_P^2);$$

one checks that D is a derivation and we are done. □

Lemma 13.11. *Let A be a Noetherian local integral domain with maximal ideal $\mathfrak{m}$ and fraction field K and M a finitely generated A-module. Let $S = A \setminus \{0\}$. Assume*

$$\dim_k(M/\mathfrak{m}M) = \dim_K(S^{-1}M) = r.$$

Then M is free of rank r.

Proof. By Nakayama M is generated by r elements. So there is an exact sequence

$$0 \to R \to A^r \to M \to 0$$

We get an exact sequence

$$0 \to S^{-1}R \to K^r \to S^{-1}M \to 0$$

So $S^{-1}R = 0$. Since R is torsion free we get $R = 0$. □

Definition 13.12. Let X be an affine variety and $P \in X$. Set $\Omega(X) := \Omega_{\mathcal{O}(X)/k}$ and

$$\Omega_{X,P} = \Omega_P := \Omega_{\mathcal{O}_P/k} = \Omega(X)_{\mathfrak{m}(P)}.$$

Call $\Omega(X)$ the module of (regular) *Kähler differentials* on X.

Proposition 13.13. *Let X be a non-singular curve and $P \in X$. Then $\Omega_{X,P} = \mathcal{O}_P dt_P$ i.e. this $\mathcal{O}_P$-module is free with basis dt_P, (where t_P is any generator of $\mathfrak{m}_P$).*

Proof. By Proposition 13.10

$$\dim_k \left(\frac{\Omega_{\mathcal{O}_P/k}}{\mathfrak{m}_P \Omega_{\mathcal{O}_P/k}} \right) = 1.$$

By Proposition 13.9, for $K = K(X)$ and $S = \mathcal{O}_P \setminus \{0\}$ we have

$$\dim_K (S^{-1}\Omega_{\mathcal{O}_P/k}) = 1.$$

We conclude by Lemma 13.11 plus Nakayama. □

In particular, in the notation of the above Proposition we have a derivation

$$\mathcal{O}_P \to \mathcal{O}_P, \quad f \mapsto \frac{df}{dt_P},$$

defined by the formula

$$df = \frac{df}{dt_P} dt_P, \quad f \in \mathcal{O}_P.$$

Corollary 13.14. *Let X be an affine non-singular curve. Then $\Omega(X)$ is a torsion free $\mathcal{O}(X)$-module (hence it is contained in $S^{-1}\Omega(X) = \Omega_{K(X)/k}$, $S = \mathcal{O}(X) \setminus \{0\}$) and*

$$\Omega(X) = \bigcap_P \Omega_{X,P}.$$

Definition 13.15. Let X be a non-singular curve (not necessarily affine). Set

$$\Omega(X) = \{\omega \in \Omega_{K(X)/k} \mid \omega \in \Omega_{X,P} \ \ \forall P \in X\}.$$

For X affine this definition coincides with the previous one due to the above Corollary.

Remark 13.16. For every non-constant morphism of projective curves $f : X \to Y$ we have naturally induced injective homomorphisms

$$f^* : \Omega(Y) \to \Omega(X),$$

$$f^* : \Omega_{Y,f(P)} \to \Omega_{X,P},$$

$$f^* : \Omega_{K(Y)/k} \to \Omega_{K(X)/k}.$$

14. Canonical class

Definition 14.1. Let X be a non-singular curve and $0 \neq \omega \in \Omega_{K(X)/k}$. Define the *divisor of* ω,

$$div(\omega) = \sum_P v_P(\omega) P \in Div(X)$$

where if $\omega = f_P dt_P$ then

$$v_P(\omega) := v_P(f_P).$$

This definition is correct because if $t = t_P = us$ for $u \in \mathcal{O}_P^\times$, $\mathfrak{m}_P = (s)$, then writing $du = hds$, $f = f_P$, we get

$$\omega = fdt = f(uds + sdu) = f(uds + shds) = (u + sh)fds$$

But $v_P(u + sh) = 0$ which shows the correctness of the definition.

Lemma 14.2.
1) $div(f\omega) = div(f) + div(\omega)$ for $f \in K(X)^\times$, $0 \neq \omega \in \Omega_{K(X)/k}$.
2) $div(\omega) \geq 0$ for $\omega \in \Omega(X)$.
3) For every $\omega, \omega' \in \Omega_{K(X)/k} \setminus \{0\}$ we have $div(\omega) \sim div(\omega')$.

Proof. 1 and 2 are clear. 3 follows from 1 because $\dim_K \Omega_{K(X)/k} = 1$. □

Definition 14.3. Let X be a projective non-singular curve. The *canonical class* of X is, by definition, $\kappa_X := cl(div(\omega)) \in Cl(X)$ where ω is any non-zero element of $\Omega_{K(X)/k}$; the definition is correct by assertion 3 in the Lemma above. Every divisor of the form $K_X = cl(div(\omega)) \in Div(X)$ is called a *canonical divisor*.

Example 14.4. Let $X = \mathbb{P}^1$ with coordinates x_0, x_1. Set $y = x_1/x_0$ and $\omega = dy$. Let $z = x_0/x_1 = y^{-1}$. So

$$dy = -\frac{1}{z^2}dz$$

Hence if $\infty = (0:1) \in \mathbb{P}^1$ we have

$$K_{\mathbb{P}^1} := div(\omega) = -2 \cdot \infty$$

is a canonical divisor.

Exercise 14.5. For $X = Z(f) \subset \mathbb{A}^2$, $A = k[x,y]/(f)$, f irreducible. Then:

1) The class of $x_P \in \mathcal{O}_P$ of $x - x(P)$ is a parameter on X at every point $P \in X \setminus Z(\partial f/\partial y)$. Similarly the class $y_P \in \mathcal{O}_P$ of $y - y(P)$ is a parameter on X at every point $P \in X \setminus Z(\partial f/\partial x)$. Hint: use Exercise 2.35.

2) Show that

$$\omega_{f,x} := \frac{dx}{\partial f/\partial y} \in \Omega(X \setminus Z(\partial f/\partial y)), \quad \omega_{f,y} := -\frac{dy}{\partial f/\partial x} \in \Omega(X \setminus Z(\partial f/\partial yx).$$

Also show that $\omega_{f,x}$ and $\omega_{f,y}$ are equal when viewed as elements of $\Omega_{K(X)/k}$ so they define an element $\omega_f \in \Omega(X)$.

3) We have $\mathcal{O}_P\omega_f = \Omega_{X,P}$ for all $P \in X$ so $\Omega(X)$ is a free $\mathcal{O}(X)$-module with basis ω_f. Hint: use Proposition 13.13.

Proposition 14.6. *Let $X = Z(F) \subset \mathbb{P}^2$ be a non-singular curve of degree d and let $H := X \cdot L$ where L is a line. Then*

$$K_X := (d-3)H$$

is a canonical divisor.

Proof. Let $U_i = \mathbb{P}^2 \setminus Z(x_i)$, $y_1 = x_1/x_0$, $y_2 = x_2/x_0$, $f(y_1, y_2) = F(1, y_1, y_2)$, and

$$\omega_f = \frac{dy_1}{\partial f/\partial y_2} = -\frac{dy_2}{\partial f/\partial y_1} \in \Omega(X \cap U_0).$$

So ω_f has 'no poles' in U_0. Set now $z_0 = x_0/x_1 = 1/y_1$, $z_2 = x_2/x_1 = y_2/y_1$, $g(z_0, z_2) = F(z_0, 1, z_2)$. We have

$$\frac{\partial f}{\partial y_2} = \frac{\partial F}{\partial x_2}(1, y_1, y_2)$$

and (by homogeneity of $\frac{\partial F}{\partial x_2}$)

$$\frac{\partial g}{\partial z_2} = \frac{\partial F}{\partial x_2}(z_0, 1, z_2) = \frac{\partial F}{\partial x_2}(1/y_1, 1, y_2/y_1) = \frac{1}{y_1^{d-1}} \frac{\partial F}{\partial x_2}(1, y_1, y_2) = z_0^{d-1} \frac{\partial f}{\partial y_2}$$

Now

$$dy_1 = -\frac{1}{z_0^2} dz_0$$

so we get

$$\omega_f = \frac{dy_1}{\partial f/\partial y_2} = -z_0^{d-3} \frac{dz_0}{\partial g/\partial z_2} = -z_0^{d-3} \omega_g$$

so

$$div(\omega_f) = (d-3)H \in Cl(X).$$

□

Exercise 14.7.
1) For X a non-singular curve in $\mathbb{P}^2$ of degree d we have $\deg(K_X) = d(d-3)$.
2) Non-singular curves in $\mathbb{P}^2$ of unequal degrees ≥ 3 cannot be isomorphic.

