Sidi Mohamed Ben Abdellah University
Faculty of Sciences Dhar El Mahraz
Department of Mathematics-Fez

A THESIS
PRESENTED TO SIDI MOHAMED BEN ABDELLAH UNIVERSITY IN FULFILLMENT OF THE REQUIREMENT FOR THE MASTER PROJECT IN PURE MATHEMATICS

Divisors in Algebraic Geometry, Central Simple Algebras and Severi-Brauer Varieties

---

Presented by :
Mr. Yassine Ait Mohamed

Supervised by :
Pr. Karim Mounirh

Contents

Acknowledgements

F*irst and foremost, I would like to express my gratitude to my supervisor, Pr. Karim Mounirh. Without his scrupulous attention and unwavering patience, this project would have been an impossibility. Furthermore, his guidance, encouragements and friendship have been an invaluable part of my experience at The Faculty of Sciences Dhar El Mehrez, in Mathematical and Humanity levels.*

My thanks also go to the jury team, Pr. Mohamed Tahar Kadaoui Abbassi and Pr. Hakima Mouanis for their availability and their presence to evaluate this work.

I would also like to thank all my friends who offered me a hand with the accomplishment of this thesis.

Finally, I must thank my family. My mother, and my father, are a constant source of strength. Thank you for your support in all of my endeavors.

Introduction

The purpose of the present work is to present how algebraic varieties offer a bridge connecting different areas in mathematics. Especially, we are interested here in making clear how ideas (and even more, theories) are converted from an algebraic (resp., number field) aspect to a purely geometric one. We also, indicate -sometimes-how reverse feedbacks are gained from the introduction of geometric language in the study of specific topics in algebra and number field theories.

This thesis is written -mostly- in a self contained manner and is designated to introduce a non-specialist reader in algebraic geometry to this mathematical world. For this end, we present in this manuscript many necessary backgrounds from various algebraic and geometric areas, and we give -as possible- detailed proofs for the results contained here.

Roughly speaking, the introduction of algebraic varieties in mathematics can be considered as an attempt to combine tools, objects and arguments from algebra (at first commutative algebra) and some corresponding topological spaces defined in a manner shaped to fit with what existed in differential manifold theory. As will be seen in more details throughout the first chapter, classical affine varieties are defined by means of polynomial functions with coefficients in a base field preferably taken to be algebraically closed. Precisely, they are the vanishing locus of families of polynomials in a finite Cartesian product of this base field. Some authors -as we will do in this work- prefer to add the extra condition that they are 'irreducible' with respect to Zariski topology. Taking (coordinates) algebras of these (affine) varieties, allows then to establish a nice correspondence with finitely generated domains over the base field. This in fact generalizes to give an equivalence of categories between the category of 'non necessary irreducible' affine varieties and the category of 'reduced' finitely generated algebras over this field. As in differential geometry, projective varieties are defined similarly by means of homogeneous polynomials, and special open covers of them are given by affine varieties, making it possible to lift properties from the affine case to the projective one.

The importance of the above equivalence of categories arises from the fact that for (some) algebraic objects, we can benefit from all topological and geometric properties of the corresponding varieties. In this sense, many purely geometric notions are connected to some algebraic ones, e.g., in the affine case, the dimension of a variety (i.e., the topological dimension of its underlying space) coincides with the (Krull) dimension of the corresponding affine coordinate algebra.

In contrast with differential setting, algebraic varieties are not Hausdorff in general, and so an algebraic group for example -defined in the same manner as Lie group in differential geometry- is not a topological group. Nevertheless, a separation notion does exist for algebraic varieties and any morphism of affine schemes turns to be separated. Moreover, the idea of working locally on a variety, especially using germs of regular functions, is a main idea that remains valid in this algebraic context. Besides, many notions inspired from differential manifolds like closed and open immersions are very helpful in the study of these algebraic varieties. We have also a notion of (algebraic) tangent space which allows benefiting from connections with Lie theory when dealing for example with algebraic groups.

In modern algebraic geometry, the use of sheaf theory made it possible to work on a general commutative base ring (not only on a base field) and affine varieties, as will be explained in the second chapter, are defined by means of the spectrum of the considered ring.

