Algebraic Geometry

Bas Edixhoven, David Holmes and Lenny Taelman

August 2016

Contents

Preface

These are lecture notes for the course M1: Algebraic Geometry 1 offered in Mastermath in Fall 2016.

Students taking the course M1: Algebraic Geometry 1 are encouraged to also follow the course M1: Commutative Algebra, which is offered simultaneously in Mastermath. The present course M1: Algebraic Geometry 1 should provide sufficient background and motivation for the course M2: Algebraic Geometry 2, offered in Mastermath in Spring 2017.

The present lecture notes are based on the lecture notes of a Mastermath course in algebraic geometry given during the Spring of 2009 at the UvA by Bas Edixhoven and Lenny Taelman. Those notes were typed, as the course went on, by Michiel Kosters. Later versions incorporated additions, corrections and suggestions by Michiel Vermeulen, Remke Kloosterman, Ariyan Javanpeykar, Samuele Anni, Jan Rozendaal and Robin de Jong. David Holmes has written Lectures 9 and 10 which focus on aspects of algebraic geometry over the field of complex numbers. We thank all those who have contributed.

The reader will see that the present lecture notes do not give a systematic introduction to algebraic geometry. Instead, we have chosen a clear goal, namely André Weil's proof of the Riemann Hypothesis for curves over finite fields using intersection theory on surfaces. Our approach has the advantage that it gets somewhere, but also the disadvantage that there will be gaps in the exposition, that the reader will have to accept or fill. Nevertheless, we think that this text is a good introduction to algebraic geometry. A student who will not continue in this matter will have seen beautiful mathematics and learned useful material. A student who will continue in this area will be motivated for reading the tougher treatments (like [EGA] or the Stacks project [Stacks]), and will have a bigger chance of not getting stuck in technicalities.

This syllabus is divided into 14 lectures. First the theory of algebraic varieties over algebraically closed fields is developed, up to the Riemann-Roch theorem and Serre duality for curves. Lectures 9 and 10 deal with aspects of varieties when the base field is that of the complex numbers: now, also topological and analytical tools become available. Lectures 12–14 deal with varieties over finite fields (note however that finite fields are not algebraically closed!) and lead up to the promised proof of the Riemann hypothesis. We need one "black box": Hodge's Index Theorem. Lecture 11 treats intersection theory on surfaces. Lecture 12 introduces the notion of a variety over a finite field. Lecture 13 establishes the rationality and the functional equation of the zeta function of curves over finite fields. In Lecture 14 intersection theory on surfaces is used to prove the Riemann hypothesis for zeta functions for curves over finite fields. The Appendix is meant to provide more background and motivation on zeta functions.

The prerequisites for this course are the standard undergraduate algebra courses on groups, rings and fields (see for example the syllabi [Stev] (in Dutch), or [Lang]), and some basic topology.

No prior knowledge of algebraic geometry is necessary. We will occasionally refer to the basic textbook [Hart] on Algebraic Geometry. It is recommended to get hold of this book. The reader is also encouraged to compare this text with the other algebraic geometry syllabi [Moo] and [Looij].

Lecture 1

Affine space and its algebraic sets

In this lecture we will basically treat Section I.1 of [Hart], i.e. we discuss the most basic notions of algebraic geometry.

Let k be an algebraically closed field. Note that k is not a finite field.

1.1 The Zariski topology

Definition 1.1.1 For n in $\mathbb{N}$ we define *affine n-space*, denoted by $\mathbb{A}^n$, as k^n. Elements of $\mathbb{A}^n$ will be called points. Furthermore, $\mathbb{A}^1$ is called the *affine line* and $\mathbb{A}^2$ is called the *affine plane*.

Let $A = k[x_1, \ldots, x_n]$. We can view an element f of A as a function from $\mathbb{A}^n$ to k by evaluating f at points of $\mathbb{A}^n$.

Definition 1.1.2 We define the *zero set* of an f in A to be $Z(f) = \{p \in \mathbb{A}^n : f(p) = 0\}$. For $S \subset A$ we define $Z(S) = \{p \in \mathbb{A}^n : \forall f \in S,\ f(p) = 0\}$.

Example 1.1.3 Let S be the subset $\{x_1^2 + x_2^2 - 1, x_1\}$ of $k[x_1, x_2]$. Then $Z(S) = \{(0,1), (0,-1)\} \subset \mathbb{A}^2$.

Remark 1.1.4 Let $S \subset A$ and $I \subset A$ be the ideal generated by S. Then $Z(I) = Z(S)$, by the following argument. Since $S \subset I$, we obviously have $Z(I) \subset Z(S)$. On the other hand, let $p \in Z(S)$ and $f \in I$. Write f as a finite sum $f = \sum_{s \in S} f_s s$ with f_s in A. Then $f(p) = \sum_s f_s(p)s(p) = 0$. Hence p is in $Z(I)$. Therefore we also have the other inclusion $Z(I) \supset Z(S)$.

Definition 1.1.5 A subset $Y \subset \mathbb{A}^n$ is called *algebraic* if there exists some $S \subset A$ such that $Y = Z(S)$. By the previous remark we can replace "some $S \subset A$" by "some ideal $I \subset A$" without changing the meaning.

Example 1.1.6 We consider the case $n = 1$. Since $A = k[x]$ is a principal ideal domain (every non-zero ideal is generated by its monic element of smallest degree; use division with remainder), the algebraic subsets are of the form $Z((f)) = Z(f)$ for some f in A. If $f = 0$ we get $Z(0) = \mathbb{A}^1$. If $f \neq 0$ then f has only a finite number of zeros, hence $Z(f)$ is a finite set. On the other hand for every finite subset Y of $\mathbb{A}^1$ we have $Y = Z(\prod_{p \in Y}(x - p))$. This shows that the algebraic subsets of $\mathbb{A}^1$ are $\mathbb{A}^1$ itself together with the finite subsets of $\mathbb{A}^1$.

Proposition 1.1.7 *Let n be in $\mathbb{N}$.*

i. Let $Y_1, Y_2 \subset \mathbb{A}^n$ be algebraic sets. Then $Y_1 \cup Y_2$ is an algebraic set.

ii. If $\{Y_\alpha\}_\alpha$ is a collection of algebraic subsets of $\mathbb{A}^n$, then $\cap_\alpha Y_\alpha \subset \mathbb{A}^n$ is algebraic.

iii. $\mathbb{A}^n$ *is algebraic.*

iv. $\emptyset$ *is algebraic.*

Proof i. We claim that for S_1 and S_2 subsets of A we have

$$Z(S_1) \cup Z(S_2) = Z(S_1 S_2), \quad \text{where} \quad S_1 S_2 = \{fg : f \in S_1,\ g \in S_2\}.$$

Obviously we have $Z(S_1) \cup Z(S_2) \subset Z(S_1 S_2)$. For the other inclusion, assume that $p \in Z(S_1 S_2)$ and $p \notin Z(S_1)$. Then there is an f in S_1 such that $f(p) \neq 0$. But we have for all g in S_2 that $0 = (fg)(p) = f(p)g(p)$. Since $f(p) \neq 0$, we get that $g(p) = 0$ for all $g \in S_2$, and hence $p \in Z(S_2)$.

ii. We obviously have $Z(\cup_\alpha S_\alpha) = \cap_\alpha Z(S_\alpha)$.

iii. Note that $Z(\emptyset) = Z(0) = \mathbb{A}^1$.

iv. Note that $Z(1) = \emptyset$. $\square$

Corollary 1.1.8 *The algebraic subsets of* $\mathbb{A}^n$ *are the* closed *subsets of a topology on* $\mathbb{A}^n$*. We will call this topology the* Zariski topology.

Remark 1.1.9 By Example 1.1.6 the Zariski topology on $\mathbb{A}^1$ is equal to the co-finite topology on $\mathbb{A}^1$.

Definition 1.1.10 On a subset $Y \subset \mathbb{A}^n$ we define the *Zariski topology* as the induced topology from the Zariski topology on $\mathbb{A}^n$.

Definition 1.1.11 A topological space X is *irreducible* if (1) $X \neq \emptyset$ and (2) if $X = Z_1 \cup Z_2$ with Z_1 and Z_2 closed subsets of X then $Z_1 = X$ or $Z_2 = X$.

Examples 1.1.12 The affine line $\mathbb{A}^1$ is irreducible, since $\mathbb{A}^1$ is infinite. The real line $\mathbb{R}$ with its usual topology is not irreducible, because $\mathbb{R} = (-\infty, 0] \cup [0, \infty)$.

Remark 1.1.13 Let Y be a non-empty subset of $\mathbb{A}^n$. Then Y is irreducible if and only if for all closed subsets Z_1 and Z_2 of $\mathbb{A}^n$ with $Y \subset Z_1 \cup Z_2$ one has $Y \subset Z_1$ or $Y \subset Z_2$.

1.2 The Nullstellensatz

Let n be in $\mathbb{N}$ and $A = k[x_1, \ldots, x_n]$. Recall that k is an algebraically closed field. In the previous subsection we defined a map:

$$Z : \{\text{subsets of } A\} \to \{\text{closed subsets of } \mathbb{A}^n\}.$$

We would like to "invert" this map Z. Note that Z is surjective, but not injective, not even when we restrict to the set of ideals: for example $Z((x)) = Z((x^2)) \subset \mathbb{A}^1$. The problem comes from the fact that if $f^m(p) = 0$ for some $f \in A$ and $m \geq 1$ then $f(p) = 0$ as well.

Definition 1.2.1 We define the following map:

$$\begin{array}{rcl} I : \{\text{subsets of } \mathbb{A}^n\} & \to & \{\text{ideals of } A\} \\ Y & \mapsto & I(Y) := \{f \in A : \forall p \in Y,\ f(p) = 0\} \end{array}$$

Definition 1.2.2 A ring R is *reduced* if its only nilpotent element is 0 (examples: integral domain, fields, products of integral domains, subrings of reduced rings). An ideal I in a ring R is *radical* if for all a in R and m in $\mathbb{Z}_{\geq 1}$ such that $a^m \in I$, a is in I.

Remark 1.2.3 Let R be a ring and I an ideal in R. Then I is radical if and only if R/I is reduced.

Example 1.2.4 In the ring $k[x]$ the ideal (x) is radical but (x^2) is not.

For any subset Y of $\mathbb{A}^n$ the ideal $I(Y)$ is radical. Hence the image of the map I in Definition 1.2.1 is contained in the set of radical ideals. Hilbert's famous Nullstellensatz says that when we restrict to this set of ideals, the maps Z and I are inverses of each other.

Theorem 1.2.5 (Nullstellensatz, Hilbert, 1893) *Let n be in $\mathbb{N}$. The maps Z and I above, when restricted to the set of radical ideals in $k[x_1, \ldots, x_n]$ and the set of closed subsets of $\mathbb{A}^n$ are inverses of each other. They reverse the partial orderings on these sets given by inclusion: for I and J radical ideals in A we have $I \subset J \Leftrightarrow Z(I) \supset Z(J)$.*

We encourage the reader to see [Eis], Chapter 4, Theorem 1.6, or see [Looij] for a proof.

Definition 1.2.6 An *integral domain* is a ring R such that (1) $1 \neq 0$ in R and (2) for $a \neq 0$ and $b \neq 0$ in R, $ab \neq 0$. A *prime ideal* of a ring R is an ideal I of R such that R/I is an integral domain.

Remark 1.2.7 Let I be an ideal in a ring R. The following two properties are each equivalent with I being prime:

i. $I \neq R$ and for all $x, y \in R$ we have that $xy \in I \implies x \in I$ or $y \in I$;

ii. $I \neq R$ and for all ideals $J, K \subset R$ we have that $JK \subset I \implies J \subset I$ or $K \subset I$.

We let the reader verify that maximal ideals are prime, and prime ideals are radical, and show by examples that the converse statements are not true.

Proposition 1.2.8 *Let $Y \subset \mathbb{A}^n$ be closed. Then:*

i. $I(Y)$ is a maximal ideal if and only if Y consists of a single point;

ii. $I(Y)$ is a prime ideal if and only if Y is irreducible.

Proof We start with i. Assume that $I(Y)$ is a maximal ideal. Then $Y \neq \emptyset$, since the radical ideal that corresponds to the empty set under the bijection from the Nullstellensatz is A. So by the Nullstellensatz Y is a minimal non-empty algebraic set. Since points are closed, Y is a point.

Now assume that Y is a point, say $Y = \{p\}$. The evaluation map $A \to k$, $f \mapsto f(p)$ is surjective, and its kernel is $I(Y)$, by definition. Hence $A/I(Y) = k$ and $I(Y)$ is a maximal ideal.

Now we prove ii. Assume that $I(Y)$ is a prime ideal of A. Then $Y \neq \emptyset$ because $I(Y) \neq A$. Suppose that $Y \subset Z_1 \cup Z_2$ with Z_1 and $Z_2 \subset \mathbb{A}^n$ closed. Then

$$I(Z_1)I(Z_2) \subset I(Z_1) \cap I(Z_2) = I(Z_1 \cup Z_2) \subset I(Y).$$

Hence by Remark 1.2.7 $I(Z_1) \subset I(Y)$ or $I(Z_2) \subset I(Y)$. So $Y \subset Z_1$ or $Y \subset Z_2$. So, Y is irreducible.

On the other hand suppose that Y is irreducible, we show that $I(Y)$ is a prime ideal. First of all $I(Y) \neq A$ because $Y \neq \emptyset$. Suppose that $fg \in I(Y)$. Then $Y \subset Z(fg) = Z(f) \cup Z(g)$. Hence $Y \subset Z(f)$ or $Y \subset Z(g)$ by the irreducibility of Y. So we have that $f \in I(Y)$ or $g \in I(Y)$. So, $I(Y)$ is a prime ideal. □

Corollary 1.2.9 *$\mathbb{A}^n$ is irreducible.*

Proof The ring $A = k[x_1, \ldots, x_n]$ is an integral domain, so $(0) \subset A$ is a prime ideal, hence by the previous proposition $\mathbb{A}^n = Z((0))$ is irreducible. □

Definition 1.2.10 Let $Y \subset \mathbb{A}^n$ be a subset. We define $A(Y)$ to be $A/I(Y)$. We have a natural map $k \to A(Y)$. This map makes $A(Y)$ into a k-algebra.

If f and g are elements of A with $f - g \in I(Y)$ then $f(p) = g(p)$ for all $p \in Y$. So elements of the quotient ring $A(Y)$ can be interpreted as functions from Y to k. We note that if Y is irreducible, then $A(Y)$ is an integral domain.

1.3 Decomposition of closed sets in $\mathbb{A}^n$

Definition 1.3.1 A ring R is called *Noetherian* if every ideal of R is finitely generated, or equivalently, if for every chain of ideals $I_1 \subset I_2 \subset \cdots$ there is an r such that $I_r = I_{r+1} = \cdots$.

Theorem 1.3.2 (Hilbert basis theorem) *If R is Noetherian, then so is $R[x]$.*

See [Eis], Chapter 4, or [Looij] for a proof. The main ingredient of the proof is the "leading term" of a non-zero element of $R[x]$.

Corollary 1.3.3 *The ring $A = k[x_1, \ldots, x_n]$ is Noetherian.*

If $Y_1 \supset Y_2 \supset Y_3 \supset \ldots$ are closed subsets of $\mathbb{A}^n$, then there is an $r > 0$ such that $I(Y_r) = I(Y_{r+1}) = \cdots$ so by the Nullstellensatz we conclude that $Y_r = Y_{r+1} = \cdots$. Also, as $A = k[x_1, \ldots, x_n]$ is Noetherian, every proper ideal $I \subset A$ is contained in a maximal ideal. We obtain from the Nullstellensatz that $Z(I) \subset \mathbb{A}^n$ is non-empty, if $I \subset A$ is a proper ideal. [1]

Proposition 1.3.4 *If $Y \subset \mathbb{A}^n$ is closed then $Y = Y_1 \cup \ldots \cup Y_t$ for a finite collection of closed and irreducible $Y_i \subset \mathbb{A}^n$.*

Proof Assume Y is not a finite union of closed irreducibles, in particular Y is not irreducible. So we can write $Y = Z_1 \cup Z_2$ with $Z_1 \subsetneq Y$, $Z_2 \subsetneq Y$ and Z_1, Z_2 closed. Hence at least one of Z_1, Z_2 is not a finite union of closed irreducibles, say Z_1. Put $Y_1 = Z_1$ and repeat. This gives us an infinite strictly decreasing chain, a contradiction. □

Proposition 1.3.5 *If $Y = Y_1 \cup Y_2 \cup \cdots \cup Y_t$ with Y_i closed, irreducible and with the property that $Y_i \subset Y_j \implies i = j$, then the Y_i are uniquely determined by Y up to ordering.*

Proof Let $Y \subset \mathbb{A}^n$ be closed. Assume $Y_1' \cup \cdots \cup Y_s' = Y = Y_1 \cup \cdots \cup Y_t$ with Y_i and Y_i' irreducible, closed and $Y_i \subset Y_j \implies i = j$ and $Y_i' \subset Y_j' \implies i = j$. Assume that the two decompositions are different. Without loss of generality we may assume that there is an i with $Y_i \neq Y_j'$ for all j. Then we have $Y_i = Y_i \cap Y = (Y_i \cap Y_1') \cup \cdots \cup (Y_i \cap Y_s')$. Since Y_i is irreducible we obtain $Y_i \subset (Y_i \cap Y_j')$ for some j. So $Y_i \subset Y_j'$. Now repeat the above argument to find a k such that $Y_j' \subset Y_k$. So $Y_i \subset Y_j' \subset Y_k$, hence $Y_i = Y_k$ and $Y_i = Y_j'$, contradiction. □

1.4 Dimension

Definition 1.4.1 If Y is an irreducible topological space, then $\dim(Y)$ is the biggest integer m such that there is a chain $Y = Y_m \supsetneq Y_{m-1} \supsetneq \cdots \supsetneq Y_0 = \{\mathrm{pt}\}$ with $Y_i \subset Y$ irreducible and closed (in Y).

Example 1.4.2 $\dim \mathbb{A}^1 = 1$, since the longest chain is $\mathbb{A}^1 \supsetneq \{\mathrm{pt}\}$.

[1] In a commutative algebra course it will be learnt that actually in *every* commutative ring A, every proper ideal $I \subset A$ is contained in a maximal ideal. This follows by an application of Zorn's Lemma.

Theorem 1.4.3 *Let n be in $\mathbb{N}$ and Y an irreducible subset of $\mathbb{A}^n$. Then $\dim(Y)$ is the transcendence degree of the field of fractions of the integral domain $A(Y)$ as extension of k. In particular, $\dim(\mathbb{A}^n) = n$.*

See [Eis], Chapter 13, Theorem 13.1 and Chapter 8, Theorem A. Note that $\dim(Y) \in \mathbb{N}$.

Proposition 1.4.4 *Let $Y \subset \mathbb{A}^n$ be closed and irreducible. Then $\dim(Y) = n-1$ if and only if $Y = Z(f)$ for some irreducible $f \in A$.*

Warning 1.4.5 One may be tempted to believe that something more general is true: that for every closed irreducible $Y \subset \mathbb{A}^n$ of dimension d there are $f_1, \ldots, f_{n-d} \in A$ so that $Y = Z((f_1, \ldots, f_{n-d}))$. This is *wrong* in general.

Definition 1.4.6 A closed irreducible algebraic subset Y is called a *hypersurface in* $\mathbb{A}^n$ if $\dim(Y) = n-1$ or equivalently $Y = Z(f)$ for some irreducible $f \in A$. An irreducible algebraic subset $Y \subset \mathbb{A}^n$ of dimension 1 is called an *affine curve*. An irreducible algebraic subset $Y \subset \mathbb{A}^n$ of dimension 2 is called an *affine surface*.

1.5 Application: the theorem of Cayley-Hamilton

Theorem 1.5.1 (Cayley-Hamilton) *Let k be any field. Let a be an m by m matrix over k and let $P_a \in k[x]$ be its characteristic polynomial, then $P_a(a) = 0$.*

Lemma 1.5.2 *If a has m distinct eigenvalues, then $P_a(a) = 0$.*

Proof Without loss of generality we may assume that k is algebraically closed. Assume that a has no multiple eigenvalues. Then a is diagonalisable, so $a = qdq^{-1}$ for some invertible matrix q and a diagonal matrix d. We find that $P_a(a) = qP_a(d)q^{-1} = 0$. □

Proof (of Theorem 1.5.1) Put $n = m^2$ and view $\mathbb{A}^n$ as the set of all m by m matrices over k by ordering the coefficients in some way.

Let $Z_1 \subset \mathbb{A}^n$ be the subset of all matrices a that satisfy $P_a(a) = 0$. Note that Z_1 is closed since it is defined by n polynomials in the entries of a.

Let $Z_2 \subset \mathbb{A}^n$ be the subset of all matrices a that have multiple eigenvalues. Also Z_2 is closed since $a \in Z_2$ if and only if the discriminant of P_a is zero, and the discriminant of P_a is a polynomial in the entries of a.

The lemma shows that $\mathbb{A}^n = Z_1 \cup Z_2$. Also $\mathbb{A}^n \neq Z_2$ since there exist matrices without multiple eigenvalues. By the irreducibility of $\mathbb{A}^n$ (Corollary 1.2.9) we conclude that $\mathbb{A}^n = Z_1$, which proves the theorem. □

1.6 Exercises

Let k be an algebraically closed field.

Exercise 1.6.1 Let $Y = \{P_1, \ldots, P_r\} \subset \mathbb{A}^n$ be a finite set consisting of r distinct points. Give generators for the ideal $I(Y) \subset k[x_1, \ldots, x_n]$.

Exercise 1.6.2 ([Hart, I.1.1])

i. Let $Y \subset \mathbb{A}^2$ be the zero set of $y - x^2$. Show that the k-algebra $A(Y)$ is isomorphic to $k[t]$.

ii. Let $Y \subset \mathbb{A}^2$ be the zero set of $xy - 1$. Show that the k-algebra $A(Y)$ is not isomorphic to $k[t]$.

Exercise 1.6.3 Let $Y \subset \mathbb{A}^2$ be the zero set of x^2+y^2-1. Show that the k-algebra $A(Y)$ is not isomorphic to $k[t]$ if the characteristic of k is different from 2. What is $A(Y)$ if k is of characteristic 2?

Exercise 1.6.4 Let $X \subset \mathbb{A}^n$ be an irreducible closed subset. Show that X, endowed with the Zariski topology, is connected.

Exercise 1.6.5 For $f \in k[x_1, \ldots, x_n]$ nonzero let $D(f) \subset \mathbb{A}^n$ be the complement of $Z(f)$. Show that the $D(f)$ form a basis for the Zariski topology of $\mathbb{A}^n$.

Exercise 1.6.6 Show that $\mathbb{A}^n$ with its Zariski topology is compact: every open cover has a finite subcover.

Exercise 1.6.7 Show that the map $\mathbb{A}^n \to \mathbb{A}^1$ defined by a polynomial $f \in k[x_1, \ldots x_n]$ is continuous when both $\mathbb{A}^n$ and $\mathbb{A}^1$ are endowed with the Zariski topology.

Exercise 1.6.8 ([Hart, I.1.3]) Let $Y \subset \mathbb{A}^3$ be the common zero set of the polynomials x^2-yz and $xz-x$. Show that Y is the union of three irreducible components. Describe them and find their prime ideals.

Exercise 1.6.9 ([Hart, I.1.4]) If one identifies $\mathbb{A}^2$ with $\mathbb{A}^1 \times \mathbb{A}^1$ in the natural way, show that the Zariski topology on $\mathbb{A}^2$ is not the product topology of the Zariski topologies on the two copies of $\mathbb{A}^1$.

Exercise 1.6.10 Assume that the characteristic of k is not 3. Show that the common zero set in $\mathbb{A}^3$ of the polynomials x^2-yz and y^2-xz is the union of four irreducible components. Describe them and find their prime ideals.

Exercise 1.6.11 Let $X \subset \mathbb{A}^n$ be an irreducible closed subset and let $U \subset X$ be a non-empty open subset. Show that U is dense in X. Show that U is irreducible. Show that $\dim(U) = \dim(X)$.

Exercise 1.6.12 ([Hart, I.1.5]) Show that a k-algebra B is isomorphic to $A(Y)$ for some algebraic set Y in some affine space $\mathbb{A}^n$ if and only if B is a finitely generated k-algebra that is reduced.

Lecture 2

Projective space and its algebraic sets

In this lecture we discuss a part of Section I.2 of [Hart], although rather differently, putting more emphasis on the origin of the graded rings that enter the stage. The reader is advised to read that section of [Hart] separately. As in the previous lecture, we let k be an algebraically closed field.

2.1 $\mathbb{P}^n$ as a set

In this section, we do not need the assumption that k is algebraically closed.

Definition 2.1.1 For $n \in \mathbb{Z}_{\geq 0}$ we define the *projective n-space* $\mathbb{P}^n$ as the quotient of $k^{n+1} - \{0\}$ by the equivalence relation $\sim$, where $a \sim b \iff \exists \lambda \in k^\times$ such that $b = \lambda a$.

Remarks 2.1.2 i. $\sim$ is the equivalence relation given by the action of $k^\times$ on $k^{n+1} - \{0\}$: $(\lambda, a) \mapsto \lambda \cdot a$. So $a \sim b \iff a$ and b are in the same orbit under this action of $k^\times$.

ii. $a \sim b \iff k \cdot a = k \cdot b \iff a$ and b lie on the same line through the origin. So we can view $\mathbb{P}^n$ as the set $\{k \cdot a : a \in k^{n+1} - \{0\}\}$ of 1-dimensional k-vector spaces in k^{n+1}.

Remark 2.1.3 If $k = \mathbb{R}$, then $\mathbb{P}^n = S^n/\sim$ where $a \sim b \iff a = \pm b$, so we identify antipodal points.

Notation 2.1.4 Let $q\colon k^{n+1} - \{0\} \to \mathbb{P}^n$ be the quotient map. For $a = (a_0, \ldots, a_n)$ in $k^{n+1} - \{0\}$ we write $q(a_0, \ldots, a_n) = (a_0 : \cdots : a_n)$. These are the so called *homogeneous coordinates*, and the ":" (colons) express the fact that we are dealing with ratios.

Examples 2.1.5 In these examples, we will discuss $\mathbb{P}^n$ for certain n.

i. $\mathbb{P}^0 = (k^1 - \{0\})/\sim = \{(1)\}$, $\mathbb{P}^0$ is a 1-point set.

ii. $\mathbb{P}^1 = \{(a_0, a_1) \in k^2 : (a_0, a_1) \neq (0,0)\}/\sim = \{(a : 1) : a \in k\} \sqcup \{(1 : 0)\} = \mathbb{A}^1 \sqcup \{\infty\}$.

iii We can generalise the procedure for $n = 1$ to the general case as follows:

$$\begin{aligned}
\mathbb{P}^n &= \{(a_0 : \cdots : a_{n-1} : 1) : a_0, \ldots, a_{n-1} \in k\} \sqcup \{(a_0 : \cdots : a_{n-1} : 0) : 0 \neq (a_0, \ldots, a_{n-1}) \in k^n\} \\
&= \mathbb{A}^n \sqcup \mathbb{P}^{n-1} \\
&= \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup \cdots \sqcup \mathbb{A}^1 \sqcup \mathbb{A}^0.
\end{aligned}$$

Remark 2.1.6 We can even make the decomposition of for example $\mathbb{P}^1$ visible in a picture. For this first draw the affine plane $\mathbb{A}^2$ with coordinates x_0 and x_1. Now $\mathbb{P}^1$ is the set of lines through the origin. We now fix some line not passing through the origin, say the line given by the equation $x_1 = 1$. Now a point on this line, say $(a_0, 1)$ gives rise to a line through the origin, $Z(x_0 - a_0 x_1)$, and if we vary a_0 we get all the lines through the origin, except the one line which is running parallel to the chosen line (in this case with the equation $x_1 = 0$), this is our point at infinity.

For $i \in \{0, \dots, n\}$, consider the following diagram:

$$\begin{array}{ccccc} U_i & := & \{(a_0 : \dots : a_n) \in \mathbb{P}^n \mid a_i \neq 0\} & = & \{(a_0 : \dots : a_{i-1} : 1 : a_{i+1} : \dots : a_n) \mid a_j \in k\} \\ \Big\downarrow \varphi_i & & (a_0 : \dots : a_n) & & \\ & & \Big\downarrow & & \\ \mathbb{A}^n & & (\frac{a_0}{a_i}, \dots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \dots, \frac{a_n}{a_i}). & & \end{array}$$

Notice that φ_i is a bijection, its inverse is given by

$$(b_0, \dots, b_{i-1}, b_{i+1}, \dots, b_n) \mapsto (b_0 : \dots : b_{i-1} : 1 : b_{i+1} : \dots : b_n).$$

2.2 $\mathbb{P}^n$ as a topological space

Let $A = k[x_0, \dots, x_n]$, the k-algebra of polynomial functions on $k^{n+1} = \mathbb{A}^{n+1}$.

We have $q\colon \mathbb{A}^{n+1} - \{0\} \to \mathbb{P}^n$, where q is the quotient map previously defined. We give $\mathbb{A}^{n+1} - \{0\}$ the topology induced from the Zariski topology on $\mathbb{A}^{n+1}$: a subset U of $\mathbb{A}^{n+1} - \{0\}$ is open if and only if it is open as subset of $\mathbb{A}^{n+1}$. We give $\mathbb{P}^n$ the quotient topology induced via q. Let Y be a subset of $\mathbb{P}^n$. Then Y is closed if and only if $q^{-1}Y \subset \mathbb{A}^{n+1} - \{0\}$ is closed, that is, if and only if there exists s closed subset Z of $\mathbb{A}^{n+1}$ such that $q^{-1}Y = Z \cap (\mathbb{A}^{n+1} - \{0\})$. Since a point is closed, this is equivalent to $q^{-1}Y \cup \{0\}$ being closed in $\mathbb{A}^{n+1}$.

So we have the following bijection:

$$\begin{array}{rcl} \{\text{closed subsets of } \mathbb{P}^n\} & \tilde{\to} & \{\text{closed } k^\times\text{-invariant subsets of } \mathbb{A}^{n+1} \text{ containing } 0\} \\ Y & \mapsto & q^{-1}Y \cup \{0\} \end{array}$$

Recall that we have the Nullstellensatz:

$$\begin{array}{rcl} \{\text{closed subsets of } \mathbb{A}^{n+1}\} & \stackrel{1:1}{\longleftrightarrow} & \{\text{radical ideals } I \subset A\} \\ Y & \mapsto & I(Y) \\ Z(I) & \leftarrow\!\shortmid & I \end{array}$$

We now ask the following question: what does the property $k^\times$-invariant become on the right hand side?

The group $k^\times$ acts on $\mathbb{A}^{n+1}$: an element $\lambda \in k^\times$ acts as the multiplication map $\lambda\cdot\colon \mathbb{A}^{n+1} \to \mathbb{A}^{n+1}$, $a \mapsto \lambda{\cdot}a$. Now $k^\times$ also acts on the set of functions from $\mathbb{A}^{n+1}$ to k as follows. Let $a \in \mathbb{A}^{n+1}$. Then $((\lambda\cdot)^*f)(a) := f(\lambda a)$. This means that we have the following commutative diagram:

$$\begin{tikzcd} \mathbb{A}^{n+1} \arrow[r, "\lambda\cdot"] \arrow[dr, "(\lambda\cdot)^*f=f\circ\lambda\cdot"'] & \mathbb{A}^{n+1} \arrow[d, "f"] \\ & k. \end{tikzcd}$$

The set $\{f\colon \mathbb{A}^{n+1} \to k\}$ of functions from $\mathbb{A}^{n+1}$ to k is a k-algebra: $(f+g)a = fa + ga$ and $(fg)a = (fa){\cdot}(ga)$ (we prefer not to write unnecessary parentheses, such as in $f(a)$). For each λ in

$k^\times$ the map $(\lambda\cdot)^*$ from $\{f\colon \mathbb{A}^{n+1} \to k\}$ to itself is a k-algebra automorphism (its inverse is $(\lambda^{-1}\cdot)^*$). For example, we check the additivity. Let f and g be functions $\mathbb{A}^{n+1} \to k$, then

$$((\lambda\cdot)^*(f+g))a = (f+g)(\lambda a) = f(\lambda a) + g(\lambda a) = ((\lambda\cdot)^* f)a + ((\lambda\cdot)^* g)a = ((\lambda\cdot)^* f + (\lambda\cdot)^* g)a.$$

As this is true for all a in $\mathbb{A}^{n+1}$, we have $(\lambda\cdot)^* f + (\lambda\cdot)^* g$.

Recall that $A = k[x_0, \ldots, x_n]$. It is a sub-k-algebra of $\{f\colon \mathbb{A}^{n+1} \to k\}$. We claim that it is preserved by the $k^\times$-action: for f in A and λ in $k^\times$, the function $(\lambda\cdot)^* f$ is again in A. Indeed, for $f = \sum_i f_i x^i$ (multi-index notation) the function $(\lambda\cdot)^* f\colon \mathbb{A}^{n+1} \to k$ is given by

$$a \mapsto \lambda\cdot a \mapsto f(\lambda a) = \sum_{i_0,\ldots,i_n} f_{i_0,\ldots,i_n} \lambda^{i_0} a_0^{i_0} \cdots \lambda^{i_n} a_n^{i_n} = \sum_{i_0,\ldots,i_n} f_{i_0,\ldots,i_n} \lambda^{i_0+\cdots+i_n} a_0^{i_0} \cdots a_n^{i_n}.$$

Hence we see that

$$(\lambda\cdot)^* f = \sum_{i_0,\ldots,i_n} f_{i_0,\ldots,i_n} \lambda^{i_0+\cdots+i_n} x_0^{i_0} \cdots x_n^{i_n} \in A.$$

We conclude that each $(\lambda\cdot)^*\colon A \to A$ is a k-algebra automorphism, with inverse $(\lambda^{-1}\cdot)^*$. So $k^\times$ acts on the k-algebra A.

Now observe that for f in A, λ in $k^\times$, and a in $\mathbb{A}^{n+1}$ we have:

$$a \in Z((\lambda\cdot)^* f) \iff ((\lambda\cdot)^* f)(a) = 0 \iff f(\lambda\cdot a) = 0 \iff \lambda\cdot a \in Z(f).$$

So: $Z((\lambda\cdot)^* f) = \lambda^{-1}\cdot Z(f)$. And for $S \subset A$ we have $Z((\lambda\cdot)^* S) = \lambda^{-1}\cdot Z(S)$. Hence restricting the bijection from the Nullstellensatz on both sides to the subset $k^\times$-invariant subsets gives the bijection:

$$\begin{matrix} \{\text{closed } k^\times\text{-invariant subsets} & \xleftrightarrow{1:1} & \{k^\times\text{-invariant radical ideals } \mathfrak{a} \subset A \\ \text{of } \mathbb{A}^{n+1} \text{ containing } 0\} & & \text{with } \mathfrak{a} \subset (x_0, \ldots, x_n) = Ax_0 + \cdots + Ax_n\} \end{matrix}$$

We now want to know which ideals are $k^\times$-invariant. For this, we first decompose A into eigenspaces for the action of $k^\times$. An eigenspace under the action of $k^\times$ is exactly the set of homogeneous polynomials of a certain degree together with the 0 polynomial: A is graded as a k-algebra. This means that

$$A = \bigoplus_{d\geq 0} A_d, \quad A_d = \bigoplus_{d_0+\cdots+d_n=d} k\cdot x_0^{d_0} \cdots x_n^{d_n}, \quad f \in A_d,\ g \in A_e \implies f\cdot g \in A_{d+e}.$$

The sub-k-vectorspace A_d of A is called the space of homogeneous polynomials of degree d. For $f \in A$ we can write $f = \sum_d f_d$ with $f_d \in A_d$, and such a decomposition is unique. The f_d are called the *homogeneous parts* of f. Then for $\lambda \in k^\times$ we get $(\lambda\cdot)^* f = \sum_d \lambda^d f_d$.

Definition 2.2.1 An ideal $\mathfrak{a}$ is homogenous if for all f in $\mathfrak{a}$ the homogeneous parts f_d are also in $\mathfrak{a}$.

Proposition 2.2.2 *Let $\mathfrak{a} \subset A$ be an ideal. Then $\mathfrak{a}$ is $k^\times$-invariant if and only if $\mathfrak{a}$ is homogeneous.*

Proof $\Leftarrow$: Assume $\mathfrak{a}$ is homogeneous. Let $f \in \mathfrak{a}, \lambda \in k^\times$. Then $(\lambda\cdot)^* f = \sum_d \lambda^d f_d \in \mathfrak{a}$ because $f_d \in \mathfrak{a}$ for all d.

$\Rightarrow$: Assume $\mathfrak{a} \subset A$ is a $k^\times$-invariant ideal. Let $f \in \mathfrak{a}$. Write $f = f_0 + \cdots + f_N$ with $f_i \in A_i$ for some $N \in \mathbb{Z}_{\geq 0}$. Take $\lambda_0, \ldots, \lambda_N \in k^\times$ distinct (we can do this since k is algebraically closed, hence infinite). We have: $\mathfrak{a} \ni (\lambda_i\cdot)^* f = f_0 + \lambda_i f_1 + \cdots + \lambda_i^N f_N$. In matrix form this gives:

$$\begin{pmatrix} (\lambda_0\cdot)^* f \\ \vdots \\ (\lambda_N\cdot)^* f \end{pmatrix} = \begin{pmatrix} 1 & \lambda_0 & \lambda_0^2 & \cdots & \lambda_0^N \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_N & \lambda_N^2 & \ldots & \lambda_N^N \end{pmatrix} \begin{pmatrix} f_0 \\ \vdots \\ f_N \end{pmatrix}$$

Now use that this Vandermonde matrix is invertible to get $f_0, \ldots, f_N$ in $\mathfrak{a}$ (we can express f_i as a k-linear combination of the $(\lambda_j\cdot)^* f$ in $\mathfrak{a}$). $\square$

Theorem 2.2.3 (Homogeneous Nullstellensatz) *The following maps are inverses:*

$$\begin{array}{rcl} \{\text{closed subsets of } \mathbb{P}^n\} & \stackrel{1:1}{\longleftrightarrow} & \{\text{homogeneous radical ideals } \mathfrak{a} \subset A \text{ with } \mathfrak{a} \subset (x_0, \ldots, x_n)\} \\ Y & \mapsto & I(q^{-1}Y \cup \{0\}) \\ q(Z(\mathfrak{a}) - \{0\}) & \leftarrow\!\shortmid & \mathfrak{a} \end{array}$$

and under this bijection we have that Y is irreducible if and only if $I(q^{-1}Y \cup \{0\})$ is prime and not equal to $(x_0, \ldots, x_n)$.

Proof The proof of the first part follows from the previous observations. The proof of the second part is one of the exercises below. □

2.3 A more direct description of the closed subsets of $\mathbb{P}^n$

Definition 2.3.1 For a homogeneous element f in some $A_d \subset A$ we define

$$Z_{\text{proj}}(f) := \{(a_0 : \cdots : a_n) \in \mathbb{P}^n : f(a_0, \ldots, a_n) = 0\}.$$

Note that the condition makes sense, as it is independent of the chosen representative $(a_0, \ldots, a_n)$ of $(a_0 : \cdots : a_n)$. In fact, $Z_{\text{proj}}(f) = q(Z(f) - \{0\})$ where $Z(f) \subset \mathbb{A}^{n+1}$.

The following proposition is a direct consequence of the results of the previous section.

Proposition 2.3.2 *The closed subsets of $\mathbb{P}^n$ are the $Z_{\text{proj}}(T) = \bigcap_{f \in T} Z_{\text{proj}}(f)$ for subsets T of the set $A^{\text{hom}} = \bigcup_{d \geq 0} A_d$ of homogeneous elements of A.*

We first consider a special case: $T \subset A_1$, the case of linear equations. These $Z_{\text{proj}}(T)$ are called linear subspaces of $\mathbb{P}^n$. Using linear algebra you can say a lot about them. For example two lines in $\mathbb{P}^2$ are equal or intersect in exactly one point, see exercise I.2.11 of [Hart]. A hyperplane is a $Z_{\text{proj}}(f)$ with $0 \neq f \in A_1$. We also have coordinate hyperplanes : $H_i = Z(x_i)$ for $0 \leq i \leq n$. Also we have the standard affine opens: $U_i = \mathbb{P}^n - H_i = \{a \in \mathbb{P}^n : a_i \neq 0\}$.

Proposition 2.3.3 *For $i \in 0, 1, \ldots, n$ the map $\varphi_i \colon U_i \to \mathbb{A}^n$,*

$$(a_0 : \cdots : a_n) \mapsto (\frac{a_0}{a_i}, \ldots, \frac{a_{i-1}}{a_i}, \frac{a_{i+1}}{a_i}, \ldots, \frac{a_n}{a_i})$$

is a homeomorphism.