15. Statement of Riemann-Roch

Definition 15.1. Let X be a non-singular projective curve and D a divisor. Define

$$L(D) := \{f \in K(X)^\times \mid D + div(f) \geq 0\} \cup \{0\}.$$

So if $D = \sum n_P P$ then

$$L(D) := \{f \in K(X)^\times \mid v_P(f) \geq -n_P, \quad \forall P\} \cup \{0\}.$$

Exercise 15.2. $L(D)$ is a k-linear subspace of $K(X)$.

Definition 15.3. Set

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

(which will be shown later it is finite) and define

$$|D| := \{E \in Div(X) \mid E \sim D, \ E \geq 0\}.$$

The latter is called the *complete linear system* attached to D.

Proposition 15.4. *If $D_1 \sim D_2$ then $\ell(D_1) = \ell(D_2)$.*

Proof. If $D_1 = D_2 + div(g)$ then multiplication by g gives an isomorphism $L(D_1) \to L(D_2)$. □

Proposition 15.5. *There is natural bijection*

$$|D| \simeq \frac{L(D) \setminus \{0\}}{\sim}$$

where

$$f \sim g \Leftrightarrow \exists \lambda \in k^\times, g = \lambda f.$$

Proof. The map $L(D) \to |D|$, $f \mapsto D + div(f)$ (for $f \neq 0$) and $0 \mapsto D$ is clearly surjective. The fiber of this map above the image of f are all $g \in K(X)^\times$ such that $div(f/g) = 0$. We conclude by the fact that $\mathcal{O}(X) = k$. □

Proposition 15.6. *For all D we have $\ell(D) < \infty$. So $|D| \simeq \mathbb{P}^{\ell(D)-1}$.*

Proof. We may assume $D = \sum n_P P \geq 0$. Consider the 'diagonal map'

$$L(D) \to \bigoplus_{P \in X} \frac{t_P^{-n_P}\mathcal{O}_P}{\mathcal{O}_P} \simeq \bigoplus_{P \in X} \frac{\mathcal{O}_P}{t_P^{n_P}\mathcal{O}_P}$$

The kernel of this map is k because $\mathcal{O}(X) = k$. □

Remark 15.7. The above argument shows that $\ell(D) \leq \deg(D) + 1$; this can be shown, by a variation of the argument, to hold for D not necessarily ≥ 0.

Exercise 15.8.
1) If $\deg(D) < 0$ then $\ell(D) = 0$ hence $|D| = \emptyset$.
2) If $\deg(D) = 0$ and $\ell(D) \geq 1$ then $D \sim 0$.

Definition 15.9. For X a non-singular projective curve define its *genus* as

$$g(X) := \dim_k \Omega(X).$$

Exercise 15.10. If $K_X = div(\omega)$ is a canonical divisor then the map $L(K_X) \to \Omega(X)$, $f \mapsto f\omega$ is an isomorphism. In particular the genus satisfies

$$g(X) = \ell(K_X) < \infty.$$

Here is the main result about curves.

Theorem 15.11. *(Riemann-Roch Theorem) Let X be a non-singular projective curve of genus $g(X) = g$, let $D \in Div(X)$, and let $K = K_X$ be a canonical divisor. Then the following holds:*

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

We postpone the proof and present first some applications; this will not lead to any circularity. The applications will be presented in the rest of this section plus the next 3 sections. The proof of Riemann-Roch will be presented after that. The proof will need: sheaves, cohomology, adeles, and residue theory. We will first introduce sheaves and cohomology. Then we will introduce adeles as a tool to understanding cohomology and we will prove a Cohomological (version of) Riemann-Roch (Theorem 21.6). Next we will introduce and study residues. With their help we will prove the so-called Serre Duality Theorem; the latter plus the Cohomological Riemann-Roch will imply the Riemann-Roch Theorem.

Exercise 15.12.
1) $\deg(K) = 2g - 2$. Hint: take $D = K$ in Riemann-Roch.
2) If $\deg(D) \geq g$ then $|D| \neq \emptyset$.
3) If $\deg(D) \geq 2g - 1$ then $\ell(K - D) = 0$ hence $\ell(D) = \deg(D) + 1 - g$.

Corollary 15.13. *We have $g(X) = 0$ if and only if $X \simeq \mathbb{P}^1$.*

Proof. The if part follows because by Example 14.4 $\deg(K_{\mathbb{P}^1}) = -2$. For the only if part take $P, Q \in X$ distinct and set $D = P - Q$. We have $\deg(K_X) = 2g - 2 = -2$ so $\deg(K - D) = -2 < 0$ so $\ell(K - D) = 0$. Then by Riemann-Roch $\ell(D) = 1$. Since $\deg(D) = 0$, by Exercise 15.8 above $D \sim 0$. We conclude by Theorem 10.16. □

Corollary 15.14. *We have $g(X) = 1$ if and only if $K_X \sim 0$.*

Proof. The if part is trivial. For the only if part we know $\ell(K_X) = 1$ and $\deg(K_X) = 2g - 2 = 0$. We conclude by Exercise 15.8.

Corollary 15.15. *For X a non-singular curve in $\mathbb{P}^2$ of degree d the genus g of X is given by the formula*

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

Proof. This follows from Exercise 14.7 and Exercise 15.12, Part 1. $\square$

So plane curves cannot gave arbitrary genus.

16. Linear systems

Definition 16.1. A *linear system* is a linear subspace Λ of a projective space of the form $|D|$ for some D. It is called *complete* if it is the whole of $|D|$. Since Λ itself is a projective space it has a well defined dimension $\dim \Lambda$. Clearly $\dim |D| = \ell(D) - 1$. We define the *base locus*

$$Bs(\Lambda) = \{P \in X \mid P \in Supp(E) \ \ \forall E \in \Lambda\}.$$

Say Λ is *base point free* if $Bs(\Lambda) = \emptyset$.

Exercise 16.2.
1) Show that if X is isomorphic to $\mathbb{P}^1$ and $P \in X$ then $|P|$ is base point free.
2) Show that if X is not isomorphic to $\mathbb{P}^1$ and $P \in X$ then $Bs(|P|) = \{P\}$.
3) Show that if $X \subset \mathbb{P}^n$ and H is a hypersurface then $X \cdot H$ is base point free.

Proposition 16.3. *Let D be a divisor and P a point. Then*

$$\ell(D) \geq \ell(D - P) \geq \ell(D) - 1$$

We have $P \in Bs(|D|)$ if and only if $\ell(D) = \ell(D - P)$. In particular (by Riemann-Roch) if $\deg(D) \geq 2g$ then $|D|$ is base point free.

Proof Let $D = \sum n_P P$. Then we conclude by considering the exact sequence

$$0 \to L(D - P) \to L(D) \to \frac{t_P^{-n_P} \mathcal{O}_P}{t_P^{-n_P+1} \mathcal{O}_P} \simeq \frac{\mathcal{O}_P}{t_P \mathcal{O}_P} \simeq k.$$

$\square$

Definition 16.4. Let X be a non-singular projective curve and $f : X \to \mathbb{P}^n$ be a morphism. We say f is *non-degenerate* if $f(X)$ is not contained in any hyperplane. Assume this is the case. Then for every hyperplane $H = Z(L) \subset \mathbb{P}^n$ one defines $f^*H \in Div(X)$ by

$$f^*H = \sum_{P \in X} (f^*H)_P P$$

where for each P, if $P \notin Z(x_i)$, we set

$$(f^*H)_P = v_P(f^*(L/x_i)).$$

So if f is an inclusion then $f^*H = X \cdot H$. We denote by $|H|$ the set of hyperplanes in $\mathbb{P}^n$; it is the dual projective space $\check{\mathbb{P}}^n$.