For non affine varieties like projective ones, scheme theory developed essentially in Alexander's pioneer work and that of his collaborators, made it possible to generalize arbitrary varieties to the context of (commutative) rings. The idea of schemes consists in some gluing of spectra of many (commutative) rings along open subsets. This theory heavily relies on category language and the landscape appears very difficult without sufficient understanding of classical varieties. Schemes theory at its earlier beginning served to settle many important conjectures like Weil conjectures and Mordell conjecture. It becomes today an important component in many mathematical areas and continues to intervene in solving many hard problems. Indeed, many algebraic results still continue to have only geometric proofs.
As in algebraic topology and also in differential geometry, a notion of (algebraic) vector bundles was defined and used to build Grothendieck groups (of varieties). More generally, all K-theory groups are defined by using these algebraic bundles in the same model as for commutative rings. Indeed, in the language of modules over schemes -see the second chapter- and up to an equivalence of categories, algebraic vector bundles are exactly coherent modules over (Noetherian) schemes. Also, when dealing with an affine scheme, they correspond categorically - under some canonical equivalence- to finitely generated projective modules over the base ring. Besides this approach relating schemes to K-groups, many properties of schemes can be described by using adequate cohomological complexes.

In this manuscript we give two applications of algebraic geometry showing the above said interplay between algebra, number field theory and varieties. The first one concerns the notion of divisors in algebraic geometry and the second one deals with Severi-Brauer varieties.

The notion of divisors for varieties is part of intersection theory in algebraic geometry. It can be considered as an extension of the well known Kronecker's divisors in algebraic number field theory. Historically, it is known that Kronecker's divisors were built on a simple but fascinating idea which consists in determining greatest common divisors inside the polynomial algebra (in one indeterminate) over the rational field. The main tool used for this end was an easy notion of the 'content' of a polynomial which is the greatest common divisor of its coefficients in the case of a polynomial with integer coefficients. Indeed, at that time such simple notions were often the starting point of flourishing theories. Hermann Weyl developed then an axiomatization of divisors built on the same principal of Dedekind's elegant 'ideal theory' to give information on prime factorizations. A divisor became then some well defined ideal and a multiplicative group was then derived from nonzero divisors. This group was then related to other groups defined in Dedekind's theory. Moreover, besides working over a rational field, divisors were extended to be defined over more base fields, e.g., number fields. The study of divisors benefited from several algebraic and number field tools, e.g., Diddekind's discriminants, Picard group.., but a great raise was due to the use of valuation theory, where divisors took another aspect based on the notion of 'places', which are closed to valuation rings. Plainly, Dedekind's and valuation approaches had opened new perspectives in the study of divisors; nevertheless, it is worthy to mention that the ancient (and almost forgotten) theory of 'contents' preserves some advantages when compared with these new approaches (e.g., it is independent of the considered base field which is not the case for Dedekind's approach).

The use of valuation language in the study of divisors, allowed for algebraic number fields at first - then for varieties - developing Riemann-Roch theory which is now widely applied in different areas of mathematics, especially in coding theory and cryptography.

Divisors in algebraic geometry were first defined on (classical) curves, since (special) discrete valuations exist on the function field of such a curve and local rings of nonsingular curve's points are regular. The theory was then extended to codimension one varieties in schemes theory and gave rise to Chow groups, where a general intersection theory was built from algebraic cycles. A (Weil) divisor is then a cycle of codimension one. Unfortunately, we

did not deal in this manuscript with this more general (intersection) theory for it would need more special background. Let's finally mention that divisors have close connection with vector bundles. Indeed, there is a one-to-one correspondence between equivalence classes of (Weil) divisors and isomorphism classes of (algebraic) line bundles.

The other example illustrating the usefulness of varieties that we treat in this manuscript concerns Severi-Brauer varieties which are widely applied in studying central simple algebras. They appeared in François Châtelet's paper [7] but historically it is announced that they appeared before and are due in part to Severi (see [2]). As will be explained in the third chapter, to every central simple algebra, one can attach a corresponding Severi-Brauer variety and this last one encodes information on splitting fields of such algebra. Indeed, Amitsur used in [1] the function field of this attached variety and defined a generic splitting field for the considered algebra. Since then, Severi-Brauer varieties became very useful in the study of Brauer groups, groups that classify central simple algebras over some fixed fields.