Proof We have already seen that φ_i is bijective. Now consider the following diagram:

$$\begin{tikzcd} \mathbb{A}^{n+1} - \{0\} \arrow[d, "q"'] & \supset & q^{-1}U_i = \mathbb{A}^{n+1} - Z(x_i) \arrow[d, "q"'] \arrow[dr, "\varphi_i \circ q"] & \\ \mathbb{P}^n & \supset & U_i \arrow[r, "\varphi_i"'] & \mathbb{A}^n \end{tikzcd}$$

We first claim that $\varphi_i \circ q \colon a \mapsto (a_0/a_i, \ldots, a_{i-1}/a_i, a_{i+1}/a_i, \ldots, a_n/a_i)$ is continuous. It suffices to show that for any f in $k[y_1, \ldots, y_n]$ the set $(\varphi_i \circ q)^{-1}Z(f)$ is closed. So, let f be in $k[y_1, \ldots, y_n]$, of degree at most some d in $\mathbb{N}$. Then, for a in $q^{-1}U_i$, the following conditions are equivalent:

$$a \in (\varphi_i \circ q)^{-1}Z(f)$$
$$f((\varphi_i \circ q)a) = 0$$
$$f(a_0/a_i, \ldots, a_{i-1}/a_i, a_{i+1}/a_i, \ldots, a_n/a_i) = 0$$
$$a_i^d f(a_0/a_i, \ldots, a_{i-1}/a_i, a_{i+1}/a_i, \ldots, a_n/a_i)) = 0$$
$$a \in Z(x_i^d f(x_0/x_i, \ldots, x_{i-1}/x_i, x_{i+1}/x_i, \ldots, x_n/x_i)).$$

Hence $(\varphi_i \circ q)^{-1}Z(f) = Z(x_i^d f(x_0/x_i, \ldots, x_{i-1}/x_i, x_{i+1}/x_i, \ldots, x_n/x_i)) \cap q^{-1}U_i$. Hence $\varphi_i \circ q$ is continuous. Since U_i has the quotient topology for q, φ_i is continuous.

On the other hand, the map $s_i \colon \mathbb{A}^n \to \mathbb{A}^{n+1} - Z(x_i) = q^{-1}U_i$,

$$(b_0, \ldots, b_{i-1}, b_i, \ldots, b_n) \mapsto (b_0, \ldots, b_{i-1}, 1, b_{i+1}, \ldots, b_n)$$

is continuous because for any $b = (b_0, \ldots, b_{i-1}, b_i, \ldots, b_n)$ and any f in $k[x_0, \ldots, x_n]$ we have that $f(s_i(b)) = 0$ if and only if $f(b_0, \ldots, b_{i-1}, 1, b_{i+1}, \ldots, b_n) = 0$, hence $s_i(b) \in Z(f)$ if and only if $b \in Z(f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n))$. Hence $\varphi_i^{-1} = q \circ s_i$ is continuous. $\square$

2.4 How to administrate $\mathbb{P}^n$

On $\mathbb{A}^{n+1}$ we have the coordinate functions $x_0, \ldots, x_n$ and the k-algebra $k[x_0, \ldots, x_n]$ generated by them. Now φ_i is given by n functions on U_i: $x_{i,j}$, $0 \leq j \leq n$, $j \neq i$, with $x_{i,j} \circ q = x_j/x_i$. So $\varphi_i(P) = (x_{i,0}(P), \ldots, \ldots, x_{i,i-1}(P), x_{i,i+1}(P), \ldots, x_{i,n}(P))$.

Now for $f \in A_d$ we have that $x_i^{-d} f$ is a $k^\times$-invariant function on $q^{-1}U_i$, and it is a polynomial in the $x_{i,j}$, $j \neq i$. We have: $\varphi_i(Z_{\text{proj}}(f)) = Z(x_i^{-d} f)$.

Example 2.4.1 Let $f = x_1^n - x_0^{n-1}x_2 + x_2^n \in k[x_0, x_1, x_2]_n$. Then:

$$\begin{aligned}
\varphi_0(Z_{\text{proj}}(f) \cap U_0) &= Z(x_{0,1}^n - x_{0,2} + x_{0,2}^n) \\
\varphi_1(Z_{\text{proj}}(f) \cap U_1) &= Z(1 - x_{1,0}^{n-1}x_{1,2} + x_{1,2}^n) \\
\varphi_2(Z_{\text{proj}}(f) \cap U_2) &= Z(x_{2,1}^n - x_{2,0}^{n-1} + 1)
\end{aligned}$$

Vice versa: For $g \in k[\{x_{i,j} : j \neq i\}]$ of degree d you can “homogenise” to go back to $k[x_0, \ldots, x_n]$: just replace $x_{i,j}$ by x_j/x_i and multiply by x_i^d.

2.5 Exercises

We recall: k is an algebraically closed field. We also recall that a topological space X is irreducible if and only if first of all it is not empty and secondly has the property that if U and V are non-empty open subsets of X, then $U \cap V$ is non-empty.

Exercise 2.5.1 Let X and Y be topological spaces, $f \colon X \to Y$ continuous. Assume that X is irreducible and that f is surjective. Show that Y is irreducible.

Exercise 2.5.2 Let X and Y be topological spaces, $f \colon X \to Y$ a map, not necessarily continuous, and $Z \subset Y$. Assume that f is *open*: for every open U in X, fU is open in Y. Show that $f \colon f^{-1}Z \to Z$ is open, if Z and $f^{-1}Z$ are equipped with the topologies induced from Y and X.

Exercise 2.5.3 Let X and Y be topological spaces, $f \colon X \to Y$ continuous. Assume that f is open and that for every y in Y the subset $f^{-1}\{y\}$ of X, with its induced topology, is irreducible. Assume that Y is irreducible. Show that X is irreducible.

Exercise 2.5.4 Let X be a topological space, and $x \in X$. Assume that X is not equal to $\{x\}$, that $\{x\}$ is closed, and that $\{x\}$ is not open. Show that $X - \{x\}$ is irreducible if and only if X is irreducible.

Exercise 2.5.5 Let $n \in \mathbb{Z}_{\geq 0}$, and $q \colon \mathbb{A}^{n+1} - \{0\} \to \mathbb{P}^n$ as in today’s lecture. Show that q is open and that for all $P \in \mathbb{P}^n$, $q^{-1}\{P\}$ is irreducible.

Exercise 2.5.6 Let $n \in \mathbb{Z}_{\geq 0}$. Let $Y \subset \mathbb{P}^n$ be a closed subset. Let $I \subset A = k[x_0, \ldots, x_n]$ be the ideal of $q^{-1}Y \cup \{0\}$. Show that Y is irreducible if and only if I is prime and not equal to $(x_0, \ldots, x_n)$.

Exercise 2.5.7 Show by means of an example that Proposition 2.2.2 is false if k is not assumed to be algebraically closed.

Exercise 2.5.8 Let $P_1 = (0,0)$, $P_2 = (1,0)$, $P_3 = (0,1)$ and $P_4 = (1,1)$. Let $Y = \{P_1, P_2, P_3, P_4\}$ and let $I \subset k[x,y]$ be the ideal of Y.

i. Show that the affine coordinate ring $A(Y) = k[x,y]/I$ of Y has dimension 4 as k-vector space. Hint: consider the k-algebra morphism $k[x,y] \to k^4$ sending f to $(f(P_1), f(P_2), f(P_3), f(P_4))$, or use the Chinese Remainder Theorem.

ii. Show that $I = (f,g)$, where $f = x^2 - x$ and $g = y^2 - y$. Hint: show that $(f,g) \subset I$, then that $(1, x, y, xy)$ gives a k-basis for $k[x,y]/(f,g)$ using divisions with remainder, then that the natural morphism $k[x,y]/(f,g) \to A(Y)$ is an isomorphism.

iii. Draw a picture of Y, $Z(f)$ and $Z(g)$.

Exercise 2.5.9 We assume now that $k \not\supset \mathbb{F}_2$. Let $Z = \{P_1, P_2, P_3\} \subset \mathbb{A}^2$, with the P_i as in Exercise 2.5.8. Let $J \subset k[x,y]$ be the ideal of Z. Our aim is to show that J can be generated by two elements. We view $\mathbb{A}^2$ as a standard open affine subset of $\mathbb{P}^2$ via $(a,b) \mapsto (a:b:1)$. Let $P_4' = (1:1:0) \in \mathbb{P}^2$, and let $Y' = \{P_1, P_2, P_3, P_4'\} \subset \mathbb{P}^2$.

i. Draw a picture of Y', the lines P_1P_2, P_3P_4', P_1P_3 and P_2P_4', and the line at infinity (draw your picture in the affine plane that is the complement of a suitable line in $\mathbb{P}^2$).

ii. Give linear equations for the lines P_1P_2, P_3P_4', P_1P_3 and P_2P_4', and deduce from this your two candidate generators f and g for J.

iii. Show that $J = (f,g)$. Hint: same strategy as in Exercise 2.5.8.ii; $\dim_k A(Z) = 3$; show that $xy \in (f,g)$.

Remark 2.5.10 Later it will be easier for us to show that $J = (f,g)$, by deducing it from the fact that $Z(f) \cap Z(g) = Z$, with "transversal intersection". More generally, there are standard algorithms based on the concept of Gröbner basis, with which one can compute in quotients such as $k[x,y]/(f,g)$.

Lecture 3

Geometry in projective space

Let k be an algebraically closed field.

3.1 Points and lines in $\mathbb{P}^2$

In this section we do not need the assumption that k is algebraically closed. First recall the following (see the previous lecture):

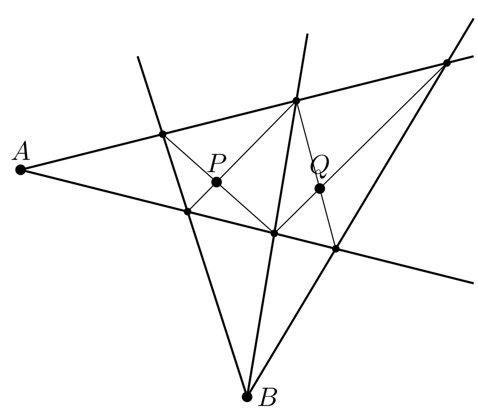
$$\mathbb{P}^2 = (k^3 - \{0\})/k^\times = \{\text{lines in } k^3 \text{ through } 0\} = \mathbb{A}^2 \sqcup \mathbb{P}^1$$

In this last description, $\mathbb{A}^2$ is the set of points of the form $(a : b : 1)$, and $\mathbb{P}^1$ is the set of points of the form $(c : d : 0)$ with $(c, d) \neq (0, 0)$. A line in $\mathbb{P}^2$ is $Z(f)$ where $f = ax + by + cz$ with $(a, b, c) \neq (0, 0, 0)$. A line in $\mathbb{A}^2$ is $Z(f)$ where $f = ax + by + c$ with $(a, b) \neq (0, 0)$.

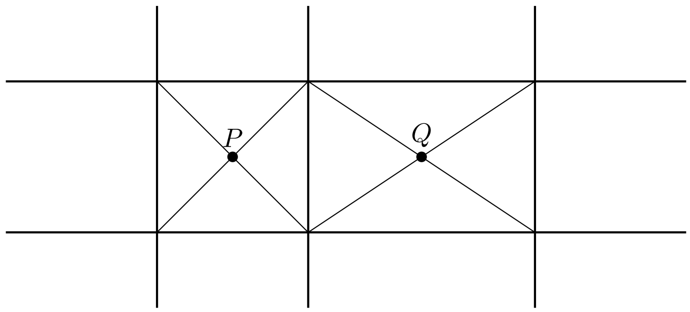
Let $l_1, l_2 \subset \mathbb{A}^2$ be *distinct* lines. Then the intersection $l_1 \cap l_2$ is empty if l_1 and l_2 are parallel, and otherwise it consists of one point. In $\mathbb{P}^2$ the situation is much nicer: two distinct lines always intersect in a unique point. Indeed, this follows from a dimension argument from linear algebra. The lines l_1 and l_2 as seen in $\mathbb{A}^3 = k^3$ are just two distinct linear subspaces of dimension 2, whose intersection is then of dimension one, which corresponds to a point in $\mathbb{P}^2$.

Using projective space, many theorems in affine geometry become easier to prove. Here is an example:

Proposition 3.1.1 *In the following configuration (say in $\mathbb{R}^2$), the points A, P, Q lie on a line.*



Proof First consider this problem in $\mathbb{P}^2$ instead of $\mathbb{A}^2$. After a linear change of coordinates we may assume that $A = (1 : 0 : 0)$ and $B = (0 : 1 : 0)$. Indeed, A and B are distinct 1-dimensional subspaces of k^3, hence we can take a basis of k^3 with these lines as the first two coordinate axes. The line AB is then the line at infinity, and therefore the two lines that intersect in A are parallel in $\mathbb{A}^2$ and similarly for the two lines that intersect in B. So we then have the following picture.



But in this case, the result is obvious, and so we are done. $\square$

3.2 Curves in $\mathbb{P}^2$

Remark 3.2.1 From now on, k is again assumed to be algebraically closed.

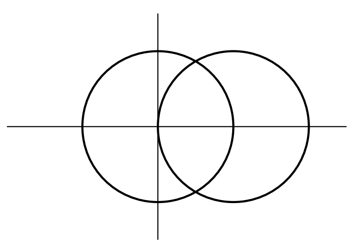
We have seen that the intersection of two distinct lines in $\mathbb{P}^2$ consists of one point. The following classical theorem from projective geometry generalizes this.

Theorem 3.2.2 (Bézout) *Let f_1 and f_2 in $k[x, y, z]$ be homogeneous irreducible polynomials of degrees d_1 and d_2, respectively. Assume $Z(f_1) \neq Z(f_2)$. Then $\#Z(f_1) \cap Z(f_2) = d_1 d_2$ "counted with multiplicity".*

Only later in this course we will be able to define the "multiplicity" occurring in the statement, but let us remark already now that it should be thought of as an "order of contact". So if the multiplicity of an intersection point is higher than one, this means that the curves are "tangent" to one another in that point.

Already the case $d_1 = d_2 = 1$ illustrates that it is important to work in the projective plane, instead of the affine plane. Below is another illustration.

Example 3.2.3 Assume that 2 is nonzero in k. Let $f_1 = x^2 + y^2 - z^2$ and $f_2 = (x - z)^2 + y^2 - z^2$. Here is a (real, affine) picture:



From the picture one can immediately read off two intersection points, namely $(1/2 : \sqrt{3}/2 : 1)$ and $(1/2 : -\sqrt{3}/2 : 1)$, and by putting $z = 0$ we find two more intersection points on the line at infinity: $(1 : \sqrt{-1} : 0)$ and $(1 : -\sqrt{-1} : 0)$. These two points at infinity correspond to the asymptotes. These asymptotes are not visible in the real affine picture, but become visible in $\mathbb{C}^2$.

3.3 Projective transformations

For n in $\mathbb{Z}_{\geq 0}$ we denote the group of invertible n by n matrices with coefficients in k with matrix multiplication by $\mathrm{GL}_n(k)$. It is the automorphism group of the k-vector space k^n.

Let n be in $\mathbb{Z}_{\geq 0}$. Since a linear map sends 0 to 0, the group $\mathrm{GL}_{n+1}(k)$ acts on $k^{n+1} - \{0\}$. Since matrix multiplication commutes with scalar multiplication, this induces an action of $\mathrm{GL}_{n+1}(k)$ on the quotient $\mathbb{P}^n$.

The normal subgroup $k^\times$ of scalar matrices in $\mathrm{GL}_{n+1}(k)$ acts trivially on $\mathbb{P}^n$. Therefore the action of $\mathrm{GL}_{n+1}(k)$ on $\mathbb{P}^n$ induces an action of the quotient $\mathrm{PGL}_{n+1}(k) := \mathrm{GL}_{n+1}(k)/k^\times$ on $\mathbb{P}^n$. An element of $\mathrm{PGL}_{n+1}(k)$ is called a projective transformation.

For f in $k[x_0, \ldots, x_n]$, viewed as function from $\mathbb{A}^{n+1}$ to k, and for g in $\mathrm{GL}_{n+1}(k)$, the function

$$g^*f \colon \mathbb{A}^{n+1} \to k \colon P \mapsto f(gP)$$

is again in $k[x_0, \ldots, x_n]$. This operation is a right-action of $\mathrm{GL}_{n+1}(k)$ on the k-algebra $k[x_0, \ldots, x_n]$. The polynomial g^*f is homogeneous of degree d if and only if f is homogeneous of degree d. Also, given a homogeneous polynomial $f \in k[x_0, \ldots, x_n]$ and a point $P \in \mathbb{P}^n$ we have $P \in Z(f)$ if and only if $g^{-1}P \in Z(g^*f)$. It follows that $\mathrm{GL}_{n+1}(k)$, and hence also $\mathrm{PGL}_{n+1}(k)$, act on $\mathbb{P}^n$ by homeomorphisms.

Remark 3.3.1 The proof of Proposition 3.1.1 could have started with “There exists a projective transformation $g \in \mathrm{PGL}_2$ such that $gA = (1:0:0)$ and $gB = (0:1:0)$, so we may assume that $A = (1:0:0)$ and $B = (0:1:0)$.”

3.4 Affine transformations

Definition 3.4.1 We define the group of affine transformations as follows:

$$\mathrm{Aff}_n = \mathrm{Aff}_n(k) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathrm{GL}_n, b \in k^n \right\} \subset \mathrm{GL}_{n+1}\,.$$

It is the stabiliser in GL_{n+1} of the element x_n in $k[x_0, \ldots, x_n]$, and therefore it stabilises all the hyperplanes $Z(x_n - a)$, with $a \in k$. The group Aff_n acts on $\mathbb{P}^n$. This action of Aff_n on $\mathbb{P}^n$ induces a morphism of groups $\mathrm{Aff}_n \to \mathrm{PGL}_n$. This morphism is injective and its image is the stabiliser in PGL_n of $Z(x_n)$, the hyperplane at infinity. This means that Aff_n acts on $\mathbb{P}^n - Z(x_n) = \mathbb{A}^n$ and on $Z(x_n) = \mathbb{P}^{n-1}$ as well.

Example 3.4.2 Consider the case where $n = 1$. An element of Aff_n has the form $g = \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ with $a \in k^\times$ and $b \in k$. Now let $P \in \mathbb{A}^1$ be the point with coordinate $p \in k$. In $\mathbb{P}^1$ this point has homogeneous coordinates $(p:1)$ and it is mapped by g to $(ap+b:1)$, so $gP \in \mathbb{A}^1$ has coordinate $ap+b$.

In the same way as before there is a compatible right-action of Aff_n on $k[x_0, \ldots, x_{n-1}]$. Explicitly:

$$g = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

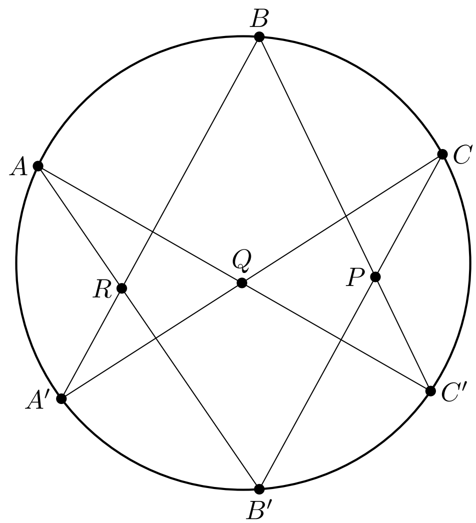
sends the polynomial f, viewed as function on k^n, to $g^*f := (x \mapsto f(ax+b))$. Note that P lies on $Z(f)$ if and only if $g^{-1}P$ lies on $Z(g^*f)$. In particular it follows that Aff_n acts as homeomorphisms on $\mathbb{A}^n$.

Remark 3.4.3 The dimension of Aff_1 is 2, but that of PGL_2 is 3. Hence the projective line has more symmetry than the affine line. In general Aff_n has dimension $n^2 + n$ (we can pick n^2 entries for the linear part, and then we can pick a vector to translate over, this gives an extra n) while PGL_{n+1} has dimension $(n+1)^2 - 1 = n^2 + 2n$.

3.5 Pascal’s theorem

In this section, we will prove Pascal’s theorem. We first state a Euclidian version of it.

Theorem 3.5.1 *Suppose that X is a circle and $A, B, C, A', B', C' \in X$ are distinct points on this circle. Let $P = B'C \cap BC'$, $Q = AC' \cap CA'$, $R = A'B \cap AB'$, assuming these intersections exist (see the picture below). Then P, Q, R lie on a line.*



To prove this it is convenient to generalize this to a projective statement.

Theorem 3.5.2 (Pascal) *Let $X = Z(g)$ with $g \in k[x_1, x_2, x_3]$ homogeneous of degree 2 and irreducible. Let $A, B, C, A', B', C' \in X$ be distinct points. Let $P = B'C \cap BC'$, $Q = AC' \cap CA'$, $R = A'B \cap AB'$. Then P, Q, R lie on a line.*

Proof Note that no three of the six points A, B, C, A', B', C' can lie on a line, for otherwise this would contradict Bézout's theorem (together with the irreducibility of X).

So, without loss of generality we may assume that $A' = (1 : 0 : 0)$, $B' = (0 : 1 : 0)$, $C' = (0 : 0 : 1)$. We now write down the equation for X:

$$g = g_{11}x_1^2 + g_{22}x_2^2 + g_{33}x_3^2 + g_{12}x_1x_2 + g_{13}x_1x_3 + g_{23}x_2x_3.$$

Since $A' = (1 : 0 : 0)$ lies on this quadric, we see that $g(1, 0, 0) = g_{11} = 0$. In the same manner, one obtains $g_{22} = g_{33} = 0$. So

$$g = g_{12}x_1x_2 + g_{13}x_1x_3 + g_{23}x_2x_3.$$

Note that none of g_{12}, g_{13}, g_{23} are zero, for otherwise our g would be reducible. After applying the projective transformation

$$\begin{pmatrix} g_{23} & 0 & 0 \\ 0 & g_{13} & 0 \\ 0 & 0 & g_{12} \end{pmatrix} \in \mathrm{PGL}_2$$

we may assume that

$$g = x_1x_2 + x_2x_3 + x_3x_1.$$

Note that A', B' and C' are fixed under this transformation.

Now let A, B, C be the points $(a_1 : a_2 : a_3)$, $(b_1 : b_2 : b_3)$ and $(c_1 : c_2 : c_3)$, respectively. Let us compute the coordinates of the point $P = B'C \cap BC'$. The line $B'C$ is given by $c_3x_1 = c_1x_3$, and BC' is given by $b_2x_1 = x_2b_1$. So we find that $P = (1 : b_2/b_1 : c_3/c_1)$. Note that b_1 is not zero, since B lies on X and B is distinct from B' and C', similarly a_i, b_i, c_i are all non-zero. By symmetry, we find that

$Q = (a_1/a_2 : 1 : c_3/c_2)$ and $R = (a_1/a_3 : b_2/b_3 : 1)$. To check that P, Q and R lie on a line, it is enough to show that

$$\det \begin{pmatrix} 1 & b_2/b_1 & c_3/c_1 \\ a_1/a_2 & 1 & c_3/c_2 \\ a_1/a_3 & b_2/b_3 & 1 \end{pmatrix} = 0.$$

But this is true. The sum of the rows is zero, this follows since A, B and C lie on our quadric. For example, for the first coordinate:

$$1 + \frac{a_1}{a_2} + \frac{a_1}{a_3} = \frac{a_2a_3 + a_1a_3 + a_1a_2}{a_2a_3} = \frac{g(a_1, a_2, a_3)}{a_2a_3} = 0.$$

□

3.6 Exercises

Exercise 3.6.1 Consider $Y_1 = Z(y - x^2)$ and $Y_2 = Z(xy - 1)$ in $\mathbb{A}^2$. Denote by $i : \mathbb{A}^2 \to \mathbb{P}^2$ the map $(a, b) \mapsto (a : b : 1)$. Let X_1 and X_2 be the closures of iY_1 and iY_2, respectively.

i. Give equations for X_1 and X_2.

ii. Describe $X_2 - iY_2$ and $X_1 - iY_1$.

iii. Show that there is no affine transformation α such that $\alpha Y_1 = Y_2$.

iv. Show that there is a projective transformation β such that $\beta X_1 = X_2$.

Exercise 3.6.2 Let P_1, P_2 and P_3 be three distinct points in $\mathbb{P}^1$. Show that there is a unique projective transformation that maps P_1 to $(1 : 0)$, P_2 to $(0 : 1)$, and P_3 to $(1 : 1)$.

Exercise 3.6.3 Let P_1, P_2, P_3 and P_4 be four points in $\mathbb{P}^2$ such that there is no line in $\mathbb{P}^2$ containing three of them. Show that there is a unique projective transformation that maps P_1 to $(1 : 0 : 0)$, P_2 to $(0 : 1 : 0)$, P_3 to $(0 : 0 : 1)$, and P_4 to $(1 : 1 : 1)$.

Exercise 3.6.4 ([Hart, 2.14]) Given positive integers r and s consider the map

$$((a_1, \ldots, a_r), (b_1, \ldots, b_s)) \to (a_1b_1 : a_1b_2 : \cdots : a_rb_s)$$

from $(\mathbb{A}^r - \{0\}) \times (\mathbb{A}^s - \{0\})$ to $\mathbb{P}^{rs-1}$.

(a) Show that the map factors through $\mathbb{P}^{r-1} \times \mathbb{P}^{s-1}$;

Denote the resulting map from $\mathbb{P}^{r-1} \times \mathbb{P}^{s-1}$ to $\mathbb{P}^{rs-1}$ by Ψ.

(b) Show that Ψ is injective;

(c) Show that the image of Ψ is closed in $\mathbb{P}^{rs-1}$.

The map Ψ is called the *Segre embedding* of $\mathbb{P}^{r-1} \times \mathbb{P}^{s-1}$ in $\mathbb{P}^{rs-1}$.

Exercise 3.6.5 ([Hart, 2.15]) Consider the Segre embedding $\Psi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$. Let $Q \subset \mathbb{P}^3$ be the image of Ψ.

i. Give equations for Q.

ii. Show that for all $P \in \mathbb{P}^1$ the images of $\{P\} \times \mathbb{P}^1$ and $\mathbb{P}^1 \times \{P\}$ are lines in $\mathbb{P}^3$ lying on Q.

iii. Show that all lines in $\mathbb{P}^3$ lying on Q can be obtained in this way (hint: choose points (A_1, A_2) and (B_1, B_2) in $\mathbb{P}^1 \times \mathbb{P}^1$ and verify that the line through $\Psi((A_1, A_2))$ and $\Psi((B_1, B_2))$ lies on Q if and only if $A_1 = B_1$ or $A_2 = B_2$).

iv. For any pair of lines L_1, L_2 lying on Q determine their intersection $L_1 \cap L_2$.

v. Draw a picture of Q.

vi. Describe all closed subsets of $\mathbb{P}^1 \times \mathbb{P}^1$ with the product topology.

vii. Show that Ψ is not continuous when $\mathbb{P}^1 \times \mathbb{P}^1$ is equipped with the product topology and Q is equipped with the induced topology from $\mathbb{P}^3$.

In fact, as we will see later, the induced topology on Q, and *not* the product topology, is the "right one" for the product $\mathbb{P}^1 \times \mathbb{P}^1$.

Lecture 4

Regular functions and algebraic varieties

In this lecture we discuss Section I.3 of [Hart], and more. We advise the reader to read that section for her/himself. As usual, k is an algebraically closed field.

4.1 Regular functions on closed subsets of $\mathbb{A}^n$

It is now time to make geometric objects of the closed subsets of $\mathbb{A}^n$ and $\mathbb{P}^n$ that we have seen so far: until now they are just topological spaces, and moreover, the topology is quite weird. The difference between topology and differential geometry comes from the kind of functions that are allowed: continuous versus differentiable. In algebraic geometry, the functions chosen are called "regular."

Lemma 4.1.1 *For $f \in k[x_1, \ldots, x_n]$ we set $D(f) := \{P \in \mathbb{A}^n : f(P) \neq 0\} = \mathbb{A}^n - Z(f)$, so the $D(f)$ are open in the Zariski topology. The set of all $D(f)$ is a basis for the Zariski topology on $\mathbb{A}^n$.*

The proof is left to the reader in Exercise 4.4.1.

Definition 4.1.2 Let $n \in \mathbb{Z}_{\geq 0}$, $Y \subset \mathbb{A}^n$ closed, $V \subset Y$ open (for the induced topology on Y), and $f\colon V \to k$ a function. Then, for $P \in V$, f is called *regular at* P if there is an open subset $U \subset \mathbb{A}^n$ with $P \in U$, and elements $g, h \in k[x_1, \ldots, x_n]$ such that for all $Q \in U$, $h(Q) \neq 0$ and for all $Q \in U \cap V$: $f(Q) = g(Q)/h(Q)$. A function $f\colon V \to k$ is called *regular* if it is regular at all $P \in V$.

The set of regular functions on $V \subset Y$ is denoted by $\mathcal{O}_Y(V)$. It is a k-algebra for point-wise addition and multiplication. We have made the topological space Y into a "ringed space," and $\mathcal{O}_Y$ is called the "sheaf of regular functions on Y."

Lemma 4.1.3 *Let X be a topological space, and Y a subset of X. Then Y is closed if and only if X can be covered by open subsets $U_i \subset X$ such that for all i, $Y \cap U_i$ is closed in U_i.*

Proof Assume that Y is closed; just take the covering $\{X\}$. Conversely, if, for all i, $Y \cap U_i$ is closed in U_i then every point in the complement $X - Y$ has an open neighborhood in $X - Y$, hence Y is closed in X. $\square$

Lemma 4.1.4 *Let n be in $\mathbb{N}$, $Y \subset \mathbb{A}^n$ be closed, $V \subset Y$ be open, and $f \in \mathcal{O}_Y(V)$. Then $f\colon V \to k = \mathbb{A}^1$ is continuous.*

Proof Since k has the co-finite topology, it is enough to show that for any $a \in k$, $f^{-1}\{a\} \subset V$ is closed. By the previous lemma it is enough to give for every $P \in V$ an open $U \subset \mathbb{A}^n$ with $P \in U$ such that $f^{-1}\{a\} \cap U$ is closed in $U \cap V$. So let $P \in V$ be given and take an open $U \subset \mathbb{A}^n$ and g and h in $k[x_1, \ldots, x_n]$ as in Definition 4.1.2. Then for $Q \in U \cap V$ the condition $f(Q) = a$ is equivalent to $Q \in Z(g - ah)$. So $f^{-1}\{a\} \cap U = Z(g - ah) \cap (U \cap V)$, hence closed in $U \cap V$. □

Remark 4.1.5 Not all continuous $f\colon \mathbb{A}^1 \to k$ are regular. For example every permutation of k is a homeomorphism of $\mathbb{A}^1$.

Corollary 4.1.6 *Let $Y \subset \mathbb{A}^n$ be closed and irreducible, $V \subset Y$ open, non-empty, f and g in $\mathcal{O}_Y(V)$ such that $f|_U = g|_U$ for some open nonempty $U \subset V$. Then $f = g$.*

Proof Note that $f - g$ is regular, hence continuous by the previous lemma. So $(f - g)^{-1}\{0\}$ is closed. As $(f - g)^{-1}\{0\}$ contains U and V is irreducible, $(f - g)^{-1}\{0\}$ is dense in V, hence equal to V. □

The following theorem generalizes Theorem I.3.2(a) of [Hart].

Theorem 4.1.7 *Let n be in $\mathbb{Z}_{\geq 0}$ and let $Y \subset \mathbb{A}^n$ be closed. Then the k-algebra morphism φ from $A := k[x_1, \ldots, x_n]$ to $\mathcal{O}_Y(Y)$ that sends a polynomial to the function that it defines is surjective and has kernel $I(Y)$, the ideal of Y. Hence it induces an isomorphism from $A/I(Y) = A(Y)$ to $\mathcal{O}_Y(Y)$.*

Proof By definition $\ker(\varphi) = \{f \in A : \forall P \in Y,\ f(P) = 0\} = I(Y)$. So we only need to prove the surjectivity of φ, the rest follows immediately.

Let $f \in \mathcal{O}_Y(Y)$. We want to show that f is in $\operatorname{im}(\varphi)$, or, equivalently, that its class $\overline{f}$ in the quotient A-module $\mathcal{O}_Y(Y)/\operatorname{im}(\varphi)$ is zero. Let $J \subset A$ be the annihilator of $\overline{f}$, that is, $J = \{h \in A : \varphi(h)f \in \operatorname{im}(\varphi)\}$. Then J is an ideal. We want to show that $1 \in J$, or, equivalently, that $J = A$. Note that $I(Y) \subset J$ since for $h \in I(Y)$ we have $hf = \varphi(h)f = 0 \cdot f = 0$.

Suppose that $J \neq A$. Take $\mathfrak{m} \subset A$ a maximal ideal such that $J \subset \mathfrak{m}$. By the Nullstellensatz there is a $P \in \mathbb{A}^n$ such that $\mathfrak{m} = \mathfrak{m}_P$, the maximal ideal corresponding to P. As $I(Y) \subset J \subset \mathfrak{m}_P$, we have $P \in Y$. Since f is a regular function on Y we can take h_1, h_2, g_2 in A such that

- $P \in D(h_1)$,
- for all $Q \in D(h_1)$ we have $h_2(Q) \neq 0$,
- for all $Q \in D(h_1) \cap Y$ we have $f(Q) = g_2(Q)/h_2(Q)$.

Then $\varphi(h_2)f = \varphi(g_2)$ on $D(h_1) \cap Y$. Hence $\varphi(h_1h_2)f = \varphi(h_1g_2)$ on Y (both are zero on $Y \cap Z(h_1)$), and $\varphi(h_1h_2)f$ is in $\operatorname{im}(\varphi)$. So $h_1h_2 \in J$. But $(h_1h_2)(P) = h_1(P)h_2(P) \neq 0$ (by construction), this gives a contradiction. Hence $J = A$ and we are done. □

4.2 Regular functions on closed subsets of $\mathbb{P}^n$

We also make closed subsets of $\mathbb{P}^n$ into ringed spaces. First we do this for $\mathbb{P}^n$ itself. Let $A = k[x_0, \ldots, x_n]$.

Definition 4.2.1 Let $U \subset \mathbb{P}^n$ be open, $f\colon U \to k$, $P \in U$. Then f is called *regular at* P if there exists a $d \in \mathbb{Z}_{\geq 0}$, $g, h \in A_d$ such that $h(P) \neq 0$ and $f = g/h$ in a neighborhood of P. (Note that for $Q \in \mathbb{A}^{n+1}$ with $h(Q) \neq 0$ and $\lambda \in k^\times$: $(g/h)(\lambda Q) = g(\lambda Q)/h(\lambda Q) = \lambda^d g(Q)/\lambda^d h(Q) = (g/h)(Q)$.) Also, f is called *regular* if f is regular at all $P \in U$. Notation: $\mathcal{O}_{\mathbb{P}^n}(U) = \{f\colon U \to k : f \text{ is regular}\}$

Definition 4.2.2 Let $Y \subset \mathbb{P}^n$ be closed, $V \subset Y$ open, $f\colon V \to k$, and $P \in V$. Then f is called *regular at* P if there exists an open $U \subset \mathbb{P}^n$ and $g \in \mathcal{O}_{\mathbb{P}^n}(U)$ such that $P \in U$ and for all $Q \in V \cap U : f(Q) = g(Q)$.

Remark 4.2.3 For $Y \subset \mathbb{A}^n$ closed we could have done the same thing: first define $\mathcal{O}_{\mathbb{A}^n}$ and then continue as above.

Theorem 4.2.4 *(Generalises Theorem I.3.4(a) of [Hart]). Let $Y \subset \mathbb{P}^n$ be closed. Then*

$$\mathcal{O}_Y(Y) = \{f \colon Y \to k : f \text{ is locally constant.}\}$$

Proof We do not give a detailed proof. The proof of Theorem I.3.4(a) in [Hart] generalises as sketched as follows. Let f be in $\mathcal{O}_Y(Y)$. Let $C \subset \mathbb{A}^{n+1}$ be the cone of Y, that is, $C = q^{-1}Y \cup \{0\}$. Then $\mathcal{O}_C(C) = A(C)$ is graded, and for N sufficiently large multiplication by f preserves the finite dimensional subspace $A(C)_N$. Therefore f satisfies a polynomial equation over k, and can only take finitely many values. As f is continuous, it is locally constant. □

4.3 The category of algebraic varieties

Now we get at a point where we really must introduce morphisms. For example, we want to compare $U_i \subset \mathbb{P}^n$ with $\mathbb{A}^n$ via the map $\varphi_i \colon U_i \to \mathbb{A}^n$ and we would like to call φ_i an isomorphism, so both φ_i and φ_i^{-1} should be morphisms. We know that φ_i and φ_i^{-1} are continuous. The idea is then to ask for a morphism to be a continuous function that, by composition, sends regular functions to regular functions. We formalize this as follows.

Definition 4.3.1 A *k-space* is a pair $(X, \mathcal{O}_X)$, with X a topological space, and for every $U \subset X$ open, $\mathcal{O}_X(U) \subset \{f \colon U \to k\}$ a sub-k-algebra such that:

i. for all $V \subset U$ (both open) and for all f in $\mathcal{O}_X(U)$, $f|_V$ is in $\mathcal{O}_X(V)$;

ii. for all U open and for all $f \colon U \to k$, f is in $\mathcal{O}_X(U)$ if and only if for all $P \in U$ there is an open $U_P \subset U$ such that $P \in U_P$ and $f|_{U_P}$ is in $\mathcal{O}_X(U_P)$.

We call this $\mathcal{O}_X$ the *sheaf of admissible functions*. The second condition in Definition 4.3.1 means that the "admissibility" condition is a local condition: a function verifies it if and only if it does so locally.

Examples 4.3.2 The $(Y, \mathcal{O}_Y)$ as defined above for closed subsets Y of $\mathbb{A}^n$ or $\mathbb{P}^n$ are k-spaces (they obviously satisfy both properties).

Definition 4.3.3 Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be k-spaces. A *morphism* from $(X, \mathcal{O}_X)$ to $(Y, \mathcal{O}_Y)$ is a map $\varphi \colon X \to Y$ such that:

i. φ is continuous;

ii. for all $U \subset Y$ open, for all $f \in \mathcal{O}_Y(U)$, $\varphi^* f \colon = f \circ \varphi \colon \varphi^{-1}U \to k$ is in $\mathcal{O}_X(\varphi^{-1}U)$.

Remark 4.3.4 Condition ii is equivalent to: for all P in X, for all $f \colon Y \to k$ regular at φP, $\varphi^* f$ is regular at P.

The k-spaces and their morphisms form a category: k-Spaces. This gives us the notion of an isomorphism: a morphism φ from $(X, \mathcal{O}_X)$ to $(Y, \mathcal{O}_Y)$ is an isomorphism if there is a morphism ψ from $(Y, \mathcal{O}_Y)$ to $(X, \mathcal{O}_X)$ with $\psi \circ \varphi = \mathrm{id}_{(X,\mathcal{O}_X)}$ and $\varphi \circ \psi = \mathrm{id}_{(Y,\mathcal{O}_Y)}$. For further theory on categories, one can see Lang's Algebra [Lang].

Remark 4.3.5 This category k-Spaces, which looks rather ad hoc, is also used by Springer in [Spri].

For $(X, \mathcal{O}_X)$ a k-space and U an open subset of X we define $\mathcal{O}_X|_U$, the restriction of $\mathcal{O}_X$ to U, by: for $V \subset U$ open, $\mathcal{O}_X|_U(V) = \mathcal{O}_X(V)$. We can now define what (very abstract) algebraic varieties are.

Definition 4.3.6 Let k be an algebraically closed field. An *algebraic variety over* k is a k-space $(X, \mathcal{O}_X)$ such that for all $x \in X$ there is an open $U \subset X$ with $x \in U$ such that $(U, \mathcal{O}_X|_U)$ is isomorphic (in k-Spaces) to a $(Y, \mathcal{O}_Y)$ with $Y \subset \mathbb{A}^n$ closed for some n, and $\mathcal{O}_Y$ the sheaf of regular functions (that is, is an *affine* algebraic variety over k). If $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ are algebraic varieties over k, a morphism from $(X, \mathcal{O}_X)$ to $(Y, \mathcal{O}_Y)$ is just a morphism in k-Spaces. The category of algebraic varieties over k is denoted $\mathrm{vaVar}(k)$. A variety is called *projective* if it is isomorphic to a $(Y, \mathcal{O}_Y)$ with Y a closed subset of some $\mathbb{P}^n$ and $\mathcal{O}_Y$ its sheaf of regular functions. A variety is called *quasi-projective* if it is isomorphic to an open subvariety of a projective variety.

Remark 4.3.7 Our notion of variety in $\mathrm{vaVar}(k)$ is much more general than that in the first chapter of [Hart]: those must be irreducible (which we don't suppose) and quasiprojective (which we don't suppose either). For those who would rather do schemes: $\mathrm{vaVar}(k)$ is equivalent to the category of k-schemes that are reduced, and locally of finite type.

Proposition 4.3.8 *(I.3.3 in [Hart]) Let $n \in \mathbb{Z}_{\geq 0}$, $i \in \{0, \ldots, n\}$, $U_i \subset \mathbb{P}^n$ as before, and $\varphi_i \colon U_i \to \mathbb{A}^n$ the map $(a_0 : \cdots : a_n)$ to $(a_0/a_i, \ldots, a_{i-1}/a_i, a_{i+1}/a_i, \ldots, a_n/a_i)$. Then φ_i is an isomorphism of k-spaces. Hence $\mathbb{P}^n$ is an algebraic variety.*

Proof We have already seen that φ_i and its inverse are continuous. It remains to be shown that the conditions "regular at P" and "regular at $\varphi_i(P)$" correspond, that is, for $f \colon U \to k$ with U a neighborhood of $\varphi_i(P)$, f is regular at $\varphi_i(P)$ if and only if $\varphi_i^* f$ is regular at P.

Let P be in U_i, and $U \subset \mathbb{A}^n$ open containing $\varphi(P)$, and $f \colon U \to k$ a function. Then f is regular at $\varphi_i(P)$ if and only if there exist $g, h \in k[\{x_{i,j} : j \neq i\}]$ such that $h(\varphi_i(P)) \neq 0$ and $f = g/h$ in a neighborhood of $\varphi_i(P)$.