Exercise 16.5. For every two hyperplanes H_1, H_2 we have $f^*H_1 \sim f^*H_2$.

So we have a map $f^* : |H| \to |f^*H|$ whose image $f^*|H|$ is a (not necessarily complete) base point free linear system. So $f^*|H| \subset |f^*H|$.

Definition 16.6. Two morphisms from X to $\mathbb{P}^n$ are called *projectively equivalent* if the two morphisms differ by an automorphism $\sigma \in PGL_{n+1}$ of $\mathbb{P}^n$.

Proposition 16.7. *If X is a non-singular projective curve there is a natural bijection between the set of projective equivalence classes of non-degenerate morphisms $X \to \mathbb{P}^n$ and the set of base point free linear systems on X of dimension n.*

Proof. Given $f : X \to \mathbb{P}^n$ we constructed a base point free linear systems $f^*|H|$ on X of dimension n. (The dimension is n because if $H = Z(L)$ we have a linear map from the space of linear forms L' in $n+1$ variables to $L(f^*H)$ defined by $L' \mapsto (L'/L)_{|X}$. This map is injective by non-degeneracy so it induces an inclusion $|H| \to |f^*H|$.) Conversely if $\Lambda \subset |D|$ is free with $\Lambda = \mathbb{P}(V) = (V \setminus \{0\})/\sim$, $V \subset L(D)$, and $D = \sum n_R R$, pick a basis $f_0, ..., f_n \in V$ and define $f : X \to \mathbb{P}^n$ around each point Q by the formula

$$f(P) = (f_0(P)t_Q^{n_Q} : ... : f_n(P)t_Q^{n_Q}).$$

One checks the two constructions are inverse to each other. □

Remark 16.8. A 'synthetic description' of the bijection above is as follows. Given Λ its associated $f = f_\Lambda$ is the map from X to the dual projective space

$$\check{\Lambda} := \{\text{hyperplanes in } \Lambda\}$$

of the projective space Λ,

$$f_\Lambda : X \to \check{\Lambda},$$

with $f(P) = \Lambda_P$ where Λ_P is the hyperplane in Λ defined by

$$\Lambda_P = \{D \in \Lambda \mid P \in Supp(D)\}.$$

If $f_1 : X \to \mathbb{P}^{n_1}$ and $f_2 : X \to \mathbb{P}^{n_2}$ correspond to Λ_1 and Λ_2 then $\Lambda_1 \subset \Lambda_2$ if and only if f_1 if the composition of f_2 with a projection $\mathbb{P}^{n_2} ... \to \mathbb{P}^{n_1}$. In particular if f_1 is linearly normal there is no non-degenerate f_2 (with $n_2 > n_1$) such that f_1 is obtained from f_2 via a projection $\mathbb{P}^{n_2} ... \to \mathbb{P}^{n_1}$.

Definition 16.9.
1) A linear system Λ is said to *separate points* if for every distinct $P, Q \in X$ there exists $D = \sum n_R R \in \Lambda$ such that $P \in Supp(D)$ (i.e., $n_P \neq 0$) and $Q \notin Supp(D)$ (i.e., $n_Q = 0$). Any such Λ is, of course, base point free.
2) A linear system Λ is said to *separate tangent vectors* if for every $P \in X$ there exists $D = \sum n_R R \in \Lambda$ such that $n_P = 1$.

Proposition 16.10. *If Λ separates points and tangent vectors then $f_\Lambda : X \to \check{\Lambda}$ is an embedding.*

Proof. The condition of separating points is equivalent to f_Λ being injective (in view of the synthetic description of f_Λ). We claim that the condition of separating tangent vectors is equivalent to the condition that the tangent map $T_P f_\Lambda$ is injective. Indeed the latter is equivalent to the condition that the map

$$\frac{\mathfrak{m}_{f(P)}}{\mathfrak{m}_{f(P)}^2} \to \frac{\mathfrak{m}_P}{\mathfrak{m}_P^2}$$

is surjective, equivalently non-zero. But the latter map is zero if and only if for every hyperplane H passing through $f(P)$ we have $(f^*H)_P \geq 2$. This proves our Claim. We conclude by Proposition 12.4. $\square$

Definition 16.11. A divisor D is called *very ample* if $f_{|D|}$ is an embedding.

Exercise 16.12. Assume D is a divisor such that for every $P, Q \in X$ we have

$$\ell(D - P - Q) = \ell(D) - 2.$$

Then D separates points and tangent vectors. Hint: use Proposition 16.3.

Corollary 16.13. *If X had genus g and $\deg(D) \geq 2g+1$ then D is very ample.*

Proof. By Riemann-Roch we have $\ell(D-P-Q) = \ell(D) - 2$ for every $P, Q \in X$. We conclude by Proposition 16.10 and Exercise 16.12. $\square$

Corollary 16.14. *For every $P \in X$ the curve $X \setminus \{P\}$ is affine.*

Proof. Let $n \geq 2g+1$. Then nP is very ample. So $f := f_{|nP|} : X \to \mathbb{P}^{\dim |nP|}$ is an embedding. Now $nP = f^*H$ for some hyperplane H. Hence $X \setminus \{P\} = f^{-1}(\mathbb{P}^n \setminus H)$. Hence $X \setminus \{P\}$ is isomorphic to a closed subvariety of the affine space $\mathbb{A}^n \simeq \mathbb{P}^n \setminus H$. $\square$

17. Hurwitz Theorem

Definition 17.1. Let $f : X \to Y$ be a non-constant morphism of non-singular projective curves. For every $P \in X$ and $Q = f(P)$ with $\mathfrak{m}_Q = (t_Q)$ define the ramification index at P to be

$$e_P := v_P(f^*t_Q) \in \mathbb{N}.$$

In other words

$$f^*Q = \sum_{f(P)=Q} e_P P.$$

We say P is *unramified* if $e_P = 1$. We say that f is unramified if $e_P = 1$ for all $P \in X$. We say P is *ramified* (or f is ramified at P) if $e_P \geq 2$. We say P is *tamely ramified* if it is ramified and e_P is not divisible by the characteristic of the field k. We say that f is tamely ramified if all ramification points are tamely ramified. In characteristic zero tame ramification is automatic. We say that f is separable if the induced homomorphism $f^* : K(Y) \to K(X)$ is separable.

Theorem 17.2. *(Hurwitz) If f is separable and K_X, K_Y are canonical divisors on X, Y respectively then the set of ramified points is finite and*

$$K_X \sim f^*K_Y + \sum_{P \in X} (e_P - 1)P + W.$$

with W a divisor satisfying $W \geq 0$. Moreover $W = 0$ if and only if f is tamely ramified.

Proof. By separability we have an injective map

$$f^* : \Omega_{K(Y)/k} \to \Omega_{K(X)/k}.$$

Let $\omega \in \Omega_{K(Y)/k}$. For all $Q \in Y$ write $\omega = u_Q t_Q^{n_Q} dt_Q$ with $u_Q \in \mathcal{O}_Q^{\times}$. So

$$K_Y \sim div(\omega) = \sum_{Q \in Y} n_Q Q.$$

Hence

$$f^*K_Y \sim \sum_{Q\in Y} n_Q f^*Q = \sum_{Q\in Y}\sum_{f(P)=Q} n_Q e_P P.$$

Now write $f^*t_Q = a_P t_P^{e_P}$ with $a_P \in \mathcal{O}_P^\times$ and set $da_P = b_P dt_P$. Also

$$\begin{aligned}
f^*\omega &= f^*(u_Q t_Q^{n_Q} dt_Q)\\
&= f^*u_Q \cdot (f^*t_Q)^{n_Q} \cdot f^*(dt_Q)\\
&= f^*u_Q \cdot a_P^{n_Q} t_P^{e_P n_Q} \cdot d(f^*t_Q)\\
&= f^*u_Q a_P^{n_Q} t_P^{e_P n_Q} \cdot d(a_P t_P^{e_P})\\
&= f^*u_Q a_P^{n_Q} t_P^{e_P n_Q} \cdot (a_P e_P t_P^{e_P-1} dt_P + t_P^{e_P} da_P)\\
&= f^*u_Q a_P^{n_Q} t_P^{e_P n_Q} \cdot (a_P e_P t_P^{e_P-1} + t_P^{e_P} b_P) dt_P.
\end{aligned}$$