Throughout different discussions in this manuscript, we don't pretend originality, and we refer the reader to a list of references at the end.

In an attempt to achieve our described aim in this work, we organize the content of this manuscript as follows.

In the first chapter, which consists of two parts, we introduce in the first part the necessary background of (classical) affine and projective varieties. In particular, we define Zariski topology for such varieties. We define regular functions, morphisms and rational maps of varieties. We describe how a coordinate ring is associated to an affine variety and how equivalence of categories relate both sides. We show how a projective variety is covered by affine opens. We prove that the dimension of an affine variety coincides with the (Krull) dimension of its corresponding coordinate algebra. We define tangent spaces and study some elementary properties of nonsingular points. Also, we define the notion of normal varieties and show that a nonsingular variety is necessarily normal. In the second part of this chapter, we introduce divisors in terms of places and study some of their properties on (classical) curves. We give in particular a detailed survey on Riemann-Roch theory on these curves.

The second chapter, consisting of three parts deals with the theory of schemes. The first part lays out the basic definitions and properties of sheaf theory. The second one discusses schemes, morphisms between schemes, fiber products and dimension of schemes. It deals also with local and global properties of schemes. This includes the notions of Noetherian, irreducible, reduced, integral, regular, normal, separated, proper, projective schemes. We also study modules over schemes. The third part deals with cohomological interpretations in scheme theory and introduce Weil and Cartier divisors (defined now in terms of schemes). For a full treatment of sheaves, schemes, Weil divisors and Cartier divisors, we refer to [9], [17] and [12].

The third chapter consists of two parts. In the first one, we give a brief survey on simple and semisimple modules, on central simple algebras and prove in particular fundamental theorems like Wedderburn's theorem, the double centralizer theorem and Skolem-Noether theorem. We show how to build and we study Brauer group of a field and show how crossed products relate this group to a second Galois cohomology group. For more details on central simple algebras, we refer to [15], [10] and [21]. The second part, concerns Severi-Brauer varieties and discusses some of their properties and the interplay between these varieties, central simple algebras and some cohomological interpretations.

Notation and terminology

k	*a field*
$k[T_1, \ldots, T_n]$	*The (commutative) k-algebra of polynomials in n indeterminates with coefficients in k.*
$\mathbb{A}^n$	*The affine space of dimension n over k.*
$\mathbb{P}^n$	*The projective space of dimension n over k*
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	*The ring of integers, rational numbers, real numbers, complex numbers.*
R	*a commutative ring with identity element.*
UFD	*Unique factorization domain.*
PID	*Principal ideal domain.*
DVR	*Discrete valuation ring.*
$Z(S)$	*The set of common zeros of the polynomials in* S.
$I(X)$	*The ideal of a set* X.
$k[X]$	*The coordinate ring of an algebraic set.*
$\mathcal{O}(X)$	*The set of all regular functions on a variety X (the ring of regular functions on X)*
$var(k)$	*The category of varieties over k.*
$\mathcal{O}_x$	*The local ring of X at* x*, also called the ring of germs of regular functions at* x.
T_xX	*The tangent space to an algebraic set X at* x.
$Der_x(k[X])$	*The set of derivations of* $k[X]$ *at* x.
RF(X,Y)	*The set of all rational functions from X to* Y.
$\mathcal{TA}_k$	*The category of spaces of functions over k.*
$V^\vee$, $Hom(V,k)$	*The dual space of* V.
$R_\mathfrak{p}$	*localization at* $\mathfrak{p}$.
$Div(E)$	*The group of divisors of a function field E/k.*
$\mathcal{L}(D)$	*The Riemann-Roch Space.*
$l(D)$	$dim_k(\mathcal{L}(D))$.
$\mathbb{A}_E$	*The set of all adèles of* E/k.
$\mathbb{P}_E$	*The set of all places P of* E/k.
$\mathcal{T}op$	*The category of topological spaces.*
$\mathcal{F}$	*(pre)sheaf on a topological space.*
$\mathcal{F}^\dagger$	*Sheafification of presheaf* $\mathcal{F}$.
$\mathcal{F}_x$	*The stalk of a presheaf* $\mathcal{F}$ *at a point* x.
$Ab\mathcal{S}h_X$	*The category of abelian sheaves.*
$\mathcal{P}reSh_X$	*The category of presheaves on the topological space X.*
$f_*\mathcal{F}$	*The pushforward of* $\mathcal{F}$.
$f^{-1}\mathcal{G}$	*The pullback sheaf.*
$\mathcal{C}$	*a category.*
$Spec(R)$	*The set of all prime ideals of R.*
$\mathcal{RS}$	*The category of ringed spaces.*
$\mathcal{S}h_X$	*The category of sheaves on X.*
$\mathcal{S}ch$	*The category of schemes.*
$A\mathcal{S}ch$	*The category of affine schemes.*
$\mathcal{O}_{Spec}$	*The Structure Sheaf on* $Spec(R)$.
$\mathcal{Q}Coh_{\mathcal{O}_X}$	*The category of quasi-coherent* $\mathcal{O}_X$*-modules.*
$\mathcal{C}oh(\mathcal{O}_X)$	*The category of coherent* $\mathcal{O}_X$*-modules.*
$S(M)$	*The set for all submodules of M.*