The function $\varphi_i^* f$ is regular at P if and only if there exist $d \in \mathbb{Z}_{\geq 0}$ and $g', h' \in k[x_0, \ldots, x_n]_d$ such that $h'(P) \neq 0$ and $\varphi_i^* f = g'/h'$ in a neighborhood of P.

Suppose that f is a regular function at $\varphi_i(P)$, locally given by g/h. Let $d = \max(\deg(g), \deg(h))$ and notice that for a in a neighborhood of P

$$\begin{aligned}
(\varphi_i^*(g/h))(a_0 : \cdots : a_n) &= g(\varphi_i(a_0 : \cdots : a_n))/h(\varphi_i(a_0 : \cdots : a_n)) \\
&= g((a_j/a_i)_{j \neq i})/h((a_j/a_i)_{j \neq i}) \\
&= a_i^d g((a_j/a_i)_{j \neq i})/a_i^d h((a_j/a_i)_{j \neq i}) \\
&= (g'/h')(a_0 : \cdots : a_n)
\end{aligned}$$

where $g' = x_i^d g((x_j/x_i)_{j \neq i})$ and $h' = x_i^d h((x_j/x_i)_{j \neq i})$ are in $k[x_0, \ldots, x_n]_d$. Hence $\varphi_i^* f$ is regular at P.

Suppose now that $\varphi_i^* f$ is regular at P, locally given as g'/h' in $k[x_0, \ldots, x_n]_d$ for some d. Then f is locally given by g/h with $g = x_i^{-d} g'$ and $h = x_i^{-d} h'$, showing that f is regular at $\varphi_i(P)$. □

Corollary 4.3.9 *Let $Y \subset \mathbb{P}^n$ be closed, then $(Y, \mathcal{O}_Y)$ is an algebraic variety.*

Proof This follows since for each i, $(Y_i, \mathcal{O}_Y|_{Y_i})$ with $Y_i = U_i \cap Y$ is an algebraic variety by the above theorem. □

Corollary 4.3.10 *We have $\mathcal{O}_{\mathbb{P}^n}(U_i) = k[x_{i,j} : i \neq j]$.*

We will now prove some things which will be useful later.

Proposition 4.3.11 *(Compare with I.3.6 in [Hart].) Let X be an algebraic variety, $U \subset X$ an open subset with its induced topology and regular functions, let $Y \subset \mathbb{A}^n$ closed, and let $\psi\colon U \to Y$ a map of sets. For i in $\{1, \ldots, n\}$ let $\psi_i = \mathrm{pr}_i \circ \psi$, hence for all P in U, $\psi(P) = (\psi_1(P), \ldots, \psi_n(P))$. Then ψ is a morphism if and only if for all i, ψ_i is in $\mathcal{O}_U(U)$.*

Proof Assume that ψ is a morphism. Let i be in $\{1, \ldots, n\}$. The restriction of the function $x_i\colon \mathbb{A}^n \to k$ to Y is in $\mathcal{O}_Y(Y)$ and we denote it still by x_i. Then $\psi_i = \psi^*(x_i)$ is in $\mathcal{O}_U(U)$.

Assume that all ψ_i are regular. We have to show that ψ is a morphism. We start with showing that ψ is continuous. For f in $k[x_1, \ldots, x_n]$, $\psi^* f$ is the function $P \mapsto f(\psi_1(P), \ldots, \psi_n(P))$, hence $\psi^* f = f(\psi_1, \ldots, \psi_n)$, the image in $\mathcal{O}_U(U)$ of f under the k-algebra morphism that sends x_i to ψ_i. Hence for all f in $k[x_1, \ldots, x_n]$ we have:

$$\psi^{-1} Z(f) = \{P \in U : f(\psi(P)) = 0\} = (\psi^* f)^{-1}\{0\}.$$

Now $\psi^* f \in \mathcal{O}_U(U)$ is continuous, because continuity is a local property and by Lemma 4.1.4 $\psi^* f$ is continuous at every P in X.

Now we show that ψ is a morphism. Let $V \subset Y$ be open and $f \in \mathcal{O}_Y(V)$. We must show that $\psi^* f\colon \psi^{-1}V \to k$ is in $\mathcal{O}_U(\psi^{-1}V)$. This is a local property by the second part of Definition 4.3.1. We must show that for all P in $\psi^{-1}V$, $\psi^* f$ is regular at P. So let P be in $\psi^{-1}(V)$. Write $f = g/h$ in a neighborhood of $\psi(P)$, with g and h in $k[x_1, \ldots, x_n]$. Then $\psi^* f = g(\psi_1, \ldots, \psi_n)/h(\psi_1, \ldots, \psi_n)$ in a neighborhood of P, hence a quotient of the two elements $g(\psi_1, \ldots, \psi_n)$ and $h(\psi_1, \ldots, \psi_n)$ in $\mathcal{O}_X(U)$, with $(h(\psi_1, \ldots, \psi_n))P = h(\psi(P)) \neq 0$. Hence, by Definition 4.1.2, $\psi^* f$ is regular at P. $\square$

We have the following theorem, which is needed for the exercises below. The proof will be given in the next lecture, see Corollary 5.1.6.

Theorem 4.3.12 *Let $Y \subset \mathbb{A}^n$ be closed, $h \in k[x_1, \ldots, x_n]$, and let V the intersection $Y \cap D(h)$. Then $(V, \mathcal{O}_Y|_V)$ is an affine variety, that is, isomorphic to a closed subset of some $\mathbb{A}^m$ with its regular functions.*

4.4 Exercises

Exercise 4.4.1 Prove Lemma 4.1.1.

Exercise 4.4.2 Let $n \in \mathbb{N}$. For $d \in \mathbb{N}$ and $f \in A_d$ ($A = k[x_0, \ldots, x_n]$) let $D_+(f) := \{a \in \mathbb{P}^n \mid f(a) \neq 0\}$. Show that the set of all $D_+(f)$ is a basis for the topology on $\mathbb{P}^n$.

Exercise 4.4.3 Let $\mathrm{pt} = \mathbb{A}^0$. Let X be a variety. Show that all maps of sets $\mathrm{pt} \to X$ and $X \to \mathrm{pt}$ are morphisms.

Exercise 4.4.4 Let X be a variety, and $U \subset X$ an open subset, equipped with the induced topology. Show that $(U, \mathcal{O}_X|_U)$ is a variety and that the inclusion map $j\colon U \to X$ is a morphism. (Hint: you can use Theorem 4.3.12.) We call U an open subvariety of X. Let $(Z, \mathcal{O}_Z)$ be a variety and $f\colon Z \to U$ a map of sets. Show that f is a morphism if and only if $j \circ f$ is a morphism.

Exercise 4.4.5 Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be varieties, and $f\colon X \to Y$ a map of sets. Show that f is a morphism if and only if for each $x \in X$ there are open subsets $U \subset X$ and $V \subset Y$ such that $x \in U$, $fU \subset V$, and $f|_U\colon (U, \mathcal{O}_X|_U) \to (V, \mathcal{O}_Y|_V)$ is a morphism.

Exercise 4.4.6 Let $n \in \mathbb{N}$, and let $a_1, \ldots, a_n$ be distinct elements of k. Show that the union of $\{x^i : i \in \mathbb{N}\}$ and $\{(x - a_j)^{-l} : j \in \{1, \ldots, n\}$ and $l \in \mathbb{Z}_{>0}\}$ is a basis of the k-vector space $\mathcal{O}_{\mathbb{A}^1}(\mathbb{A}^1 - \{a_1, \ldots, a_n\})$. Give also a basis for $\mathcal{O}_{\mathbb{P}^1}(\mathbb{P}^1 - \{a_1, \ldots, a_n\})$. (Hint: prove that every regular function on a non-empty open subset of $\mathbb{A}^1$ is uniquely represented as g/h with g and h in $k[x]$ relatively prime and h monic.)

Exercise 4.4.7 Let X be a variety, and $Y \subset X$ a closed subset, equipped with the induced topology. For $V \subset Y$ open, $f\colon V \to k$, and $P \in V$, we define f to be regular at P if and only if there is an open $U \subset X$ and a $g \in \mathcal{O}_X(U)$ such that $P \in U$, and for all $Q \in V \cap U$, $f(Q) = g(Q)$. Notation: $\mathcal{O}_Y(V)$. Show that $(Y, \mathcal{O}_Y)$ is a variety and that the inclusion map $i\colon Y \to X$ is a morphism. We call Y a closed subvariety of X. Let $(Z, \mathcal{O}_Z)$ be a variety and $f\colon Z \to Y$ a map of sets. Show that f is a morphism if and only if $i \circ f$ is a morphism.

Exercise 4.4.8 Do Exercise I.3.4 of [Hart] for $n = 1$ and $d = 2$. Hint: do not do all of [Hart], Exercise I.2.12, but use as much as you can the exercises above (4.4.4, 4.4.5 and 4.4.7). So, just show that the image Y of $\varphi\colon \mathbb{P}^1 \to \mathbb{P}^2$ is closed (by giving equations for it), and show that the inverse $\psi\colon Y \to \mathbb{P}^1$, on suitable standard open subsets, is given by the inclusion followed by a projection.

Exercise 4.4.9 Let $X \subset \mathbb{A}^2$ be the zero set of the polynomial $x^2 - y^3$. Consider the map of sets $\varphi\colon \mathbb{A}^1 \to X$ given by $t \mapsto (t^3, t^2)$. Show that φ is a morphism of algebraic varieties. Show that φ is bijective. Show that φ is not an isomorphism of algebraic varieties.

Exercise 4.4.10 Give an example of two affine varieties X, Y and a morphism $\varphi\colon X \to Y$ such that the image of φ is not locally closed in Y. Recall that a subset Z of a topological space is called locally closed if Z is the intersection of an open subset and a closed subset of X.

Lecture 5

The category of algebraic varieties (continued)

Here are some references for categories, functors, equivalence of categories:

i. the wikipedia pages *category*, *functor*, *equivalence of categories*;

ii. the section “categories and functors” in Lang’s book “Algebra”;

iii. the chapter “Categorieën en functoren” in [Stev].

5.1 Affine varieties

Definition 5.1.1 A variety $(Y, \mathcal{O}_Y)$ is called *affine* if there is an $n \in \mathbb{Z}_{\geq 0}$ and $Z \subset \mathbb{A}^n$ closed such that $(Y, \mathcal{O}_Y) \cong (Z, \mathcal{O}_Z)$ where $\mathcal{O}_Z$ is the sheaf of regular functions on Z.

Suppose $\varphi\colon (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is a morphism of k-spaces. Then we obtain a map φ^* from $\mathcal{O}_Y(Y)$ to $\mathcal{O}_X(X)$, $f \mapsto f \circ \varphi$. This φ^* is a morphism of k-algebras, for example, for every P in X,

$$(\varphi^*(f+g))P = (f+g)(\varphi P) = f(\varphi P) + g(\varphi P) = (\varphi^* f)P + (\varphi^* g)P = (\varphi^* f + \varphi^* g)P.$$

This procedure *is* a contravariant functor from the category k-Spaces to that of k-algebras, sending an object $(X, \mathcal{O}_X)$ to $\mathcal{O}_X(X)$, and a morphism $\varphi\colon X \to Y$ to $\varphi^*\colon \mathcal{O}_Y(Y) \to \mathcal{O}_X(X)$. Indeed, for $\varphi\colon (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ and $\psi\colon (Y, \mathcal{O}_Y) \to (Z, \mathcal{O}_Z)$ in k-Spaces, we get $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.

Proposition 5.1.2 *Let X be a variety and Y an affine variety. Then the map*

$$\mathrm{Hom}_{\mathrm{vaVar}(k)}(X, Y) \to \mathrm{Hom}_{k-\mathrm{algebras}}(\mathcal{O}_Y(Y), \mathcal{O}_X(X)), \quad \varphi \mapsto \varphi^*$$

is a bijection.

Proof We may and do assume that Y is a closed subset of $\mathbb{A}^n$, with its sheaf of regular functions, as Y is isomorphic to such a k-space. We construct an inverse of $\varphi \mapsto \varphi^*$. So let $h\colon \mathcal{O}_Y(Y) \to \mathcal{O}_X(X)$ be a k-algebra morphism. We have $k[x_1, \ldots, x_n] \to \mathcal{O}_Y(Y)$, surjective, and with kernel $I := I(Y)$, see Theorem 4.1.7. Let $\tilde{h}\colon k[x_1, \ldots, x_n] \to \mathcal{O}_X(X)$ be the composition of this morphism with h. Let $\psi_i := \tilde{h}(x_i)$. Let $\psi\colon X \to \mathbb{A}^n$ be the map $P \mapsto (\psi_1(P), \ldots, \psi_n(P))$. Then ψ is a morphism of varieties by Proposition 4.3.11. We claim that $\psi(X)$ is contained in Y. Indeed, for $P \in X$ we have the following commuting diagram (where eval_P is the k-algebra morphism which evaluates a function from X to k in P):

$$\begin{tikzcd} k[x_1,\ldots,x_n] \arrow[r, "\tilde{h}"] \arrow[dr, "\mathrm{eval}_P \circ \tilde{h}"'] & \mathcal{O}_X(X) \arrow[d, "\mathrm{eval}_P"] \\ & k. \end{tikzcd}$$

We see that $\mathrm{eval}_P \circ \tilde{h}$ is the composition of two k-algebra morphisms, hence a k-algebra morphism. So as $x_i \mapsto \psi_i \mapsto \psi_i(P)$, f in $k[x_1,\ldots,x_n]$ goes to $f(\psi_1(P),\ldots,\psi_n(P))$. Hence for f in $I(Y)$ and P in X we have:

$$f(\psi(P)) = f(\psi_1(P),\ldots,\psi_n(P)) = (\mathrm{eval}_P \circ \tilde{h})f = \mathrm{eval}_P(\tilde{h}f) = \mathrm{eval}_P(0) = 0.$$

We will now check that the two given maps are inverse to each other. We will write ψ_h for the map $\psi : X \to Y$ obtained in the previous part of this proof for $h\colon \mathcal{O}_Y(Y) \to \mathcal{O}_X(X)$.

Let $\varphi : X \to Y$ be a morphism in $\mathrm{vaVar}(k)$. Then we have, for all $P \in X$:

$$\psi_{\varphi^*}(P) = ((\varphi^* x_1)P,\ldots,(\varphi^* x_n)P) = (x_1(\varphi P),\ldots,x_n(\varphi P)) = \varphi(P).$$

This shows that $\psi_{\varphi^*} = \varphi$.

For h in $\mathrm{Hom}_{k-\mathrm{algebra}}(\mathcal{O}_Y(Y), \mathcal{O}_X(X))$ and $P \in X$ we have, writing x_i for its image in $\mathcal{O}_Y(Y)$:

$$(\psi_h^* x_i)(P) = x_i(\psi_h P) = x_i((hx_1)P,\ldots,(hx_n P)) = (hx_i)P.$$

Hence $(\psi_h)^*$ and h have the same value on each x_i, hence are equal (the x_i generate $\mathcal{O}_Y(Y)$). □

Remark 5.1.3 Let $(X,\mathcal{O}_X)$ be an affine variety, closed in some $\mathbb{A}^n$. Then $\mathcal{O}_X(X) = A(X)$ by Theorem 4.1.7. Hence the k-algebra $\mathcal{O}_X(X)$ is reduced and finitely generated. On the other hand, by Exercise 1.6.12 every reduced finitely generated k-algebra occurs as $A(Y)$ for some closed Y in some $\mathbb{A}^n$. Actually, we have a bit more, as the following theorem tells us.

Theorem 5.1.4 *We have the following anti-equivalence of categories:*

$$\begin{array}{rcl} \{\textit{affine varieties}\} & \to & \{\textit{reduced } k\textit{-algebras of finite type}\} \\ (X,\mathcal{O}_X) & \mapsto & \mathcal{O}_X(X) \\ \varphi & \mapsto & \varphi^* \end{array}$$

Proof For the reader who knows some category theory: a functor is an equivalence of categories if and only if it is fully faithful and essentially surjective. By Proposition 5.1.2 we see that the functor is fully faithful, and the remarks above tell us that it is essentially surjective. □

This theorem basically tells us that "the only categorical difference between the two categories is the direction of the arrows".

We will now start proving Theorem 4.3.12.

Theorem 5.1.5 *Let $f \in k[x_1,\ldots,x_n]$. Then $(D(f), \mathcal{O}_{\mathbb{A}^n}|_{D(f)})$ is an affine variety.*

Proof Consider the closed subset $Z := Z(x_{n+1}f - 1) \subset \mathbb{A}^{n+1}$. Then we have the following maps:

$$D(f) \to Z, \quad (a_1,\ldots,a_n) \mapsto \left(a_1,\ldots,a_n,\frac{1}{f(a_1,\ldots,a_n)}\right)$$

and

$$Z \to D(f), \quad (a_1, \ldots, a_n, a_{n+1}) \mapsto (a_1, \ldots, a_n)$$

These maps are inverses of each other. Both maps are morphisms since they are given by regular functions (Proposition 4.3.11). So $D(f)$ is an affine variety and $\mathcal{O}_{D(f)}(D(f)) \cong k[x_1, \ldots, x_{n+1}]/(x_{n+1}f - 1)$. $\square$

We now easily obtain the following corollaries, the first of which is a strengthening of Theorem 4.3.12:

Corollary 5.1.6 *Let $X = Z(g_1, \ldots, g_r) \subset \mathbb{A}^n$ be a closed subset, and let f be in $k[x_1, \ldots, x_n]$. Then $(X \cap D(f), \mathcal{O}|_{X \cap D(f)})$ is an affine variety isomorphic to $Z(g_1, \ldots, g_r, x_{n+1}f - 1) \subset \mathbb{A}^{n+1}$ with its regular functions.*

Corollary 5.1.7 *Every variety has a basis for the topology consisting of affine open subvarieties.*

5.2 Products of varieties

This is a special case of Theorem II.3.3 of [Hart]. We will first construct products in the affine case. Let $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ be closed. Let $I = I(X)$ and let $f_1, \ldots, f_a$ in $k[x_1, \ldots, x_m]$ be a system of generators. Similarly, let $J = I(Y)$ with system of generators $g_1, \ldots, g_b$ in $k[y_1, \ldots, y_n]$.

Lemma 5.2.1 *In this situation, $X \times Y \subset \mathbb{A}^{m+n}$ is closed, and $I(X \times Y)$ is generated by the subset $\{f_1, \ldots, f_a, g_1, \ldots, g_b\}$ of $k[x_1, \ldots, x_m, y_1, \ldots, y_n]$.*

Proof We have $X \times Y = Z(f_1, \ldots, f_a, g_1, \ldots, g_b)$, hence $X \times Y$ is closed in $\mathbb{A}^{m+n}$. We must show that $f_1, \ldots, f_a, g_1, \ldots, g_b$ generate $I(X \times Y)$. Showing this is equivalent to showing that the k-algebra morphism

$$\varphi\colon k[x_1, \ldots, x_m, y_1, \ldots, y_n]/(f_1, \ldots, f_a, g_1, \ldots, g_b) \longrightarrow A(X \times Y)$$

is an isomorphism. The morphism φ is surjective because the images of x_i and y_j generate $A(X \times Y)$. Let us show that φ is injective. We have

$$k[x_1, \ldots, x_m, y_1, \ldots, y_n]/(f_1, \ldots, f_a) = A(X)[y_1, \ldots, y_n].$$

Let h be in $A(X)[y_1, \ldots, y_n]$ such that its image in $A(X \times Y)$ is zero. Write $h = \sum_{i=1}^{p} a_i h_i$ with a_i in $A(X)$ and h_i in $k[y_1, \ldots, y_n]$. By choosing a basis of the sub-k-vector space of $A(X)$ generated by the a_i, and expressing the a_i as k-linear combinations of the elements of that basis, we may and do assume that the a_i are k-linearly independent. For each Q in Y we have $0 = \sum_{i=1}^{p} a_i h_i(Q)$ in $A(X)$, implying that for each Q in Y and each i we have $h_i(Q) = 0$ in k. So, for each i, h_i is in $I(Y)$, and therefore h is in the ideal of $A(X)[y_1, \ldots, y_n]$ that is generated by $g_1, \ldots, g_b$. $\square$

Definition 5.2.2 For closed subvarieties $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ as above, we let $\mathcal{O}_{X \times Y}$ be the sheaf of regular functions on $X \times Y$ induced from those on $\mathbb{A}^{m+n}$. This makes $X \times Y$ into an affine variety.

Example 5.2.3 Consider $\mathbb{A}^m \times \mathbb{A}^n = \mathbb{A}^{m+n}$. Note that the Zariski topology is larger than the product topology. For example, the diagonal in $\mathbb{A}^2$ is not closed in the product topology on $\mathbb{A}^2 = \mathbb{A}^1 \times \mathbb{A}^1$.

Remark 5.2.4 For those who know tensor products of k-algebras. In the situation of Definition 5.2.2 we have:

$$\mathcal{O}_{X \times Y}(X \times Y) = k[x_1, \ldots, x_m, y_1, \ldots, y_n]/(f_1, \ldots, f_a, g_1, \ldots, g_b) = \mathcal{O}_X(X) \otimes_k \mathcal{O}_Y(Y).$$

The statement that, for k an algebraically closed field, the tensor product of two reduced k-algebras is reduced requires a non-trivial proof. In fact, if k is not perfect then such a statement is false.

Remark 5.2.5 The projections $p_X : X \times Y \to X$, and $p_Y : X \times Y \to Y$ are morphisms. This follows from Proposition 4.3.11.

Theorem 5.2.6 *(Universal property of the product) Let X and Y be affine varieties and Z a variety. Let $f : Z \to X$ and $g : Z \to Y$ be morphisms. Then there exists a unique morphism $h : Z \to X \times Y$ such that $p_X \circ h = f$ and $p_Y \circ h = g$. This means that we have the following commutative diagram:*

$$\begin{tikzcd}
 & & X \\
Z \arrow[r, dotted, "\exists ! h"] \arrow[urr, bend left, "f"] \arrow[drr, bend right, "g"'] & X \times Y \arrow[ur, "p_X"] \arrow[dr, "p_Y"] & \\
 & & Y.
\end{tikzcd}$$

Proof For h as a map of sets, there is a unique solution, namely for $P \in Z$ we set $h(P) = (f(P), g(P))$. This map is a morphism by Proposition 4.3.11. $\square$

Corollary 5.2.7 *The topology on $X \times Y$ and the sheaf $\mathcal{O}_{X \times Y}$ do not depend on the embeddings of X and Y in affine spaces.*

Proof The proof goes as follows. Suppose we have another product with the same universal property, say $(X \times Y)'$ with projections p'_X and p'_Y, obtained from other closed embeddings of X and Y in affine spaces. This means that $(X \times Y)'$ is, as a set, $X \times Y$, but with maybe another topology and another sheaf of regular functions. We apply the universal property in the following situation:

$$\begin{tikzcd}
 & & X \\
(X \times Y)' \arrow[r, dotted, "\exists ! h"] \arrow[urr, bend left, "p'_X"] \arrow[drr, bend right, "p'_Y"'] & X \times Y \arrow[ur, "p_X"] \arrow[dr, "p_Y"] & \\
 & & Y
\end{tikzcd}$$

and conclude that the identity map of sets of $X \times Y$ to itself is a morphism of varieties from $(X \times Y)'$ to $X \times Y$. By symmetry, the same holds for the identity map of sets from $X \times Y$ to $(X \times Y)'$. $\square$

Now let X and Y be arbitrary varieties. We will construct the product variety $X \times Y$ as follows. As a set, just take $X \times Y$. Let T be the set of subsets W that are open in some $U \times V$ where $U \subset X$ and $V \subset Y$ are open and affine and where $U \times V$ has the Zariski topology as defined above. Then for all W and W' in T the intersection $W \cap W'$ is a union of elements of T. Therefore the unions of subsets of T are the open sets for a topology on $X \times Y$ that we call the Zariski topology, and T is a basis for that topology. We define the notion of regular functions. We only need to do this on the basis T above (since a function is regular iff it is locally regular). A function $W \to k$ (with W as above) is regular if it is regular as a function on W as open subset of $U \times V$ with U open affine in X and V open affine in Y (this does not depend on U and V as long as $U \times V$ contains W).

Theorem 5.2.8 *The projections p_X and p_Y are morphisms and the product $X \times Y$ with its projections has the universal property (as in the affine case).*

Proof Apply Exercise 4.4.5 to see that we only need to prove it locally. The local case follows by Theorem 5.2.6. $\square$

Theorem 5.2.9 *The product of projective varieties is a projective variety.*

Proof Exercise 6.7.1. $\square$

5.3 Not all curves can be parametrised

Although not necessary for the development of the theory in this syllabus, we include this section in order to illustrate an essential point in the theory of algebraic varieties. We defined algebraic varieties as k-spaces that are locally isomorphic to algebraic subsets of affine spaces. Smooth manifolds can be defined as $\mathbb{R}$-spaces that are locally isomorphic to $(\mathbb{R}^n, \mathcal{O})$ with $\mathcal{O}(U)$ the set of smooth functions $f\colon U \to \mathbb{R}$. Complex manifolds can be defined as $\mathbb{C}$-spaces that are locally isomorphic to $(U, \mathcal{O})$ with U open in $\mathbb{C}^n$ for some n, and $\mathcal{O}$ the sheaf of holomorphic complex functions. One *could* think that in algebraic geometry (over $k = \overline{k}$) defining algebraic manifolds as k-spaces that are locally isomorphic to open pieces of affine spaces gives all non-singular algebraic varieties. But that is far from true. There is no implicit function theorem for polynomial or rational functions.

The next theorem shows that no Fermat curve over $\mathbb{C}$ of degree at least 3 has a non-empty open subset that is isomorphic to an open subset of $\mathbb{A}^1$. Indeed, let n be in $\mathbb{Z}_{\geq 3}$ and $C := Z(x_0^n + x_1^n - x_2^n)$ in $\mathbb{P}^2$ over $\mathbb{C}$. Let $U \subset C$ be a non-empty open subset of $\mathbb{P}^1$ and let $\varphi\colon U \to C$ be a morphism. We claim that φ is constant. We may assume that U is affine, and that $\varphi(U)$ is contained in $C \cap D_+(x_2)$. Then $\varphi\colon U \to Z(x^n + y^n - 1) \subset \mathbb{A}^2$ is a morphism between affine varieties and corresponds to $\varphi^*\colon \mathbb{C}[x,y]/(x^n + y^n - 1) \to \mathcal{O}(U) \subset \mathbb{C}(t)$. Then there are relatively prime a, b and c in $\mathbb{C}[t]$ ($\gcd(a,b,c) = 1$), all three non-zero, such that $\varphi^*(x) = a/c$ and $\varphi^*(y) = b/c$. By the next theorem, a, b and c are constant.

Theorem 5.3.1 *Let n be in $\mathbb{Z}_{\geq 3}$. If a, b and c in $\mathbb{C}[t]$ satisfy $a^n + b^n = c^n$ and are relatively prime, then a, b and c are of degree zero, that is, are in $\mathbb{C}$.*

Proof The method is called “infinite descent,” and is due to Fermat. Let us suppose that there are a, b and c in $\mathbb{C}[t]$, relatively prime and not all constant, satisfying $a^n + b^n = c^n$. Then we may and do assume that the maximum of the degrees of a, b and c is minimal. We note that a, b and c are pairwise relatively prime, all non-zero and that at most one of them is constant. We have:

$$a^n = c^n - b^n = \prod_{\{\zeta : \zeta^n = 1\}} (c - \zeta b).$$

The factors $c - \zeta b$ are pairwise relatively prime, because each pair among them is a basis of the sub-$\mathbb{C}$-vector space of $\mathbb{C}[t]$ generated by b and c (note that this subspace is of dimension two because b and c are non-zero, relatively prime and not both constant). By the unique factorisation in $\mathbb{C}[t]$, we obtain that the $c - \zeta b$ are, up to units, nth powers. But as the units in $\mathbb{C}[t]$ are the non-zero constants, they are themselves nth powers. Hence there exist x_ζ in $\mathbb{C}[t]$ such that

$$c - \zeta b = x_\zeta^n.$$

As the $c - \zeta b$ are pairwise relatively prime, so are the x_ζ. Looking at the leading terms of c and of b, one sees that at most one of the x_ζ is constant. Let us now take any triple x, y, and z among the x_ζ (this is possible because n is at least 3). As x^n, y^n and z^n are in the sub-$\mathbb{C}$-vector space of $\mathbb{C}[t]$ generated by b and c, there is a non-trivial linear relation between them, say:

$$\alpha x^n + \beta y^n = \gamma z^n,$$

with α, β and γ in $\mathbb{C}$, not all zero. As x, y and z are pairwise relatively prime, α, β and γ are all non-zero. As each element of $\mathbb{C}$ is an nth power, we find, choosing nth roots of α, β and γ, a relation:

$$x_1^n + y_1^n = z_1^n,$$

with x_1, y_1 and z_1 pairwise relatively prime, not all constant, and of the same degree as x, y and z, respectively. But that contradicts the minimality in terms of the degrees of (a, b, c) that we started with. □

5.4 Exercises

Exercise 5.4.1 Show that $\mathbb{P}^n$ is not affine if $n > 0$. (Use Theorem 4.2.4.)

Exercise 5.4.2 Let $f\colon X \to Y$ be a morphism of affine varieties and assume that the corresponding morphism of k-algebras $f^*\colon \mathcal{O}_Y(Y) \to \mathcal{O}_X(X)$ is surjective. Show that f is injective, that fX is closed in Y and that f defines an isomorphism of X to the closed subvariety fX of Y.

Exercise 5.4.3 Let $f\colon X \to Y$ be a morphism of affine varieties and assume that the corresponding morphism of k-algebras $f^*\colon \mathcal{O}_Y(Y) \to \mathcal{O}_X(X)$ is injective. Show that fX is dense in Y. Give an example with $fX \neq Y$.

Exercise 5.4.4 Assume $\mathrm{char}(k) \neq 2$. Give an isomorphism between $\mathbb{P}^1$ and $Z(x^2 + y^2 - z^2) \subseteq \mathbb{P}^2$. Parametrise all integer solutions to the equation $x^2 + y^2 = z^2$.

Exercise 5.4.5 Let q and n be positive integers. Show that

$$f\colon \mathbb{P}^n \to \mathbb{P}^n, \quad (a_0 : \cdots : a_n) \mapsto (a_0^q : \cdots : a_n^q)$$

is a morphism of varieties. Assume now that k has characteristic $p > 0$ and that $q = p^d$ for some integer $d > 0$. Show that f is bijective but not an isomorphism of varieties. Find all $P \in \mathbb{P}^n$ such that $f(P) = P$.

Exercise 5.4.6 Let $n > m$. Show that any morphism $\mathbb{P}^n \to \mathbb{P}^m$ is constant.

Lecture 6

Presentations, smooth varieties and rational functions

6.1 Separated varieties

(Compare with Section II.4 of [Hart].)

The following lemma from topology will only serve to motivate what follows.

Lemma 6.1.1 *Let X be a topological space, and $\Delta \subset X \times X$ be the diagonal, that is, Δ is the subset $\{(x,x) : x \in X\} \subset X \times X$. We give $X \times X$ the product topology. Then X is Hausdorff if and only if $\Delta \subset X \times X$ is closed.*

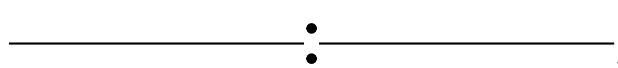
Proof Let $x, y \in X$ with $x \neq y$. Then $(x,y) \notin \Delta$ has an open neighborhood U with $U \cap \Delta = \emptyset$ if and only if there are $V \subset X$, $W \subset X$ open with $x \in V, y \in W$ with $V \times W \cap \Delta = \emptyset$ (since the sets of the form $V \times W$ with $V, W \subset X$ open form a basis of the product topology). Note that $(V \times W) \cap \Delta = \emptyset$ if and only if $V \cap W = \emptyset$. □

We take this description of the Hausdorff property in the case of a variety.

Definition 6.1.2 A variety X is *separated* if $\Delta = \{(x,x) : x \in X\}$ is closed in $X \times X$ (product of varieties).

Examples 6.1.3 $\mathbb{A}^n$ is separated. Indeed, $\Delta \subset \mathbb{A}^n \times \mathbb{A}^n$ is the zero set of $(x_1 - y_1, \ldots, x_n - y_n)$. Let $X \subset \mathbb{A}^n$ be closed. Then X is separated. Indeed, let $X = Z(f_1, \ldots, f_r)$. Then $\Delta_X \subset X \times X \subset \mathbb{A}^n \times \mathbb{A}^n$ is given by $Z(f_1, \ldots, f_r, f_1', \ldots, f_r', x_1 - y_1, \ldots, x_n - y_n)$ where the f_i are the polynomials in the x_i, and the f_i' the corresponding polynomials in the y_i. Even all quasi-projective varieties are separated (exercise 6.7.1).

Example 6.1.4 In the exercises, we will see that affine and quasi-projective varieties are separated. Exercise 6.7.3 gives an example of a variety which is not separated. This variety "looks" like:



.

Proposition 6.1.5 *Let X be a separated variety, and let U and $V \subset X$ be open and affine. Then $U \cap V$ is open and affine.*

Proof Consider the following diagram:

$$\begin{array}{ccccc} U \cap V & \xrightarrow{\sim} & (U \times V) \cap \Delta_X & \subset & X \times X \\ \cap & & \cap & & \\ X & \xrightarrow{\sim} & \Delta_X & \subset & X \times X. \end{array}$$

The map from $X \to \Delta_X$ just sends a point x to (x, x), and one can show that this is an isomorphism (using the universal property, use the identity morphisms on X and for the inverse use a projection). This isomorphism restricts to an isomorphism on $U \cap V \to (U \times V) \cap \Delta_X$. Now $(U \times V) \cap \Delta_X$ is closed in the affine space $U \times V$, hence it is affine. □

6.2 Glueing varieties

We now want to construct new varieties from varieties that we already have. The process will be similar to the construction of topological spaces in topology by glueing. Assume that:

i. I a set;

ii. $\forall i \in I$, X_i is a variety;

iii. $\forall i, j \in I$, $X_{ij} \subset X_i$ is an open subvariety;

iv. $\forall i, j \in I$, $\varphi_{ij} \colon X_{ij} \tilde{\to} X_{ji}$ is an isomorphism of varieties.

Assume moreover that these data satisfy the following compatibility conditions:

v. $\forall i, j, k \in I$, $\varphi_{ij}(X_{ij} \cap X_{ik}) = X_{ji} \cap X_{jk}$;

vi. $\forall i, j, k \in I$, $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$ on $X_{ij} \cap X_{ik}$;

vii. $\forall i \in I$, $X_{ii} = X_i$ and $\varphi_{ii} = \mathrm{id}_{X_i}$.

Remark 6.2.1 The condition in (vii) that $\varphi_{ii} = \mathrm{id}_{X_i}$ is in fact automatic, because $\varphi_{ii} \circ \varphi_{ii} = \varphi_{ii}$ and φ_{ii} is an isomorphism.

Example 6.2.2 Let X be a variety, and let $X_i \subset X$ be open subvarieties for some set I. Now let $X_{ij} = X_i \cap X_j$ and let $\varphi_{ij} \colon X_{ij} \to X_{ji}$ be the identity.

We construct a variety from these glueing data. The first step is to define the disjoint union $X' := \bigsqcup_{i \in I} X_i$ of the X_i as a variety. As a set it is simply the disjoint union, and for every i in I we have the inclusion map $j_i \colon X_i \to X'$. We give X' the sum topology for the maps $(j_i)_{i \in I}$: a subset U of X' is open if and only if for each i in I the subset $j_i^{-1}U$ of X_i is open. This simply means that all the j_i are *open immersions*, that is, $j_i(X_i)$ is open in X' and j_i is a homeomorphism from X_i to $j_i(X_i)$ with the topology induced from X'. For $U \subset X'$ we define $\mathcal{O}_{X'}(U)$ as the set of functions $f \colon U \to k$ such that for all i in I the function $j_i^* f$ from $j_i^{-1}U$ to k is in $\mathcal{O}_{X_i}(j_i^{-1}U)$. We leave it to the reader to check that $(X', \mathcal{O}_{X'})$ is a variety and that the $j_i \colon X_i \to X'$ are open immersions. The pair $((X', \mathcal{O}_{X'}), (j_i)_{i \in I})$ has the following universal property: for any variety Y and any set of morphisms $f_i \colon X_i \to Y$, there exists a unique morphism $f \colon X' \to Y$ such that for all i in I, $f_i = f \circ j_i$. Note that up to now we have only used the set I and the collection of varieties $(X_i)_{i \in I}$.

The second step is to define a quotient $q \colon X' \to X$ as a set. In order to simplify our notation we view X_i as a subset of X', that is, we omit the inclusion maps j_i. We define a relation $\sim$ on X' by:

$(x \sim y)$ if and only if (there exist $i, j \in I$ such that $x \in X_{ij}$, $y \in X_{ji}$, and $\varphi_{ij}(x) = y$).

The reader is asked to check that this is indeed an equivalence relation. This gives us the quotient $q\colon X' \to X$ as a map of sets. The third step is to make X into a topological space. We simply give it the quotient topology.

The fourth and last step is to define the notion of regular functions on X. For U an open subset of X we define $\mathcal{O}_X(U)$ to be the set of functions $f\colon U \to k$ such that $q^*f\colon q^{-1}U \to k$ is in $\mathcal{O}_{X'}(q^{-1}U)$. Then $\mathcal{O}_X$ is a sheaf of k-algebras on X.

We state without proof:

Proposition 6.2.3 *The k-space X is a variety and the $j_i\colon X_i \to X$ are open immersions.*

Example 6.2.4 We construct $\mathbb{P}^1$ by glueing two copies of $\mathbb{A}^1$. So let $X_0 = \mathbb{A}^1$ and $X_1 = \mathbb{A}^1$. Let $X_{00} = X_0, X_{11} = X_1$ and $X_{01} = \mathbb{A}^1 - \{0\} \subset X_0$ and $X_{10} = \mathbb{A}^1 - \{0\} \subset X_1$. Let φ_{00} and φ_{11} be the identities, $\varphi_{01}\colon X_{01} \to X_{10}$, $t \mapsto t^{-1}$, and $\varphi_{10} := \varphi_{01}^{-1}$. Then $X = \mathbb{A}^1 \sqcup \mathbb{A}^1/\sim\, = \mathbb{P}^1$.

6.3 Presentations of varieties

We want to give presentations of varieties, that is, we want to be able to write down a variety in a finite amount of data, so that for example it can be put into a computer. We assume that we can write down elements of k. This is not a trivial assumption: k might be uncountable!

For an affine variety we can just write down equations defining the variety (we can take a finite set of equations, since $k[x_1, \ldots, x_n]$ is Noetherian). We can also use the equivalence of categories between affine varieties and finitely generated reduced k-algebras (note that it is better to have generators for the ideal then just equations).

Here is a more general case. Let X be a variety and assume that $X = \bigcup_{i \in I} X_i$ with I a finite set, X_i open affine and $X_{ij} = X_i \cap X_j$ affine. (The last condition is implied by the other ones if X is separated by Proposition 6.1.5). Then X is determined by the following data, called a *presentation* of X:

i. $\forall i \in I$, the finitely generated reduced k-algebra $\mathcal{O}_X(X_i)$;

ii. $\forall i, j \in I$, the finitely generated reduced k-algebra $\mathcal{O}_X(X_{ij})$;

iii. $\forall i, j \in I$, the restriction morphism $\mathcal{O}_X(X_i) \to \mathcal{O}_X(X_{ij})$ coming from the inclusion $X_{ij} \to X_i$;

iv. $\forall i, j \in I$, the isomorphism (identity map, in fact) of k-algebras $\mathcal{O}_X(X_{ij}) \tilde{\to} \mathcal{O}_X(X_{ji})$ coming from the identity map $X_{ji} \to X_{ij}$.

Indeed, using the equivalence between affine varieties and finitely generated reduced k-algebras these determine glueing data for X.

Example 6.3.1 Let $X = \mathbb{P}^2$. Write $X = X_0 \cup X_1 \cup X_2$ with $X_i = D(x_i) = U_i$, the standard open affine cover. Then, as in Section 2.4, $\mathcal{O}_X(X_0) = k[x_{01}, x_{02}]$, $\mathcal{O}_X(X_1) = k[x_{10}, x_{12}]$ and $\mathcal{O}_X(X_2) = k[x_{20}, x_{21}]$. We describe for example $\mathcal{O}_X(X_{01})$ and its maps from $\mathcal{O}_X(X_0)$ and $\mathcal{O}_X(X_1)$. By Theorem 5.1.5 we know that $\mathcal{O}_X(X_{01}) = k[x_{01}, x_{02}, x_{10}, x_{12}]/(x_{01}x_{10} - 1, x_{01}x_{12} - x_{02}, x_{12} - x_{10}x_{02})$. We can now directly describe the map from say $\mathcal{O}_X(X_0)$ to $\mathcal{O}_X(X_{01})$, which just sends x_{01} to x_{01} and x_{02} to x_{02} and analogously for the other map(s).

6.4 Smooth varieties

One often sees other terminology for the word smooth: regular, non-singular. See also Section I.5 of [Hart], and Section 16.9 in [Eis].