Now since u_Q, a_P are invertible we have

$$v_P(f^*\omega) = v_P(f^*u_Q a_P^{n_Q} t_P^{e_P n_Q} \cdot (a_P e_P t_P^{e_P-1} + t_P^{e_P} b_P)) \geq e_P n_Q + e_P - 1$$

with equality if and only if e_P is not divisible by p. So, for some $W \geq 0$, we have

$$K_X \sim div(f^*\omega) = \sum_P (e_P n_Q + e_P - 1)P + W \sim f^*K_Y + \sum_P (e_P - 1)P + W.$$

□

Exercise 17.3. In the above theorem

$$2g(X) - 2 \geq (\deg f)(2g(Y) - 2) + \sum_{P\in X}(e_P - 1)$$

with equality if and only if f is tamely ramified. In particular $g(X) \geq g(Y)$. Hint: take degrees in Hurwitz's Theorem and use Exercise 15.12 and Proposition 10.9.

Exercise 17.4. (Lüroth's Theorem) If $X \to Y$ is separable and $X \simeq \mathbb{P}^1$ then $Y \simeq \mathbb{P}^1$.

Definition 17.5. An *elliptic curve* is a non-singular projective curve of genus 1.

Exercise 17.6. Every non-constant separable morphism of elliptic curves is unramified.

18. Elliptic curves

We next apply the theory above to elliptic curves. We assume from now on the characteristic of k is $\neq 2$.

Lemma 18.1. *If X is an elliptic curve and $P_1, P_2 \in X$ then:*

1) The linear system $|P_1 + P_2|$ is base point free of dimension 1 so it defines a morphism $f = f_{|P_1+P_2|} : X \to \mathbb{P}^1$ such that $P_1 + P_2 = f^*Q$ for some point $Q \in \mathbb{P}^1$.

2) There is an automorphism $\sigma : X \to X$ such that $\sigma(P_1) = P_2$.

3) f has exactly 4 ramification points R_1, R_2, R_3, R_4 on X and their images $Q_i = f(R_i)$ are 4 distinct points in $\mathbb{P}^1$

Proof. Part 1 follows from Riemann-Roch. Part 2 follows from the fact that the generator of the Galois group of the degree 2 extension $K(Y) \to K(X)$ acts on $f^{-1}(V)$ for each affine $V \subset Y$ transitively on the fibers; the latter is proved by an algebraic argument. Part 3 follows from Hurwitz. $\square$

Lemma 18.2. *Let X be an elliptic curve and $P_1, P_2 \in X$. Consider the morphisms $f_1 = f_{|2P_1|} : X \to \mathbb{P}^1$ and $f_2 = f_{|2P_2|} : X \to \mathbb{P}^1$. Then there exists a commutative diagram*

$$\begin{array}{ccc} X & \xrightarrow{\sigma} & X \\ f_1 \downarrow & & \downarrow f_2 \\ \mathbb{P}^1 & \xrightarrow{\tau} & \mathbb{P}^1 \end{array}$$

with σ and τ isomorphisms.

Proof. Take σ as in Lemma 18.1 and τ the induced automorphism. $\square$

Exercise 18.3. For every 3 distinct points $Q_1, Q_2, Q_3 \in \mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$ there exists an automorphism $\tau : \mathbb{P}^1 \to \mathbb{P}^1$ (hence $\tau \in PGL_2$) such that

$$\tau(Q_1) = 0, \quad \tau(Q_2) = 1, \quad \tau(Q_3) = \infty.$$

Define the rational function

$$j(x) = 2^8 \frac{(x^2 - x + 1)^3}{x^2(x-1)^2}.$$

The factor 2^8 is motivated by considerations that will not be touched upon.

Exercise 18.4. Let $\lambda, \lambda' \in k \setminus \{0, 1\}$. Prove that the following are equivalent:

1) There exists an automorphism $\tau : \mathbb{P}^1 \to \mathbb{P}^1$ that sends the set $\{0, 1, \infty\}$ onto itself and sends λ into λ'.

2) There exists an automorphism $\tau : \mathbb{P}^1 \to \mathbb{P}^1$ that sends the set $\{0, 1, \lambda, \infty\}$ onto the set $\{0, 1, \lambda', \infty\}$.

3) $\lambda' \in \{\lambda, 1-\lambda, \frac{1}{\lambda}, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\}$.

4) $j(\lambda) = j(\lambda')$.

Hint. 1 implies 2 implies 3 implies 4 are trivial/easy. To check 4 impples 1 consider the group G of automorphisms in 1 acting on the field $k(x)$ and show, using Galois theory that the field of invariants $k(x)^G$ equals $k(j(x))$. Then use the fact that G acts transitively on the fibers of the map $j : \mathbb{P}^1 \to \mathbb{P}^1$.

Definition 18.5. Let X be an elliptic curve. Define its *j-invariant* $j(X) \in k$ as follows. Let $P \in X$, consider the morphism $f_{|2P|} : X \to \mathbb{P}^1$, consider the images $Q_1, Q_2, Q_3, Q_4 \in \mathbb{P}^1$ of the 4 ramification points of $f_{|2P|}$ (cf. Lemma 18.1), let $\tau : \mathbb{P}^1 \to \mathbb{P}^1$ be an automorphism sending Q_1, Q_2, Q_3 into $0, 1, \infty$, respectively (cf. Exercise 18.3), let $\lambda = \tau(Q_4)$, and set

$$j(X) = j(\lambda)$$

By Lemma 18.2 and Exercise 18.4 $j(X)$ does not depend on P or τ.

Lemma 18.6. *For every elliptic curve X and every point $P \in X$ there is an embedding $f : X \to \mathbb{P}^2$ whose image is a cubic such that (viewing f and inclusion) we have $3P = X \cdot L$ for some line L.*

Proof. Take $f = f_{|3P|}$; by Riemann-Roch $|3P|$ has dimension 2 and f is an embedding by Corollary 16.13. Also we have $3P = f^*L$ for some L. $\square$

Theorem 18.7. *For every elliptic curve X and every point P there is an isomorphism of X to the projective closure E_φ in $\mathbb{P}^2$ of a curve $Z(y^2 - \varphi(x)) \subset \mathbb{A}^2$, where $\varphi(x) \in k[x]$ is a cubic polynomial with distinct roots, such that P is mapped to the point $E_\varphi \cap Z(x_0)$. Moreover:*

1) One can choose $\varphi(x) = x(x-1)(x-\lambda)$ (the Legendre form) in which case $j(X) = j(\lambda)$. We then write $E_\varphi = E_\lambda$.

2) If the characteristic if k is not 3 one can choose $\varphi(x)$ of the form $x^3 + ax + b$.

Proof. By the Lemma above $X \simeq E := Z(F) \subset \mathbb{P}^2$ with F a homogeneous cubic such that $E \cdot L = 3P$ for some line L. We may assume $L = Z(x_0)$. Since $E \cdot L = 3P$, F must have the form $F = x_0 Q + C$ where Q is a quadratic form in x_0, x_1, x_2 and C is a cubic form in x_1, x_2 whose zeroes in $\mathbb{P}^1$ coincide. Changing the variables x_1, x_2 we may assume $C = x_1^3$. Let $q(x, y) = Q(1, x_1, x_2)$. We claim that q has a y^2 term; indeed if not then (check!) the curve E is rational. Completing the terms that contain y^2 and y to a square we may change the variables such that $F(1, x, y) = y^2 - \varphi(x)$ for some cubic $\varphi(x)$. The cubic φ must have distinct roots (otherwise E is singular). Statements 2 and 3 are easy. □

Corollary 18.8.

1) For every $c \in k$ there is an elliptic curve X with $j(X) = c$.

2) Two elliptic curves X_1 and X_2 are isomorphic if and only if $j(X_1) = j(X_2)$.