To define this notion, we need the concept of partial derivatives of polynomials. For n in $\mathbb{N}$ and f in $k[x_1, \ldots, x_n]$ the partial derivatives $\partial f/\partial x_i$ in $k[x_1, \ldots, x_n]$ are defined formally, that is, the partial derivatives $\partial/\partial x_i \colon k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]$ are k-linear, satisfy the Leibniz rule and satisfy $\partial(x_j)/\partial x_i = 1$ if $j = i$ and is zero otherwise. For example, for $m \in \mathbb{N}$, $\partial(x_1^m)/\partial x_1 = mx_1^{m-1}$ (which is 0 if $m = 0$). This is a purely algebraic operation on $k[x_1, \ldots, x_n]$ and there is no need to take limits of any kind. But note that in characteristic p we have $\partial(x^p)/\partial x = px^{p-1} = 0$.

Definition 6.4.1 Let X be a variety and d in $\mathbb{N}$. For P in X, X is *smooth of dimension d at P* if there is an open subvariety U of X containing P and an isomorphism $\varphi\colon U \xrightarrow{\sim} Z(f_1, \ldots, f_{n-d}) \subset \mathbb{A}^n$ for some n and $f_1, \ldots, f_{n-d}$, such that the rank of the $n-d$ by n matrix over k:

$$\left(\frac{\partial f_i}{\partial x_j}(\varphi P)\right)_{i,j}$$

equals $n - d$. The variety X is *smooth of dimension d* if it is smooth of dimension d at all its points. The variety X is *smooth at P* if it is smooth of dimension d at P for some d. Finally, X is *smooth* if at every point P it is smooth of some dimension d_P.

Remark 6.4.2 The matrix of partial derivatives of the f_j at the point φP is called the Jacobian matrix. For those who have learned some differential topology (manifolds) it should be a familiar object. The Jacobian matrix at φP has rank $n-d$ if and only if the map $f = (f_1, \ldots, f_{n-d})$ from $\mathbb{A}^n$ to $\mathbb{A}^{n-d}$ has surjective derivative at φP, that is, is a submersion at φP, if and only if the fibre of φP, $f^{-1}\{f\varphi P\}$ is smooth at φP.

In other words, X is smooth of dimension d at P if locally at P, X can be given as the zero set of $n-d$ equations in n variables, for some n, such that the gradients of the equations are linearly independent at P. For linear subspaces of $\mathbb{A}^n$ this linear independence is indeed sufficient and necessary for the dimension to be d.

In Lecture 7 we will see how the Jacobian matrix arises naturally from the definition of the tangent space of X at P: the tangent space is the kernel of $k^n \to k^{n-d}$, $v \mapsto Jv$, with J the Jacobian matrix. This will prove that for X a variety, P in X and U any affine open neighborhood of P, and φ an isomorphism of U with a closed subset Y of $\mathbb{A}^n$, and $(f_1, \ldots, f_m)$ a set of generators of $I(Y)$, the integer $n - \mathrm{rank}(J)$, where J is the Jacobian matrix at φP, is the dimension of the tangent space of X at P and hence does not depend on the choice of U nor φ.

Finally, there are relations with the dimension of varieties as in Section 1.4. We state them in the following theorem.

Theorem 6.4.3 *Let X be a variety.*

i. *If X is connected and smooth of dimension d, then X is irreducible and its dimension as a topological space is d.*

ii. *If X is irreducible and of dimension d, and P is a point of X, then X is smooth at P if and only if the dimension of the tangent space of X at P is d.*

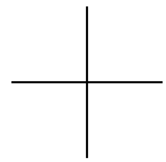
iii. *The set of P in X such that X is smooth at P is a dense open subset.*

iv. *The variety X is smooth of dimension d at $P \in X$ if and only if the dimension of the tangent space of X at P is d.*

v. *If $X = Z(f_1, \ldots, f_{n-d})$ such that at each P in X the rank of the matrix of partial derivatives as in Definition 6.4.1 is $n-d$, then $I(X) = (f_1, \ldots, f_{n-d})$.*

Example 6.4.4 The affine space $\mathbb{A}^d$ is smooth of dimension d. Indeed, it is given by zero equations as subset of $\mathbb{A}^d$.

Example 6.4.5 Consider $X := Z(xy) \subset \mathbb{A}^2$. We have the following picture of X:



We see that X is the union of the x and y axes, and it appears to have a 1-dimensional tangent space at all points except at the origin (where it is 2-dimensional). Later we will see more about the connection between the tangent space and smoothness.

It is easy to check that X is smooth of dimension one at all $P \neq (0,0)$. Theorem 6.4.3 shows that X is not smooth of any dimension at $(0,0)$ because every open neighborhood in X of $(0,0)$ is connected but not irreducible.

6.5 Rational functions

Definition 6.5.1 Let X be a variety. Now let

$$K(X) := \{(U,f) : U \subset X \text{ is open and dense and } f \in \mathcal{O}_X(U)\}/\sim$$

where $(U,f) \sim (V,g)$ if and only if there is an open and dense $W \subset U \cap V$ such that $f = g$ on W (or equivalently $f = g$ on $U \cap V$). Elements of $K(X)$ are called rational functions on X.

Remark 6.5.2 The set $K(X)$ is a k-algebra, because addition and multiplication are compatible with $\sim$: we just define $(U,f) + (V,g) = (U \cap V, f+g)$ and $(U,f) \cdot (V,g) = (U \cap V, f \cdot g)$.

Proposition 6.5.3 *Let X be a variety.*

i. If $U \subset X$ is open and dense then $K(U) \to K(X)$: $(V,f) \mapsto (V,f)$ is an isomorphism;

ii. If X is irreducible and affine then $K(X)$ is the field of fractions of $\mathcal{O}_X(X)$;

iii. If X is irreducible then $K(X)$ is a field (which we will call the function field *of X).*

Proof i. We have an obvious inverse, namely $K(X) \to K(U)$, $(V,f) \mapsto (V \cap U, f|_{V \cap U})$.

ii. Suppose $X \subset \mathbb{A}^n$ is affine and irreducible. Let $A = k[x_1,\ldots,x_n]$ and $I(X) = I$ which is prime (since X is irreducible). Then $\mathcal{O}_X(X) = A/I$. Hence A/I is a domain and it has a field of fractions $Q(\mathcal{O}_X(X)) = Q(A/I)$. We now have the map $Q(A/I) \to K(X)$ given by $g/h \mapsto (X \cap D(h), g/h)$, where of course $h \notin I$. Notice that $X \cap D(h)$ is dense (every non-empty open set in an irreducible space is dense) and g/h is regular on $D(h) \subset \mathbb{A}^n$ by definition. This map is a k-algebra morphism, and it is automatically injective since $Q(A/I)$ is a field. We just need to show that it is surjective. That it is surjective follows from the definition of a regular function on an open part of an affine variety (Definition 4.1.2).

iii. Use i. and ii. $\square$

6.6 Local rings

Let R be a commutative ring (with 1, as always). We call R a *local ring* if R has precisely one maximal ideal. Equivalently, if the set of non-units of R is an ideal of R. For example, each field is a local ring. The following construction produces local rings attached to points on varieties.

Definition 6.6.1 (Local ring at a point) Let X be a variety, and let $P \in X$ a point. Let

$$\mathcal{O}_{X,P} := \{(U, f) : U \subset X \text{ is open and dense, } P \in U, \text{ and } f \in \mathcal{O}_X(U)\}/\sim$$

where $(U, f) \sim (V, g)$ if and only if there is an open and dense $W \subset U \cap V$ with $P \in W$ such that $f = g$ on W (or equivalently $f = g$ on $U \cap V$).

Notice the similarity of this definition with the definition of $K(X)$; in fact we have a natural injective map $\mathcal{O}_{X,P} \to K(X)$. The difference is that we only take regular functions defined in a neighborhood of our fixed point P. In order to show that $\mathcal{O}_{X,P}$ is a local ring, consider the (well-defined) subset

$$\mathfrak{m}_{X,P} = \{(U, f) : U \subset X \text{ is open and dense, } P \in U, f \in \mathcal{O}_X(U), \text{ and } f(P) = 0\}/\sim$$

of $\mathcal{O}_{X,P}$. Then $\mathfrak{m}_{X,P}$ is a maximal ideal, as it is the kernel of the evaluation map $\mathcal{O}_{X,P} \to k$ that sends $[(U, f)] \mapsto f(P)$. Moreover, if $[(U, f)] \notin \mathfrak{m}_{X,P}$, then $f(P) \neq 0$, and $[(U, f)] = [(U \setminus Z(f), f)]$ is invertible in $\mathcal{O}_{X,P}$.

If X is irreducible then $K(X)$ is naturally the fraction field of $\mathcal{O}_{X,P}$. If X is affine and irreducible, let $\mathfrak{m}_P \subset \mathcal{O}_X(X)$ be the maximal ideal at P, and let

$$\mathcal{O}_X(X)_{\mathfrak{m}_P} := \{g/h : g, h \in \mathcal{O}_X(X), h \notin \mathfrak{m}_P\} \subset Q(\mathcal{O}_X(X))$$

be the *localization* of $\mathcal{O}_X(X)$ at m_P. Then under the identification of $K(X)$ with the fraction field of $\mathcal{O}_X(X)$ (cf. Proposition 6.5.3(ii)) we have that $\mathcal{O}_{X,P} \subset K(X)$ is identified with $\mathcal{O}_X(X)_{\mathfrak{m}_P}$. Thus, on arbitrary irreducible varieties X, local rings can be computed by first choosing a suitable affine open neighborhood, and then localizing. The reader is encouraged to verify that the rings $\mathcal{O}_X(X)_{\mathfrak{m}_P}$ are Noetherian. It follows that the local rings of varieties are Noetherian.

6.7 Exercises

Exercise 6.7.1 Let $\Psi\colon \mathbb{P}^{m-1} \times \mathbb{P}^{n-1} \to \mathbb{P}^{mn-1}$ be the Segre map (of sets):

$$((a_1 : \cdots : a_m), (b_1 : \cdots : b_n)) \mapsto (a_1b_1 : \cdots : a_mb_n).$$

Let $X \subset \mathbb{P}^{m-1}$ and $Y \subset \mathbb{P}^{n-1}$ be closed.

i. Show that Ψ is a morphism of varieties.

ii. Show that $\Psi(\mathbb{P}^{m-1} \times \mathbb{P}^{n-1})$ is closed in $\mathbb{P}^{mn-1}$.

iii. Show that Ψ is an isomorphism from the product variety $\mathbb{P}^{m-1} \times \mathbb{P}^{n-1}$ to the projective variety $\Psi(\mathbb{P}^{m-1} \times \mathbb{P}^{n-1})$.

iv. Show that Ψ restricts to an isomorphism from the product variety $X \times Y$ to the projective variety $\Psi(X \times Y)$.

v. Show that the diagonal $\Delta_{\mathbb{P}^{n-1}}$ is closed in $\mathbb{P}^{n-1} \times \mathbb{P}^{n-1}$.

vi. Show that projective varieties are separated.

Exercise 6.7.2 Let $X = Z(xy) \subset \mathbb{A}^2$. Show that $K(X)$ is not a field.

Exercise 6.7.3 Let X be the variety obtained from the following gluing data: $X_1 = X_2 = \mathbb{A}^1$ and $X_{12} = X_{21} = \mathbb{A}^1 - \{0\}$ with $\varphi_{12} = \text{id}$. Give the presentation of X corresponding to this glueing data. Describe the topology on X and the sheaf of regular functions on X. What is the diagonal $\Delta_X \subset X \times X$? What is the closure of the diagonal? Conclude that X is not separated.

Exercise 6.7.4 Consider the open subvariety $X = \mathbb{A}^2 - \{0\}$ of $\mathbb{A}^2$. Denote the embedding by $i\colon X \to \mathbb{A}^2$. Show that $i^*\colon \mathcal{O}_{\mathbb{A}^2}(\mathbb{A}^2) \to \mathcal{O}_X(X)$ is an isomorphism of k-algebras and deduce that X is not an affine variety. Give a presentation of X.

Exercise 6.7.5 If X is smooth of dimension m and Y smooth of dimension n show that $X \times Y$ is smooth of dimension $m+n$.

Exercise 6.7.6 Show that the product of two separated varieties is separated. Show that a locally closed subvariety of a separated variety is separated.

Exercise 6.7.7 Let n in $\mathbb{Z}_{>1}$ be an integer and k an algebraically closed field. Let $X \subset \mathbb{P}^2_k$ be the curve given by $x_1^n = x_2 x_0^{n-1} - x_2^n$. Give a presentation of X using an index set of 2 elements. Is X smooth? (The answer can depend on both n and the characteristic of k.) Give a presentation of the product $X \times X$.

Exercise 6.7.8 This exercise is a prequel of what will be discussed in Lecture 8.

Let X be a variety and d a positive integer. Assume given for all $i \in I := \{1, \ldots, d\}$ an open $X_i \subset X$, such that $X = \cup_{i \in I} X_i$. Put $X_{ij} := X_i \cap X_j$. Consider the diagram of k-vector spaces

$$\mathcal{O}_X(X) \xrightarrow{\delta_0} \prod_{i \in I} \mathcal{O}_X(X_i) \xrightarrow{\delta_1} \prod_{\substack{i,j \in I \\ i<j}} \mathcal{O}_X(X_{ij})$$

with

$$\delta_0 : f \mapsto (f_{|X_i})_i \quad \text{and} \quad \delta_1 : (f_i)_i \mapsto \big((f_i)_{|X_{ij}} - (f_j)_{|X_{ij}}\big)_{ij} \, .$$

Show that δ_0 is injective and that its image is the kernel of δ_1.

Now let $X \subset \mathbb{P}^2_k$ be the curve given by $x_1^n = x_2 x_0^{n-1} - x_2^n$, let $d = 2$ and let X_1 and X_2 be the two open affines that you used in the previous exercise.

Show that $\mathcal{O}_X(X) = k$.

Show that the dimension of the cokernel of δ_1 is $(n-1)(n-2)/2$. (Hint: work with bases for the infinite-dimensional vector spaces $\mathcal{O}_X(X_1)$, $\mathcal{O}_X(X_2)$ and $\mathcal{O}_X(X_{12})$ that are as simple as possible.)

(Note that the same argument works for any curve of degree n, as long as it does not contain the point $(0:1:0)$.)

Exercise 6.7.9 Let $X \subset \mathbb{P}^n_k$ be a smooth hypersurface of degree $d > 1$. Let m be an integer such that $2m \geq n$. Prove that X contains no linear varieties of dimension m. Recall that a linear variety is a closed subvariety of $\mathbb{P}^n_k$ whose homogeneous ideal is generated by linear forms.

Lecture 7

Tangent spaces and 1-forms

7.1 Tangent spaces of embedded affine varieties

See also Exercise I.5.10 of [Hart].

Definition 7.1.1 Let $X \subset \mathbb{A}^n$ be an affine variety and let $I \subset A := k[x_1, \ldots, x_n]$ be its ideal. Let $(f_1, \ldots, f_r)$ be a system of generators for I. For $a \in X$ we define the tangent space of X at a as:

$$
\begin{aligned}
T_X(a) &= \{v \in k^n : \forall f \in I,\ \lambda \mapsto f(a+\lambda v) \text{ has order} \geq 2 \text{ at } 0\} \\
&= \{v \in k^n : \forall f \in I,\ \frac{\partial f}{\partial v}(a) := \left(\frac{d}{d\lambda} f(a+\lambda v)\right)(0) = 0\} \\
&= \{v \in k^n : \forall i,\ \sum_j \frac{\partial f_i}{\partial x_j}(a) \cdot v_j = 0\} \\
&= \ker \left(\begin{pmatrix} \frac{\partial f_1}{\partial x_1}(a) & \cdots & \frac{\partial f_1}{\partial x_n}(a) \\ \vdots & \ddots & \vdots \\ \frac{\partial f_r}{\partial x_1}(a) & \cdots & \frac{\partial f_r}{\partial x_n}(a) \end{pmatrix} : k^n \to k^r \right)
\end{aligned}
$$

Example 7.1.2 Assume that $k \not\supset \mathbb{F}_2$. Let $X = Z(x^2+y^2-z^2) \subset \mathbb{A}^3$; note that $x^2+y^2-z^2$ is irreducible, so $I = (x^2+y^2-z^2)$. It is a good idea to make a drawing of X: it is a cone. Let $P = (a, b, c) \in X$. Then we obtain:

$$T_Z(P) = \{(u, v, w) \in k^3 : 2au + 2bv - 2cw = 0\}.$$

So $\dim T_X(P) = 2$ if $P \neq 0$, and $\dim T_X(0) = 3$.

7.2 Intrinsic definition of the tangent space

Notation as in Definition 7.1.1. We let $\mathfrak{m} = \mathfrak{m}_a \subset A$ be the maximal ideal of $a = (a_1, \ldots, a_n) \in X \subset \mathbb{A}^n$, so $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$. Let $B := A/I = \mathcal{O}_X(X)$, let $\overline{\mathfrak{m}} = (\overline{x_1 - a_1}, \ldots, \overline{x_n - a_n})$ be the maximal ideal in B of a. This gives us the following exact sequences:

$$0 \to I \to A \to B \to 0, \quad \text{and} \quad 0 \to I \to \mathfrak{m} \to \overline{\mathfrak{m}} \to 0.$$

The image of $\mathfrak{m}^2$ in B equals $\overline{\mathfrak{m}}^2$, so the inverse image in $\mathfrak{m}$ of $\overline{\mathfrak{m}}^2$ is $I + \mathfrak{m}^2$. This gives us the exact sequences:

$$0 \to I + \mathfrak{m}^2 \to \mathfrak{m} \to \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 \to 0 \quad \text{and} \quad 0 \to (I + \mathfrak{m}^2)/\mathfrak{m}^2 \to \mathfrak{m}/\mathfrak{m}^2 \to \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 \to 0.$$

Now consider the following map:

$$\langle \cdot, \cdot \rangle : \mathfrak{m} \times T_{\mathbb{A}^n}(a) \to k, \quad (f, v) \mapsto \left(\frac{\partial f}{\partial v} \right)(a).$$

Lemma 7.2.1 *The map $\langle \cdot, \cdot \rangle$ is bilinear and induces a perfect pairing $\langle \cdot, \cdot \rangle : \mathfrak{m}/\mathfrak{m}^2 \times T_{\mathbb{A}^n}(a) \to k$ of k-vector spaces ("perfect" means that each side is identified with the dual of the other side).*

Proof The map $(f, v) \mapsto \langle f, v \rangle$ is obviously linear in f. It is linear in v as $\langle f, v \rangle = \sum_j (\partial f/\partial x_j)(a) \cdot v_j$. Hence it is bilinear. Now $\langle \cdot, \cdot \rangle$ gives a map $\mathfrak{m} \to T_{\mathbb{A}^n}(a)^\vee$, $f \mapsto \langle f, \cdot \rangle$. The kernel of this map is $\{f \in \mathfrak{m} : \forall i,\ (\partial f/\partial x_i)(a) = 0\}$. By translation, we may assume that $a = 0$. Let f be in the kernel. We write $f = \sum_i f_i$, with f_i homogeneous of degree i. Since $f(0) = 0$, the constant term f_0 is zero and since all the partial derivatives at 0 vanish, f_1 is zero as well. This shows that $f \in (x_1, \ldots, x_n)^2 = \mathfrak{m}^2$. So we have an injection $\mathfrak{m}/\mathfrak{m}^2 \to T_{\mathbb{A}^n}(0)^\vee$. Note that $T_{\mathbb{A}^n}(0) = k^n$ and that $(\overline{x_1}, \ldots, \overline{x_n})$ is a k-basis of $\mathfrak{m}/\mathfrak{m}^2$, so since the dimensions agree, our map is surjective and hence we have an isomorphism. □

Proposition 7.2.2 *The pairing $\langle \cdot, \cdot \rangle$ induces a perfect pairing $\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 \times T_X(a) \to k$.*

Proof Remember that we have the following exact sequence:

$$0 \to (I + \mathfrak{m}^2)/\mathfrak{m}^2 \to \mathfrak{m}/\mathfrak{m}^2 \to \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 \to 0$$

By Lemma 7.2.1, we have the perfect pairing $\langle \cdot, \cdot \rangle : \mathfrak{m}/\mathfrak{m}^2 \times T_{\mathbb{A}^n}(a) \to k$. By definition:

$$T_X(a) = \{v \in k^n : \langle \overline{f}, v \rangle = 0 \text{ for all } \overline{f} \in (I + \mathfrak{m}^2)/(\mathfrak{m}^2) \subset \mathfrak{m}/\mathfrak{m}^2.\}$$

So we get a perfect pairing between $T_X(a)$ and the quotient $(\mathfrak{m}/\mathfrak{m}^2)/((I+\mathfrak{m}^2)/\mathfrak{m}^2)$, which is $\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$ by the short exact sequence above. Here we have used that if $\langle \cdot, \cdot \rangle$ is a perfect pairing between finite dimensional k-vector spaces V and W, and W' is a subspace of W, then we get an induced perfect pairing between V/V' and W', with V' the orthogonal complement of W'. □

Definition 7.2.3 For X a variety, $x \in X$, we define $T_X(x) = (\mathfrak{m}/\mathfrak{m}^2)^\vee$, where $U \subset X$ is an affine open containing x and $\mathfrak{m} \subset \mathcal{O}_X(U)$ is the maximal ideal of x.

This is independent of the chosen affine open U. Actually, let $\mathcal{O}_{X,x}$ be the local ring of X at x, and $\mathfrak{m}_{X,x} \subset \mathcal{O}_{X,x}$ its maximal ideal. Then there is a natural isomorphism $T_X(x) \to (\mathfrak{m}_{X,x}/\mathfrak{m}_{X,x}^2)^\vee$ of k-vector spaces. The reader is encouraged to verify this, using the natural maps $\mathcal{O}_X(U) \to \mathcal{O}_{X,x}$ for $U \subset X$ affine open containing x, and the fact that the affine open neighborhoods of x form a basis of open neighborhoods of x.

7.3 Derivations and differentials

See also Section II.8 of [Hart] or [Serre]. In this section we introduce differential forms. We will use the pairing $\langle \cdot, \cdot \rangle$ of the previous section, although we will change the order of its arguments.

Let X be an affine variety and let $A := \mathcal{O}_X(X)$. For $x \in X$ and $v \in T_X(x)$ we have a map (notice that $f - f(x) \in \mathfrak{m}$): $\partial_v : A \to k$, $f \mapsto \partial_v f := \langle v, \overline{f - f(x)} \rangle$. These maps ∂_v are k-linear and satisfy the Leibniz rule: $\partial_v(f \cdot g) = f(x)\partial_v g + g(x)\partial_v f$. Indeed:

$$\begin{aligned}
\langle v, \overline{fg - f(x)g(x)} \rangle &= \langle v, \overline{(f - f(x))g} + \overline{f(x)(g - g(x))} \rangle \\
&= \langle v, \overline{(f - f(x))(g - g(x))} + \overline{(f - f(x))g(x)} + \overline{f(x)(g - g(x))} \rangle \\
&= \langle v, g(x)\overline{(f - f(x))} \rangle + \langle v, f(x)\overline{(g - g(x))} \rangle \\
&= f(x)\partial_v g + g(x)\partial_v f.
\end{aligned}$$

In order to define the algebraic analogue of C^∞-vector fields on manifolds we introduce the concept of k-derivations of A-modules. Recall that $A = \mathcal{O}_X(X)$.

Definition 7.3.1 Let M be an A-module. *A k-derivation* $D : A \to M$ is a k-linear map $D : A \to M$ such that for all $f, g \in A$: $D(fg) = fD(g) + gD(f)$. We denote the set of those derivations by $\mathrm{Der}_k(A, M)$.

Remark 7.3.2 If D is a derivation then $D(1) = D(1 \cdot 1) = 1 \cdot D(1) + 1 \cdot D(1)$. Hence $D(1) = 0$ and by k-linearity we see for $c \in k$ that $D(c) = 0$.

Example 7.3.3 Let $x \in X$, $A \to k = A/\mathfrak{m}_x$: $f \mapsto f(x)$. This makes k into an A-module and $\mathrm{Der}_k(A, A/\mathfrak{m}) = T_X(x)$ (Exercise 7.6.4).

Proposition 7.3.4 *There is a universal pair (Ω^1_A, d): Ω^1_A is an A-module, $d\colon A \to \Omega^1_A$ is a k-derivation, such that for any A-module M and any derivation $D\colon A \to M$ there exists a unique A-linear map φ making the following diagram commute:*

$$\begin{tikzcd} A \arrow[r, "d"] \arrow[d, "D"'] & \Omega^1_A \arrow[dl, dotted, "\varphi"] \\ M & \end{tikzcd}$$

Proof Let N be the free A-module with basis the symbols da for all a in A: $N = \bigoplus_{a \in A} Ada$. Let $N' \subset N$ be the submodule generated by the relations $d(\lambda a) = \lambda \cdot d(a)$, $d(a + b) = d(a) + d(b)$ and $d(ab) = a \cdot db + b \cdot da$ for all $a, b \in A, \lambda \in k$. We claim that we can take Ω^1_A to be N/N' with d which sends a to $\overline{da} \in N/N'$. Indeed one easily checks that $(N/N', d)$ satisfies the universal property. $\square$

Example 7.3.5 For $A = k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$ one has:

$$\Omega^1_A = \left(\bigoplus_{i=1}^{n} A \cdot dx_i \right) / \left(A \cdot df_1 + \cdots + A \cdot df_r \right)$$

where $df_i = \sum_j (\partial f_i / \partial x_j) dx_j$. Hence Ω^1_A is presented as follows:

$$A^r \xrightarrow{J\cdot} A^n \to \Omega^1_A \to 0, \quad \text{where} \quad J = \begin{pmatrix} \partial f_1/\partial x_1 & \cdots & \partial f_r/\partial x_1 \\ \vdots & \ddots & \vdots \\ \partial f_1/\partial x_n & \cdots & \partial f_r/\partial x_n \end{pmatrix}.$$

A proof is given in Exercise 7.6.6.

Remark 7.3.6 Let $\varphi\colon A \to B$ be a morphism of k-algebras and M a B-module. Then M becomes an A-module via φ: $a \cdot m := \varphi(a)m$. This gives a map $\mathrm{Der}_k(B, M) \to \mathrm{Der}_k(A, M)$, $D \mapsto D \circ \varphi$. Indeed, we check the Leibniz rule (where the last part follows from the A module structure on M):

$$\begin{aligned} (D \circ \varphi)(fg) &= D(\varphi(fg)) \\ &= D(\varphi(f)\varphi(g)) \\ &= \varphi(f)D(\varphi(g)) + \varphi(g)D(\varphi(f)) \\ &= fD(\varphi(g)) + gD(\varphi(f)). \end{aligned}$$

In particular we have a unique A-linear map $\Omega^1(\varphi)$ making the following diagram commute:

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "d_A"'] \arrow[dr, "d_B\circ\varphi"] & B \arrow[d, "d_B"] \\ \Omega^1_A \arrow[r, "\Omega^1(\varphi)"'] & \Omega^1_B \end{tikzcd}$$

For morphisms of k-algebras $\varphi_1\colon A_1 \to A_2$ and $\varphi_2\colon A_2 \to A_3$ one has $\Omega^1(\varphi_2\circ\varphi_1) = \Omega^1(\varphi_2)\circ\Omega^1(\varphi_1)$.

7.4 Differential 1-forms on varieties

Let X be a variety, obtained from glueing data:

$$\left(I, (X_i)_{i\in I}, \left(\varphi_{i,j} : X_{i,j} \xrightarrow{\sim} X_{j,i}\right)_{i,j\in I}\right)$$

in which all X_i and $X_{i,j}$ are affine (this is no restriction if the variety X is separated, cf. Proposition 6.1.5). Then we define the $\mathcal{O}_X(X)$-module of 1-forms on X:

$$\Omega^1_X(X) = \{(\omega_i \in \Omega^1_{\mathcal{O}_{X_i}(X_i)})_{i\in I} : \forall i,j,\ \Omega^1(\varphi^*_{ij})\colon \omega_j|_{X_{j,i}} \mapsto \omega_i|_{X_{i,j}}\}.$$

More precisely, the compatibility condition between the ω_i is that for all i and j in I, the images of ω_i and ω_j in $\Omega^1_{\mathcal{O}(X_{i,j})}$ and $\Omega^1_{\mathcal{O}(X_{j,i})}$ obtained by applying Ω^1 to the restriction maps $\mathcal{O}(X_i) \to \mathcal{O}(X_{i,j})$ and $\mathcal{O}(X_j) \to \mathcal{O}(X_{j,i})$ correspond to each other via the isomorphism $\Omega^1(\varphi^*_{i.j})$ from $\Omega^1_{\mathcal{O}(X_{j,i})}$ to $\Omega^1_{\mathcal{O}(X_{i,j})}$.

It is a fact that $\Omega^1_X(X)$ does not depend on the choice of presentation of X.

Remark 7.4.1 For simplicity of notation we will sometimes omit the subscript "X" in $\mathcal{O}_X(U)$ and in $\Omega^1_X(U) = \Omega^1_U(U)$.

Example 7.4.2 Let X be an affine variety. Then we have $\Omega^1_X(X) = \Omega^1_{\mathcal{O}_X(X)}$. For $x\in X$, Example 7.3.3 gives:

$$T_X(x) = \mathrm{Der}_k(\mathcal{O}_X(X), \mathcal{O}_X(X)/\mathfrak{m}_x) = \mathrm{Hom}_{\mathcal{O}_X(X)}(\Omega^1_X(X), k) = \left(\Omega^1_X(X)/\mathfrak{m}\Omega^1_X(X)\right)^\vee.$$

Example 7.4.3 For $X = \mathbb{A}^n$: $\Omega^1(\mathbb{A}^n) = \{\sum_{i=1}^n f_i dx_i : f_i \in k[x_1,\ldots,x_n]\}$; it is a free $k[x_1,\ldots,x_n]$-module with basis $(dx_1,\ldots,dx_n)$.

Example 7.4.4 Let $n\in\mathbb{Z}_{\geq 2}$, $X = Z(-y^n + x^{n-1} - 1) \subset \mathbb{A}^2$ and suppose that $n(n-1)\in k^\times$. Let $A := \mathcal{O}_X(X) = k[x,y]/(f)$ where $f = -y^n + x^{n-1} - 1$. Then:

$$\Omega^1_A = (A\cdot dx \oplus A\cdot dy)\,/\,\left(-ny^{n-1}dy + (n-1)x^{n-2}dx\right)$$

On $D(y)\subset X$ we have: $dy = \frac{n-1}{n}\frac{x^{n-2}}{y^{n-1}}dx$, so $\Omega^1(D(y))$ is free over $\mathcal{O}_X(D(y))$ with basis dx. On $D(x)\subset X$: $dx = \frac{n}{n-1}\frac{y^{n-1}}{x^{n-2}}dy$. Hence $\Omega^1(D(x)) = \mathcal{O}_X(D(x))dy$ (so it is free again). Note that $X = D(x)\cup D(y)$. We say that Ω^1_X is locally free of rank 1.

Remark 7.4.5 For X a variety, and for varying $U\subset X$ open, $U\mapsto \Omega^1(U)$ is a sheaf, denoted Ω^1_X. It is a "coherent sheaf of $\mathcal{O}_X$-modules". For X smooth of dimension d, Ω^1_X is locally free of rank d. If X is moreover irreducible, then the equivalence classes of (U,ω) with $U\subset X$ non-empty open and $\omega\in\Omega^1(U)$ form the d-dimensional $K(X)$-vector space of "rational 1-forms", $\Omega^1_{K(X)}$.

7.5 Functions and 1-forms on smooth irreducible curves, orders and residues

Definition 7.5.1 Let k be an algebraically closed field. A *curve over* k is a quasi-projective algebraic variety over k all of whose irreducible components are of dimension one.

Definition 7.5.2 Let X be a smooth irreducible curve, and $x \in X$. Let $U \ni x$ be an affine open, and let $\mathfrak{m}_x \subset \mathcal{O}_X(U)$ be the maximal ideal at x. The smoothness assumption implies that $\dim(\mathfrak{m}_x/\mathfrak{m}_x^2) = 1$.

i. For $x \in X$ and $g \neq 0$ in $K(X)$ we define $v_x(g) \in \mathbb{Z}$, the *order of* g *at* x, as follows. Let $U \ni x$ be an affine open and $t \in \mathcal{O}(U)$ such that $t \in \mathfrak{m}_x$, $t \notin \mathfrak{m}_x^2$. Such a t is called a *parameter* or *uniformizer* at x. Then there is a unique n in $\mathbb{Z}$ and an h in $K(X)$ that is regular at x and with $h(x) \neq 0$ such that $g = t^n h$. Then we define $v_x(g) := n$, it is independent of the choices made (see the remarks at the end of this section).

ii. For $0 \neq \omega \in \Omega^1_{K(X)}$ and $x \in X$ we define $v_x(\omega) \in \mathbb{Z}$ as follows. Let t be a uniformizer at x. Then there is a unique $g \in K(X)$ such that $\omega = g{\cdot}dt$ in $\Omega^1_{K(X)}$. We put $v_x(\omega) = v_x(g)$; this is independent of the choice of t.

iii. For $\omega \in \Omega^1_{K(X)}$ and $x \in X$ we define $\mathrm{res}_x(\omega)$, the *residue* of ω at x, as follows. Write $\omega = g{\cdot}dt$ with t a parameter at x. If $v_x(g) \geq 0$, then $\mathrm{res}_x(\omega) := 0$. If $v_x(g) = -n$ with $n \geq 1$, write $g = a_{-n}t^{-n} + \cdots + a_{-1}t^{-1} + h$ with $h \in K(X)$ regular at x. Then $\mathrm{res}_x(\omega) := a_{-1}$. This is independent of the choice of t. See III.7.14 in [Hart] for more details.

Proposition 7.5.3 *Let X be a smooth affine curve, $x \in X$, and $t \in \mathcal{O}(X)$ such that $t \in \mathfrak{m}_x$, $t \notin \mathfrak{m}_x^2$, and, for all y in $X - \{x\}$, $t(y) \neq 0$. Then $\mathfrak{m}_x = (t)$. For all i in $\mathbb{Z}_{\geq 0}$ we have $\dim_k(\mathfrak{m}_x^i/\mathfrak{m}_x^{i+1}) = 1$ and $\dim_k(\mathcal{O}(X)/\mathfrak{m}_x^i) = i$.*

Proof As x is the only zero of t in X, we have $\sqrt{(t)} = \mathfrak{m}_x$. Write $\mathfrak{m}_x = (f_1, \ldots, f_r)$ (use that $\mathcal{O}(X)$ is noetherian). We take $n \in \mathbb{Z}_{\geq 1}$ such that for all i we have $f_i^n \in (t)$. Hence $\mathfrak{m}_x^{nr} \subset (t)$. Now for each i in $\mathbb{Z}_{\geq 1}$, t^i generates $\mathfrak{m}_x^i/\mathfrak{m}_x^{i+1}$, because the smoothness assumption on X implies that $\dim_k(\mathfrak{m}_x/\mathfrak{m}_x^2) = 1$ and therefore t generates it. So for each i we have $a_i \in k$ and $g_i \in \mathfrak{m}_x^2$ such that $f_i = a_i t + g_i$. Then $f_i f_j - a_i a_j t^2$ is in $\mathfrak{m}_x^3$, etc. Let now f be in $\mathfrak{m}_x$. Then there exist $b_1, \ldots, b_{nr-1}$ such that $f - (b_1 t + \cdots + b_{nr-1}t^{nr-1})$ is in $\mathfrak{m}_x^{nr}$, hence is in (t). We have proved that $\mathfrak{m}_x = (t)$.

Let us now prove that for all i in $\mathbb{Z}_{\geq 0}$ we have $\dim_k(\mathfrak{m}_x^i/\mathfrak{m}_x^{i+1}) = 1$. As t^i generates $\mathfrak{m}_x^i/\mathfrak{m}_x^{i+1}$, we have $\dim_k(\mathfrak{m}_x^i/\mathfrak{m}_x^{i+1}) \leq 1$. Suppose that for some i in $\mathbb{Z}_{\geq 0}$ we have $\mathfrak{m}_x^i = \mathfrak{m}_x^{i+1}$. Then we have $(t^i) = (t^{i+1})$, hence there is a g in $\mathcal{O}(X)$ such that $t^i = t^{i+1}g$. But then $t^i(1 - gt) = 0$ in $\mathcal{O}(X)$. It follows that t^i is zero on a neighborhood of x. But then $X = \{x\}$, and this contradicts the fact that every irreducible component of X is of dimension one.

The last claim follows from what we have just proved: use that $\mathcal{O}(X) \supset \mathfrak{m}_x \supset \cdots \supset \mathfrak{m}_x^i$. □

Remark 7.5.4 To compute the a_i for i in $\{-n, \ldots, -1\}$, write $t^n g = a_{-n} + a_{-n+1}t + \cdots + a_{-1}t^{n-1}$ in $\mathcal{O}(U)/\mathfrak{m}_x^n\mathcal{O}(U)$, using that $\dim_k(\mathfrak{m}_x^i/\mathfrak{m}_x^{i+1}) = 1$, with basis $\overline{t}^i$.

Remark 7.5.5 (Connection to discrete valuation rings) Let R be a Noetherian local domain, with maximal ideal $\mathfrak{m}$. Write l for the field $R/\mathfrak{m}$. You can write down a natural l-module structure on $\mathfrak{m}/\mathfrak{m}^2$. We call R a *discrete valuation ring* if $\dim_l \mathfrak{m}/\mathfrak{m}^2 = 1$. Using the theory of discrete valuation rings (as learnt in a commutative algebra course), the above constructions can be motivated/elucidated as follows. Let X be a smooth irreducible curve, and let $x \in X$ be a point. Let $\mathfrak{m}_{X,x} \subset \mathcal{O}_{X,x}$ be the maximal ideal of the local ring $\mathcal{O}_{X,x}$ of X at x. Note that $\mathcal{O}_{X,x}/\mathfrak{m}_{X,x} = k$. We have that $\dim_k(\mathfrak{m}_{X,x}/\mathfrak{m}_{X,x}^2) = 1$ and that $\mathcal{O}_{X,x}$ is a Noetherian local domain. It follows that $\mathcal{O}_{X,x}$ is a discrete valuation ring. By general theory, every discrete valuation ring has a unique surjective valuation to $\mathbb{Z}_{\geq 0} \cup \{\infty\}$. What is this valuation? Note that $K(X)$

is the field of fractions of $\mathcal{O}_{X,x}$, so we get an injection $\mathcal{O}_{X,x} \to K(X)$. Given an element $g \in \mathcal{O}_{X,x}$ we define its valuation to be ∞ if $g = 0$ and to be $v_x(g)$ otherwise (with v_x as defined in (i) of definition 7.5.2 above). The existence of a uniformiser t ensures that v_x is surjective.

Note that if R is a discrete valuation ring with maximal ideal $\mathfrak{m}$ and $R/\mathfrak{m} = l$ then $\mathfrak{m}$ is a principal ideal, and for all i in $\mathbb{Z}_{\geq 0}$ we have $\dim_l(\mathfrak{m}^i/\mathfrak{m}^{i+1}) = 1$ and $\dim_l(R/\mathfrak{m}^i) = i$. If $v \colon R \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ is the unique surjective valuation, then v extends naturally to a map $\mathrm{Frac}(R) \to \mathbb{Z} \cup \{\infty\}$, and R is exactly the set of elements with non-negative valuation.

7.6 Exercises

Exercise 7.6.1 Give a basis of the tangent space at $(0 : 0 : 1)$ along the curve $Z \subset \mathbb{P}^2$ given by the polynomial $y^2z - x^3$.

Exercise 7.6.2 Let k be a field, A a k-algebra and M an A-module. Show that $\mathrm{Der}_k(A, M)$ is an A-module for the addition and multiplication defined by $(D_1 + D_2)g = D_1g + D_2g$, $(fD)g = f(Dg)$.

Exercise 7.6.3 Show that if $\varphi \colon A \to B$ is a morphism of k-algebras and $D \in \mathrm{Der}_k(B, M)$, then $D \circ \varphi$ is in $\mathrm{Der}_k(A, M)$ (what is the A-module structure on M?).

Exercise 7.6.4 Let k be a field, A a k-algebra and $\mathfrak{m} \subset A$ a maximal ideal such that the morphism $k \to A \to A/\mathfrak{m} = k$ is an isomorphism.

i. Let $D \in \mathrm{Der}_k(A, A/\mathfrak{m})$. Show that D is zero on $\mathfrak{m}^2$, and hence factors through a derivation $\overline{D} \colon A/\mathfrak{m}^2 \to k$.

ii. Show that the map $\mathrm{Der}_k(A, A/\mathfrak{m}) \to (\mathfrak{m}/\mathfrak{m}^2)^\vee$, $D \mapsto \overline{D}|_{\mathfrak{m}/\mathfrak{m}^2}$ is an isomorphism of A-modules.

Exercise 7.6.5 Let k be a field, $A = k[x_1, \ldots, x_n]$. Show that $(dx_1, \ldots, dx_n)$ is an A-basis of Ω^1_A, and give a formula for df, where $f \in A$.

Exercise 7.6.6 Let k and A be as in the previous exercise. Let $I = (f_1, \ldots, f_r)$ be an ideal in A, and let $q \colon A \to B := A/I$ be the quotient map.

i. Show that, for any B-module M, $q^* \colon \mathrm{Der}_k(B, M) \to \mathrm{Der}_k(A, M)$ is injective and has image the set of those D such that for all i one has $D(f_i) = 0$.

ii. Use the universal property of Ω^1_A to show that $d \colon B \to \Omega^1_A/(A{\cdot}df_1 + \cdots A{\cdot}df_r)$ is a universal derivation.