3) For every elliptic curve X and every $P_0 \in X$ the map $X \to Cl^0(X)$ given by $P \mapsto cl(P - P_0)$ is a bijection and X with the group structure induced by the above bijection is an algebraic group.

Assertion 2 says that the set of isomorphism classes M_1 of elliptic curves is in bijection (given by j) with the set of points on the line $\mathbb{A}^1$.

Proof. For 1 the projective closure of the Legendre curve E_λ with parameter λ satisfying $j(\lambda) = c$ has j-invariant c. The only if part of 2 was already checked. For the if part, if $X_1 \simeq E_{\lambda_1}$ and $X_2 \simeq E_{\lambda_2}$ and $j(X_1) = j(X_2)$ then $j(\lambda_1) = j(\lambda_2)$ so by Exercise 18.4 there is an automorphism τ of $\mathbb{P}^1$ sending $\{0, 1, \lambda_1, \infty\}$ onto the set $\{0, 1, \lambda_2, \infty\}$. This isomorphism can be extended to an automorphism of $\mathbb{P}^2$ that sends E_{λ_1} onto E_{λ_2} (check!). Part 3 follows because every elliptic curve is isomorphic to a cubic $E_{a,b}$ and we already know Part 3 for $E_{a,b}$ at least if k has characteristic $\neq 2, 3$; cf. Theorem 11.11. In these remaining cases a similar argument can be given. □

Remark 18.9. A deep result in algebraic geometry says that the set of isomorphism classes M_g of non-singular projective curves of genus $g \geq 2$ is in a natural bijection with the set of points of a variety M_g of dimension $3g - 3$ (called the moduli space of curves of genus g).

19. Sheaves

Definition 19.1. Let X be a topological space. A *presheaf* $\mathcal{F}$ of abelian groups consists of the following data:

1) For every open set $U \subset X$ one is given an abelian group $\mathcal{F}(U)$;

2) For every open sets $V \subset U \subset X$ one is given a group homomorphism $\rho_{UV} : \mathcal{F}(U) \to \mathcal{F}(V)$;

satisfying the properties:

a) $\mathcal{F}(\emptyset) = 0$

b) For all U we have $\rho_{UU} = id$;
c) For all $W \subset V \subset U$ we have $\rho_{UV} \circ \rho_{VW} = \rho_{UW}$.

A similar definition is given where "abelian groups" are replaced by "vector spaces", "rings", etc.

The maps ρ_{UV} are called restriction maps and we write $\rho_{UV}(s) = s_{|V}$ for all $s \in \mathcal{F}(U)$. Also we set $H^0(U, \mathcal{F}) = \mathcal{F}(U)$.

Definition 19.2. A presheaf is called a *sheaf* if for every open set U and every open cover $U = \cup U_i$ the following conditions are satisfied:
c) For all $s \in \mathcal{F}(U)$ if $s_{|U_i} = 0$ for all i then $s = 0$;
d) If (s_i) is a family with $s_i \in \mathcal{F}(U_i)$ such that for all i, j we have

$$s_{i|U_i \cap U_j} = s_{j|U_i \cap U_j}$$

then there exists a (unique by c above) $s \in \mathcal{F}(U)$ such that $s_{|U_i} = s_i$ for all i.

Example 19.3.
1) Every sheaf of (k-valued) functions of a topological space is a sheaf of rings. So if X is a variety then $U \mapsto \mathcal{O}(U)$ is a sheaf $\mathcal{O} = \mathcal{O}_X$ of rings.
2) If X is a non-singular curve then $U \mapsto \Omega(U)$ is a sheaf Ω_X of k-vector spaces called the canonical sheaf. If $D = \sum n_P P$ is a divisor on X we define

$$\mathcal{O}(D)(U) := \{f \in K(X)^\times \mid v_P(f) \geq -n_P, \forall P \in U\} \cup \{0\};$$

$$\Omega(D)(U) := \{f \in \Omega_{K(X)/k} \setminus \{0\} \mid v_P(\omega) \geq -n_P, \forall P \in U\} \cup \{0\}.$$

Then $U \mapsto \mathcal{O}(D)(U)$ is a sheaf of k-vector spaces $\mathcal{O}(D) = \mathcal{O}_X(D)$ and $U \mapsto \Omega(D)(U)$ is a sheaf of k-vector spaces $\Omega(D) = \Omega_X(D)$. Hence,

$$H^0(X, \mathcal{O}) = \mathcal{O}(X), \quad H^0(X, \mathcal{O}(D)) = L(D),$$

$$H^0(X, \Omega) = \Omega(X), \qquad H^0(X, \Omega(D)) \simeq L(K + D).$$

Here K is any canonical divisor.

Definition 19.4. A presheaf $\mathcal{F}$ is called *constant* if there exists an abelian group A such that $\mathcal{F}(U) = A$ for all $U \neq \emptyset$; we write $\mathcal{F} = A$.

Exercise 19.5. A constant presheaf on an irreducible topological space X is a sheaf.

Definition 19.6. A morphism of presheaves $\mathcal{F} \to \mathcal{G}$ is a collection of morphisms $\mathcal{F}(U) \to \mathcal{G}(U)$ that are compatible in the obvious sense with the restriction maps.

Definition 19.7. For a presheaf $\mathcal{F}$ on X and for $P \in X$ we define the *stalk* of $\mathcal{F}$ at P,

$$\mathcal{F}_P := \{(U, s) \mid P \in U, \ s \in \mathcal{F}(U)\} / \sim,$$

where $(U, s) \sim (U', s')$ if there exists (U'', s'') with $P \in U'' \subset U \cap U'$ and $s''_{|U} = s$, $s''_{|U'} = s'$.

For $P \in U$ there is a natural map $\mathcal{F}(U) \to \mathcal{F}_P$ which we denote by $s \mapsto s_P$.

Example 19.8. For an variety the formerly defined $\mathcal{O}_P$ is the stalk of $\mathcal{O}$ at P. Similarly for $\Omega_{X,P}$.

Proposition 19.9. *For every presheaf $\mathcal{F}$ on X there exists a morphism of presheaves $\mathcal{F} \to \mathcal{F}^+$ such that $\mathcal{F}^+$ is a sheaf and such that every morphism of presheaves $\mathcal{F} \to \mathcal{G}$, where $\mathcal{G}$ is a sheaf, factors through a unique morphism of sheaves $\mathcal{F}^+ \to \mathcal{G}$. Moreover the induced maps between stalks $\mathcal{F}_P \to \mathcal{F}^+_P$ are isomorphisms. Finally if $\mathcal{F}$ is already a sheaf then $\mathcal{F} \to \mathcal{F}^+$ is an isomorphism.*

Proof. One defines $\mathcal{F}^+(U)$ to be the set of all families $(s_P)_{P \in U}$ with $s_P \in \mathcal{F}_P$ with the property that for every $P \in U$ there exists an open set $P \in V \subset U$ and there exists $t \in \mathcal{F}(V)$ such that $s_P = t_P$ for all $P \in V$. One then easily checks the rest of the properties. □

Definition 19.10. A *subsheaf* of a sheaf $\mathcal{F}$ is a sheaf $\mathcal{F}'$ such that $\mathcal{F}'(U) \subset \mathcal{F}(U)$ for all U. (Then $\mathcal{F}'_P \subset \mathcal{F}_P$ for all $P \in X$.) We define the *quotient sheaf* $\mathcal{F}/\mathcal{F}'$ as being

$$\mathcal{F}/\mathcal{F}' := \mathcal{G}^+$$

where $\mathcal{G}$ is the presheaf defined by

$$\mathcal{G}(U) = \mathcal{F}(U)/\mathcal{F}'(U).$$

Note that $(\mathcal{F}/\mathcal{F}')_P = \mathcal{F}_P/\mathcal{F}'_P$ for all P.

Exercise 19.11. Let $\mathcal{F}'$ be a subsheaf of a sheaf $\mathcal{F}$. Let $s \in \mathcal{F}(U)$ be such that $s_P \in \mathcal{F}'_P$ for all $P \in U$. Then $s \in \mathcal{F}'(U)$.