Exercise 7.6.7 Consider the rational 1-form $x^{-1}dx$ on $\mathbb{P}^1$. Compute its order and residue at all $P \in \mathbb{P}^1$.

Exercise 7.6.8 Prove that for all rational 1-forms ω on $\mathbb{P}^1$ we have $\sum_P \mathrm{res}_P(\omega) = 0$, where the sum is over all $P \in \mathbb{P}^1$. Hint: write $\omega = f{\cdot}dx$, with $f \in k(x)$, and use a suitable k-basis of $k(x)$.

Exercise 7.6.9 Let $n \in \mathbb{Z}_{\geq 2}$, $X = Z(-x_1^n + x_0^{n-1}x_2 - x_2^n) \subset \mathbb{P}^2$. Assume that $n(n-1)$ is in $k^\times$. We have already seen that X is smooth. You may now use without proof that X is irreducible (in fact, Bezout's theorem implies that reducible plane projective curves are singular). Let $U := X \cap \mathbb{A}^2$. Then $U = Z(f)$ with $f = -y^n + x^{n-1} - 1$.

i. Show that in $\Omega^1(U)$ we have $(n-1)x^{n-2}dx = ny^{n-1}dy$.

ii. We define a rational 1-form ω_0 by:

$$\omega_0 = \frac{dx}{ny^{n-1}} = \frac{dy}{(n-1)x^{n-2}}.$$

Show that ω_0 has no poles on U. Hint: $U = (U \cap D(x)) \cup (U \cap D(y))$.

iii. Show that ω_0 has no zeros on U. Hint: both dx and dy are multiples of ω_0, and, for each $P \in U$, at least one of dx and dy is a generator of $\Omega^1(U)/m_P\Omega^1(U)$. Hence (you do not need to prove this) $\Omega^1(U)$ is a free $\mathcal{O}(U)$-module, with basis ω_0.

iv. Let $P = X \cap Z(x_2)$ be the point at infinity of X. Compute $v_P(\omega_0)$.

v. For $n \in \{2, 3, 4\}$, give a basis (and hence the dimension) of $\Omega^1(X)$.

Exercise 7.6.10 Let $Q = Z(z - xy)$ in $\mathbb{A}^3$ and let $a \in Q$. Compute $T_Q(a)$. Show that $(a + T_Q(a)) \cap Q$ is a union of two lines, and that all lines on Q are obtained in this way.

Exercise 7.6.11 Let X be the union of the three coordinate axes in $\mathbb{A}^3$, and let $Y := Z(xy(x-y))$ in $\mathbb{A}^2$. Are X and Y isomorphic?

Lecture 8

The theorem of Riemann-Roch

8.1 Exact sequences

In the next sections, we use the concept of complexes and exact sequences of k-vector spaces and some properties of these.

Definition 8.1.1 A *sequence* of k-vector spaces is a diagram of k-vector spaces

$$\cdots \xrightarrow{\alpha_0} V_1 \xrightarrow{\alpha_1} V_2 \xrightarrow{\alpha_2} V_3 \xrightarrow{\alpha_3} \cdots$$

with k-vector spaces V_i and linear maps α_i indexed by i in $\mathbb{Z}$. Such a sequence is called a *complex* if for all i in $\mathbb{Z}$, $\alpha_{i+1} \circ \alpha_i = 0$, and most often the maps α_i are then denoted d_i. A complex is called *exact* or an *exact sequence* if for all i in $\mathbb{Z}$, $\ker(\alpha_{i+1}) = \mathrm{im}(\alpha_i)$. When writing sequences, terms that are omitted are zero. A short exact sequence is an exact sequence of the following form:

$$0 \xrightarrow{\alpha_0} V_1 \xrightarrow{\alpha_1} V_2 \xrightarrow{\alpha_2} V_3 \xrightarrow{\alpha_3} 0.$$

In other words, this means that α_1 is injective, $\mathrm{im}\,\alpha_1 = \ker \alpha_2$ and α_2 is surjective. In still other words: V_3 is the quotient of V_2 by V_1.

Lemma 8.1.2 *Let*

$$0 \xrightarrow{\alpha_0} V_1 \xrightarrow{\alpha_1} V_2 \xrightarrow{\alpha_2} \cdots \xrightarrow{\alpha_{n-1}} V_n \xrightarrow{\alpha_n} 0$$

be an exact sequence of finite dimensional vector spaces. Then

$$\sum_{i=1}^{n} (-1)^i \dim(V_i) = 0.$$

Proof For all i define $V_i' = \ker \alpha_i = \mathrm{im}\,\alpha_{i-1}$ and choose a subspace $V_i'' \subset V_i$ such that $V_i = V_i' \oplus V_i''$. Then α_i restricts to an isomorphism $V_i'' \to V_{i+1}'$ hence $\dim V_i'' = \dim V_{i+1}'$ for all i. Together with the identity $\dim V_i = \dim V_i' + \dim V_i''$ for all i this proves the lemma. $\square$

8.2 Divisors on curves

We recall that "curve" is as defined in Definition 7.5.1. We do not assume curves to be smooth. The reason is that in Lecture 11 we need the generality of this section for treating intersection of divisors on surfaces. We will add smoothness conditions at the necessary places.

Let X be an irreducible curve. Let $P \in X$ and $f \in K(X)^\times$. We want to define an integer $v_P(f)$, the order of vanishing of f at P, extending Definition 7.5.2 for smooth curves. Intuitively it should satisfy:

$$\begin{aligned} v_P(f) &= 0 \quad \text{if } f(P) \neq 0, \infty, \\ &< 0 \quad \text{if } f \text{ has a pole at } P, \\ &> 0 \quad \text{if } f \text{ has a zero at } P. \end{aligned}$$

We will now give an example, which one can justify with the definition given later (see Exercise 8.5.1).

Example 8.2.1 Let $X = \mathbb{P}^1$. By Proposition 6.5.3, $K(\mathbb{P}^1) = K(\mathbb{A}^1) = Q(k[x]) = k(x)$. Let $f \in K(\mathbb{P}^1)^\times$, so $f = g/h$ with $g, h \in k[x]$ both non-zero. Let P be in $\mathbb{A}^1$. Then we can write $g = (x-P)^l g'$ and $h = (x-P)^m h'$ for $g', h' \in k[x]$ with $g'(P), h'(P) \neq 0$ and we set $v_P(f) = l - m$. For the point $P = (1:0) = \infty$, we set $v_\infty(f) = \deg(h) - \deg(g)$.

Definition 8.2.2 Let X be an irreducible curve, $P \in X$ and $f \in K(X)^\times$. If there exists an affine open $U \subset X$ with $P \in U$ such that $f|_U \in \mathcal{O}_X(U)$ and f has no zeros on $U - \{P\}$, then we define:

$$v_P(f) = \dim_k \mathcal{O}_X(U)/(f|_U).$$

Proposition 8.2.3 *In the situation of Definition 8.2.2, and with g satisfying the same conditions as f, we have:*

i. $v_P(f) < \infty$;

ii. $v_P(f)$ *does not depend on* U;

iii. $v_P(fg) = v_P(f) + v_P(g)$.

Proof i: P corresponds to a maximal ideal $\mathfrak{m} \subset \mathcal{O}_X(U)$. We have $\sqrt{(f)} \supset \mathfrak{m}$. Write $\mathfrak{m} = (f_1, \ldots, f_t)$ with $f_i \in \mathcal{O}_X(U)$ (this can be done since $\mathcal{O}_X(U)$ is Noetherian, i.e. every ideal of $\mathcal{O}_X(U)$ is finitely generated). Since $\mathfrak{m}$ is maximal, it follows that either f is a unit or $\mathfrak{m} = \sqrt{(f)}$. It follows that there exists $a_i \in \mathbb{Z}_{\geq 1}$ such that $f_i^{a_i} \in (f)$. Now let $a = \sum_{i=1}^t a_i$, then by the pigeon hole principle $\mathfrak{m}^a \subset (f)$. And this gives:

$$\dim \mathcal{O}_X(U)/(f) \leq \dim \mathcal{O}_X(U)/\mathfrak{m}^a = \dim \mathcal{O}_X(U)/\mathfrak{m} + \dim \mathfrak{m}/\mathfrak{m}^2 + \cdots + \dim \mathfrak{m}^{a-1}/\mathfrak{m}^a.$$

Notice that $\mathcal{O}_X(U)/\mathfrak{m} = k$. It is enough to show that $\dim \mathfrak{m}^b/\mathfrak{m}^{b+1} < \infty$ (for any $b \in \mathbb{Z}_{\geq 1}$). First observe that $\mathfrak{m}^b/\mathfrak{m}^{b+1}$ is a finitely generated $\mathcal{O}_X(U)$-module. Now $\mathfrak{m} \subset \mathcal{O}_X(U)$ annihilates $\mathfrak{m}^b/\mathfrak{m}^{b+1}$ (indeed, if $x \in \mathfrak{m}^b$ and $y \in \mathfrak{m}$, then $xy \in \mathfrak{m}^{b+1}$). So $\mathfrak{m}^b/\mathfrak{m}^{b+1}$ is even a finitely generated $\mathcal{O}_X(U)/\mathfrak{m}$-module, hence a finite dimensional k-vector space. So $\dim_k \mathcal{O}_X(U)/(f) < \infty$.

ii: Let U and V be two such opens; one easily reduces to the case where $V \subset U$. The natural map $\mathcal{O}_X(U)/(f|_U) \to \mathcal{O}_X(V)/(f|_V)$ is injective; we need to show that it is surjective. Note that V is the union of distinguished opens $D(g_i) \subset U$ for suitable $g_i \in \mathcal{O}_X(U)$; it suffices to consider the case that g is one of the g_i and $V = D(g)$. Then $\mathcal{O}_X(V) = \mathcal{O}_X(U)[1/g]$ and the task is to show that for each $r \in \mathbb{N}$ and each $h \in \mathcal{O}_X(U)$ there exist $l, m \in \mathcal{O}_X(U)$ such that $h/g^r - lf|_U = m$. Equivalently, we need to write $h = lf|_U + mg^r$ for suitable $l, m \in \mathcal{O}_X(U)$. This would follow if $(f|_U, g^r)$ were equal to the unit ideal in $\mathcal{O}_X(U)$. But this is true: the assumptions guarantee that $Z(f|_U, g^r)$ is empty.

iii: Consider the following short exact sequence:

$$0 \longrightarrow \mathcal{O}_X(U)/(g) \xrightarrow{f\cdot} \mathcal{O}_X(U)/(fg) \longrightarrow \mathcal{O}_X(U)/(f) \longrightarrow 0,$$

where $f\cdot$ is multiplication by f. Lemma 8.1.2 gives $\mathcal{O}_X(U)/(fg) = \dim \mathcal{O}_X(U)/(f) + \dim \mathcal{O}_X(U)/(g)$, that is, $v_P(fg) = v_P(f) + v_P(g)$. $\square$

Definition 8.2.4 Let X be an irreducible curve, $P \in X$ and $f \in K(X)^\times$. Then choose U affine open containing P, and $g, h \in \mathcal{O}_X(U)$ such that $f = g/h$ (Proposition 6.5.3) such that g and h have no zeros on $U - \{P\}$ and define $v_P(f) = v_P(g) - v_P(h)$. We call $v_P(f)$ the *order of vanishing* or *valuation* of f at P.

Remark 8.2.5 Definition 8.2.4 is compatible with Definition 7.5.2. But note once more that in the present section we are not (yet) assuming that X is smooth. If X is not smooth at P, then $\dim_k \mathfrak{m}/\mathfrak{m}^2 > 1$ and $\mathcal{O}_{X,P}$ is *not* a discrete valuation ring.

Definition 8.2.6 Let X be a curve. A *divisor* on X is a $\mathbb{Z}$-valued function D on X such that for at most finitely many P in X, $D(P) \neq 0$. In other words, it is a function $D \colon X \to \mathbb{Z}$ with finite support. The $\mathbb{Z}$-module of divisors is $\mathbb{Z}^{(X)}$, the free $\mathbb{Z}$-module with basis X. Often a divisor D is written as a formal finite sum $D = \sum_{P \in X} D(P) \cdot P$. The degree of a divisor D is defined as $\deg(D) = \sum_P D(P)$.

Example 8.2.7 A typical element of $\mathbb{Z}^{(X)}$ looks something like $2P + 3Q - R$ for some $P, Q, R \in X$. The degree of this divisor is 4.

Lemma 8.2.8 *Let X be an irreducible curve, and f in $K(X)^\times$. Then the set of P in X with $v_P(f) \neq 0$ is finite.*

Proof Recall that our standing assumption is that curves are quasi-projective. Hence X can be covered by finitely many nonempty open affines U_i, such that for each of them, $f|_{U_i} = g_i/h_i$ with g_i and h_i in $\mathcal{O}_X(U_i)$, both non-zero. For each i, U_i is irreducible and affine and of dimension one, hence $Z(g_i)$ and $Z(h_i)$ are zero-dimensional affine varieties, hence finite. □

Definition 8.2.9 Let $f \in K(X)^\times$. Then we define the *divisor of f* as $\mathrm{div}(f) = \sum_{P \in X} v_P(f) P$.

Theorem 8.2.10 *Let X be an irreducible curve. The map $K(X)^\times \to \mathbb{Z}^{(X)}$, $f \mapsto \mathrm{div}(f)$, is a group morphism.*

Proof This is a direct consequence of Proposition 8.2.3 iii. □

Definition 8.2.11 Let X be an irreducible curve, and D and D' divisors on X. Then we say that $D \leq D'$ if for all $P \in X$, $D(P) \leq D'(P)$. This relation "$\leq$" is a partial ordering.

Example 8.2.12 Let P, Q and R be disctinct points on X. Then $P - 3Q + R \leq 2P - 2Q + R$. Note however that $P + Q \not\leq 2Q$ and that $2Q \not\leq P + Q$, so the partial ordering is not a total ordering.

Definition 8.2.13 For X an irreducible curve, D a divisor on X, and $U \subset X$ open and non-empty, we define

$$\mathcal{L}(U, \mathcal{O}_X(D)) := \{f \in K(X)^\times : \mathrm{div}(f|_U) + D|_U \geq 0\} \cup \{0\}.$$

We will often abbreviate $\mathcal{L}(U, \mathcal{O}_X(D))$ to $\mathcal{L}(U, D)$ and $\mathcal{L}(U, \mathcal{O}_X(0))$ to $\mathcal{L}(U, \mathcal{O}_X)$.

Example 8.2.14 Let X be an irreducible curve, $U \subset X$ open and non-empty, and P in X. If P is not in U then $\mathcal{L}(U, P)$ is the set of rational functions f with no pole in U. If P is in U, then $\mathcal{L}(U, P)$ is the set of rational functions f with a pole of order at most 1 at P and no other poles in U.

We will state the following result without proof.

Proposition 8.2.15 *Let X be an irreducible curve.*

i. *If X is projective then $\mathcal{L}(X, D)$ is a k-vector space of finite dimension.*

ii. *If $U \subset X$ is open, non-empty and smooth, then $\mathcal{L}(U, \mathcal{O}_X) = \mathcal{O}_X(U)$.*

The reader with some background in commutative algebra (especially, localization) may want to prove item (ii) in this result as follows. Let $P \in U$. As X is smooth at P we have that $\mathcal{O}_{X,P}$ is a discrete valuation ring and in particular we have $\mathcal{O}_{X,P} = \{f \in K(X)^\times : v_P(f) \geq 0\}$. It follows that $\mathcal{L}(U, \mathcal{O}_X)$ is equal to the intersection of all $\mathcal{O}_{X,P}$ for P running through U. Now a general result in commutative algebra (try to prove this yourself!) states that if R is a domain, then $R = \cap_{\mathfrak{m}} R_{\mathfrak{m}}$, where the intersection is taken inside the fraction field of R and runs over all maximal ideals $\mathfrak{m}$ of R. Here $R_{\mathfrak{m}}$ denotes the localization of R at $\mathfrak{m}$. We obtain (ii) by applying this result to the domain $\mathcal{O}_X(U)$, and by noting that $\mathcal{O}_X(U)_{\mathfrak{m}_P}$ is identified with $\mathcal{O}_{X,P}$ for all $P \in U$.

Example 8.2.16 The smoothness assumption in (ii) is necessary. Let A be the sub-k-algebra $k[t^2, t^3]$ of $k[t]$. It is finitely generated and it is an integral domain. Let X be the affine variety such that $\mathcal{O}_X(X) = A$; it is irreducible. Then $\mathcal{L}(X, \mathcal{O}_X) = k[t]$, which is strictly larger than A. Note that X is not smooth: it is the curve $Z(y^2 - x^3)$ in $\mathbb{A}^2$ (the morphism $k[x, y] \to A$, $x \mapsto t^2$, $y \mapsto t^3$ is surjective and has kernel $(y^2 - x^3)$).

Corollary 8.2.17 *Let X be a smooth irreducible projective curve. Then $\mathcal{O}_X(X) = \mathcal{L}(X, 0) = k$.*

Proof Proposition 8.2.15 gives that $\mathcal{O}_X(X) = \mathcal{L}(X, \mathcal{O}_X)$, and that this is a finite dimensional k-vector space. It is a sub-k-algebra of $K(X)$, hence an integral domain. Hence it is a field (indeed, for f nonzero in $\mathcal{O}(X)$, multiplication by f on $\mathcal{O}(X)$ is injective, hence surjective, hence there is a g in $\mathcal{O}(X)$ such that $fg = 1$. So, $k \to \mathcal{O}(X)$ is a finite field extension. As k is algebraically closed, $k = \mathcal{O}(X)$. □

8.3 H^0 and H^1

Let X be an irreducible curve. Then there exist nonempty open and affine subsets U_1 and U_2 of X such that $X = U_1 \cup U_2$ (see Exercise 8.5.4).

Definition 8.3.1 Let $H^0(X, \mathcal{O}_X)$ be the kernel of the map

$$\delta\colon H^0(U_1, \mathcal{O}_X) \oplus H^0(U_2, \mathcal{O}_X) \to H^0(U_1 \cap U_2, \mathcal{O}_X)\,,$$

given by $(f_1, f_2) \mapsto f_1|_{U_1 \cap U_2} - f_2|_{U_1 \cap U_2}$. In the same way, we define $H^0(X, D)$ to be the kernel of the map:

$$\delta\colon H^0(U_1, D) \oplus H^0(U_2, D) \to H^0(U_1 \cap U_2, D), \quad (f_1, f_2) \mapsto f_1|_{U_1 \cap U_2} - f_2|_{U_1 \cap U_2}. \tag{8.3.2}$$

Proposition 8.3.3 *We have $H^0(X, \mathcal{O}_X) = \mathcal{O}_X(X)$.*

Proof See Exercise 6.7.8. □

Note that if X is smooth, irreducible and projective, we get $H^0(X, \mathcal{O}_X) = \mathcal{O}_X(X) = \mathcal{L}(X, 0) = k$. In fact, more generally we have that if X is smooth, irreducible and projective and D is a divisor on X, that $H^0(X, D) = \mathcal{L}(X, D)$. From Proposition 8.2.15 we obtain that $H^0(X, D)$ is finite dimensional as a k-vector space. For a different approach we refer to Exercise 8.5.7.

Definition 8.3.4 Assume again that X is an irreducible curve. Let δ be as in (8.3.2). We define

$$H^1(X, \mathcal{O}_X(D)) = H^1(X, D) := \operatorname{coker} \delta\,.$$

Facts 8.3.5 i. $H^1(X,D)$ does not depend on the choice of U_1 and U_2. For example, if U_1' and U_2' are non-empty open affines contained in U_1 and U_2, respectively, and cover X, then the restriction maps induce a map from $\operatorname{coker}(\delta)$ to $\operatorname{coker}(\delta')$. The claim is that such maps are isomorphisms and that all open affine covers can be related via common refinements, resulting in unique isomorphisms between the $\operatorname{coker}(\delta)$'s.

ii. If X is affine, then $H^1(X,D)=0$.

Definition 8.3.6 Let X be an irreducible projective curve. Then $\dim H^1(X,\mathcal{O}_X)$ is called the *genus* of X.

Example 8.3.7 We have already calculated the genus of a particular curve; see Exercise 6.7.8.

8.4 The Riemann-Roch theorem

Theorem 8.4.1 *Let X be a smooth, irreducible projective curve. Let g be the genus of X and D a divisor on X. Then $\dim H^0(X,D)-\dim H^1(X,D)=1-g+\deg(D)$.*

In particular, $H^1(X,D)$ is finite-dimensional!

Proof Note that the statement is true for $D=0$, as $\dim H^0(X,0)=1$ and $\dim H^1(X,0)=g$. It now suffices to show that for all D and all $P\in X$, the statement is true for D if and only if it is true for $D':=D+P$.

We have the following two exact sequences (with the notations from above):

$$0\to H^0(X,D)\to H^0(U_1,D)\oplus H^0(U_2,D)\to H^0(U_1\cap U_2,D)\to H^1(X,D)\to 0$$

$$0\to H^0(X,D')\to H^0(U_1,D')\oplus H^0(U_2,D')\to H^0(U_1\cap U_2,D')\to H^1(X,D')\to 0$$

We also have the following inclusions:

$$\begin{aligned}\alpha: H^0(U_1,D)\oplus H^0(U_2,D) &\to H^0(U_1,D')\oplus H^0(U_2,D')\\ \beta: H^0(U_1\cap U_2,D) &\to H^0(U_1\cap U_2,D')\end{aligned}$$

Now we can form a large diagram as follows (with exact rows and columns):

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
 & H^0(X,D) \arrow[d] & H^0(X,D') \arrow[d] & A' \arrow[d] & \\
0 \arrow[r] & H^0(U_1,D)\oplus H^0(U_2,D) \arrow[r, "\alpha"] \arrow[d, "\delta"] & H^0(U_1,D')\oplus H^0(U_2,D') \arrow[r] \arrow[d, "\delta"] & A \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & H^0(U_1\cap U_2,D) \arrow[r, "\beta"] \arrow[d] & H^0(U_1\cap U_2,D') \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & 0 \\
 & H^1(X,D) \arrow[d] & H^1(X,D') \arrow[d] & B' \arrow[d] & \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

In this diagram A and B are the cokernels of α respectively β; γ is the map induced by the δ's above it and A' and B' are the kernel and cokernel of γ, respectively.

We can now apply the snake lemma (see for example Wikipedia), and we obtain the following exact sequence:

$$0 \to H^0(X, D) \to H^0(X, D') \to A' \to H^1(X, D) \to H^1(X, D') \to B' \to 0.$$

We apply Lemma 8.1.2 a few times. If A and B are finite dimensional then we see from the last column of the large diagram that:

$$\dim B' - \dim A' = \dim B - \dim A.$$

From the exact sequence obtained from the snake lemma and from the previous line we get:

$$\begin{aligned}(\dim H^0(X, D) - \dim H^1(X, D)) - (\dim H^0(X, D') - \dim H^1(X, D'))&\\ = \dim B' - \dim A'&\\ = \dim B - \dim A.&\end{aligned}$$

So it suffices to show that $\dim A$ and $\dim B$ are finite and that $\dim A - \dim B = 1$. We claim that for $U \subset X$ open affine and non-empty:

$$\dim \operatorname{coker}\left(H^0(U, D) \to H^0(U, D')\right) = \begin{cases} 0 & \text{if } P \notin U \\ 1 & \text{if } P \in U \end{cases}$$

If $P \notin U$, the claim is obvious as $D|_U = D'|_U$.

Suppose that $P \in U$. Let us first argue that the cokernel of $H^0(U, D) \to H^0(U, D')$ has dimension at most one. Let $t \in \mathcal{O}_X(V)$ be a uniformiser at P, with V open in U. Let $n := -D'(P)$. As in Definition 7.5.2 and Remark 7.5.4, each element f in $H^0(U, D')$ can be written uniquely as $f = a_n(f)t^n + t^{n+1}h$ with $a_n(f)$ in k and h in $K(X)$ regular at P. Such an f is in $H^0(U, D)$ if and only if $a_n(f) = 0$. Hence $H^0(U, D)$ is the kernel of the map $H^0(U, D') \to k$, $f, \mapsto a_n(f)$. Hence the cokernel has dimension at most one. To prove that it is one, it suffices to show that there is an f in $H^0(U, D')$ that is not in $H^0(U, D)$. We put $g := t^n$. Then g is in $K(X)^\times$, and $v_P(g) = n = -D'(P)$. We claim that there exists an h in $\mathcal{O}_X(U)$ such that $h(P) = 1$ and $f := h{\cdot}g$ is in $H^0(U, D')$. A element $h \neq 0$ in $\mathcal{O}_X(U)$ has this property if and only if $h(P) = 1$ and for all Q in U, $v_Q(h) \geq -v_Q(g) - D'(Q)$. This means that $h(P) = 1$ and at a finite number of distinct points $Q_1, \ldots, Q_r$, and elements n_i in $\mathbb{N}$, we must have $v_{Q_i}(h) \geq n_i$. This is a consequence of the Chinese remainder theorem, that says that the morphism of k-algebras $\mathcal{O}_X(U) \to \mathcal{O}_X(U)/\mathfrak{m}_P \times \prod_{i=1}^r \mathcal{O}_X(U)/\mathfrak{m}_{Q_i}^{n_i}$ is surjective. This finishes the proof of the claim.

Using the claim, we can now finish the proof. From the claim we get:

	$\dim A$	$\dim B$
$P \in U_1 \cap U_2$	2	1
$P \notin U_1 \cap U_2$	1	0

So indeed $\dim B - \dim A = -1$, and we are done with the proof. □

8.5 Exercises

Exercise 8.5.1 Consider the standard affine $\mathbb{A}^1 \subset \mathbb{P}^1$, and denote by ∞ the point $(1 : 0)$, so that $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$. Let g and h be nonzero elements of $k[x] = \mathcal{O}_{\mathbb{A}^1}(\mathbb{A}^1)$. Verify using the definition that $v_\infty(g/h) = \deg(h) - \deg(g)$.

Exercise 8.5.2 In this exercise we consider divisors on $\mathbb{P}^1$.

i. Compute $\dim(H^0(\mathbb{P}^1, \mathcal{O}(n\infty)))$;

ii. Show that for every $P \in \mathbb{P}^1$ there exists an $f \in K(\mathbb{P}^1)$ with $\mathrm{div}(f) = P - \infty$;

iii. Show that the dimensions of $H^0(\mathbb{P}^1, \mathcal{O}(D))$ and $H^1(\mathbb{P}^1, \mathcal{O}(D))$ depend only on the degree of D. Give formulas for these dimensions.

Exercise 8.5.3 Let X be a smooth projective and irreducible curve and P a point of X. Use the Riemann-Roch theorem to show that $\mathcal{O}_X(X - \{P\})$ is infinite-dimensional.

Exercise 8.5.4 Let $X \subset \mathbb{P}^n$ be a closed curve. Show that there exists hyperplanes H_1 and H_2 in $\mathbb{P}^n$ such that $H_1 \cap H_2 \cap X = \emptyset$. Deduce that X is the union of two open affine subsets. Now generalise this as follows (quite a lot harder): for $X \subset \mathbb{P}^n$ a quasi-projective curve there exist hypersurfaces $Z(f_1)$ and $Z(f_2)$ in $\mathbb{P}^n$ such that $Z(f_1) \cap Z(f_2) \cap X = \emptyset$ and $X \cap D(f_i)$ is closed in $D(f_i)$ for both i.

Exercise 8.5.5 Let X be a smooth, projective and irreducible curve. Let $f\colon X \to \mathbb{P}^1$ be a morphism of varieties.

i. Show that f is either constant or surjective (hint: use that all morphisms from X to $\mathbb{A}^1$ are constant);

ii. Let U be the complement of $f^{-1}((1:0))$ and assume that U is non-empty. Show that $f_{|U}$, seen as a map to $\mathbb{A}^1 = k$ defines an element $\tilde{f}$ of $K(X)$;

iii. Show that $f \mapsto \tilde{f}$ defines a bijection between the set of morphisms $X \to \mathbb{P}^1$ whose image is not $\{(1:0)\}$ and $K(X)$.

iv. Let $X = \mathbb{P}^1$ and $f\colon X \to \mathbb{P}^1$ an isomorphism. Show that there exist $a, b, c, d \in k$ such that $\tilde{f} = (ax+b)/(cx+d)$, where we have identified $K(\mathbb{P}^1)$ with the field of fractions of $k[x] = \mathcal{O}_{\mathbb{P}^1}(\mathbb{A}^1)$. Deduce that $\mathrm{PGL}_2(k)$ is the group of automorphisms of the variety $\mathbb{P}^1$.

Exercise 8.5.6 Let $X \subset \mathbb{A}^2$ be the curve defined by $x^3 - y^2$.

i. Show that X is irreducible;

ii. Show that X is not smooth;

iii. Let P be the point $(0, 0)$. Show that there is no pair (U, f) with $P \in U \subset X$ open affine, $f \in \mathcal{O}_X(U)$ and $v_P(f) = 1$. (Hint: consider $k[x, y]/m^2$ with $m = (x, y)$.)

Exercise 8.5.7 Let X be a smooth and irreducible curve. Let D be a divisor on X. The purpose of this exercise is to show that $H^0(X, D)$ is finite dimensional if and only if $H^0(X, 0)$ is finite dimensional. For example, if X is projective, it follows that $H^0(X, D)$ is finite dimensional, since $H^0(X, 0) = k$. Note that we can reduce to the case that D is effective.

i. Assume that $D \geq 0$. For every $Q \in X$ let U_Q be an open affine neighborhood of Q and $t_Q \in \mathcal{O}_X(U_Q)$ be a uniformizer at Q such that t_Q has no zeroes on U_Q except at Q. Show that we have a natural exact sequence

$$0 \to H^0(X, 0) \to H^0(X, D) \to \bigoplus_{Q \in X} t_Q^{-D(Q)} \mathcal{O}_X(U_Q)/\mathcal{O}_X(U_Q)$$

of k-vector spaces.

ii. Show that the right hand side of the sequence is finite dimensional.

iii. Show that $H^0(X, D)$ is finite dimensional if and only if $H^0(X, 0)$ is finite dimensional.

Lecture 9

Complex varieties and complex manifolds; analytification

9.1 Holomorphic functions in several variables

There is a very rich theory of holomorphic functions in several complex variables. We will only touch on a tiny part of it.

In this section, we work with the standard Euclidean topology on $\mathbb{C}^n$, which is not the same as the Zariski topology unless $n = 0$.

For further reading on the topics of this and the next lecture, we suggest to browse through [Hart, Appendix B].

Definition 9.1.1 Let $U \subset \mathbb{C}^n$ be an open subset, and $f: U \to \mathbb{C}$. Let $u = (u_1, \ldots, u_n) \in U$. We say f *is holomorphic at* u if there exist $\epsilon \in \mathbb{R}_{>0}$ and complex numbers $c_{\underline{i}} : \underline{i} \in \mathbb{N}^n$ such that on the ball $B_\epsilon(u)$ we have an equality of functions

$$f(z_1, \ldots, z_n) = \sum_{\underline{i} \in \mathbb{N}^n} c_{\underline{i}} \prod_{j=1}^{n} (z_j - u_j)^{i_j} .$$

Implicitly we mean that the right hand side converges absolutely at every point in $B_\epsilon(u)$.

We say f *is holomorphic on* U if f is holomorphic at u for every $u \in U$.

If $g: U \to \mathbb{C}^m$ is another function and $u \in U$, we say g is *holomorphic at* u if each of the m components of g is holomorphic at u (i.e. if for each of the m coordinate projections $\mathbb{C}^m \to \mathbb{C}$, the composite with g is holomorphic). Similarly, we say g is *holomorphic on* U if it is holomorphic at u for every $u \in U$.

Lemma 9.1.2 *Holomorphic functions are continuous, even C^∞ (smooth).*

Proof Easy, omitted. $\square$

Examples:

i. Any polynomial function, or power series which converges on U gives a holomorphic function.

ii. If f and g are polynomials and g has no zeros on U then the rational function f/g is holomorpic on U. For example, if $U = \mathbb{C} \setminus \{0\}$, $f = 1$ and $g = z$ then we see that not every holomorphic function can be globally defined by a power series.

iii. Not every holomorphic function can be written as a ratio of polynomials, even locally. For example, the exponential function.

Lemma 9.1.3 *i. Let $f: U \to \mathbb{C}$ be a holomorphic function which does not vanish anywhere. Then $1/f$ is also holomorphic.*

ii. Let $f: U \to V \subset \mathbb{C}^n$ and $g: V \to \mathbb{C}^m$ be holomorphic. Then $g \circ f$ is holomorphic.

Proof Omitted. □

Lemma 9.1.4 *Let $f: U \to \mathbb{C}^n$ be holomorphic. Then $\{u \in U : f(u) = 0\}$ is a closed subset (in the Euclidean topology).*

Proof Immediate since f is continuous. □

9.2 Complex manifolds

Definition 9.2.1 Let $U \subset \mathbb{C}^n$ be Euclidean open. Define a $\mathbb{C}$-space $(U, \mathrm{hol}(U, \mathbb{C}))$ where U has the Euclidean topology, and $\mathrm{hol}(U, \mathbb{C})$ is the subsheaf of complex valued functions which are holomorphic.

These $\mathbb{C}$-spaces will play the role of 'affine varieties' in defining complex manifolds. Note that they are always *open* in $\mathbb{C}^n$, in contrast to affine varieties.

Definition 9.2.2 A *complex manifold* is a $\mathbb{C}$-space which is everywhere locally isomorphic to $(U, \mathrm{hol}(U, \mathbb{C}))$ for some n and some open subset $U \subset \mathbb{C}^n$.

A morphism of complex manifolds is just a morphism as $\mathbb{C}$-spaces (so the complex manifolds form a full subcategory of $\mathbb{C}$-spaces, just like $\mathbb{C}$-varieties).

There is an obvious notion of the dimension of a complex manifold. If you have seen real manifolds, note that the underlying topological space of a complex manifold of dimension n is a real manifold of dimension $2n$ - we will come back to this in the next lecture.

Example 9.2.3 i. Any union of open subsets of $\mathbb{C}^n$ gives a complex manifold, these are never compact unless empty or $n = 0$.

ii. Glueing complex manifolds works in exactly the same way as glueing varieties, cf. section 6.2. Let $X_1 = X_2 = \mathbb{C}$ with its sheaf of holomorphic functions. Let $X_{12} = \{z \in X_1 : z \neq 0\}$ and similarly $X_{21} = \{z \in X_2 : z \neq 0\}$, these are open submanifolds. Define $\varphi_{1,2}: X_{12} \to X_{21}$ by $\varphi(z) = 1/z$ (with the obvious map on sheaves, cf 9.1.3). Then the complex manifold obtained from this glueing data is called $\mathbb{CP}^1$, 'complex projective space'. As a ringed space, this is not isomorphic to the variety $\mathbb{P}^1_{\mathbb{C}}$. For example, on the level of topological spaces, $\mathbb{CP}^1$ is Hausdorff but $\mathbb{P}^1_{\mathbb{C}}$ is not! Note that the constructions of $\mathbb{P}^1_{\mathbb{C}}$ and $\mathbb{CP}^1$ look rather similar, though they are carried out in different categories. This will be generalised when we talk about 'analytification' of complex smooth varieties - it will turn out that $\mathbb{CP}^1$ is the analytification of $\mathbb{P}^1_{\mathbb{C}}$.

Though they are both special kinds of $\mathbb{C}$-spaces, $\mathbb{C}$-varieties and complex manifolds are very different - this is illustrated a bit in the exercises.

9.3 Sheaves on a base for a topology

For a moment we work in somewhat greater generality than usual, to develop an important tool that we will use to define the analytification.

Let T be a topological space. Recall that a *base* for T is a set B of open subsets of T such that every open $U \subset T$ can be written as a union of elements of B. For example, if T is $\mathbb{R}^n$ with the Euclidean topology then ϵ-balls around points give a base for the topology.

Let k be a field. Let T be a topological space and B a base for T.

Definition 9.3.1 Suppose for every $U \in B$ we are given a subset $\mathcal{F}(U) \subset \{f : U \to k\}$. We say the assignment $\mathcal{F}$ is a *sheaf on* B if

i. for all $V \subset U$ with $U, V \in B$ and for all f in $\mathcal{F}(U)$, $f|_V$ is in $\mathcal{F}(V)$;

ii. for all U in B and for all $f : U \to k$, f is in $\mathcal{F}(U)$ if and only if for all $P \in U$ there is a $U_P \subset U$ such that $U_P \in B$ and $P \in U_P$ and $f|_{U_P}$ is in $\mathcal{F}(U_P)$.

If we take B to be the set of all opens in T, then to give a sheaf on B is trivially the same as to give a k-space structure on the topological space T.

Theorem 9.3.2 *Let B, B' be two bases for the topological space T with $B' \subset B$.*

i. If $\mathcal{F}$ is a sheaf on B then restricting to opens in B' gives a sheaf on B';

ii. The above restriction map induces a bijection between sheaves on B and sheaves on B',

Proof Exercise. □

If B_1 and B_2 are bases and their intersection is also a base, and if $\mathcal{F}_1$ and $\mathcal{F}_2$ are sheaves on B_1 and B_2 respectively then we can see if $\mathcal{F}_1$ and $\mathcal{F}_2$ come from the same k-space structure by seeing if their restrictions to $B_1 \cap B_2$ are equal. This is a key thing we will need in defining analytifications. The most important examples will be of the following form: let X be a topological space, and $U = \{U_i\}_{i \in I}$ an open cover of X. Define a base B for the topology on X to consist of those opens which are contained in at least one U_i. Suppose U' is another cover, and define B' analogously. Then $B \cap B'$ is also a base, and so we can compare sheaves on B and B' by looking at their restrictions to $B \cap B'$.

9.4 Analytification

Let $\mathrm{SmVar}_{\mathbb{C}}$ be the full subcategory of $\mathrm{Var}_{\mathbb{C}}$ consisting of varieties that are smooth. The *analytification functor* takes as input a smooth complex variety (or map of such) and outputs a complex manifold (or map of such). From now until the end of this section, fix a smooth complex variety X. We will define a complex manifold X^{an}, called the 'analytification of X'.

9.4.1 The underlying set

This is easy: we define the underlying set of X^{an} to be the same as the underlying set of X.

9.4.2 The topology

First we treat the case where X is affine. Then there exist $n \geq 0$ and an ideal $I \subset \mathbb{C}[x_1, \ldots, x_n]$ and an isomorphism of varieties from X to $Z(I) \subset \mathbb{A}^n$. We give $\mathbb{A}^n = \mathbb{C}^n$ the Euclidean topology, and then we define the topology on X to be (the pullback of) the subspace topology. A priori this depends on the choice of the ideal I and the isomorphism, but in fact this is not the case, as can be easily deduced from the following lemma:

Lemma 9.4.3 *Let $I, J \subset \mathbb{C}[x_1, \ldots, x_n]$ be ideals. Let $f\colon Z(I) \to Z(J)$ be an isomorphism of varieties. Then f is a homeomorphism between the sets $Z(I)$ and $Z(J)$ with the subspace topologies from the Euclidean topology.*

Proof Rational functions without poles are continuous in the Euclidean topology. □

Now we treat the general case: by definition, there is an open cover of X by affine $\mathbb{C}$-varieties. Choose such a cover $X = \cup_j X_j$. Then (applying again the above lemma) we find that on overlaps $X_i \cap X_j$ the subspace topologies from X_i and X_j coincide. We then define the topology on X to be the one induced by the X_i. Again, this depends a priori on the choice of cover, but applying the above lemma again we find this is not the case.

For interest and future use, we note:

Lemma 9.4.4 *Let X be a complex variety, let X_{Zar} be the underlying Zariski topological space, and X_{Eu} be the topology we have just defined. Let $id\colon X_{Eu} \to X_{Zar}$ be the identity map on sets. Then id is continuous.*

Proof Exercise. □

9.4.5 The $\mathbb{C}$-space structure

Up to now we have not used the smoothness of X, but at this point it will be crucial. We repeat definition 6.4.1 for the convenience of the reader:

Definition 9.4.6 Let X be a variety and d in $\mathbb{N}$. For P in X, X is *smooth of dimension d at P* if there is an open subvariety U of X containing P and an isomorphism $\varphi\colon U \xrightarrow{\sim} Z(f_1, \ldots, f_{n-d}) \subset \mathbb{A}^n$ for some n and $f_1, \ldots, f_{n-d}$, such that the rank of the $n-d$ by n matrix over k:

$$\left(\frac{\partial f_i}{\partial x_j}(\varphi P)\right)_{i,j}$$

equals $n-d$. The variety X is *smooth of dimension d* if it is smooth of dimension d at all its points. The variety X is *smooth at P* if it is smooth of dimension d at P for some d. Finally, X is *smooth* if at every point P it is smooth of some dimension d_P.

The key to the construction is the *implicit function theorem*, which we recall here without proof:

Theorem 9.4.7 (Holomorphic implicit function theorem) *Let $U \subset \mathbb{C}^n$ be Euclidean open and $f_1, \ldots, f_{n-d}$ be holomorphic functions on U. Let $p \in U$ be such that the $n-d$ by $n-d$ matrix over $\mathbb{C}$*

$$\left(\frac{\partial f_i}{\partial x_j}(p)\right)_{1 \leq i \leq n-d, 1 \leq j \leq n-d}$$

is invertible. Then there exist

- *an open neighbourhood* U' *of* p *contained in* U
- *a open subset* $W \subset \mathbb{C}^d$*;*
- *holomorphic functions* $w_1, \ldots, w_{n-d} \colon W \to \mathbb{C}$*;*

such that for all $(z_1, \cdots, z_n) \in U'$ *we have that*

$$(f_i(z_1, \cdots, z_n) = 0 \text{ for all } 1 \leq i \leq n-d) \iff (w_i(z_{n-d+1}, \cdots, z_n) = z_i \text{ for all } 1 \leq i \leq n-d).$$

Proof Omitted, see for example [KK, Section 0.8] or Wikipedia. □

If you have never seen the classical (eg. differentiable) version of this theorem and some applications, it may help to look at the Wikipedia page on the implicit function theorem.

To define a $\mathbb{C}$-space structure, it suffices to define it on a base for the topology as discussed above. To check it is independent of choices, we only need to check that two sheaves obtained by different choices agree on a small enough base for the topology (by theorem 9.3.2).

Let $p \in X$ be a point. Because X is smooth at p (say of dimension d) there exist:

- an open subvariety U of X containing P;
- an isomorphism $\varphi \colon U \xrightarrow{\sim} Z(f_1, \ldots, f_{n-d}) \subset \mathbb{A}^n$ for some n and $f_1, \ldots, f_{n-d}$;

such that the rank of the $n-d$ by n matrix over $\mathbb{C}$:

$$\left(\frac{\partial f_i}{\partial x_j}(\varphi(p))\right)_{i,j}$$

equals $n-d$. Without loss of generality we assume that the left $n-d$ by $n-d$ block is invertible.

By the implicit function theorem, there exist

- a Euclidean open neighbourhood $V_{\varphi(p)}$ of $\varphi(p)$ in $\mathbb{A}^n$;
- a Euclidean open $W \subset \mathbb{C}^d$;
- holomorphic functions $w_1, \ldots, w_{n-d} \colon W \to \mathbb{C}$;

such that for all $(z_1, \ldots, z_n) \in V_{\varphi(p)}$ we have that

$$f(z_1, \ldots, z_n) = 0 \iff (w_i(z_{n-d+1}, \cdots, z_n) = z_i \text{ for all } 1 \leq i \leq n-d).$$

In other words, we get a homeomorphism $\psi \colon W \to V_{\varphi(p)} \cap Z(f_1, \ldots, f_{n-d})$ by sending $z = (z_{n-d+1}, \ldots, z_n)$ to

$$(w_1(z), \ldots, w_{n-d}(z), z_{n-d+1}, \ldots, z_n),$$

where the inverse is given by just forgetting the first $n-d$ coordinates.

We will now define a sheaf of holomorphic functions on small open neighbourhoods of p.

Let V' be any open neighbourhood of p contained in $\varphi^{-1}V_{\varphi(p)}$. As p varies, it is clear that such V' give a base of the (analytic) topology on X that we defined above. So by theorem 9.3.2 it is enough to tell you what the holomorphic functions on V' are. Well, given $f \colon V' \to \mathbb{C}$, we say f is holomorphic if and only if the composite

$$\psi^{-1}V' \to V' \xrightarrow{f} \mathbb{C}$$

is holomorphic, which is defined because $\psi^{-1}V'$ is an open subset of $\mathbb{C}^d$.

It is not clear at this point that these holomorphic functions are well-defined (even after making the various choices that we have), because the same V' could have its holomorphic functions 'defined' with respect to several different points p. But using that composites of holomorphic functions are holomorphic, this can be checked.

We should check that we have defined a sheaf on the base. If $V'' \subset V'$ it is clear that the restriction of a holomorphic function on V' is again holomorphic on V''. The second condition follows from the local nature of the definition of a holomorphic function.

During the definition of the sheaf, we made several choices, and we must check that the definition is independent of the choices. This is largely analogous to checking that the definition of 'holomorphic functions on V'' does not depend on the p with respect to which it is taken, the key extra input is our theorem that sheaves on two different bases induce the same $\mathbb{C}$-space structure if they agree on a sub-base of the intersection of the bases.

9.4.8 Analytification of morphisms

If $f\colon X \to Y$ is a morphism of $\mathbb{C}$-varieties, we want to get a morphism of complex manifolds from X^{an} to Y^{an}. This is straightforward because rational functions without poles are holomorphic; we omit the details.

This sends the inclusion of open sub varieties to the inclusion of open submanifolds. For example, for smooth quasi-projective $\mathbb{C}$-varieties $X \subset \mathbb{P}^n_{\mathbb{C}}$ we can obtain X^{an} by restriction of the structure sheaf from the analytification $\mathbb{CP}^n$ of projective space $\mathbb{P}^n_{\mathbb{C}}$. We will study the latter a bit further in the next lecture.

9.5 Examples

We can now give a huge number of examples of complex manifolds - any smooth complex variety gives one after analytification!

9.5.1 Projective line

We have already seen $\mathbb{CP}^1$, but now you can check that $\mathbb{CP}^1 = \left(\mathbb{P}^1_{\mathbb{C}}\right)^{an}$. Note that the latter is compact and Hausdorff (it is a sphere). We will come back to this next week.

9.5.2 Affine space

The analytification of $\mathbb{A}^n$ is just $\mathbb{C}^n$ with the usual sheaf of holomorphic functions. It works similarly for any open subvariety of $\mathbb{A}^n$.

Note that (with the Zariski topology) any open subset X of $\mathbb{A}^n$ is compact. On the other hand, the analytification X^{an} of such a subset is never compact unless $n = 0$ or it is empty.

Again with the Zariski topology, an open subset X of $\mathbb{A}^n$ is Hausdorff if and only if it is empty or $n = 0$. On the other hand, the analytification X^{an} of such a subset is always Hausdorff, since $\mathbb{C}^n$ is.

This suggests that studying X^{an} may not be a good way to gain information on X, but in fact this is far from true, and in the next lecture we will begin to develop a bit of a dictionary between them.

9.6 Exercises

Exercise 9.6.1 Show that an open subset U of $\mathbb{C}^n$ in the Zariski topology is Hausdorff if and only if $n = 0$ or U is empty.

Exercise 9.6.2 Give an example of a holomorphic function on $\mathbb{C}$ whose zero set is not closed in the Zariski topology.

Exercise 9.6.3 Here we check some basic facts about rational and holomorphic functions, in the 1-variable case for simplicity. Let U be an open neighbourhood of $0 \in \mathbb{C}$. Let $f \in \mathbb{C}[x]$ be a polynomial which does not vanish at 0.

i. Show that the image of f in the ring $\mathbb{C}[[x]]$ of formal power series is a unit.

ii. Show that the formal inverse of f that you found above has a positive radius of convergence.

iii. If you are following the commutative algebra course, show that $\mathbb{C}[[x]]$ is a *local ring*.

Exercise 9.6.4 Show that the underlying topological space of $\mathbb{CP}^1$ is a sphere. If you get stuck, google 'stereographic projection'.

Exercise 9.6.5 Let X be a complex variety.

i. Assume X is separated. Show that X^{an} is Hausdorff.

ii. Assume X^{an} is connected. Show that X is connected.

In fact the converses also hold, but this is harder and is omitted.

Exercise 9.6.6 Prove theorem 9.3.2.

Exercise 9.6.7 Prove lemma 9.4.4.

Exercise 9.6.8 If you do not know what the fundamental group of a pointed topological space is, ignore this exercise (it is just for fun). Let X be the complement of the origin in $\mathbb{A}^1_{\mathbb{C}}$. Pick any basepoint in X.

i. Compute the fundamental group of X^{an} with the Euclidean topology.

ii. Compute the fundamental group of X with the Zariski topology.

It turns out that there is a good notion of the fundamental group of an algebraic variety, even for varieties not over $\mathbb{C}$ (the 'étale fundamental group'), but its definition takes more work.

Lecture 10

Riemann surfaces

The main aim of this lecture is to discuss the analytification functor in more detail in the case of varieties of dimension 1. We will see that the topological space underlying a complex manifold is much nicer to work with than the topological space underlying a variety. First, we give a bit of a 'dictionary' relating properties of varieties and properties of manifolds (with no restrictions on dimension yet).

10.1 Dictionary between varieties and manifolds

10.1.1 Projective varieties and compactness

The complex variety $\mathbb{P}^n_{\mathbb{C}}$ is smooth, so you can analytify it. This is a very important example:

Theorem 10.1.2 *The (underlying topological space of the) complex manifold $\mathbb{CP}^n$ obtained by analytifying $\mathbb{P}^n_{\mathbb{C}}$ is compact.*

Proof [Sketch of proof] Recall that the continuous image of a compact space is compact, so it is enough to construct a continuous surjection from a compact space. In fact, we will construct a continuous surjection from the $(2n+1)$-sphere S^{2n+1}.

Recall that we can think of $\mathbb{P}^n_{\mathbb{C}}$ as the space of (complex) lines through the origin in $\mathbb{C}^{n+1}$. Note that $\{z \in \mathbb{C}^m : |z| = 1\}$ is naturally S^{2m-1}. Given a point $z \in \mathbb{C}^{n+1}$ with $|z| = 1$, there is a unique (complex) line through 0 and z, and every complex line arises in this way. This gives a surjection from $S^{2(n+1)-1}$ to $\mathbb{CP}^n$. We leave the (straightforward, but slightly messy) verification of continuity to the reader. □

Exercise 10.9.1 suggests an alternative proof.

Corollary 10.1.3 *Let X be a smooth projective complex variety. Then X^{an} is compact.*

Proof There exists a closed embedding $X \to \mathbb{P}^n$ for some n. Then X^{an} is a subspace of $\mathbb{CP}^n$ given as the zero set of some (continuous) homogeneous rational functions and so is a closed subset of $\mathbb{CP}^n$. Hence it is compact by the above theorem. □

10.1.4 Further properties

Above, we saw that if X is projective then X^{an} is compact. The converse fails, though it is true up to dimension 1. What about Hausdorff?

Theorem 10.1.5 *X is separated if and only if X^{an} is Hausdorff.*

Proof The direction 'X separated implies X^{an} Hausdorff was in last week's homework.

The converse is a lot harder. The key is to prove that an immersion of varieties whose analytification is closed is itself closed. We omit this. □

Theorem 10.1.6 *X is connected if and only if X^{an} is connected.*

Proof One direction was in last week's homework. Again, the converse is harder, and is omitted. □

We summarise this (and a few other easy properties) in a table:

X		X^{an}
projective	$\Longrightarrow$	compact
separated	$\Longleftrightarrow$	Hausdorff
connected	$\Longleftrightarrow$	connected
dimension n	$\Longleftrightarrow$	dimension n

We also mention a rather wonderful theorem:

Theorem 10.1.7 *The analytification functor is fully faithful on smooth projective varieties.*

Proof See [Artin, Algebrization of formal moduli II, theorem 7.3]. □

10.2 Riemann surfaces

We now look much more closely at the case of complex varieties of dimension 1, with particular attention to the projective case.

Definition 10.2.1 A *Riemann surface* is a Hausdorff complex manifold of dimension 1.

Example 10.2.2

- We have already seen $\mathbb{CP}^1$;
- If X is a separated complex variety of dimension 1 then X^{an} is a Riemann surface. If X is projective then X^{an} is compact. Moreover, X is connected if and only if X^{an} is connected.

If we restrict to compact Riemann surfaces, it turns out that this is the only source of examples. We noted above that the analytification functor is fully faithful on projective varieties. In the case of dimension 1 it is also essentially surjective:

Theorem 10.2.3 *The analytification gives an equivalence of categories between*

- *smooth projective complex varieties of dimension 1;*
- *compact Riemann surfaces.*

Proof Omitted, see e.g. [Algebraic Curves and Riemann Surfaces by Rick Miranda]. □

10.3 Fermat curves

We saw these before, but now we will look more closely, and also at the analytic aspects.

Definition 10.3.1 Fix $d \geq 1$. The d-th (complex) Fermat curve is the curve in $\mathbb{P}^2_{\mathbb{C}}$ given by the equation $X^d + Y^d = Z^d$.

Note that 'Fermat's last theorem' says that such a curve with $d \geq 3$ has few points with rational coordinates...

From now on we fix some $d \geq 0$, and we denote by F_d the d-th fermat curve.

Lemma 10.3.2 *F_d is smooth.*

Proof Exercise. □

So F_d^{an} is a compact Riemann surface. Let us make the complex manifold structure more explicit. First, let T^0 be the set

$$T^0 = \{(x, y) \in \mathbb{C}^2 : x^d + y^d = 1\} \tag{10.1}$$

with the subspace topology from $\mathbb{C}^2$. Let ζ_d be a primitive d-th root of 1 in $\mathbb{C}$. Now if $f \colon U \to \mathbb{C}$ is holomorphic function on an open subset of $\mathbb{C}^n$ and $u \in U$ is a point with $f(u) \neq 0$, then there exists an open neighbourhood $u \in V \subset U$ such that f has a holomorphic dth root on V (you could check this with the implicit function theorem, though it is overkill). Abusing notation, we write $\sqrt[d]{f}$ for some such. We will start by giving a Riemann surface structure to T^0, and will then deal with the 'missing points at infinity' separately.

We will give a Riemann surface structure to T^0 by giving an open neighbourhood V of every point $t_0 = (x_0, y_0)$ and a homeomorphism φ to V from an open subset U of $\mathbb{C}$, such that the corresponding transition functions are holomorphic on overlaps (cf. our construction of the analytification). There are two cases to consider:

10.3.3 $t_0 = (x_0, y_0)$ with $y_0 \neq 0$

The fact that $y_0 \neq 0$ is equivalent to x_0 not being a power of ζ_d. We write $y_0 = \zeta_d^j \sqrt[d]{1 - x_0^d}$ for some j. Then we define

$$\varphi(z) = (z, \zeta^j \sqrt[d]{1 - z^d}) \tag{10.2}$$

which makes sense when $|z - x_0|$ is small enough (using that x_0 is not a d-th root of 1). Note that $\zeta(x_0) = (x_0, y_0)$ and that for all $|x_0 - z|$ sufficiently small we have

$$z^d + \left(\zeta^j \sqrt[d]{1 - z^d}\right)^d = 1.$$

10.3.4 $t_0 = (x_0, 0)$

Then $x_0 = \zeta^j$ for some j. We define

$$\varphi(z) = \left(z^d + \zeta^j, \sqrt[d]{1 - (z^d + \zeta^j)^d}\right)$$

which makes sense when the absolute value of z is small enough. We have $\zeta(0) = (x_0, y_0)$ and for all $|z|$ sufficiently small we have

$$\left(z^d + \zeta^j\right)^d + \left(\sqrt[d]{1 - (z^d + \zeta^j)^d}\right)^d = 1.$$

10.3.5 Points at infinity

Above we have given the necessary data to define a complex manifold structure on T^0, and hence describe the analytification of the affine variety defined by $x^d + y^d = 1$. However, we want to describe the analytification of the projective variety F_d. There are d points of F_d which are not contained in T^0, given by

$$(\xi^j : 1 : 0) \text{ where } \xi \text{ is a primitive } d\text{th root of } -1.$$

Fixing some $0 \leq j < d$, we give a coordinate neighbourhood of the point $(\xi^j : 1 : 0)$ by

$$\varphi(z) = (\xi^j : \sqrt[d]{z^d - 1} : z)$$

in just the same way as the previous two cases.

Remark 10.3.6 We could have worked out all of the above using the implicit function theorem. If we had set things up just right, we would even have got the same answer. On the other hand, be warned that very naively applying the implicit function theorem can lead to a bit of a mess...

10.4 A map from the Fermat curve to $\mathbb{P}^1$

It is easy to give a map of varieties from F_d to $\mathbb{P}^1$; just take the x-coordinate. More precisely, we can cover F_d by two affine patches given by $x = 1$ and $y = 1$ (note that if both $x = 0$ and $y = 0$ then also $z = 0$ which is not a point in $\mathbb{P}^2$). On the $y = 1$ patch the curve is given by the equation $x^d + 1 = z^d$, and we take the map of affine varieties corresponding to the ring map

$$\mathbb{C}[s] \to \frac{\mathbb{C}[x,z]}{x^d + 1 - z^d}; s \mapsto x.$$

Similarly on the patch $x = 1$ the curve is given by the equation $1 + y^d = z^d$, and we take the map of affine varieties corresponding to the ring map

$$\mathbb{C}[t] \to \frac{\mathbb{C}[y,z]}{1 + y^d - z^d}; t \mapsto y.$$

If s and t are the standard coordinates on $\mathbb{P}^1$ (so $st = 1$) then one checks these maps are compatible, and so gives a map of varieties. Another way to think of it is that we send a point $(X : Y : Z)$ to $(X : Z)$, which is always well-defined because the point $(0 : 1 : 0)$ is not on F_d.

Analytification of maps of smooth varieties gives maps of the corresponding complex manifolds. What does this look like in terms of the holomorphic charts we described above on the Fermat curve? More precisely, for each point $p \in F_d^{an}$ we gave an open subset $U_p \subset \mathbb{C}$, an open neighbourhood $V_p \subset F_d$, and a homeomorphism $\varphi_p \colon U_p \to V_p$ (the open subsets were only implicitly described, by saying our constructions worked on 'small enough neighbourhoods'). There were three 'types' of points:

i. points $(x_0 : y_0 : 1)$ with $y_0 \neq 0$. Then the map to $\mathbb{CP}^1$ is given by $(x : y : 1) \mapsto (x : 1)$, and the composite with φ sends z to $(z : 1)$.

ii. points $(x_0 : 0 : 1)$. Then the map to $\mathbb{CP}^1$ is given by $(x : 0 : 1) \mapsto (x : 1)$, and the composite with φ sends z to $(z^d + \zeta^j : 1)$.

iii. points $(\xi^j : 1 : 0)$. Then the map to $\mathbb{CP}^1$ is given by $(x : y : z) \mapsto (x : z)$, and the composite with φ sends z to $(\xi^j : z)$.

In each case, the composite map is clearly holomorphic. Moreover, it is bijective (even a homeomorphism) in cases (1) and (3), and in case (2) it is d-to-1 except at the point $(x_0 : 0 : 1)$, where it is 1-to-1. This will be important later.

10.5 Triangulations of Riemann surfaces, Euler characteristic

For a little while, we will forget about varieties and complex manifolds (mostly), and do some topology.

Definition 10.5.1 A (real) manifold is a topological space T such that for every $t \in T$ there exists an open neighbourhood U of T and an open subset $V \subset \mathbb{R}^n$ for some n and a homeomorphism $U \to V$.

Note that being a real manifold is a *property* of a topological space, there is no extra data attached. There is an obvious notion of dimension. A real surface is a real manifold of dimension 2.

It is an easy exercise that if M is a complex manifold (say of dimension m) then the underlying topological space is a real manifold of dimension $2m$. In particular, a Riemann surface (1-dimensional complex manifold) has a real surface as its underlying topological space, which makes the terminology a little less weird.

Just as studying complex manifolds can tell us things about complex varieties, so studying real manifolds can tell us about complex manifolds. Be warned that real manifolds are much less 'rigid' than complex manifolds - for example, many non-isomorphic compact Riemann surfaces can have isomorphic underlying real manifold.

We want to talk about triangulations of Riemann surfaces. Let T be the closed subset

$$T = \{(x, y) \in \mathbb{R}^2 : x \geq 0 \text{ and } y \geq 0 \text{ and } x + y \leq 1\}.$$

The faces and corners are the obvious closed subsets.

Definition 10.5.2 Let X be a real surface. A *triangulation of X* consists of:

- A decomposition $X = \bigcup_{i \in I} X_i$ of X into finitely many closed subsets;
- for each $i \in I$ a homeomorphism $\tau_i \colon X_i \to T$

such that for every $i, j \in I$ we have that $\tau_i(X_i \cap X_j)$ is a face, edge or corner of T.

Theorem 10.5.3 *Every compact Hausdorff real surface admits a triangulation.*

Proof This is deep, and is omitted. Due to Radó. False in dimension 4 and higher! A nice exposition can be found in [*The Jordan-Schoenflies theorem and the classification of surfaces* by Carsten Thomassen, `http://www.maths.ed.ac.uk/~aar/jordan/thomass.pdf`]. □

Definition 10.5.4 Let X be a real surface and T a triangulation $X = \bigcup_{i \in I} X_i$. We define $F(X, T) = \#I$ ('the number of faces'), and analogously $E(X, T)$ to be the number of edges and $V(X, T)$ to be the number of vertices. We define the *Euler characteristic* of (X, T) to be

$$\chi(X, T) = V(X, T) - E(X, T) + F(X, T).$$

Clearly $V(X, T)$, $E(X, T)$ and $F(X, T)$ depend on T as well as X. However:

Theorem 10.5.5 *If T and T' are two triangulations of X then $\chi(X, T) = \chi(X, T')$.*

Proof Omitted. Not too hard compared to the existence of a triangulation. □

We can now connect back to complex manifolds (and so varieties):

Theorem 10.5.6 *Let X be a smooth connected projective complex curve of genus g. Then $\chi(X^{an}) = 2-2g$.*

Proof Omitted. Not technically particularly difficult, but needs a lot of tools for comparing topological and algebraic geometry. □

We will not prove this, but let us consider the example of $\mathbb{P}^1_{\mathbb{C}}$. You checked that the topological space is a sphere. The simplest triangulation is probably as a tetrahedron. Then there are 4 vertices, 6 edges and 4 faces, so $\chi(\mathbb{CP}^1) = 4 - 6 + 4 = 2$. On the other hand, the genus is 0, so we have $2 - 2g = 2$.

10.6 Genus of a topological cover

Definition 10.6.1 Let $f\colon X \to S$ be a morphism of topological spaces. We say f is a *covering of degree* n if for every $s \in S$ there exists an open neighbourhood U of p and a homeomorphism

$$f^{-1}U \to \sqcup_{1 \le i \le n} U.$$

Theorem 10.6.2 *Let $f\colon X \to S$ be a degree-n cover of real surfaces. Then*

$$\chi(X) = n\chi(S).$$

Proof [Sketch of proof] Because the Euler characteristic of S does not depend on the triangulation of S, we may assume the latter is arbitrarily fine, so that each face, edge (and vertex!) is contained in at least one of the opens U in the definition of a cover. Further, we can give X a triangulation by just pulling these back in the obvious manner. Then it is clear that there are n faces of X over every face of S, and the same for edges and vertices. $\square$

This theorem is neat, but we would really like to apply it to the map from the Fermat curve to $\mathbb{P}^1$, and this is not a topological cover (the map is d-to-1 almost everywhere, but 1-to-1 at exactly d-points). It turns out that we can 'correct' the above theorem to allow for this.

10.7 Riemann-Hurwitz formula

The following is a special case of the Riemann-Hurwitz formula. The general case is not very much harder to state or prove, and applies to any surjective map of connected compact Riemann surfaces.

Theorem 10.7.1 *Let $f\colon X \to S$ be a (holomorphic) map of connected compact Riemann surfaces. Assume that there is a finite set of points $R \subset S$ and an integer $d \ge 1$ such that:*

i. the restriction of f from $f^{-1}(S \setminus R)$ to $S \setminus R$ is a topological cover of degree d;

ii. for every $r \in R$, there exists an analytic neighbourhood U of r such that the map $f^{-1}U \to U$ is isomorphic (in the analytic category) to the map

$$\Delta \to \Delta; z \mapsto z^d$$

where $\Delta = \{z \in \mathbb{C} : |z| < 1\}$.

Then we have

$$\chi(X) = d\chi(S) + (1-d)\#R$$

Note that (i) above is actually always true, but we will not prove this and you should not assume it in exercises.

Proof [Sketch of proof] As before, we choose a 'fine enough' triangulation of S, but now we also impose that every point in R is a vertex. Again, we make a triangulation of X by pulling back the one on S. Then every face of S has d faces of X lying over it, and every edge of S has d edges of X lying over it. The vertices not in R also have d vertices over them, while the ones in R have exactly one vertex lying over them. We find

$$\chi(X) = V(X) - E(X) + F(X) = d(V(S) - \#R) + \#R - dE(S) + dF(S) = d\chi(S) + (1-d)\#R.$$

$\square$

10.8 Example: genus of a Fermat curve

The map we described before from F_d to $\mathbb{P}^1$ satisfies the conditions of the Riemann-Hurwitz theorem as stated above, with $d = d$. We take R to be the set of points $(\zeta^j : 1)$ for $0 \leq j < d$, so $\#R = d$. We know that $\chi(\mathbb{CP}^1) = 2$, so we find

$$\chi(F_d) = 2d - d(d-1)$$

If we write $g(F_d)$ for the genus of the Fermat curve, we see that

$$g(F_d) = \frac{(d-1)(d-2)}{2}. \tag{10.3}$$

10.9 Exercises

Exercise 10.9.1 The closed unit polydisk in $\mathbb{C}^n$ is defined to be the set of $(z_1, \ldots, z_n)$ in $\mathbb{C}^n$ such that for each $i = 1, \ldots, n$ we have $|z_i| \leq 1$. Take the open cover (in the complex topology!) of $\mathbb{CP}^n$ by standard affine opens $U_0, \ldots, U_n$. Show that $\mathbb{CP}^n$ is covered by the closed unit polydisks in the U_i. Show that $\mathbb{CP}^n$ is compact.

Exercise 10.9.2 Prove lemma 10.3.2.

Exercise 10.9.3 Compute the Euler characteristic of the surface of a doughnut.

Exercise 10.9.4 Suppose $f\colon \mathbb{P}^1 \to \mathbb{P}^1$ is a map of complex varieties such that $f^{an}\colon \mathbb{CP}^1 \to \mathbb{CP}^1$ is a topological cover of degree d for some d. What are the possible values of d?

Exercise 10.9.5 Let a, b, c be distinct complex numbers. Define a curve $C \subset \mathbb{P}^2_{\mathbb{C}}$ by the equation

$$y^2 = (x-a)(x-b)(x-c).$$

Define $\pi\colon C \to \mathbb{P}^1_{\mathbb{C}}$ by sending $(X : Y : Z)$ to $(X : Z)$ if $(X : Y : Z)$ is not equal to $(0 : 1 : 0)$, and sending $(0 : 1 : 0)$ to $(1 : 0)$.

i. Verify that π is a map of complex varieties.

ii. Verify that π^{an} satisfies the hypotheses of theorem 10.7.1 for some d (what is that d?). Take care with the point at $Z = 0$.

iii. Compute the genus of C.

Exercise 10.9.6 Give an example of a map of topological spaces from $\mathbb{CP}^1$ to $\mathbb{CP}^1$ which does not arise as the analytification of any map of varieties $\mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$. You can describe your map in words, but you must show that it does not come from a map of varieties.

Lecture 11

Curves on surfaces

We return to working with varieties over an arbitrary algebraically closed field.

In this lecture, for closed curves Z_1 and Z_2 on a smooth irreducible projective surface X, we will define their intersection number $Z_1 \cdot Z_2$. This intersection product will be important for the proof of the Hasse-Weil inequality.

11.1 Divisors

Let X be a connected, quasi-projective variety, smooth of dimension d. So in particular X is irreducible.

Definition 11.1.1 A *prime divisor* on X is a closed irreducible subset $Z \subset X$ of dimension $d-1$.

Definition 11.1.2 A *divisor* is an element of the free abelian group generated by the prime divisors. We denote this group by $\mathrm{Div}(X)$.

So divisors are formal expressions of the form $\sum_Z n_Z Z$ with Z ranging over the set of prime divisors, and with the n_Z integers, all but finitely many zero. We state without proof the following proposition (which uses the smoothness of X).

Proposition 11.1.3 *Let X be a smooth, connected, quasi-projective variety. Let $Z \subset X$ be a prime divisor. Then there is a finite open affine cover $\{U_i\}_i$ of X, such that there are nonzero $f_i \in \mathcal{O}_X(U_i)$ with the property that $I(Z \cap U_i) = (f_i)$ as ideals in $\mathcal{O}_X(U_i)$.*

Now we want to associate a valuation to a prime divisor. Let $Z \subset X$ be a prime divisor. Use an affine cover $\{U_i : i \in I\}$ as in the above proposition. Then choose an i with $Z \cap U_i \neq \emptyset$. For $0 \neq f \in \mathcal{O}_X(U_i)$ we define:

$$v_Z(f) := \text{the largest integer } n \text{ such that } f \in (f_i^n).$$

Such a largest integer exists and it does not depend on the chosen cover $\{U_i : i \in I\}$ and the particular choice of i. This v_Z has the property $v_Z(fg) = v_Z(f) + v_Z(g)$. As usual we extend this to a morphism $v_Z \colon K(X)^\times \to \mathbb{Z}$.

Definition 11.1.4 Let X be a smooth, connected, quasi-projective variety. Then we define the divisor map

$$\mathrm{div}\colon K(X)^\times \longrightarrow \mathrm{Div}(X), \quad f \mapsto \mathrm{div}(f) := \sum_{Z \text{ prime}} v_Z(f) Z.$$

Note that div is a group homomorphism. To see that the sum occurring in $\operatorname{div}(f)$ is finite, first reduce to the case that X is affine (it has a cover by finitely many), then write f as g/h and note that nonzero coefficients only occur at Z that are irreducible components of $Z(g)$ or $Z(h)$. A divisor of the form $\operatorname{div}(f)$ is called a *principal divisor*.

Definition 11.1.5 For X a smooth, connected, quasi-projective variety we define the *Picard group* as $\operatorname{Pic}(X) := \operatorname{Div}(X)/\operatorname{div}(K(X)^\times)$, that is, the quotient of $\operatorname{Div}(X)$ by the subgroup of principal divisors.

Example 11.1.6 We determine the Picard group of $X = \mathbb{A}^d$. Recall that the prime divisors of $\mathbb{A}^d$ are the $Z(f)$ for $f \in k[x_1, \dots, x_d]$ irreducible. But then every prime divisor is principal, hence hence $\operatorname{Pic}(\mathbb{A}^d) = 0$.

Proposition 11.1.7 *Let $X = \mathbb{P}^d$ with $d \in \mathbb{Z}_{\geq 1}$. Then $\operatorname{Pic}(\mathbb{P}^d) \cong \mathbb{Z}$, generated by the class of a hyperplane.*

Proof We first determine the prime divisors of $\mathbb{P}^d$. These are the $Z(f)$ where $f \in k[x_0, \dots, x_d]$ is homogeneous and irreducible. We now define $\deg(Z(f)) = \deg(f)$ (indeed, $Z(f)$ determines f up to scalar multiple). We extend this to a morphism of groups and obtain a map deg as follows:

$$\deg\colon \operatorname{Div}(X) \longrightarrow \mathbb{Z}, \quad \sum_Z n_Z Z \mapsto \sum_Z n_Z \deg(Z).$$

We now claim that $\sum_Z n_Z Z$ is principal if and only if $\deg(\sum_Z n_Z Z) = 0$. Indeed, consider a divisor $\operatorname{div}(f)$ for some $f \in K(X)^\times$ and write $f = g/h$ with g and h in $k[x_0, \dots, x_d]$ homogeneous of the same degree. Decompose g and h into irreducibles, $g = \prod_i g_i^{n_i}$ and $h = \prod_i h_i^{m_i}$, then

$$\deg(\operatorname{div}(f)) = \sum_i n_i \deg(g_i) - \sum_i m_i \deg(h_i) = \deg(g) - \deg(h) = 0.$$

On the other hand, if $\deg(\sum n_i Z_i) = 0$, then let $Z_i = Z(f_i)$ and consider $f := \prod f_i^{n_i}$. By construction $\deg(f) = 0$ and so $f \in K(X)^\times$ and $\operatorname{div}(f) = \sum n_i Z_i$.

So the degree factors through an injective map $\operatorname{Pic}(X) \to \mathbb{Z}$. The map is also surjective, since for example $\deg Z(x_0) = 1$. □

Proposition 11.1.8 *Let X be a smooth, irreducible projective curve. Every principal divisor on X has degree zero.*

Proof Let D be a divisor on X, let $f \in K(X)^\times$, and let $D' = D - \operatorname{div}(f)$. Then multiplication by f induces an isomorphism from $H^0(X, D)$ to $H^0(X, D')$ and from $H^1(X, D)$ to $H^1(X, D')$ (the reader is requested to verify this for herself!). Riemann-Roch now gives:

$$\begin{aligned} \deg(D) + 1 - g &= \dim H^0(X, D) - \dim H^1(X, D) \\ &= \dim H^0(X, D') - \dim H^1(X, D') \\ &= \deg(D') + 1 - g \end{aligned}$$

So $\deg(D) = \deg(D') = \deg(D) - \deg(\operatorname{div}(f))$. Hence $\deg(\operatorname{div}(f)) = 0$. □

11.2 The intersection pairing on surfaces

Let X be a smooth connected projective surface (a smooth connected projective variety of dimension 2). In this section we define the intersection pairing on $\operatorname{Div}(X)$, show that it factors through $\operatorname{Pic}(X)$, and derive Bézout's theorem for $\mathbb{P}^2$ as a very simple consequence.

For prime divisors Z_1 and Z_2 on X the intersection number $Z_1{\cdot}Z_2$ in $\mathbb{Z}$ is defined as the degree on Z_1 of a locally free $\mathcal{O}_{Z_1}$-module of rank one, $\mathcal{O}_X(Z_2)|_{Z_1}$. As we have not defined these notions (lack of time) we give the procedure that produces $Z_1{\cdot}Z_2$ in terms of concepts that we have defined, and that one would use even if one had the notions that we did not define. This definition of $Z_1{\cdot}Z_2$ does not assume that Z_1 and Z_2 are distinct.

Definition 11.2.1 Let Z_1 and Z_2 be prime divisors on X.

i. Choose open subsets $(U_i)_{i\in I}$ ($I = \{1,\ldots,r\}$ for some r) in X and f_i in $\mathcal{O}_X(U_i)$ such that the U_i cover Z_2, each U_i meets Z_2, and such that $\mathrm{div}(f_i) = Z_1 \cap U_i$ on U_i. In particular, $I(Z_1 \cap U_i) = (f_i)$ (as in Proposition 11.1.3).

ii. Since f_i and f_j generate the same ideal of $\mathcal{O}_X(U_{ij})$ there are unique f_{ij} in $\mathcal{O}_X(U_{ij})^\times$ such that $f_i = f_{ij}f_j$ in $\mathcal{O}_X(U_{ij})$. Note that $f_{ij}{\cdot}f_{jk} = f_{ik}$ on $U_{ijk} := U_i \cap U_j \cap U_k$.

iii. Define $g_i := f_{i1} \in \mathcal{O}_{Z_2}(Z_2 \cap U_{i1})^\times$. Remark that $g_1 = 1$ and that $g_i = f_{ij}g_j$ in $\mathcal{O}_{Z_2}(Z_2 \cap U_{ij})$. This shows that $g_i \neq 0$ in $\mathcal{O}_{Z_2}(Z_2 \cap U_{i1})$. For $P \in Z_2$ and i such that $P \in U_i$, the number $v_P(g_i)$ depends only on P. We finally define:
$$Z_1{\cdot}Z_2 := \sum_{P\in Z_2} v_P(g_{i_P}) = \sum_{P\in Z_2 - Z_2\cap U_1} v_P(g_{i_P}), \quad \text{where } i_P \in I \text{ such that } P \in U_{i_P}.$$

Remark 11.2.2 The ideas behind Definition 11.2.1 can be understood, very briefly, as follows. On U_i, the $\mathcal{O}_X$-module $\mathcal{O}_X(Z_1)$ is generated by $1/f_i$. The $\mathcal{O}_{Z_2}$-module $\mathcal{O}_X(Z_1)|_{Z_2}$ has the rational section $1/f_1$, and on U_i we have $1/f_1 = (f_i/f_1){\cdot}(1/f_i)$, hence f_i/f_1 on $U_i \cap Z_2$ measures how far $1/f_1$ is from a generator.

As promised, we will show that this really is a good definition. We will make frequent use of the following fact, which we will not prove. We refer to Proposition 11.1.8 for a proof in the smooth case.

Proposition 11.2.3 *If f is a rational function on an irreducible projective curve X then* $\deg \mathrm{div}(f) = 0$.

Lemma 11.2.4 *The integer $Z_1{\cdot}Z_2$ does not depend on the choice of the f_i.*

Proof Assume that f_i' for i in I satisfy the same conditions as the f_i. Then $f_i' = u_if_i$ with $u_i \in \mathcal{O}_X(U_i)^\times$, and $f_{ij}' := f_i'/f_j' = (u_i/u_j)f_{ij}$ and $g_i' = (u_i/u_1)g_i$. This then gives (we use that $v_P(u_i) = 0$ for all $P \in U_i$ and that the degree of a principal divisor is 0):
$$(Z_1{\cdot}Z_2)' = Z_1{\cdot}Z_2 + \sum_P v_P(u_{i_P}/u_1) = Z_1{\cdot}Z_2 + \deg(\mathrm{div}(1/u_1)) = Z_1{\cdot}Z_2.$$
□

Lemma 11.2.5 *The integer $Z_1{\cdot}Z_2$ does not depend on the choice of* 1 *in* $\{1,\ldots,r\}$ *in step iii.*

Proof Assume that we use U_2 instead. Then $g_i' = f_{i2} = f_{i1}f_{12} = g_if_{12}$. Hence:
$$(Z_1{\cdot}Z_2)' = Z_1{\cdot}Z_2 + \deg(\mathrm{div}(f_{12})) = Z_1{\cdot}Z_2$$
□

Lemma 11.2.6 *The integer $Z_1{\cdot}Z_2$ does not depend on the choice of the open cover $\{U_i : i \in I\}$.*

Proof Given two covers $\{U_i : i \in I\}$ and $\{U_j' : j \in J\}$, one can consider a common refinement (given by for example the open $\{U_i \cap U_j' : i \in I, j \in J\}$). So it is enough to show that the lemma holds for a refinement, and this is just a calculation which we leave to the reader. □

As $\mathrm{Div}(X)$ is the free $\mathbb{Z}$-module with basis the set of prime divisors on X, the map "$\cdot$" extends bilinearly and obtain a bilinear map:

$$\cdot\colon\ \mathrm{Div}(X)\times\mathrm{Div}(X)\longrightarrow\mathbb{Z},\quad (Z_1,Z_2)\mapsto Z_1{\cdot}Z_2.$$

Proposition 11.2.7 *Let $Z_1\neq Z_2$ be prime divisors. Then $Z_1\cap Z_2$ is finite. For all P in $Z_1\cap Z_2$ there is an open affine $U_P\subset X$ with $P\in U_P$ such that $U_P\cap Z_1\cap Z_2=\{P\}$ and $f_{1,P}$ and $f_{2,P}\in\mathcal{O}_X(U_P)$ such that $I(Z_1\cap U_P)=(f_{1,P})$ and $I(Z_2\cap U_P)=(f_{2,P})$. For such a collection of U_P we have:*

$$Z_1{\cdot}Z_2=\sum_{P\in Z_1\cap Z_2}\dim\mathcal{O}_X(U_P)/(f_{1,P},f_{2,P}).$$

For each $P\in Z_1\cap Z_2$ the integer $\dim\mathcal{O}_X(U_P)/(f_{1,P},f_{2,P})$ is independent of the choice of U_P, and is called the local intersection multiplicity of Z_1 and Z_2 at P.

Proof As $Z_1\cap Z_2$ is closed in the projective curve Z_1, and not equal to Z_1, it is finite. The existence of a collection of $(U_P,f_{1,P},f_{2,P})$ as in the proposition follows from the fact that the set of open affines in X is a basis for the topology, together with Proposition 11.1.3. But note that $Z_1\cap Z_2$ may be empty. We extend this collection of $(U_P,f_{1,P},f_{2,P})$ to one $(U_i,f_{1,i},f_{2,i})$, $i\in I$, such that the $U_i\cap Z_1\cap Z_2$ have at most one element and are disjoint, and the conditions in step i of Definition 11.2.1 are met: the U_i cover Z_2 and all meet Z_2. For P in Z_2, let i_P be an $i\in I$ such that U_i contains P; this i_P is unique if P is in $Z_1\cap Z_2$.

As Z_1 and Z_2 are distinct all $f_{1,i}\in\mathcal{O}_X(U_i)$ are not identically zero on $Z_2\cap U_i$, and give nonzero rational functions on Z_2, regular on $U_i\cap Z_2$, that we still denote by $f_{1,i}$. Definition 11.2.1 gives

$$Z_1{\cdot}Z_2=\sum_{P\in Z_2}v_P(f_{1,i_P}/f_{1,1}).$$

As for every i we have $\mathcal{O}_{Z_2}(U_i\cap Z_2)=\mathcal{O}_X(U_i)/(f_{2,i})$, and the degree of a principal divisor on a projective curve is zero, and for $i\in I$ such that $U_i\cap Z_1\cap Z_2$ is empty, $\mathcal{O}_X(U_i)/(f_{1,i},f_{2,i})=0$, we get:

$$\begin{aligned}
Z_1{\cdot}Z_2&=\sum_{P\in Z_2}v_P(f_{1,i_P})-\sum_{P\in Z_2}v_P(f_{1,1})=\sum_{P\in Z_2}\dim\mathcal{O}_{Z_2}(Z_2\cap U_{i_P})/(f_{1,i_P})\\
&=\sum_{P\in Z_2}\dim\mathcal{O}_X(U_{i_P})/(f_{2,i_P},f_{1,i_P})\\
&=\sum_{P\in Z_1\cap Z_2}\dim\mathcal{O}_X(U_{i_P})/(f_{1,i_P},f_{2,i_P}).
\end{aligned}$$

$\square$

Using local rings, the above definition of the local intersection multiplicity may be made more intrinsic (and hence more visibly independent of choices) as follows. Let $Z_1\neq Z_2$ be prime divisors, and $P\in Z_1\cap Z_2$. Inside the local ring $\mathcal{O}_{X,P}$ we have the ideal $I(Z_1)$ given by classes of (U,f) such that f vanishes along $Z_1\cap U$. The ideal $I(Z_1)$ is principal, say $I(Z_1)=(f_1)$. Similarly we have an ideal $I(Z_2)\subset\mathcal{O}_{X,P}$ associated to Z_2 and an element $f_2\in\mathcal{O}_{X,P}$ such that $I(Z_2)=(f_2)$. Then the local intersection multiplicity of Z_1,Z_2 at P is equal to $\dim\mathcal{O}_{X,P}/(f_1,f_2)$. We leave the verification of this as an exercise for the interested reader.