Definition 19.12. A sequence of sheaves

$$\mathcal{F}' \to \mathcal{F} \to \mathcal{F}''$$

is called *exact* if for all $P \in X$ the sequence

$$\mathcal{F}'_P \to \mathcal{F}_P \to \mathcal{F}''_P$$

is exact.

Note that for an exact sequence of sheaves as above it is NOT generally true that the sequences

$$\mathcal{F}'(U) \to \mathcal{F}(U) \to \mathcal{F}''(U)$$

are exact.

Remark 19.13. By the above Proposition for every subsheaf $\mathcal{F}' \subset \mathcal{F}$ the sequence

$$0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}/\mathcal{F}' \to 0$$

is exact.

Recall the notation $\mathcal{F}(U) = H^0(U, \mathcal{F})$.

Exercise 19.14. For every exact sequence of sheaves

$$0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$$

the induced sequences

$$0 \to H^0(U, \mathcal{F}') \to H^0(U, \mathcal{F}) \to H^0(U, \mathcal{F}'')$$

are exact.

Definition 19.15. Let A be an abelian group and $P \in X$ a closed point. We define the *skyscraper presheaf* A_P by setting $A_P(U) = U$ is $P \in U$ and $A_P = 0$ if $P \notin U$.

Exercise 19.16. Assume the points of X are closed. Prove that the skyscraper presheaves are sheaves. Prove that the stalk $(A_P)_Q$ of A_P at $Q \in X$ is A or 0 according as $P = Q$ or $P \neq Q$.

20. Cohomology

Definition 20.1. Let X be a topological space and $\mathcal{U}$ an open cover, i.e. a map

$$\mathcal{U} \to \{\text{open sets of } X\},$$

such that the open sets in the image of $\mathcal{U}$ cover X. For each $U \in \mathcal{U}$ we still denote by $U \subset X$ the open set which is the image of U; this is, of course, an abuse of notation, as the map above is not assumed to be injective so one should keep in mind this fact. Then for a sheaf $\mathcal{F}$ of groups (vector spaces, rings,...) we let $Z^1(\mathcal{U}, \mathcal{F})$ be the group of all families

$$(a_{UV}) \in \prod_{U,V} \mathcal{F}(U \cap V)$$

satisfying

$$a_{UU} = 0, \quad a_{UV} + a_{VU}, \quad a_{UV} + a_{VW} + a_{WU} = 0$$

for all $U, V, W \in \mathcal{U}$. Here, for simplicity, we continued to write a_{UV} for its restriction to $U \cap V$ in the second equality and we continued to write a_{UV} for its restriction to $U \cap V \cap W$ in the third equality. Also we let $B^1(\mathcal{U}, \mathcal{F}) \subset Z^1(\mathcal{U}, \mathcal{F})$ be the subgroup of all families as above for which there exists a family

$$(f_U) \in \prod_{U} \mathcal{F}(U)$$

such that

$$a_{UV} = f_U - f_V$$

for all U, V. Again, for simplicity we continued to write f_U, f_V for their restriction to $U \cap V$. Finally we set

$$H^1(\mathcal{U}, \mathcal{F}) = \frac{Z^1(\mathcal{U}, \mathcal{F})}{B^1(\mathcal{U}, \mathcal{F})}.$$

The groups Z^1, B^1, H^1 above are called the *group of Cech cocycles*, group of *Cech coboundaries*, and the *Cech cohomology group* with respect to $\mathcal{U}$, respectively. We say $\mathcal{V}$ is a *refinement* of $\mathcal{U}$ if there is a map $r : \mathcal{V} \to \mathcal{U}$ such that $r(V) \supset V$ for all V. Such a refinement induces a group homomorphism

$$H^1(\mathcal{U}, \mathcal{F}) \to H^1(\mathcal{V}, \mathcal{F})$$

and we set

$$H^1(X, \mathcal{F}) := \varinjlim_{\mathcal{U}} H^1(\mathcal{U}, \mathcal{F}).$$

Proposition 20.2. *For every exact sequence of sheaves of abelian groups*

$$0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$$

there is an induced 'long' exact sequence

$$0 \to H^0(X, \mathcal{F}') \to H^0(X, \mathcal{F}) \to H^0(X, \mathcal{F}'') \xrightarrow{\partial} H^1(X, \mathcal{F}') \to H^1(X, \mathcal{F}) \to H^1(X, \mathcal{F}'')$$

Proof. To define ∂ take an element $x'' \in H^0(X, \mathcal{F}'')$; it is represented by a family $(\widehat{t_V})$ where V is in a cover and $\widehat{t_V} \in \mathcal{F}(V)/\mathcal{F}'(V)$ is the class of some $t_V \in \mathcal{F}(V)$. Then by Exercise 19.11 the family

$$(t_U - t_V) \in \prod_{UV} \mathcal{F}(U \cap V)$$

belongs to

$$\prod_{UV} \mathcal{F}'(U \cap V);$$

the latter family defines an element $\partial(x'') \in H^1(X, \mathcal{F}')$. Checking exactness of the sequence is an easy exercise. □

Exercise 20.3. If $\mathcal{F}$ is a constant sheaf or a skyscraper sheaf on X then

$$H^1(X, \mathcal{F}) = 0.$$

Definition 20.4. Let $\mathcal{F}$ be a sheaf of k-vector spaces. If $H^i(X, \mathcal{F})$ are finite dimensional for $i = 0, 1$ we say that the *Euler characteristic* $\chi(X)$ of X is defined and equal to

$$\chi(X) = \dim H^0(X, \mathcal{F}) - \dim H^1(X, \mathcal{F}) \in \mathbb{Z}.$$

Exercise 20.5. Let

$$0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$$

be an exact sequence of sheaves of k-vector spaces where $\mathcal{F}''$ is either constant or a skyscraper. Then $\chi(\mathcal{F})$ is defined if and only if $\chi(\mathcal{F}')$ is defined and in this case we have

$$\chi(\mathcal{F}) = \chi(\mathcal{F}') + \chi(\mathcal{F}'').$$

Hint: Use the previous exercise and decompose the long exact sequence into short exact sequences.

21. Adeles

Definition 21.1. Let X be nonsingular projective curve. The *ring of adeles* is the ring R of all families $r = (r_P)_{P \in X}$, $r_P \in K(X)$, such that $r_P \in \mathcal{O}_P$ for all but finitely many $P \in X$. If $D = \sum n_P P$ is a divisor let

$$R(D) := \{r \in R \mid v_P(r_P) + n_P \geq 0\}$$

So

$$R = \bigcup_D R(D)$$

There is an injective 'diagonal' map $K(X) \to R$, $f \mapsto (f_P)$ with $f_P = f$ for all P.

Proposition 21.2. *For every divisor D one has a canonical isomorphism*

$$H^1(X, \mathcal{O}(D)) \simeq \frac{R}{R(D) + K(X)}.$$

Proof. Consider the exact sequence

$$0 \to \mathcal{O}(D) \to K(X) \to K(X)/\mathcal{O}(D) \to 0$$

Since $K(X)$ is constant its H^1 group is trivial so by the cohomology long exact sequence we get

$$H^1(X, \mathcal{O}(D)) \simeq \frac{H^0(X, K(X)/\mathcal{O}(D))}{Im(K(X))}$$

But one can check that the map

$$R \to H^0(X, K(X)/\mathcal{O}(D)), \quad (r_P) \mapsto (r_P + \mathcal{O}(D)_P),$$

where $r_P + \mathcal{O}(D)_P \in \frac{K(X)}{\mathcal{O}(D)_P}$ is the clas of r_P, is correctly defined (i.e., the latter family is a section) and induces an isomorphism

$$\frac{R}{K(X) + R(D)} \to \frac{H^0(X, K(X)/\mathcal{O}(D))}{Im(K(X))}.$$

□

Proposition 21.3. *If $D \geq E$ are divisors then*

$$\deg(D) - \deg(E) = \dim \frac{R(D) + K(X)}{R(E) + K(X)} + \ell(D) - \ell(E).$$