Corollary 11.2.8 *If $Z_1\neq Z_2$ are distinct then $Z_1{\cdot}Z_2\geq 0$.*

Remark 11.2.9 If $Z_1=Z_2$, then $Z_1{\cdot}Z_2$ can be negative, as can be seen in Exercise 11.3.1.

Corollary 11.2.10 *The intersection pairing $\cdot\colon\ \mathrm{Div}(X)\times\mathrm{Div}(X)\to\mathbb{Z}$, $(Z_1,Z_2)\mapsto Z_1{\cdot}Z_2$ is symmetric.*

Proof In view of Proposition 11.2.7 this is now obvious. □

Proposition 11.2.11 *Situation as in Proposition 11.2.7. If $Z_1 \neq Z_2$ and for all P in $Z_1 \cap Z_2$ the tangent spaces $T_{Z_1}P$ and $T_{Z_2}P$ have a trivial intersection (inside $T_X P$), then $Z_1 {\cdot} Z_2 = \#(Z_1 \cap Z_2)$. In this case we say that Z_1 and Z_2 intersect transversally.*

Theorem 11.2.12 *The intersection pairing* $\cdot\colon \operatorname{Div}(X) \times \operatorname{Div}(X) \to \mathbb{Z}$ *factors through* $\operatorname{Pic}(X) \times \operatorname{Pic}(X)$.

Proof It suffices (by symmetry) to verify that $Z_1{\cdot}Z_2 = 0$ for $Z_1 = \operatorname{div}(f)$ for some $f \in K(X)^\times$ and Z_2 a prime divisor. Write $Z_1 = \sum_Z Z_1(Z)Z$ with Z ranging over the set of prime divisors on X. We take an open cover $\{U_i : i \in I\}$ such that for all the Z with $Z_1(Z) \neq 0$ and for each i in I we have an $f_{i,Z} \in \mathcal{O}_X(U_i)$ such that $\mathcal{O}_X(U_i){\cdot}f_{i,Z}$ is the ideal of $Z \cap U_i$ (take a common refinement if necessary). Then for each i there is a u_i in $\mathcal{O}_X(U_i)^\times$ such that $\prod_Z f_{i,Z}^{Z_1(Z)} = u_i f$. Linearity in Z_1, Definition 11.2.1, the fact that $v_P(u_{i_P}) = 0$, and Theorem 12.1.10 ii, give

$$
\begin{aligned}
Z_1{\cdot}Z_2 &= \sum_Z Z_1(Z) \sum_{P\in Z_2} v_P(f_{i_P,Z}/f_{1,Z}) = \sum_{P\in Z_2} v_P\left(\frac{\prod_Z f_{i_P,Z}^{n_Z}}{\prod_Z f_{1,Z}^{n_Z}}\right) = \sum_{P\in Z_2} v_P\left(\frac{u_{i_P} f}{u_1 f}\right) \\
&= \sum_{P\in Z_2} v_P(u_{i_P}/u_1) = -\sum_{P\in Z_2} v_P(u_1) = -\deg(\operatorname{div}(u_1|_{Z_2})) = 0.
\end{aligned}
$$

□

Corollary 11.2.13 (Bézout) *Let Z_1 and Z_2 be prime divisors in $\mathbb{P}^2$, then $Z_1{\cdot}Z_2 = \deg(Z_1){\cdot}\deg(Z_2)$.*

Proof By Theorem 11.2.12 the intersection pairing is given by $\cdot\colon \operatorname{Pic}(\mathbb{P}^2) \times \operatorname{Pic}(\mathbb{P}^2) \to \mathbb{Z}$. The degree map $\deg\colon \operatorname{Pic}(\mathbb{P}^2) \to \mathbb{Z}$ is an isomorphism by Lemma 11.1.7. The induced bilinear map $\cdot\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is determined by the value of $(1, 1)$. So it suffices to prove that there are two lines Z_1 and Z_2 in $\mathbb{P}^2$ such that $Z_1{\cdot}Z_2 = 1$. Take the lines $Z_1 = Z(x_1)$ and $Z_2 = Z(x_2)$, and apply Proposition 11.2.7. □

11.3 Exercises

Exercise 11.3.1 Assume that the characteristic of k is not 3. Let $X \subset \mathbb{P}^3$ be the surface given by $x_0^3 - x_1^3 + x_2^3 - x_3^3 = 0$. Verify that X is smooth. Let $Z \subset X$ be the line consisting of the points $(s : s : t : t)$ with $(s, t) \in k^2 - \{0\}$. Compute the intersection number $Z{\cdot}Z$.

Exercise 11.3.2 Show that any morphism $f\colon \mathbb{P}^2 \to \mathbb{P}^1$ is constant. Hint: if not show that f is surjective and that $f^{-1}(0 : 1)$ and $f^{-1}(1 : 0)$ are curves. Use Bézout to obtain a contradiction.

Exercise 11.3.3 Assume that 6 is invertible in k. Let $C \subset \mathbb{P}^2$ be a smooth curve given by a homogeneous polynomial $f \in k[x_0, x_1, x_2]$ of degree 3. Given a point $P \in C$ denote by $L_P \subset \mathbb{P}^2$ the tangent line in P to C.

i. Show that L_P intersects C in only the point P if and only if the local intersection multiplicity of L_P and C at P is 3. If this is the case P is called a flex-point of C.

ii. Show that $P = (p_0 : p_1 : p_2)$ is a flex point if and only if the determinant of the matrix $(\partial^2 f/\partial x_i \partial x_j)$ is zero at $(x, y, z) = (p_0, p_1, p_2)$.

iii. Show that C has 9 flex-points.

Exercise 11.3.4 Consider $X = \mathbb{P}^1 \times \mathbb{P}^1$ and use coordinates $x : y$ on the first factor and $u : v$ on the second factor.

If $f \in k[x, y, u, v]$ is polynomial which is homogeneous of degree d in x, y and homogeneous of degree e in u, v then we say that f is bihomogeneous and has bidegree (d, e). For example, $x^3u + xy^2v - y^3v$ is bihomogeneous of bidegree $(3, 1)$.

Denote the prime divisors $\{(0 : 1)\} \times \mathbb{P}^1$ and $\mathbb{P}^1 \times \{(0 : 1)\}$ by V and H, respectively.

i. Show that V is equivalent with $V' = \{(1 : 1)\} \times \mathbb{P}^1$ and deduce that $V \cdot V = 0$. Same for $H \cdot H$.

ii. Show that $H \cdot V = 1$.

iii. If f is irreducible and bihomogeneous of bidegree (d, e) show that

$$Z(f) = \{((a_0 : a_1), (b_0 : b_1)) \in \mathbb{P}^1 \times \mathbb{P}^1 : f(a_0, a_1, b_0, b_1) = 0\}$$

is a prime divisor on $\mathbb{P}^1 \times \mathbb{P}^1$ which is equivalent with $dV + eH$.

Lecture 12

Serre duality, varieties over $\mathbb{F}_q$ and their zeta function

12.1 Serre duality

Let X be an irreducible projective smooth curve and let $D = \sum_{P \in X} D(P)P$ be a divisor on X. For $\omega \in \Omega^1_{K(X)}$ a non-zero rational 1-form on X we define:

$$\operatorname{div}(\omega) = \sum_{P \in X} v_P(\omega) P.$$

We define:

$$\begin{aligned} H^0(X, \Omega^1(-D)) &:= \{0 \neq \omega \in \Omega^1_{K(X)} : \operatorname{div}(\omega) - D \geq 0\} \cup \{0\} \\ &= \{0 \neq \omega \in \Omega^1_{K(X)} : \forall P \in X,\ v_P(\omega) \geq D(P)\} \cup \{0\}. \end{aligned}$$

Fact 12.1.1 $H^0(X, \Omega^1(-D))$ is finite dimensional.

Recall that we have the following map for $X = U_1 \cup U_2$, U_1, U_2 affine open:

$$\delta\colon H^0(U_1, D) \oplus H^0(U_2, D) \to H^0(U_1 \cap U_2, D), \quad (f_1, f_2) \mapsto f_1|_{U_1 \cap U_2} - f_2|_{U_1 \cap U_2}.$$

The cokernel of this map was defined to be $H^1(X, D)$. We define the following pairing:

(12.1.2) $$\langle \cdot, \cdot \rangle : H^0(U_1 \cap U_2, D) \times H^0(X, \Omega^1(-D)) \to k, \quad (g, \omega) \mapsto \sum_{P \in X - U_2} \operatorname{res}_P(g \cdot \omega).$$

Theorem 12.1.3 (Serre duality) *Let X be a smooth irreducible projective curve. The pairing in (12.1.2) induces a perfect pairing*

$$H^1(X, D) \times H^0(X, \Omega^1(-D)) \to k.$$

It does not depend on the choice of the pair (U_1, U_2) in the same sense as in Facts 8.3.5.

Remark 12.1.4 We have chosen to sum over residues at the points missing U_2. One can also decide to do it for the points missing U_1, and this would change the pairing by a factor -1. To see this, first notice that $U_1^c \cap U_2^c = \emptyset$ and by definition $g \cdot \omega$ is regular at the points of $U_1 \cap U_2$. Furthermore, one can show that for all $\theta \in \Omega^1_{K(X)}$ one has $\sum_{P\in X} \mathrm{res}_P(\theta) = 0$. This gives:

$$\begin{aligned} 0 &= \sum_{P\in X} \mathrm{res}_P(g\cdot\omega) \\ &= \sum_{P\in X-U_1} \mathrm{res}_P(g\cdot\omega) + \sum_{P\in X-U_2} \mathrm{res}_P(g\cdot\omega) + \sum_{P\in U_1\cap U_2} \mathrm{res}_P(g\cdot\omega) \\ &= \sum_{P\in X-U_1} \mathrm{res}_P(g\cdot\omega) + \sum_{P\in X-U_2} \mathrm{res}_P(g\cdot\omega). \end{aligned}$$

Corollary 12.1.5 *Let X be a smooth irreducible projective curve. Then $H^0(X,\Omega^1)$ and $H^1(X,\mathcal{O}_X)$ are both of dimension g, the genus of X.*

Proof By Theorem 12.1.3 the finite dimensional k-vector spaces $H^0(X,\Omega^1)$ and $H^1(X,\mathcal{O}_X)$ are isomorphic to each other's dual, hence they have the same dimension. □

Using Riemann-Roch and Serre duality, one obtains the following theorem.

Theorem 12.1.6 *Let X be a smooth irreducible projective curve, and D a divisor on X. Then*

$$\dim H^0(X,D) - \dim H^0(X,\Omega^1(-D)) = \deg(D) + 1 - g.$$

Definition 12.1.7 Let X be a smooth irreducible projective curve. For $\omega_0 \in \Omega^1_{K(X)}$ non-zero, the divisor $\mathrm{div}(\omega_0)$ is called *a canonical divisor*.

Remark 12.1.8 Let X be a smooth irreducible projective curve. For $\omega = f\cdot\omega_0$ with $f \in K(X)^\times$ and ω_0 as above, $\mathrm{div}(\omega) = \mathrm{div}(\omega_0) + \mathrm{div}(f)$, so two canonical divisors differ by a principal divisor.

Lemma 12.1.9 *Let X be a smooth irreducible projective curve. For D a divisor on X, consider the following map $\varphi\colon K(X) \to \Omega^1_{K(X)}$, $f \mapsto f\cdot\omega_0$. This map induces an isomorphism of k-vector spaces $H^0(X,\mathrm{div}(\omega_0)-D) \to H^0(X,\Omega^1(-D))$.*

Proof Notice that:

$$\begin{aligned} f\cdot\omega_0 \in H^0(X,\Omega^1(-D)) &\iff \mathrm{div}(f\cdot\omega_0) - D \geq 0 \\ &\iff \mathrm{div}(f) + (\mathrm{div}(\omega_0) - D) \geq 0 \\ &\iff f \in H^0(X,\mathrm{div}(\omega_0) - D). \end{aligned}$$

□

Theorem 12.1.10 *Let X be a smooth irreducible projective curve.*

i. Let $\omega_0 \in \Omega^1_{K(X)}$ be non-zero. Then $\deg(\mathrm{div}(\omega_0)) = 2g-2$. In other words, every canonical divisor on X has degree $2g-2$.

ii. Let f be in $K(X)^\times$. Then $\deg(\mathrm{div}(f)) = 0$. In other words, every principal divisor has degree zero.

iii. Let D be a divisor on X. Then $H^0(X,D) = \{0\}$ if $\deg D < 0$, and $\dim H^0(X,D) = \deg D + 1 - g$ if $\deg D > 2g-2$.

Proof i. We use Theorem 12.1.6 with $D = \mathrm{div}(\omega_0)$ in combination with the above lemma and Corollary 12.1.5. We get:

$$\begin{aligned} \deg(D) &= g - 1 + \dim H^0(X,D) - \dim H^0(X,\Omega^1(-D)) \\ &= g - 1 + \dim H^0(X,\Omega^1(0)) - \dim H^0(X,0) \\ &= g - 1 + g - 1 \\ &= 2g-2. \end{aligned}$$

ii. We have proved this already in Proposition 11.1.8. Here is another proof, using a canonical divisor. Let f be in $K(X)^\times$. Take $\omega \in \Omega^1_{K(X)}$ nonzero. Then $\mathrm{div}(f\cdot\omega) = \mathrm{div}(f) + \mathrm{div}(\omega)$. Hence $\mathrm{div}(f)$ is the difference of two canonical divisors and therefore it has degree zero.

iii. The first case follows directly from ii. For the second case, notice that $H^0(X, \Omega^1(-D)) = \{0\}$ and apply Theorem 12.1.6. □

Remark 12.1.11 We note that $2-2g$ is the Euler characteristic of the sphere with g handles attached to it.

12.2 Projective varieties over $\mathbb{F}_q$

Let $\mathbb{F}_q$ be a finite field with $\#\mathbb{F}_q = q$ elements. Let $\mathbb{F}_q \to \mathbb{F}$ be an algebraic closure. Now consider $\sigma\colon \mathbb{F} \to \mathbb{F}$, $a \mapsto a^q$. Then σ is an automorphism of $\mathbb{F}$ and $\mathbb{F}_q = \{a \in \mathbb{F} : \sigma(a) = a\}$.

Let $X \subset \mathbb{P}^n = \mathbb{P}^n(\mathbb{F})$ be closed and let $I \subset \mathbb{F}[x_0, \ldots, x_n]$ be its ideal; I homogeneous and radical. Assume that I is generated by elements in $\mathbb{F}_q[x_0, \ldots, x_n]$, that is, $I = (f_1, \ldots, f_r)$ with $f_i \in \mathbb{F}_q[x_0, \ldots, x_n]$ for all i. We say: "X is defined over $\mathbb{F}_q$. " This gives X some extra structures.

i. The q-Frobenius endomorphism $F_X\colon X \to X$, $a = (a_0 : \cdots : a_n) \mapsto (a_0^q : \cdots : a_n^q)$. This is a morphism of varieties over $\mathbb{F}$. Note that for a in X, $F_X(a) = a$ if and only if $a \in X(\mathbb{F}_q) := \mathbb{P}^n(\mathbb{F}_q) \cap X$.

ii. An affine presentation of X "defined over $\mathbb{F}_q$." Let $X_i = Z(f_{i,1}, \ldots, f_{i,r}) \subset \mathbb{A}^n$ with

$$f_{i,k} = f_k(x_{i,0}, \ldots, x_{i,n}) \in \mathbb{F}_q[\{x_{i,j} : j \neq i\}]$$

and $X_{i,j} = D(x_{i,j}) \cap X_i$ with $\varphi_{i,j}\colon X_{i,j} \tilde{\to} X_{j,i}$ where $\varphi_{i,j}$ is defined by polynomials over $\mathbb{F}_q$.

Definition 12.2.1 The category of projective varieties over $\mathbb{F}_q$ has as objects the pairs (X, F_X) as above, and as morphisms the $f\colon X \to Y$ (morphisms of varieties over $\mathbb{F}$) such that $F_Y \circ f = f \circ F_X$.

12.3 Divisors on curves over $\mathbb{F}_q$

Let $X_0 := (X, F_X)$ be a projective variety over $\mathbb{F}_q$, with X irreducible and smooth of dimension 1 (so X is a smooth irreducible projective curve).

Definition 12.3.1 A *prime divisor* on X_0 of degree d is a divisor $D = P_1 + \cdots + P_d$ on X with the P_i in X distinct and transitively permuted by F_X. We let $\deg(D) = d$.

Example 12.3.2 If $X_0 = (\mathbb{P}^1, F_{\mathbb{P}^1})$ and D is a prime divisor on X_0, then either $D = \infty$ or there is an irreducible $f \in \mathbb{F}_q[x]$ such that D is the formal sum of the zeros of f in $\mathbb{F}$.

Note that $\dim_{\mathbb{F}_q}(\mathbb{F}_q[x]/(f)) = \deg(f) = \deg(D)$. So the prime divisors are closely related to maximal ideals of a certain ring, and this motivates our next definition.

Definition 12.3.3 We define the zeta function of X_0 as

$$Z(X_0, t) := \prod_{D \text{ prime}} \frac{1}{1 - t^{\deg D}} \in \mathbb{Z}[[t]].$$

Remark 12.3.4 This product indeed converges because for all $r \geq 1$, $X(\mathbb{F}_{q^r}) \subset \mathbb{P}^n(\mathbb{F}_{q^r})$ is finite. So the number of F_X-orbits of length r is finite.

Definition 12.3.5 Let P be the set of prime divisors on X_0. We define the group of divisors on X_0 as $\mathrm{Div}(X_0) := \mathbb{Z}^{(P)}$, and $\mathrm{Div}(X_0)^+ := \mathbb{N}^{(P)}$, the subset of effective divisors.

The map $F_X : X \to X$ induces a homomorphism $F_X\colon \operatorname{Div} X \to \operatorname{Div} X$ and we have that $\operatorname{Div} X_0$ is the subgroup of $\operatorname{Div} X$ consisting of those divisors D that satisfy $F_X(D) = D$.

Proposition 12.3.6 *We have* $Z(X_0, t) = \sum_{n\geq 0} d_n \cdot t^n$, *with* $d_n = \#\{D \in \operatorname{Div}(X_0)^+ : \deg(D) = n\}$.

Proof

$$Z(X_0, t) = \prod_{D\in P} \frac{1}{1 - t^{\deg(D)}} = \prod_{D\in P} \sum_{n\geq 0} t^{n\cdot\deg(D)} = \sum_{D\in\operatorname{Div}(X_0)^+} t^{\deg D} = \sum_{n\geq 0} d_n t^n.$$

□

The same argument is used for establishing the Euler product for the Riemann zeta function.

We want to study $\operatorname{Div}(X_0)$ using finite dimensional $\mathbb{F}_q$-vector spaces $H^0(X_0, D)$. We take the shortest route to define these: via the action of σ on $K(X)$.

Let $U \subset X$ be a nonempty open affine subset, defined over $\mathbb{F}_q$: U is closed in $\mathbb{A}^n$, $I(U) = (f_1, \ldots, f_r)$, with $f_i \in \mathbb{F}_q[x_1, \ldots, x_n]$. Then σ acts on $\mathbb{F}[x_1, \ldots, x_n]$, $g = \sum_i g_i x^i$ is mapped to $\sigma g := \sum_i (\sigma g_i)x^i$. Note that $\sigma(I(U)) = I(U)$, since the f_i are fixed by σ. So we even have an induced action of σ on $\mathcal{O}(U) = \mathbb{F}[x_1, \ldots, x_n]/I(U)$. One can show that this action of σ on $\mathcal{O}(U)$ is independent of the chosen embedding in $\mathbb{A}^n$.

Now recall that $K(X) = Q(\mathcal{O}(U))$ (the fraction field), so we have an action on $K(X)$ as well. We put $K(X_0) := K(X)^\sigma = \{f \in K(X) : \sigma(f) = f\}$. For $D \in \operatorname{Div}(X_0)$ we have an induced action of σ on $H^0(X, D)$ and we put $H^0(X_0, D) := H^0(X, D)^\sigma$.

Theorem 12.3.7 *In this situation,* $\dim_{\mathbb{F}_q} H^0(X_0, D) = \dim_{\mathbb{F}} H^0(X, D)$.

Now consider the following exact sequence (where $\operatorname{Pic}(X_0) := \operatorname{coker}(\operatorname{div})$):

$$0 \to \mathbb{F}_q^\times \to K(X_0)^\times \xrightarrow{\operatorname{div}} \operatorname{Div}(X_0) \to \operatorname{Pic}(X_0) \to 0$$

We also have the degree map $\deg\colon \operatorname{Div}(X_0) \to \mathbb{Z}$. Since the degree of an element coming from $K(X_0)^\times$ is zero, this factors through $\operatorname{Pic}(X_0)$, so we obtain a map $\deg\colon \operatorname{Pic}(X_0) \to \mathbb{Z}$.

Theorem 12.3.8 *The map* $\deg\colon \operatorname{Div}(X_0) \to \mathbb{Z}$ *is surjective.*

Proof We use the Hasse-Weil inequality, which will be proved later, but not using the results of this lecture and the next.

If there is a point in $X_0(\mathbb{F}_q)$, then we directly find an element with degree 1, and we are done. So suppose that this does not happen. Let r be prime, and large enough such that $q^r + 1 - 2g{\cdot}q^{r/2} > 0$. Then by the Hasse-Weil inequality $X_0(\mathbb{F}_{q^r}) \neq \emptyset$, hence there is a prime divisor of degree r. Now take two such primes r to find divisors which have coprime degree and hence our map is surjective. □

The following proposition gives the zeta function as a counting function for the number of rational points on X_0 over finite extensions of $\mathbb{F}_q$.

Proposition 12.3.9 *Let* $X_0 = (X, F_X)$ *be a projective curve over* $\mathbb{F}_q$, *with* X *smooth and irreducible. The identity*

$$Z(X_0, t) = \exp\Big(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n})\frac{t^n}{n}\Big)$$

holds.

Proof For $a \in X(k)$ denote by $\mathrm{Orb}_{F_X}(a) \subset X(k)$ the F_X-orbit of a. Note that

$$\begin{aligned} X(\mathbb{F}_{q^n}) &= \{a \in X(k) : F_X^n(a) = a\} \\ &= \bigsqcup_{d|n} \{a \in X(k) : \#\,\mathrm{Orb}_{F_X}(a) = d\}\,. \end{aligned}$$

Also note that

$$\#\{a \in X(k) : \#\,\mathrm{Orb}_{F_X}(a) = d\} = d \cdot \#\{D \in P : \deg P = d\}$$

for each $d \in \mathbb{N}$, so that

$$\sum_{d|n} d \cdot \#\{D \in P : \deg P = d\} = \#X(\mathbb{F}_{q^n})\,.$$

It follows that

$$\begin{aligned} \log Z(X_0, t) &= \sum_{D \in P} \log\left(\frac{1}{1 - t^{\deg D}}\right) \\ &= \sum_{D \in P} \sum_{i > 0} \frac{t^{i \deg D}}{i \deg D} \deg D \\ &= \sum_{n=1}^{\infty} \frac{t^n}{n} \sum_{d|n} d \cdot \#\{D \in P : \deg P = d\} \\ &= \sum_{n=1}^{\infty} \frac{t^n}{n} \#X(\mathbb{F}_{q^n}) \end{aligned}$$

as required. □

12.4 Exercises

Exercise 12.4.1 Let X be an irreducible affine curve, $x \in X$, $t \in \mathcal{O}(X) := \mathcal{O}_X(X)$ non-zero with $\mathrm{div}(t) = x$, and $m \subset \mathcal{O}(X)$ the maximal ideal of x.

i. Show that $m = (t)$. Hint: we have $(t) \subset m$; consider $\mathcal{O}(X)/(t) \to \mathcal{O}(X)/m$.

ii. Show that for $f \in \mathcal{O}(X)$ with $f(x) = 0$, there is a unique $g \in \mathcal{O}(X)$ with $f = tg$.

iii. Let $f \in \mathcal{O}(X)$ be non-zero, with $\mathrm{div}(f) = nx$ for some $n \in \mathbb{Z}_{\geq 0}$. Show that there is a unique invertible element $g \in \mathcal{O}(X)$ such that $f = t^n g$.

Exercise 12.4.2 Let $n \in \mathbb{Z}_{\geq 0}$.

i. Compute a k-basis for $H^1(\mathbb{P}^1, -n{\cdot}0)$.

ii. Compute a k-basis for $H^0(\mathbb{P}^1, \Omega^1(n{\cdot}0))$.

iii. Give the Serre duality pairing explicitly.

Exercise 12.4.3 Let X and D and g and ω be as in (12.1.2). Show that $\sum_{P \in X - U_2} \mathrm{res}_P(g\omega)$ does not depend on the choice of representative g in the class $\overline{g}$, i.e., for $g_1 \in H^0(U_1, D)$ show that

$$\sum_{P \in X - U_2} \mathrm{res}_P((g + g_1)\omega) = \sum_{P \in X - U_2} \mathrm{res}_P(g\omega),$$

and similarly for $g_2 \in H^0(U_2, D)$. Here, you can use that for any $\eta \in \Omega^1_{K(X)}$ one has $\sum_{P \in X} \mathrm{res}_P(\eta) = 0$.

Exercise 12.4.4 This is a continuation of exercise 11.3.4.

Consider $X = \mathbb{P}^1 \times \mathbb{P}^1$ and use coordinates $x : y$ on the first factor and $u : v$ on the second factor. Denote the prime divisors $\{(0:1)\} \times \mathbb{P}^1$ and $\mathbb{P}^1 \times \{(0:1)\}$ by V and H, respectively.

Assume that k is of characteristic p and that q is a power of p. Let

$$F\colon \mathbb{P}^1 \to \mathbb{P}^1, \quad (a_0 : a_1) \mapsto (a_0^q : a_1^q)$$

be the q-Frobenius endomorphism. Let $\Delta \subset \mathbb{P}^1 \times \mathbb{P}^1$ be the diagonal and let $\Gamma = \{(P, F(P)) : P \in \mathbb{P}^1\}$ be the graph of the q-Frobenius.

i. Show that $\Delta = Z(f)$ for some f which is irreducible and bihomogeneous of bidegree $(1,1)$.

ii. Show that $\Gamma = Z(f)$ for some f which is irreducible and bihomogeneous of bidegree $(q,1)$.

iii. Compute the four by four symmetric matrix whose entries are the intersection products of all pairs of divisors in $\{H, V, \Delta, \Gamma\}$.

Lecture 13

Rationality and functional equation

13.1 Divisors of given degree

Let $\mathbb{F}_q \to \mathbb{F}$ be an algebraic closure, $X \subset \mathbb{P}^n = \mathbb{P}^n(\mathbb{F})$ be closed, irreducible, smooth of dimension 1 and defined over $\mathbb{F}_q$. Let $X_0 = (X, F_X)$ be the corresponding variety over $\mathbb{F}_q$. We introduce some more notation concerning (effective) divisors and divisor classes. Let $\mathrm{Div}(X_0)^+ \subset \mathrm{Div}(X_0)$ be the space of effective divisors (that is, those divisors $D \geq 0$).

Definition 13.1.1 For $n \in \mathbb{Z}$, let $\mathrm{Div}^n(X_0) := \deg^{-1}\{n\}$, the set of divisors of degree n. Also, let $\mathrm{Div}^n(X_0)^+ := \mathrm{Div}^n(X_0) \cap \mathrm{Div}(X_0)^+$ and $\mathrm{Pic}^n(X_0) := \deg^{-1}\{n\}$.

The zeta function of X_0 is $Z(X_0, t) = \sum_{n \geq 0} d_n t^n$, where $d_n = \# \mathrm{Div}^n(X_0)^+$.

Remark 13.1.2 As the degree map is a surjective morphism of groups, there are bijections, for all integers n, $\mathrm{Div}^0(X_0) \to \mathrm{Div}^n(X_0)$ and $\mathrm{Pic}^0(X_0) \to \mathrm{Pic}^n(X_0)$.

Let $\varphi\colon \mathrm{Div}(X_0) \to \mathrm{Pic}(X_0)$ be the map that sends a divisor to its class in the Picard group.

Lemma 13.1.3 *Let $D \in \mathrm{Div}(X_0)^+$. Write $\overline{D}$ for the image of D in $\mathrm{Pic}\, X_0$. Then the map*

$$\left(H^0(X_0, D) - \{0\}\right)/\mathbb{F}_q^\times \longrightarrow \varphi^{-1}\{\overline{D}\}, \quad \overline{f} \mapsto \mathrm{div}(f) + D$$

is a bijection.

Proof For $f \in K(X_0)^\times$ we have $f \in H^0(X_0, D)$ if and only if $\mathrm{div}(f) + D \geq 0$. For $f_1, f_2 \in K(X_0)^\times$ we have $\mathrm{div}(f_1) = \mathrm{div}(f_2)$ if and only if $f_1 = \lambda f_2$ for some $\lambda \in \mathbb{F}_q^\times$. Lastly, observe that $\varphi^{-1}\{\overline{D}\}$ consists precisely of the $E \in \mathrm{Div}^+ X_0$ such that $E - D = \mathrm{div}(f)$ for some $f \in K(X_0)^\times$. □

Corollary 13.1.4 *For all $n \in \mathbb{Z}$, we have*

$$d_n = \sum_{D \in \mathrm{Pic}^n(X_0)} \frac{q^{h^0(D)} - 1}{q - 1},$$

where $h^0(D) = \dim_{\mathbb{F}_q} H^0(X_0, D)$.

Corollary 13.1.5 *For all $n \geq 2g - 1$, we have*

$$d_n = (\# \mathrm{Pic}^n(X_0)) \frac{q^{n+1-g} - 1}{q - 1}.$$

The group $\mathrm{Pic}^0(X_0)$ is finite.

13.2 The zeta function of X_0

We are now ready to prove the rationality of the zeta function.

Theorem 13.2.1 *(Rationality) There is a $P \in \mathbb{Z}[t]_{\leq 2g}$ such that*

$$Z(X_0, t) = \frac{P(t)}{(1-t)(1-qt)}.$$

Proof This is now a direct computation:

$$\begin{aligned} Z(X_0, t) &= \sum_{n\geq 0} d_n t^n \\ &= \sum_{n=0}^{2g-2} d_n t^n + \left(\# \operatorname{Pic}^0(X_0)\right) \sum_{n\geq 2g-1} \frac{q^{n+1-g}-1}{q-1} t^n \\ &= \sum_{n=0}^{2g-2} d_n t^n + \frac{\# \operatorname{Pic}^0(X_0)}{q-1} t^{2g-1} \left(\frac{q^g}{1-qt} - \frac{1}{1-t} \right). \end{aligned}$$

□

By Proposition 12.3.9 we have $Z(X_0, 0) = 1$, and it follows that $P(0) = 1$.

The next step is to use Serre duality to deduce the functional equation for $Z(X_0, t)$. Let $\omega \in \Omega^1_{K(X_0)}$ be non-zero. Then the involution $D \mapsto \operatorname{div}(\omega) - D$ on $\operatorname{Div}(X_0)$ induces for every $n \in \mathbb{Z}$ bijections

$$\operatorname{Div}^n(X_0) \longrightarrow \operatorname{Div}^{2g-2-n}(X_0) \quad \text{and} \quad \operatorname{Pic}^n(X_0) \longrightarrow \operatorname{Pic}^{2g-2-n}(X_0).$$

From Serre duality we know that $h^0(D) - h^0(\operatorname{div}(\omega) - D) = \deg(D) + 1 - g$.

Lemma 13.2.2 *For all $n \in \mathbb{Z}$ with $0 \leq n \leq 2g-2$ we have*

$$d_n - q^{n+1-g} d_{2g-2-n} = \frac{q^{n+1-g}-1}{q-1} \# \operatorname{Pic}^0(X_0).$$

Proof Let $D \in \operatorname{Div}^n(X_0)$. Recall that

$$\#\varphi^{-1}(\overline{D}) = \frac{q^{h^0(D)}-1}{q-1}$$

and

$$\#\varphi^{-1}(\overline{\operatorname{div}(\omega) - D}) = \frac{q^{h^0(\operatorname{div}(\omega)-D)}-1}{q-1} = \frac{q^{h^0(D)-(n+1-g)}-1}{q-1}.$$

From this we see that

$$\#\varphi^{-1}(\overline{D}) - q^{n+1-g} \#\varphi^{-1}(\overline{\operatorname{div}(\omega) - D}) = \frac{q^{n+1-g}-1}{q-1}.$$

The result follows by summing over all classes in $\operatorname{Pic}^n(X_0)$. □

For the rest of the proof of the functional equation we will do our bookkeeping in the $\mathbb{Q}[t, t^{-1}]$-module

$$\mathbb{Q}[[t, t^{-1}]] = \left\{ \sum_{n\in\mathbb{Z}} a_n t^n : \forall n \in \mathbb{Z},\ a_n \in \mathbb{Q} \right\}.$$

Despite the notation, this object is *not* a ring. It contains $\mathbb{Q}[[t]]$ and $\mathbb{Q}[[t^{-1}]]$.

Note that $d_n = 0$ for $n < 0$, so we have $Z(X_0, t) = \sum_{n\in\mathbb{Z}} d_n t^n$ and

$$Z(X_0, (qt)^{-1}) = \sum_{n\in\mathbb{Z}} d_n (qt)^{-n} = \sum_{n\in\mathbb{Z}} d_{-n} q^n t^n.$$

Hence we have

$$\sum_{n\in\mathbb{Z}} q^{n+1-g} d_{2g-2-n} t^n = (t^2 q)^{g-1} Z(X_0, (qt)^{-1}).$$

So in $\mathbb{Q}[[t, t^{-1}]]$, we have

$$Z(X_0, t) - (t^2 q)^{g-1} Z(X_0, (qt)^{-1}) = \frac{\#\operatorname{Pic}^0(X_0)}{q-1} \sum_{n\in\mathbb{Z}} (q^{n+1-g} - 1) t^n.$$

The sum on the right-hand side splits as

$$q^{1-g} \sum_{n\in\mathbb{Z}} (qt)^n \; - \; \sum_{n\in\mathbb{Z}} t^n.$$

The first sum is annihilated by $1 - qt$ and the second one by $1 - t$, so in $\mathbb{Q}[[t, t^{-1}]]$ we have

$$(1-t)(1-qt)\left(Z(X_0, t) - (t^2 q)^{g-1} Z(X_0, (qt)^{-1})\right) = 0.$$

Rearranging the terms, we see that

$$(1-t)(1-qt) Z(X_0, t) = (1-t)(1-qt)(t^2 q)^{g-1} Z(X_0, (qt)^{-1}).$$

The left-hand side is in $\mathbb{Q}[[t]]$ and the right-hand side is in $t^{2g}\mathbb{Q}[[t^{-1}]]$. It follows that both sides are in $\mathbb{Q}[t]_{\leq 2g}$ and are equal. This not only gives us the functional equation, but also proves the rationality in a different way. In conclusion, we have proven the following theorem.

Theorem 13.2.3 *(Functional equation) In $\mathbb{Q}(t)$, we have $Z(X_0, t) = (t\sqrt{q})^{2g-2} Z(X_0, (qt)^{-1})$.*

Corollary 13.2.4 *We have $P(t) = (t\sqrt{q})^{2g} P((qt)^{-1})$. That is, if we write $P(t) = P_0 t^0 + \cdots + P_{2g} t^{2g}$, then $P_{2g-n} = q^{g-n} P_n$. In particular, since $P_0 = 1$ we have $P_{2g} = q^g$ and hence P has degree precisely $2g$.*

Corollary 13.2.5 *There are $\alpha_1, \ldots, \alpha_g \in \mathbb{C}$, all non-zero such that*

$$P(t) = (1-\alpha_1 t)\cdots(1-\alpha_g t)(1-(q/\alpha_1)t)\cdots(1-(q/\alpha_g)t).$$

In the next, final lecture we will prove the Riemann Hypothesis for curves over finite fields, which is the following more precise statement:

Theorem 13.2.6 *(Riemann Hypothesis) Let $X_0 = (X, F_X)$ be a projective curve defined over $\mathbb{F}_q$, with X smooth and irreducible. Write $Z(X_0, t) = P(t)/(1-t)(1-qt)$ for the zeta function of X_0, with $P(t) = (1-\alpha_1 t)\cdots(1-\alpha_g t)(1-(q/\alpha_1)t)\cdots(1-(q/\alpha_g)t)$, then for each $i = 1, \ldots, g$ we have $|\alpha_i| = \sqrt{q}$.*

In other words, all the zeroes of $\zeta(X_0, s) := Z(X_0, q^{-s})$ have real part equal to $1/2$; whence the terminology.

13.3 Exercises

Exercise 13.3.1 Let k be an arbitrary algebraically closed field, and X an irreducible projective variety over k, smooth of dimension one, and of genus zero. Let P, Q and R in X be distinct.

i. Using RR+SD, show that there is a unique $f \in K(X)^\times$ such that $\operatorname{div}(f) = P - R$ and $f(Q) = 1$.

ii. Show that the morphism of k-algebras $k[x] \to \mathcal{O}_X(X - \{R\})$ that sends x to f is an isomorphism. Hint: use that $\mathcal{O}_X(X - \{R\})$ is the union of the $H^0(X, n{\cdot}R)$, $n \in \mathbb{N}$.

iii. Similar for $k[x^{-1}] \to \mathcal{O}_X(X - \{P\})$, $x^{-1} \mapsto f^{-1}$.

iv. Show that f gives an isomorphism $X \to \mathbb{P}^1$.

Exercise 13.3.2 Let k be an arbitrary algebraically closed field, and X an irreducible projective variety over k, smooth of dimension one, and of genus one.

i. Show, using RR+SD, that the map of sets $X \to \operatorname{Pic}^1(X)$, $P \mapsto \overline{P}$, is bijective.

ii. Let $O \in X$. Show that the map $\varphi\colon X \to \operatorname{Pic}^0(X)$, $P \mapsto \overline{P - O}$ is bijective.

iii. Deduce that given P and Q in X there is a unique R in X such that $(R+O)-(P+Q)$ is a principal divisor, and that the map (of sets) $\oplus\colon X \times X \to X$, $(P, Q) \mapsto R$ defines a group law on X with O as neutral element.

Exercise 13.3.3 Let $\mathbb{F}_2 \to \mathbb{F}$ be an algebraic closure. Let $X = Z(x_1^2x_2 + x_1x_2^2 + x_0^3 + x_2^3) \subset \mathbb{P}^2(\mathbb{F})$; it is defined over $\mathbb{F}_2$ and we let X_0 denote this variety over $\mathbb{F}_2$. You may assume that $x_1^2x_2 + x_1x_2^2 + x_0^3 + x_2^3$ is irreducible in $\mathbb{F}[x_0, x_1, x_2]$. The intersection $X \cap D_+(x_2) \subset \mathbb{A}^2$ (notation as in Exercise 4.4.2) is given by the equation $y^2 + y = x^3 + 1$, where $x = x_0/x_2$ and $y = x_1/x_2$. Note that X has exactly one point $\infty := (0 : 1 : 0)$ on $Z(x_2)$.

i. Show that X is smooth of dimension 1.

ii. Show that the rational 1-form $\omega := dx = x^{-2}dy$ has no poles and no zeros on X. Deduce that the genus of X is 1.

iii. List the elements of $X(\mathbb{F}_2)$ and $X(\mathbb{F}_4)$. Use the following notation for $\mathbb{F}_4$: $\mathbb{F}_4 = \{0, 1, z, z^{-1}\}$, with $z^2 + z + 1 = 0$.

iv. Show that $Z(X_0, t) = (1 + 2t^2)/(1 - t)(1 - 2t)$.

v. Compute $\#\operatorname{Div}^2(X_0)^+$ by expanding $Z(X_0, t)$ in $\mathbb{Z}[[t]]$ up to order 2.

vi. List all the elements of $\operatorname{Div}^2(X_0)^+$. For example, 2∞ and $(0, z) + (0, z^{-1})$ are two of them.

vii. Compute the divisors of the functions x, $x + 1$, y, $y + 1$, $x + y$ and $y + x + 1$.

viii. Give explicitly the map $\operatorname{Div}^2(X_0)^+ \to \operatorname{Pic}^2(X_0)$, $D \mapsto \overline{D}$; you may use without proof that $\operatorname{Pic}^0(X_0) = \{0, \overline{(1, 0) - \infty}, \overline{(1, 1) - \infty}\}$ (this works as in Exercise 13.3.2).

Lecture 14

Hasse-Weil inequality and Riemann Hypothesis

14.1 Introduction

In the exercise at the end of this lecture we will show how the Riemann Hypothesis for curves over finite fields (Theorem 13.2.6) follows from: the rationality of $Z(X_0, t)$, the functional equation of $Z(X_0, t)$, and the so-called Hasse-Weil inequality. This exercise is the same as Exercise 5.7 of Appendix C of [Hart]. We refer to this same Appendix C for more background material and the statement of a wide generalization of the Riemann hypothesis for curves.

In this lecture we prove the Hasse-Weil inequality (Theorem 14.1.1), using the Hodge index theorem (that we admit without proof) and intersection theory on the surface $X \times X$.

Recall that the rationality of $Z(X_0, t)$ is given by Theorem 13.2.1, and the functional equation by Theorem 13.2.3.