Proof. If $D = \sum n_P P$ and $E = \sum m_P P$ we have an exact sequence

$$0 \to \mathcal{O}(E) \to \mathcal{O}(D) \to A \to 0$$

where

$$A = \bigoplus \frac{t^{-n_P}\mathcal{O}_P}{t^{-m_P}\mathcal{O}_P}$$

hence

$$H^0(X, A) = k^{\ell(D) - \ell(E)}.$$

We conclude by taking the cohomology long exact sequence and using Proposition 21.2. □

Theorem 21.4. *Let X be a non-singular projective curve. Then $H^1(X, \mathcal{O})$ is finite dimensional. So $\chi(\mathcal{O})$ is defined.*

Proof. Let $y \in K(X)$, $y : X \to \mathbb{P}^1$, $\Delta := y^*\infty = \sum e_i P_i$ so $y \in L(\Delta)$. Let $\deg(\Delta) = d$. Let $z_1, ..., z_d$ be a basis of $K(X)/K(\mathbb{P}^1)$. There exists n_0 such that $z_1, ..., z_d \in L(n_0\Delta)$. Let $n >> n_0$. Then for $0 \leq s \leq n - n_0$ we have $y^s z_j \in L(n\Delta)$. Hence $\ell(n\Delta) \geq (n - n_0 + 1)d$. Set

$$N_n = \dim \frac{R(n\Delta) + K(X)}{R(0) + K(X)}.$$

By Proposition 21.3 we get

$$nd = N_n + \ell(n\Delta) - \ell(0) \geq N_n + (n - n_0 + 1)d - 1$$

hence

$$N_n \leq n_0 d - d + 1.$$

For every divisor D set $r(D) := \deg(D) - \ell(D)$; then $r(D)$ only depends on the linear equivalence class of D. Then for every $D \geq E$, by Proposition 21.3 we have

$$r(D) - r(E) = \dim \frac{R(D) + K(X)}{R(E) + K(X)} \tag{21.1}$$

Setting $D = n\Delta$, $E = 0$ we get that $r(n\Delta) = r(0) + N_n$ is bounded b ya constant C as $n \to \infty$. Let B be any divisor and take $z \in k[y]$ such that z has high order zeroes at all points of $Supp(B) \backslash Supp(\Delta)$. Then there exists n such that $div(z) + n\Delta \geq B$. So

$$-1 = r(0) \leq r(B) \leq r(div(z) + n\Delta) = r(n\Delta) \leq C$$

so the set

$$\{r(B) \mid B \in Div(X)\}$$

is bounded. (Lang says: 'the whole thing is of course pure magic'). By (21.1) with $D = B$, $E = 0$, it follows that the set

$$\{\dim \frac{R(B) + K(X)}{R(0) + K(X)} \mid B \in Div(X)\}$$

is bounded. Since

$$R = \bigcup_{B \in Div(X)} R(B)$$

we get that

$$\dim \frac{R}{R(0) + K(X)} < \infty$$

and we are done by Proposition 21.2. $\square$

Proposition 21.5. *Let X be a non-singular projective curve and D a divisor. Then $\chi(\mathcal{O}(D))$ is defined and*

$$\chi(\mathcal{O}(D)) = \deg(D) + \chi(\mathcal{O}).$$

Proof. It is enough to show that the above is true for D if and only if it is true for $D + P$ where P is a point. Consider the exact sequence

$$0 \to \mathcal{O}(D) \to \mathcal{O}(D + P) \to k_P \to 0.$$

This sequence is exact because if $D = \sum n_P P$ then $\mathcal{O}(D)_P = t_P^{-n_P} \mathcal{O}_P$ and similarly for $D + P$ so

$$\frac{\mathcal{O}(D + P)_P}{\mathcal{O}(D)_P} = \frac{t_P^{-n_P - 1} \mathcal{O}_P}{t_P^{-n_P} \mathcal{O}_P} \simeq \frac{\mathcal{O}_P}{t_P \mathcal{O}_P} \simeq k.$$

Then we have

$$\chi(\mathcal{O}(D + P)) = \chi(\mathcal{O}(D)) + 1$$

and the Proposition follows. $\square$

For every divisor D we set $i(D) = \dim H^1(X, \mathcal{O}(D))$. We conclude:

Theorem 21.6. *(Cohomological Riemann-Roch Theorem) For every divisor D we have*

$$\ell(D) - i(D) = \deg(D) + 1 - i(\mathcal{O})$$

where g is the genus of X.

Theorem 21.6 is our first step in proving the Riemann-Roch theorem. In order to deduce Riemann-Roch theorem from the cohomological Riemann-Roch above we will need the so-called Serre Duality Theorem. The proof of the latter needs residue theory. Residues are dealt with in the next section.

22. Residues

Definition 22.1. Let $\mathcal{O}$ be a DVR with maximal ideal $\mathfrak{m}$ and containing a field k. Assume $\mathcal{O}/\mathfrak{m} = k$. Consider the completion of $\mathcal{O}$,

$$\widehat{\mathcal{O}} = \varprojlim_{n} \mathcal{O}/\mathfrak{m}^n := \{(a_1, a_2, a_3, ...) \mid a_n \in \mathcal{O}/\mathfrak{m}^n,\ a_n \mapsto a_{n-1}\}.$$

Then $\widehat{\mathcal{O}}$ is a ring containing $\mathcal{O}$.

Proposition 22.2. *If $t \in \mathfrak{m}$ is a parameter (i.e., a generator) there is an isomorphism*
$$\widehat{\mathcal{O}} \simeq k[[t]]$$
sending t into t where $k[[t]]$ is the ring of formal power series in t. In particular $Frac(\mathcal{O}) \simeq k((t))$, the field of Laurent series. Moreover if $D : \mathcal{O} \to \mathcal{O}$ is a k-derivation with $Dt = 1$ then D extends uniquely to the 'usual' derivation d/dt on $k[[t]]$.

Proof. One checks by induction that the natural homomorphism $k[[t]]/(t^n) \to \mathcal{O}/\mathfrak{m}^n$ is an isomorphism for all n. Then one takes projective limits. The statement about the derivations follows by noting that D induces a linear map $\mathcal{O}/\mathfrak{m}^n \to \mathcal{O}/\mathfrak{m}^{n-1}$ and the induced map $k[[t]]/(t^n) \to k[[t]]/(t^{n-1})$ must send $t^i + (t^n)$ into $it^{i-1} + (t^{n-1})$ by the Leibniz rule. □

From now we view the isomorphism in the above Proposition as an equality.

We say $\mathcal{O}$ is complete if it is equal to $\widehat{\mathcal{O}}$.

Definition 22.3. Let $\mathcal{O}$ be complete with fraction field K. Define
$$\Omega'_{K/k} = K dt$$
to be the one dimensional K-vector space with basis dt where t is any parameter. We identify Kdt with Kds for every two parameters t and s by viewing $k((s)) = k((t))$, writing $s = \sum c_i t^i$ and identifying ds with $(\sum i c_i t^{i-1})dt$. (Note that $\Omega'_{K/k} \neq \Omega_{K/k}$ in general!) For
$$\omega = \sum_{i=-\infty}^{\infty} a_i t^i dt \in \Omega'_{K/k}$$
we set
$$res_t(\omega) = a_{-1}.$$

Exercise 22.4. The following hold:
1) The map $\Omega'_{K/k} \to k$, $\omega \mapsto res_t(\omega)$ is k-linear.
2) $res_t(\omega) = 0$ if $\omega \in \mathcal{O}dt$.
3) $res_t(df) = 0$ for $f \in K$.
4) $res_t(df/f) = v(f)$ for $f \in K^\times$ where $v : K^\times \to \mathbb{Z}$ is the valuation on K.

Proposition 22.5. *Let $\mathcal{O}$ be complete with fraction field K and let $t, s \in \mathcal{O}$ be two parameters. Then for all ω,*
$$res_t(\omega) = res_s(\omega).$$
So we set $res(\omega) = res_t(\omega)$ for every t.

Proof. We only the give the proof in characteristic zero; one can prove the characteristic p case by 'reduction to characteristic zero' (but we omit that). Write
$$\omega = \sum_{n \geq 1} a_n \frac{ds}{s^n} + \omega_0, \quad \omega_0 \in \mathcal{O}ds = \mathcal{O}dt.$$
So $res_s(\omega) = a_1$. Now by Exercise 22.4 we have
$$res_t(\omega) = \sum_{n \geq 1} a_n res_t\left(\frac{ds}{s^n}\right) = a_1 v(s) + res_t\left(d\left(-\sum_{n \geq 2} \frac{a_n}{(n-1)s^{n-1}}\right)\right) = a_1.$$
□

Definition 22.6. For P a point on a non-singular curve X we consider the composition:

$$res_P : \Omega_{K(X)/k} \to \Omega'_{K_P/k} \stackrel{res}{\to} k,$$

where K_P is the fraction field of $\widehat{\mathcal{O}_P}$.

Theorem 22.7. *(Residue formula). If X is a nonsingular projective curve then for all $\omega \in \Omega_{k(X)/k}$ we have*

$$\sum_{P \in X} res_P(\omega) = 0.$$

Sketch of proof. First one checks the above for $X = \mathbb{P}^1$ (see the Exercise below). Next consider $t \in K(X)$ such that $k(t) \subset K(X)$ is separable and consider the morphism $f : X \to \mathbb{P}^1$ defined by this field extension. The trace map

$$Tr : K(X) \to k(t), \quad Tr(g) = Tr(K(X) \to K(X),\ h \mapsto gh)$$

induces an intrinsic map

$$Tr : \Omega_{K(X)/k} = K(X)dt \to \Omega_{k(t)/t} = k(t)t, \quad Tr(gdt) = Tr(g)dt.$$

One then checks (by a local computation which we omit) that for every $Q \in \mathbb{P}^1$

$$\sum_{f(P)=Q} res_P(\omega) = res_Q(Tr(\omega)).$$

Taking $\sum_{Q \in \mathbb{P}^1}$ in the above equality we conclude by the $X = \mathbb{P}^1$ case of the theorem. $\square$

Exercise 22.8. Prove the residue formula in case $X = \mathbb{P}^1$. Hint: write $\omega = f(t)dt \in k(t)dt$ and write $f(t)$ as a polynomial plus sum of simple fractions $\frac{1}{(t-\lambda)^n}$. Then prove the residue formula by direct computation for monomials t^n and for simple fractions.

Exercise 22.9. Let $X = Z(f) \subset \mathbb{A}^2$ be non-singular, $A = k[x,y]/(y^2 - x^3 - x)$, $P = (0,0)$. Compute

$$res_P(dy/x) \ \text{ and, } \ res_P(dx/y), \ res_P(dx/x) \ \text{ and, } \ res_P(dy/y).$$

23. Proof of Riemann-Roch

We prove here the Serre Duality Theorem which, in combination with the Cohomological Riemann-Roch Theorem will prove the Riemann-Roch Theorem.

Definition 23.1. For a divisor D on X let

$$J(D) := \left(\frac{R}{R(D) + K(X)} \right)^{\circ}$$

Elements $\alpha \in J(D)$ will be identified with k-linear maps $\alpha : R \to k$ vanishing on $R(D) + K(X)$.

For $D' \geq D$ we have $R(D') \supset R(D)$ and $J(D') \subset J(D)$. Define

$$J = \bigcup_D J(D)$$

Note that J is a $K(X)$-linear space: for $\alpha \in J(D)$ and $f \in L(D')$ we define $f \cdot \alpha : R \to k$ by the formula

$$(f \cdot \alpha)(r) = \alpha(f \cdot r).$$

One checks that $f \cdot \alpha \in J(D - D')$.

Proposition 23.2. $\dim_{K(X)} J \leq 1$.

Proof. Assume $\alpha, \alpha' \in J$ are $K(X)$-linearly independent. Let $\alpha, \alpha' \in J(D)$, $\deg(D) = d$. Take any $P \in X$. The map

$$L(nP) \oplus L(nP) \to J(D - nP), \quad (f, g) \mapsto f \cdot \alpha + g \cdot \alpha'$$

is injective so

$$\dim J(D - nP) \geq 2\ell(nP).$$

We will make $n \to \infty$ and get a contradiction. By finite dimensionality we have

$$\begin{aligned} \dim J(D - nP) &= \dim H^1(X, \mathcal{O}(D - nP)) \\ &= \ell(D - nP) - \chi(\mathcal{O}(D - nP)) \\ &= \ell(D - nP) - \deg(D - nP) - \chi(\mathcal{O}) \\ &= \ell(D - nP) + n - d - \chi(\mathcal{O}) \\ &= n - d - \chi(\mathcal{O}) \quad \text{for } n > d \end{aligned} \tag{23.1}$$

On the other hand

$$\ell(nP) \geq \chi(\mathcal{O}(nP)) = \deg(nP) + \chi(\mathcal{O}) = n + \chi(\mathcal{O}).$$

Hence

$$\dim J(D - nP) \geq 2n + 2\chi(\mathcal{O}). \tag{23.2}$$

By (23.1) and (23.2) we get a contradiction. $\square$

Definition 23.3. Let $\langle\ ,\ \rangle : \Omega_{K(X)/k} \times R \to k$ be the map

$$\langle \omega, r \rangle := \sum_{P \in X} res_P(r_P \omega).$$

Exercise 23.4.
1) $\langle\ ,\ \rangle$ is k-bilinear.
2) $\langle \omega, r \rangle = 0$ for $r \in K(X)$.
3) $\langle \omega, r \rangle = 0$ for $\omega \in H^0(X, \Omega(-D))$ and $r \in R(D)$.
4) $\langle f \cdot \omega, r \rangle = \langle \omega, f \cdot r \rangle$ for $f \in K(X)$.

Let $\theta : \Omega_{K(X)/k} \to R^\circ$ be the map

$$\theta(\omega) = (r \mapsto \langle \omega, r \rangle).$$

By the above Exercise

$$\theta(H^0(X, \Omega(-D)) \subset J(D)$$

hence

$$Im(\theta) \subset J.$$

Lemma 23.5. *Let $\omega \in \Omega_{K(X)/k}$ be such that $\theta(\omega) \in J(D)$. Then $\omega \in H^0(X, \Omega(-D))$.*

Proof. Let $D = \sum n_P P$. Assume the conclusion is false so there exists $P \in X$ such that $v_P(\omega) - n_P \leq -1$. Set $n = v_P(\omega)$. Define $r \in R$ by letting $r_Q = 0$ for $Q \neq P$ and $r_P = t_P^{-n-1}$. Then $v_P(r_P\omega) = -1$ so $\langle \omega, r \rangle \neq 0$. Now $r \in R(D)$ because

$$v_P(r_P) + n_P = -n - 1 + n_P = -v_P(\omega) - 1 + n_P \geq 0.$$

We got a contradiction because $\theta(\omega)$ vanishes on $R(D)$. □

Proposition 23.6. *The map $\theta : \Omega_{K(X)/k} \to J$ is injective (hence an isomorphism because it is $K(X)$-linear, the source has dimension 1 and the target has dimension ≤ 1).*

Proof. Assume $\omega \in \Omega_{K(X)/k}$ is such that $\theta(\omega) = 0$. Then $\theta(\omega) = 0 \in J(D)$ for all D. By Lemma 23.5 above $\omega \in H^0(X, \Omega(-D))$ for all D. This forces $\omega = 0$. □

Corollary 23.7. *The map $\theta : H^0(X, \Omega(-D)) \to J(D)$ is a bijection.*

Proof. Injectivity follows from Proposition 23.6. Surjectivity follows from Proposition 23.6 plus Lemma 23.5. □

We are ready for:

Theorem 23.8. *(Serre Duality) Let X be a non-singular projective curve and D a divisor. Then*

$$H^1(X, \mathcal{O}(D)) \simeq H^0(X, \mathcal{O}(K - D))^\circ.$$

In particular

$$i(D) = \ell(K - D).$$

Proof. It follows from Corollary 23.7 and Proposition 21.2. □

Finally we can give:

Proof of the Riemann-Roch Theorem 15.11. It follows from the Serre Duality Theorem 23.8 plus the Cohomological Riemann-Roch Theorem 21.6. □