Theorem 14.1.1 *(Hasse-Weil inequality) Let X be a projective variety over $\mathbb{F}_q$, which, as variety over $\overline{\mathbb{F}}_q$, is a smooth projective irreducible curve of genus g. Then:*

$$|\#X(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}$$

Example 14.1.2 (of Theorem 14.1.1) Let q be a prime power, $n \in \mathbb{Z}_{\geq 1}$. Let $f \in \mathbb{F}_q[x, y, z]_n$ be a homogeneous polynomial of degree n. Write

$$f = \sum_{\substack{i,j,k \geq 0 \\ i+j+k=n}} f_{i,j,k} x^i y^j z^k$$

and assume that f, $\partial f/\partial x$, $\partial f/\partial y$, $\partial f/\partial z$ have no common zero in $\overline{\mathbb{F}}_q^3 - \{0\}$. In this case the genus is equal to $(n-1)(n-2)/2$. Then we have:

$$\left| \frac{\#\{(a,b,c) \in \mathbb{F}_q^3 - \{0\} : f(a,b,c) = 0\}}{q-1} - (q+1) \right| \leq 2 \cdot \frac{(n-1)(n-2)}{2}\sqrt{q}.$$

Here one should really think of $\mathbb{P}^2(\mathbb{F}_q) = (\mathbb{F}_q^3 - \{0\})/\mathbb{F}_q^\times$, the set of lines through 0 in $\mathbb{F}_q^3$; the "projective plane".

Note that for n equal to 1 or 2 the theorem gives an equality that we can check, and it also shows why we need the "points at ∞", that is, why we must "compactify". Indeed, for $n = 1$ we have a non-zero linear homogeneous polynomial. In $\mathbb{F}_q^3 - \{0\}$ we find $q^2 - 1$ points satisfying the equation given by f, and indeed $(q^2-1)/(q-1) = q+1$. For the case $n = 2$ one can parametrise a conic using a rational point.

14.2 Self-intersection of the diagonal

(Here we assume that k is any algebraically closed field) In this section we will sketch a proof of the following theorem:

Theorem 14.2.1 *Let X be a smooth irreducible projective curve, g its genus, and $\Delta \subset X \times X$ the diagonal. Then $\Delta{\cdot}\Delta = 2 - 2g$.*

Remark 14.2.2 Note that $2-2g$ is minus the degree of a canonical divisor. We give a proof relating $\Delta{\cdot}\Delta$ with the degree of such a canonical divisor.

We start with some affine geometry. Let Y be an affine variety and $A(Y) = k[x_1, \ldots, x_n]/(f_1, \ldots, f_s)$ its coordinate ring. Then the coordinate ring of $Y \times Y$ is

$$A(Y \times Y) = k[x, y]/(f_1(x), \ldots, f_s(x), f_1(y), \ldots, f_s(y)),$$

where $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$. The projection $\mathrm{pr}_1 \colon Y \times Y \to Y$, $(P, Q) \mapsto P$ gives the k-algebra morphism $\mathrm{pr}_1^* \colon A(Y) \to A(Y \times Y)$. It sends $\overline{x}_i$ in $A(Y)$ to $\overline{x}_i$ in $A(Y \times Y)$. It makes $A(Y \times Y)$ into an $A(Y)$-algebra. We also have the diagonal embedding:

$$\Delta \colon Y \longrightarrow Y \times Y, \quad P \mapsto (P, P),$$

giving us a k-algebra morphism in the other direction:

$$\Delta^* \colon A(Y \times Y) \longrightarrow A(Y), \quad x_i \mapsto x_i, \quad y_i \mapsto x_i.$$

Let I be the kernel of Δ^*. This is the ideal of Δ. It is an $A(Y)$-module via pr_1^*, and it is generated by the $(\overline{y}_i - \overline{x}_i)_{1 \le i \le s}$.

Proposition 14.2.3 *The map $D \colon A(Y) \to I/I^2$, $f \mapsto \overline{\mathrm{pr}_1^* f - \mathrm{pr}_2^* f}$ is a derivation, and the induced morphism of $A(Y)$-modules $\Omega^1_{A(Y)} \to I/I^2$ is an isomorphism.*

Proof For f in $A(Y)$ we have $\Delta^*(\mathrm{pr}_1^* f - \mathrm{pr}_2^* f) = f - f = 0$, hence $\mathrm{pr}_1^* f - \mathrm{pr}_2^* f \in I$. We claim that D is indeed a derivation. That D is k-linear is obvious. We now check that the Leibniz rule is satisfied. Computing modulo I^2 we find:

$$\begin{aligned} D(fg) &= (\mathrm{pr}_1^* f)(\mathrm{pr}_1^* g) - (\mathrm{pr}_2^* f)(\mathrm{pr}_2^* g) \\ &= (\mathrm{pr}_1^* f)(\mathrm{pr}_1^* g) - (\mathrm{pr}_2^* f)(\mathrm{pr}_2^* g) + ((\mathrm{pr}_1^* f) - (\mathrm{pr}_2^* f))\,((\mathrm{pr}_1^* g) - (\mathrm{pr}_2^* g)) \\ &= (\mathrm{pr}_1^* f)((\mathrm{pr}_1^* g) - (\mathrm{pr}_2^* g)) + (\mathrm{pr}_1^* g)((\mathrm{pr}_1^* f) - (\mathrm{pr}_2^* f)) \\ &= f{\cdot}Dg + g{\cdot}Df. \end{aligned}$$

As $D \colon A(Y) \to I/I^2$ is a k-derivation, there is a unique morphism of $A(Y)$-modules $\varphi \colon \Omega^1_{A(Y)} \to I/I^2$ such that $D = \varphi \circ d$.

We give an inverse to φ. Let $\psi \colon k[x, y] \to \Omega^1_{A(Y)}$ be the k-linear map that sends, for all f and g in $k[x]$, $(\mathrm{pr}_1^* f)(\mathrm{pr}_2^* g)$ to $-f{\cdot}dg$; to see that this exists, use the k-basis of all monomials. Then for f in $I(Y)$, and g in $k[x]$, $\psi((\mathrm{pr}_1^* f)(\mathrm{pr}_2^* g)) = 0$ and $\psi((\mathrm{pr}_1^* g)(\mathrm{pr}_2^* f)) = 0$, hence ψ factors through $k[x, y] \to A(Y \times Y)$. The resulting k-linear map $\psi \colon A(Y \times Y) \to \Omega^1_{A(Y)}$ is a morphism of $A(Y)$-modules. We claim that ψ is zero on I^2. As ψ is k-linear, even $A(Y)$-linear, and I is generated as ideal by the $\mathrm{pr}_1^* f - \mathrm{pr}_2^* f$, it suffices to show that ψ is zero on all elements of the form $(\mathrm{pr}_1^* f - \mathrm{pr}_2^* f)(\mathrm{pr}_1^* g - \mathrm{pr}_2^* g)\mathrm{pr}_2^* h$, with f, g, and h in $A(Y)$. This computation is as follows. We have

$$(\mathrm{pr}_1^* f - \mathrm{pr}_2^* f)(\mathrm{pr}_1^* g - \mathrm{pr}_2^* g)\mathrm{pr}_2^* h = (\mathrm{pr}_1^*(fg))(\mathrm{pr}_2^* h) - (\mathrm{pr}_1^* f)(\mathrm{pr}_2^*(gh)) - (\mathrm{pr}_1^* g)(\mathrm{pr}_2^*(fh)) + \mathrm{pr}_2^*(fgh).$$

Under ψ, this is sent to:

$$
\begin{aligned}
&-fg{\cdot}dh + f{\cdot}d(gh) + g{\cdot}d(fh) - d(fgh)\\
&\qquad = -fg{\cdot}dh + fg{\cdot}dh + fh{\cdot}dg + gf{\cdot}dh + gh{\cdot}df - gh{\cdot}df - fh{\cdot}dg - fg{\cdot}dh = 0.
\end{aligned}
$$

So, we have our morphism $\psi\colon I/I^2 \to \Omega^1_{A(Y)}$, and, for f in $A(Y)$, it sends $\overline{\mathrm{pr}_1^* f - \mathrm{pr}_2^* f}$ to $0-(-df) = df$. Therefore, this ψ is the inverse of φ. □

Remark 14.2.4 The notation and some arguments in our proof of Proposition 14.2.3 would be much simpler if we used the tensor product, $A(Y \times Y) = A(Y) \otimes_k A(Y)$, and even more simple and very conceptual if we had developed relative differentials. So, the reader should not be worried by the complicated notation here, and by the seemingly meaningless computations.

Now we go back to the situation as in Theorem 14.2.1.

Proposition 14.2.5 *Let P be in X, and $t \in \mathcal{O}_X(U)$ a uniformiser at P. Then there is an open neighborhood V of (P,P) in $X \times X$ such that $\mathrm{pr}_1^* t - \mathrm{pr}_2^* t$ is a generator for the ideal of $\Delta \cap V$.*

Proof By Proposition 11.1.3, there is an open affine neighborhood V of (P,P) on which the ideal of Δ is generated by some f in $\mathcal{O}_{X\times X}(V)$. By intersecting with $U \times U$, we may and do assume that $\mathrm{pr}_1^* t - \mathrm{pr}_2^* t$ is regular on V. As $\mathrm{pr}_1^* t - \mathrm{pr}_2^* t$ is zero on Δ, there is a unique g in $\mathcal{O}_{X\times X}(V)$ such that $\mathrm{pr}_1^* t - \mathrm{pr}_2^* t = gf$. Let $i\colon X \to X \times X$ be the map $Q \mapsto (Q,P)$. Then, under $i^*\colon \mathcal{O}_{X\times X}(V) \to \mathcal{O}_X(i^{-1}V)$ we get $t = (i^*g){\cdot}(i^*f)$. But t is not in m^2, where m is the maximal ideal of P, and i^*f is in m, so i^*g is not in m. Hence $g(P,P) \neq 0$, and g is a unit on a neighborhood of (P,P). □

Proof (of Theorem 14.2.1) We follow the procedure in Definition 11.2.1. By Proposition 14.2.5 there are an r in $\mathbb{N}$, non-empty affine opens $V_i \subset U_i \times U_i$, for $i \in \{1,\ldots,r\}$, covering Δ and all meeting Δ, open affines U_i in X and t_i in $\mathcal{O}_X(U_i)$, such that the ideal of $\Delta \cap V_i$ is generated by $\mathrm{pr}_1^* t_i - \mathrm{pr}_2^* t_i$. Then we have:

$$
\Delta{\cdot}\Delta = \sum_{P\in X} v_{(P,P)}\left(\left.\frac{\mathrm{pr}_1^* t_{i_P} - \mathrm{pr}_2^* t_{i_P}}{\mathrm{pr}_1^* t_1 - \mathrm{pr}_2^* t_1}\right|_\Delta \right), \quad \text{where } (P,P) \text{ is in } V_{i_P}.
$$

Let ω be the rational one-form dt_1 on X. Then we have:

$$
\begin{aligned}
\deg(\mathrm{div}(\omega)) &= \sum_{P\in X} v_P(\omega)\\
&= \sum_{P\in X} v_P\left(\frac{\omega}{dt_{i_P}}\right) \qquad (dt_{i_P} \text{ generates } \Omega^1_X \text{ at } P \text{ by Proposition 14.2.3})\\
&= \sum_{P\in X} v_{(P,P)}\left(\left.\frac{\mathrm{pr}_1^* t_1 - \mathrm{pr}_2^* t_1}{\mathrm{pr}_1^* t_{i_P} - \mathrm{pr}_2^* t_{i_P}}\right|_\Delta \right) \qquad (\omega = dt_1 \text{ and Proposition 14.2.3})\\
&= -\sum_{P\in X} v_{(P,P)}\left(\left.\frac{\mathrm{pr}_1^* t_{i_P} - \mathrm{pr}_2^* t_{i_P}}{\mathrm{pr}_1^* t_1 - \mathrm{pr}_2^* t_1}\right|_\Delta \right)\\
&= -\Delta{\cdot}\Delta.
\end{aligned}
$$

□

14.3 Hodge's index theorem

Hodge's index theorem is discussed in Theorem V.1.9 and Remark V.1.9.1 in [Hart]. Let S be a connected smooth projective surface over an algebraically closed field k. We have the intersection pairing

$\cdot\colon \operatorname{Pic}(S) \times \operatorname{Pic}(S) \to \mathbb{Z}$. It is symmetric and bilinear. Let N be its kernel:

$$N = \{x \in \operatorname{Pic}(S) : \forall y \in \operatorname{Pic}(S),\ x{\cdot}y = 0\}.$$

Let $\operatorname{Num}(S) := \operatorname{Pic}(S)/N$. Then the intersection pairing on $\operatorname{Pic}(S)$ induces a non-degenerate symmetric bilinear pairing $\cdot\colon \operatorname{Num}(S) \times \operatorname{Num}(S) \to \mathbb{Z}$. It is a theorem by Néron and Severi (see the discussion in [Hart]) that $\operatorname{Num}(S)$ is finitely generated as $\mathbb{Z}$-module. Hence it is free of some finite rank d, because the intersection pairing injects it into $\operatorname{Hom}_{\mathbb{Z}\text{-Mod}}(\operatorname{Num}(S), \mathbb{Z})$. We have $d \geq 1$, since a hyperplane section of S defines a non-zero element of $\operatorname{Num}(S)$. Choosing a $\mathbb{Z}$-basis $b = (b_1, \ldots, b_d)$ of $\operatorname{Num}(S)$ gives the intersection pairing as a symmetric d by d matrix with coefficients in $\mathbb{Z}$ and with non-zero determinant. One can take a basis c of $\mathbb{Q} \otimes \operatorname{Num}(S)$ such that the matrix of the intersection pairing with respect to c is diagonal. The diagonal coefficients of c are then non-zero, and it is a well-known result in linear algebra (over $\mathbb{R}$ if you want) that the numbers of positive and of negative coefficients do not depend on the choice of the basis c. Hodge's index theorem tells us what these numbers are.

Theorem 14.3.1 *(Hodge index theorem) The intersection pairing on $\mathbb{Q} \otimes \operatorname{Num}(S)$ has exactly one $+$.*

Remark 14.3.2 Another way to state Hodge's index theorem (without using Néron-Severi first) is that for any morphism of $\mathbb{Z}$-modules $f\colon \mathbb{Z}^d \to \operatorname{Pic}(S)$, the symmetric bilinear form on $\mathbb{Z}^d$ given by sending (x, y) to $(fx){\cdot}(fy)$ has, after extending scalars to $\mathbb{R}$ and diagonalisation, at most one $+$, and there are f for which there is exactly one $+$.

14.4 Proof of the Hasse-Weil inequality

Let $X/\mathbb{F}_q$ as in the statement of the Hasse-Weil inequality (Theorem 14.1.1) and let $F\colon X \to X$ be the Frobenius map. We now work with four prime divisors, each isomorphic to X and we will calculate the matrix of the intersection pairing for the subspace generated by these four prime divisors. The divisors are:

$$H = \{(x, \mathrm{pt}) : x \in X\}, \quad V = \{(\mathrm{pt}, x) : x \in X\},$$
$$\Delta = \{(x, x) : x \in X\}, \quad \Gamma = \{(x, F(x)) : x \in X\}.$$

We calculate the tangent spaces at the point (P, Q) (assuming that it lies on the divisor), as seen as a subspace of $T_X(P) \times T_X(Q) = T_{X\times X}(P, Q)$. One then finds:

$$T_H(P, Q) = k{\cdot}(1, 0), \quad T_V(P, Q) = k{\cdot}(0, 1), \quad T_\Delta(P, Q) = k{\cdot}(1, 1).$$

For the tangent space to Γ consider the two projection maps to X. The first one

$$\mathrm{pr}_1\colon \Gamma \to X, \quad (P, F(P)) \mapsto P$$

is an isomorphism (an inverse is given by $P \mapsto (P, F(P))$), so induces an isomorphism on tangent spaces. If we use pr_1 to identify Γ with X then pr_2 is the same as the Frobenius map $F\colon X \to X$. The Frobenius map induces the zero map on tangent spaces since the derivative of any p-th power of a function is zero. So we get:

$$T_\Gamma(P, Q) = k{\cdot}(1, 0).$$

Notice that Γ is not constant horizontal, but its tangent direction is everywhere horizontal. (Compare with the function $x \mapsto x^q$ which is non-constant, but its derivative is 0).

We compute the intersection matrix. Here we have to do 10 calculations (by symmetry):

- $H{\cdot}H = 0$. If $H = X \times \{\mathrm{pt}\}$, then find a divisor D on X with $D \sim \{\mathrm{pt}\}$ such that D and $\{\mathrm{pt}\}$ are disjoint. Then $H{\cdot}H = H{\cdot}(X \times D) = 0$, since $H \cap X \times D = \emptyset$.

- $H \cdot V = 1$. Indeed, we have one intersection point and the intersection is transversal there (see the calculation of the tangent spaces).
- $H \cdot \Delta = 1$. Again, we have a transversal intersection.
- $H \cdot \Gamma = q$. We have one intersection point $(P, F(P))$ since $F \colon X \to X$ is a bijection, but we don't have a transversal intersection here, so we need to do more computations. Let t be a uniformiser at FP. Then $\mathrm{pr}_2^* t$ is a local equation for H, near $(P, F(P))$. Restricting $\mathrm{pr}_2^* t$ to Γ, and pulling back via the isomorphism $X \to \Gamma$, $a \mapsto (a, Fa)$, gives $F^* t$ near P. One can show that $v_P(F^* t) = q$. For example, when $X = \mathbb{P}^1$ and $P = 0$ one finds $\dim k[x,y]/(y, x^q - y) = q$ (a basis consists of $1, x, \ldots, x^{q-1}$).
- $V \cdot V = 0$. By symmetry, $V \cdot V = H \cdot H$.
- $V \cdot \Delta = 1$. By symmetry, $V \cdot \Delta = H \cdot \Delta$.
- $V \cdot \Gamma = 1$. Since $F \colon X \to X$ is a bijection, we have one intersection point, but this time we have a transversal intersection.
- $\Delta \cdot \Delta = 2 - 2g$. This is Theorem 14.2.1.
- $\Delta \cdot \Gamma = \#X(\mathbb{F}_q) := N$. We have a transversal intersection again. We calculate:

$$\Delta \cdot \Gamma = \#\Delta \cap \Gamma = \#\{(x,y) \in X \times X : x = y,\ F(x) = y\} = \#X(\mathbb{F}_q).$$

- $\Gamma \cdot \Gamma = q(2 - 2g)$. This is again a harder case (it uses some techniques which we don't have yet). Consider $(F, \mathrm{id}) \colon X \times X \to X \times X$. This inverse image under this map of Δ is Γ. One then obtains (from a general theorem) that $\Gamma \cdot \Gamma = \deg(F, \mathrm{id}) \cdot (\Delta \cdot \Delta)$. This degree is the degree of the corresponding extension of function fields, and one can show that this degree is q in our case.

We put these calculations in a matrix with respect to H, V, Δ, Γ. One then gets:

$$\begin{pmatrix} 0 & 1 & 1 & q \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 2-2g & N \\ q & 1 & N & q(2-2g) \end{pmatrix}$$

Now one can make some entries 0 by choosing some other divisors (by some linear invertible transformation), namely $H, V, \Delta - V - H, \Gamma - qV - H$. With these divisors one gets the following matrix A:

$$A := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -2g & N-1-q \\ 0 & 0 & N-1-q & -2gq \end{pmatrix}$$

Remark that this matrix consists of two diagonal blocks. There are now two cases to consider. In the first case H, V, Δ, Γ are dependent in $\mathrm{Num}(X \times X)$. Then $\det(A) = 0$. In the other case, H, V, Δ, Γ are independent in $\mathrm{Num}(X \times X)$. Then Theorem 14.3.1 tells us that there is at most 1 positive eigenvalue. Notice that the eigenvalues of the first block are 1 and -1. Hence the second block has determinant ≥ 0. In other words:

$$4g^2 q - (N - 1 - q)^2 \geq 0.$$

Hence $|N - 1 - q| \leq 2g\sqrt{q}$. This finishes the proof of the Hasse-Weil inequality.

14.5 Exercises

Exercise 14.5.1 This is Exercise 5.7 of Appendix C of [Hart], with some explanations added. It shows how the Riemann Hypothesis for curves over finite fields follows from the Hasse-Weil inequality, plus rationality plus functional equation (apply the series of steps below, with $\nu_n = \#X(\mathbb{F}_{q^n})$).

Let q be a prime power, $g \in \mathbb{Z}_{\geq 1}$, $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$ and let $Z(t)$ in $\mathbb{C}(t)$ be the rational function with:

$$Z(t) = \frac{P_1(t)}{(1-t)(1-qt)}, \quad P_1(t) = \prod_{i=1}^{2g}(1-\alpha_i t).$$

i. Define the complex numbers ν_n ($n \geq 1$) by:

$$\log Z(t) = \sum_{n \geq 1} \frac{\nu_n}{n} t^n.$$

Show that $\nu_n = q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n$.

ii. Assume that for all $n \geq 1$: $|q^n + 1 - \nu_n| \leq 2gq^{n/2}$. Prove that for all $n \geq 1$:

$$\left| \sum_{i=1}^{2g} \alpha_i^n \right| \leq 2gq^{n/2}.$$

iii. (This is the essential step!) Prove that for all i: $|\alpha_i| \leq q^{1/2}$. Hints. There are at least two strategies. First, you can consider the power series expansion of $\sum_{i=1}^{2g} \alpha_i t/(1-\alpha_i t)$ and use a little bit of complex function theory. Or as follows, by contradiction: assume that for some i one has $|\alpha_i| > q^{1/2}$. Renumber the α_i such that the first m are non-zero, and the others are zero. Let

$$\beta = (\alpha_1/|\alpha_1|, \ldots, \alpha_m/|\alpha_m|) \in (S^1)^m$$

be the m-tuple of arguments of the α_i. Show that the sequence $(\beta^n)_{n \geq 1}$ has a convergent subsequence. Show that it has a subsequence that converges to $1 = (1, \ldots, 1)$. Get a contradiction.

iv. Assume that $Z(t)$ satisfies the following functional equation:

$$Z(1/qt) = q^{1-g} t^{2-2g} Z(t).$$

Prove that for all $i \in \{1, \ldots, 2g\}$ there is a $j \in \{1, \ldots, 2g\}$ such that $\alpha_i \alpha_j = q$. Deduce that for all i: $|\alpha_i| = q^{1/2}$, and that all the zeros of $\zeta(s) := Z(q^{-s})$ have real part equal to $1/2$.

Lecture 15

Appendix: Zeta functions and the Riemann hypothesis

The purpose of this Appendix is to give the reader some more motivation and background for the study of zeta functions of varieties over finite fields. Probably the proper context is "zeta functions of schemes of finite type over $\mathbb{Z}$". We will get as far as discussing zeta functions of rings of finite type.

15.1 The Riemann zeta function

We start with the definition of the classical Riemann zeta function.

Definition 15.1.1 We define the *Riemann zeta function* as $\zeta(s) = \sum_{n>0} n^{-s}$, where, for n in $\mathbb{Z}_{>0}$ and s in $\mathbb{C}$, $n^{-s} = e^{-s \log n}$.

We have some facts about this function.

Fact 15.1.2 The series defining the Riemann zeta function $\zeta(s)$ converges absolutely for $\Re(s) > 1$. This can be easily deduced from the fact that for $s = a + bi$ with $a, b \in \mathbb{R}$ we have that $|n^{-s}| = |n^{-a}|$ and the fact that $\sum_{n>0} n^{-a}$ converges (absolutely) for $a > 1$.

Fact 15.1.3 The Riemann zeta function $\zeta(s)$ extends uniquely to a holomorphic function on $\mathbb{C} - \{1\}$. This extension has the property that $\zeta(-2n) = 0$ for $n \in \mathbb{Z}_{>0}$.

Conjecture 15.1.4 *(Riemann hypothesis) All other zeros $s \in \mathbb{C}$ of the Riemann zeta function ζ satisfy $\Re(s) = 1/2$.*

Remark 15.1.5 The Riemann zeta function has an *Euler product expansion* . For $s \in \mathbb{C}$ with $\Re(s) > 1$:

$$\zeta(s) = \prod_{\substack{p>0 \\ p \text{ prime}}} \frac{1}{(1 - p^{-s})}.$$

This last expression will be generalized to define the zeta function of a ring of finite type.

15.2 Rings of finite type

Definition 15.2.1 Let R be a ring. A *generating subset* of R is a subset S such that for all subrings $R' \subset R$ with $S \subset R'$ we have that $R' = R$.

Definition 15.2.2 A ring R is said to be of *finite type*, or *finitely generated*, if it has a finite generating subset.

Examples 15.2.3 Here are some examples of rings of finite type:

i. $\mathbb{Z}$ (take $S = \emptyset$);

ii. Any finite ring R (take $S = R$);

iii. If R is a ring of finite type then so is $R[X]$ (take $S' = S \cup \{X\}$);

iv. If R is of finite type and $I \subset R$ an ideal then R/I is finitely generated (take $S' = \{\overline{s} : s \in S\}$, where $\overline{s}$ denotes the image of s in R/I).

Examples 15.2.4 Not all rings are of finite type:

i. $\mathbb{Z}[X_1, X_2, \ldots]$ is not of finite type (given a finite candidate generating set S let $\{X_{i_1}, \ldots, X_{i_k}\}$ be the finite set of variables occurring in the polynomials in S. Then S is contained in the strict subring $\mathbb{Z}[X_{i_1}, \ldots, X_{i_k}]$ of $\mathbb{Z}[X_1, X_2, \ldots]$);

ii. $\mathbb{Q}$ is not of finite type (given a finite candidate generating set S let N be the least common multiple of the denominators of the elements of S. Take $R' = \mathbb{Z}[1/N] = \{a/N^b : a \in \mathbb{Z}, b \in \mathbb{N}\}$. Then $S \subset R' \subsetneq \mathbb{Q}$.)

Theorem 15.2.5 *Let R a ring of finite type which is a field. Then R is a finite field.*

For a proof, see [Eis], Theorem 4.19. Chapter 4 of this reference provides the proper context for this result: integral dependence and Hilbert's Nullstellensatz. See also [Looij].

Corollary 15.2.6 *Let R be a ring of finite type and $\mathfrak{m} \subset R$ a maximal ideal. Then the quotient $R/\mathfrak{m}$ is a finite field.*

15.3 Zeta functions of rings of finite type

Definition 15.3.1 Let R be a ring of finite type. The *zeta function* of R is defined as follows (for $s \in \mathbb{C}$ with $\Re(s)$ sufficiently large):

$$\zeta(R, s) = \prod_{\substack{\mathfrak{m} \subset R \\ \mathfrak{m} \text{ maximal ideal}}} \frac{1}{1 - (\#R/\mathfrak{m})^{-s}}$$

Examples 15.3.2

i. $\zeta(\mathbb{Z}, s) = \zeta(s)$;

ii. $\zeta(\{0\}, s) = 1$ (since there are no maximal ideals);

iii. Let k be a field of q elements. Then $\zeta(k, s) = (1 - q^{-s})^{-1}$ (since 0 is the unique maximal ideal).

Fact 15.3.3 Let R be a ring of finite type. Then there is a $\rho \in \mathbb{R}$ such that the product defining $\zeta(R,s)$ converges absolutely for $\Re(s) > \rho$. For example, for $R = \mathbb{Z}[x_1, \ldots, x_n]$, the product converges for $\Re(s) > n+1$ (use exercise 15.5.8).

Remark 15.3.4 From now on we will manipulate certain products and series without carefully looking at convergence. We implicitly assume that these manipulations are done in the domain of absolute convergence.

Proposition 15.3.5 *Let R be a ring of finite type. Then*

$$\zeta(R,s) = \prod_{p \text{ is prime}} \zeta(R/(p), s).$$

Proof Let $\mathfrak{m} \subset R$ be a maximal ideal of R. Since $R/\mathfrak{m}$ is a finite field, it has a finite characteristic $p > 0$. This gives us the element $p = \sum_{i=1}^{p} 1 \in \mathfrak{m}$. Moreover, we have the following bijection, where we only consider maximal ideals:

$$\begin{array}{rcl} \{\mathfrak{m} \subset R \mid p \in \mathfrak{m}\} & \overset{1:1}{\longleftrightarrow} & \{\mathfrak{m}' \subset R/(p)\} \\ \mathfrak{m} & \mapsto & \mathfrak{m}/(p) \\ \mathfrak{m}' + (p) & \leftarrow\!\shortmid & \mathfrak{m}' \end{array}$$

Now recall that

$$R/\mathfrak{m} = {R/(p)}\big/{\mathfrak{m}/(p)},$$

so they have the same number of elements. $\square$

In general one has the following conjecture (Riemann hypothesis for rings of finite type).

Conjecture 15.3.6 *Let R be a ring of finite type. Then $s \mapsto \zeta(R,s)$ extends to a meromorphic function on $\mathbb{C}$, and for every s in $\mathbb{C}$ at which $\zeta(R,-)$ has a pole or a zero we have $2\Re(s) \in \mathbb{Z}$.*

For $R = \mathbb{Z}$ this conjecture is equivalent to the Riemann hypothesis, as the zeros and poles of $\zeta(\mathbb{Z},-)$ with $\Re(s) > 1$ or $\Re(s) < 0$ are known. The main result of this course implies the conjecture for R that are an $\mathbb{F}_p$-algebra (for some prime number p) generated by two elements.

15.4 Zeta functions of $\mathbb{F}_p$-algebras

For p a prime number we denote by $\mathbb{F}_p$ the finite field $\mathbb{Z}/p\mathbb{Z}$. A ring R in which $p = 0$ has the property that *the* ring morphism $\mathbb{Z} \to R$ factors as $\mathbb{Z} \to \mathbb{F}_p \to R$. Such rings are called $\mathbb{F}_p$-*algebras*. Proposition 15.3.5 allows us to express the zeta function of a ring of finite type as a product of zeta functions of $\mathbb{F}_p$-algebras.

If R is an $\mathbb{F}_p$-algebra of finite type and $\mathfrak{m} \subset R$ a maximal ideal then $R/\mathfrak{m}$ is a field with $q = p^n$ elements for some $n \in \mathbb{Z}_{\geq 1}$. We write $\deg(\mathfrak{m}) = n$.

Definition 15.4.1 Let R be an $\mathbb{F}_p$-algebra of finite type. We define a formal power series $Z(R,t)$ as follows:

$$Z(R,t) = \prod_{\substack{\mathfrak{m} \subset R \\ \mathfrak{m} \text{ maximal ideal}}} \frac{1}{1 - t^{\deg(\mathfrak{m})}} = \prod_{\mathfrak{m}} \left(\sum_{n \geq 0} t^{n \cdot \deg(m)} \right) \in \mathbb{Z}[[t]].$$

Remark 15.4.2 Note that $\zeta(R,s) = Z(R, p^{-s})$.

Here is a deep theorem of Bernard Dwork and Alexander Grothendieck that we will not use, nor prove. See [Dwork] and [SGA5].

Theorem 15.4.3 *Let p be a prime number and R an $\mathbb{F}_p$-algebra of finite type. Then there exist f and g in $\mathbb{Z}[t]$ with $f(0) = 1$ and $g(0) = 1$ such that $Z(R, t) = f/g$.*

This implies the meromorphic continuation of Conjecture 15.3.6 for $\mathbb{F}_p$-algebras of finite type. Pierre Deligne has proved Conjecture 15.3.6 for $\mathbb{F}_p$-algebras of finite type; see [Del].

Now let $\mathbb{F}_p \to \overline{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}_p$ and for n in $\mathbb{Z}_{>0}$ let $\mathbb{F}_{p^n}$ be the unique subfield of $\overline{\mathbb{F}}_p$ of p^n elements, that is, $\mathbb{F}_{p^n}$ is the set of roots in $\overline{\mathbb{F}}_p$ of $X^{p^n} - X$. For R an $\mathbb{F}_p$-algebra of finite type we let $\nu_n(R)$ be the number of ring morphisms from R to $\mathbb{F}_{p^n}$.

Remark 15.4.4 Let p be prime and $R = \mathbb{F}_p[X_1, \ldots, X_r]/I$ with I the ideal generated by polynomials $f_1, \ldots, f_m$. What are the ring morphisms $R \to \mathbb{F}_{p^n}$? We first note that a ring morphism is completely determined by its values at the generators X_i. Suppose a ring morphism sends X_i to $x_i \in \mathbb{F}_{p^n}$. Since a ring morphism sends 0 to 0, it follows that $f_j(x_1, \ldots, x_r) = 0$ in $\mathbb{F}_{p^n}$ for all j. On the other hand, if we have $(x_1, \ldots, x_r)$ in $\mathbb{F}_{p^n}^r$ such that $f_j(x_1, \ldots, x_r) = 0$ for all j, the ring morphism from $\mathbb{F}_p[X_1, \ldots, X_r]$ to $\mathbb{F}_{p^n}$ that sends X_i to x_i factors through R. Hence we get:

$$\nu_n(R) = \#\{(x_1, \ldots, x_r) \in \mathbb{F}_{p^n}^r : f_i(x_1, \ldots, x_r) = 0 \text{ for } i = 1, \ldots, m\}.$$

Definition 15.4.5 The *logarithm* (of power series) is defined as the map

$$\begin{aligned} \log\colon 1 + x\mathbb{Q}[[x]] &\to x\mathbb{Q}[[x]] \\ 1 - a \in 1 + x\mathbb{Q}[[x]] &\mapsto -\sum_{n>0} \frac{a^n}{n}. \end{aligned}$$

Remark 15.4.6 Note that this sum converges to a formal power series: since x divides a, only finitely many terms contribute to the coefficient of x^n in $\log(1 - a)$.

Fact 15.4.7 The logarithm is a group morphism from the multiplicative group $1 + x\mathbb{Q}[[x]]$ to the additive group $x\mathbb{Q}[[x]]$.

The following theorem gives a very convenient expression for $Z(R, t)$.

Theorem 15.4.8 *For p prime and R an $\mathbb{F}_p$-algebra of finite type, we have:*

$$\log Z(R, t) = \sum_{n=1}^{\infty} \frac{\nu_n(R) t^n}{n}.$$

Proof First of all we have the following bijection:

$$\begin{array}{rcl} \{\text{ring morphisms } \beta\colon R \to \mathbb{F}_{p^n}\} & \stackrel{1:1}{\longleftrightarrow} & \{(\mathfrak{m}, \alpha) : \alpha \text{ a ring morphism } R/\mathfrak{m} \to \mathbb{F}_{p^n}\} \\ \beta & \mapsto & (\ker(\beta), \overline{\beta} : R/\ker(\beta) \to \mathbb{F}_{p^n}) \\ R \to R/\mathfrak{m} \stackrel{\alpha}{\to} \mathbb{F}_{p^n} & \leftarrow\!\shortmid & (\mathfrak{m}, R/\mathfrak{m} \stackrel{\alpha}{\to} \mathbb{F}_{p^n}). \end{array}$$

Let now $\mathfrak{m}$ be a maximal ideal of R. Note that $R/\mathfrak{m}$ has $\deg \mathfrak{m}$ embeddings in $\overline{\mathbb{F}}_p$ and that the image of each embedding is $\mathbb{F}_{p^{\deg(\mathfrak{m})}}$. Recall that the subfields of $\mathbb{F}_{p^n}$ are the $\mathbb{F}_{p^d}$ with d dividing n. Hence the number of ring morphisms $R/\mathfrak{m} \to \mathbb{F}_{p^n}$ is $\deg(\mathfrak{m})$ if $\deg(\mathfrak{m})$ divides n and is zero otherwise. This gives us:

$$\nu_n(R) = \sum_{d|n} d \cdot \#\{\mathfrak{m} \subset R |\ \deg(\mathfrak{m}) = d\}.$$

Now we just calculate:

$$\log Z(R,t) = \log \prod_{\mathfrak{m}} \frac{1}{1-t^{\deg(\mathfrak{m})}} = \sum_{\mathfrak{m}} \log\left(\frac{1}{1-t^{\deg(\mathfrak{m})}}\right) = \sum_{\mathfrak{m}} \sum_{i>0} \frac{t^{i\cdot\deg(\mathfrak{m})}}{i}$$

$$= \sum_{\mathfrak{m}} \sum_{i>0} \frac{t^{i\cdot\deg(\mathfrak{m})}}{i\cdot\deg(\mathfrak{m})} \cdot \deg(\mathfrak{m}) = \sum_{n=1}^{\infty} \frac{t^n}{n} \sum_{d|n} d \cdot \#\{\mathfrak{m} \subset R|\ \deg(\mathfrak{m}) = d\} = \sum_{n=1}^{\infty} \nu_n(R) \cdot \frac{t^n}{n}.$$

□

15.5 Exercises

Exercise 15.5.1 Show that a ring is of finite type if and only if it is isomorphic to a quotient of a polynomial ring over $\mathbb{Z}$ with finitely many variables.

Exercise 15.5.2 Let n be a positive integer. Compute $\zeta(\mathbb{Z}/n\mathbb{Z}, s)$.

Exercise 15.5.3 Let p be a prime, $r \in \mathbb{Z}_{>0}$, $q = p^r$ and $R = \mathbb{F}_q[X,Y]/(XY-1)$. Compute $Z(R,t)$ and show that it is a rational function of t.

Exercise 15.5.4 Same as the previous one but with $R = \mathbb{F}_q[X,Y,Z]/(X+Y^2+Z^3)$.

Exercise 15.5.5 Same as the previous one but with $R = \mathbb{F}_3[X,Y]/(X^2+Y^2+1)$.

In the following exercises you may assume that $\Re(s)$ is sufficiently large so that all occurring infinite products are absolutely convergent.

Exercise 15.5.6 Let R_1 and R_2 be rings of finite type. Show that $R_1 \times R_2$ is of finite type and that $\zeta(R_1 \times R_2, s) = \zeta(R_1, s)\zeta(R_2, s)$.

Exercise 15.5.7 Show that $\zeta(\mathbb{Z}[X]/(X^n), s) = \zeta(\mathbb{Z}, s)$.

Exercise 15.5.8 Let R be a ring of finite type. Show that $R[X]$ is of finite type and that

$$\zeta(R[X], s) = \zeta(R, s-1).$$

Exercise 15.5.9 Let p be a prime, $R = \mathbb{F}_p[X_1,\ldots,X_i]/(f_1,\ldots,f_j)$, and $R' = \mathbb{F}_{p^r}[X_1,\ldots,X_i]/(f_1,\ldots,f_j)$. Show that $Z(R',t) = \prod_{z^r=1} Z(R, zt)$, with the product taken over the $z \in \mathbb{C}$ with $z^r = 1$.

Exercise 15.5.10 Let R be the ring $\mathbb{F}_2[X,Y]/(Y^2+Y+X^3+1)$. From the theory developed in the lectures one may deduce that there exists an $\alpha \in \mathbb{C}$ with

$$Z(R,t) = \frac{(1-\alpha t)(1-\bar{\alpha} t)}{1-2t}.$$

Denote the number of solutions of $y^2+y+x^3+1=0$ with x and y in the field $\mathbb{F}_{2^n}$ by ν_n.

i. Show that $\nu_n = 2^n - \alpha^n - \bar{\alpha}^n$ for all positive integers n;

ii. compute ν_1 and ν_2 and use this to determine α;

iii. compute ν_3 by counting solutions and verify that the formula obtained in (i) and (ii) is correct in these cases;

iv. determine all the zeroes of $\zeta(R,s) = Z(R, 2^{-s})$.

Optional exercise: use a computer algebra package to do (iii) for ν_n with larger values of n.

Bibliography

[Del] P. Deligne. *La conjecture de Weil. I.* Inst. Hautes Études Sci. Publ. Math. 43 (1974), 273–307.

[Dwork] B. Dwork. *On the rationality of the zeta function of an algebraic variety.* Amer. J. Math. 82 1960 631–648.

[EGA] A. Grothendieck. *Eléments de géométrie algébrique, I, II, III, IV.* (rédigés avec la collaboration de Jean Dieudonné) Publications Mathématiques de l'IHÉS 4, 8, 11, 17, 20, 24, 28, 32. All available on:
`http://www.numdam.org/?lang=en`

[Eis] D. Eisenbud. *Commutative algebra. With a view toward algebraic geometry.* Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.

[Hart] R. Hartshorne. *Algebraic geometry.* Graduate Texts in Mathematics 52. Springer, New York, 1977.

[KK] L. Kaup and B. Kaup. *Holomorphic Functions of Several Variables*. De Gruyter Studies in Mathematics.

[Stacks] J. de Jong et. al. *Stacks project.*
`http://math.columbia.edu/algebraic_geometry/stacks-git/`

[Lang] S. Lang. *Algebra.* Addison-Wesley. 2nd and 3rd editions.

[Looij] E. Looijenga. *A first course on algebraic geometry.* Available at:
`http://www.staff.science.uu.nl/~looij101/AG2014.pdf`

[Moo] B. Moonen. *Introduction to Algebraic Geometry*. Available at:
`http://www.math.ru.nl/~bmoonen/AlgGeom/alggeom.pdf`

[SGA5] *Cohomologie l-adique et fonctions L*. Séminaire de Géométrie Algébrique du Bois-Marie 1965–1966 (SGA 5). Edité par Luc Illusie. Lecture Notes in Mathematics 589. Springer, Berlin, 1977.

[Serre] J-P. Serre. *Groupes algébriques et corps de classes.* Hermann, Paris, 1959.

[Spri] T.A. Springer. *Linear algebraic groups.* Reprint of the 1998 second edition. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2009.

[Stev] P. Stevenhagen. *Algebra 1, 2, en 3.* Available at:
`http://websites.math.leidenuniv.nl/algebra/`