Notation and terminology

$Cadiv(X)$	*The group of Cartier divisors.*
$Cadiv_{+}(X)$	*The set of effective Cartier divisors.*
$CaCl(X) := CaDiv(X)/\sim$	*Cartier divisors class group.*
$Div(X)$	*The group of Weil divisors.*
$Div^0(X)$	*The principal divisors.*
$Cl(X) := Div(X)/Div^0(X)$	*Weil class group of X*
CSA(F)	*The class of all central simple algebras over F.*
$Br(F)$	*The Brauer group of F.*
$Br(E/F)$	*The relative Brauer group of the field extension $E \supseteq F$.*
$G := Gal(E/F)$	*The Galois group of E/F.*
(E, G, a)	*The crossed product algebra over F determined by E and a.*
$A = (E/F, \sigma, \beta)$	*The cyclic algebra over F determined by E and β.*
$\mathcal{A}b\mathcal{G}rp$	*The category of abelian groups*
$H^0(G, M)$	*The zeroth cohomology set of G with coefficients in M.*
$H^1(G, M)$	*The first cohomology set of G with coefficients in M.*
Az_n^F	*The set of all isomorphy classes of central simple algebras A of dimension n^2 over F.*
$Az_n^{E/F}$	*The set of all isomorphy classes of central simple algebras A which are of dimension n^2 over F and split over E.*
BS_m^F	*The set of all isomorphy classes of Severi-Brauer varieties X of dimension m over F.*
$BS_m^{E/F}$	*The set of all isomorphy classes of Severi-Brauer varieties X of dimension m over F.*

Chapter 1

Introduction to the Geometry of Affine and Projective Spaces

In Algebraic Geometry, we study geometric objects - varieties - that are defined by polynomial equations. One fascinating aspect of this is that we can do geometry over arbitrary fields, however we can gain a lot of geometric intuition from looking at algebraically closed fields k. * *The theory developed here is often described as the commutative part of algebraic geometry for it relies heavily on concepts and results from commutative algebra. In particular, unless otherwise mentioned, all considered algebras in this chapter -as well as in the second one- are assumed to be commutative. More details about the content of this chapter were given in the general introduction of this manuscript and we see no interest to repeat this description here.*

1.1 Affine and projective varieties

In this section, we will define the basic objects of our study : Algebraic sets in affine space of dimension an arbitrary integer n $\mathbb{A}^n = k^n$. *We define also affine and projective varieties and give some of their first properties.*
Throughout the rest, we let $k[T_1, \ldots, T_n]$ *denote the (commutative) k-algebra of polynomials in n indeterminates* $T_1, \ldots, T_n$, *with coefficients in k. A polynomial* $f \in k[T_1, \ldots, T_n]$ *defines a function* $\tilde{f} : \mathbb{A}^n \longrightarrow k$, *given by* $(a_1, \ldots, a_n) \longmapsto f(a_1, \ldots, a_n)$. *The k-valued functions on* $\mathbb{A}^n$ *form a k-algebra via pointwise addition and multiplication.*
The map

$$\begin{array}{rccc} \varphi : & k[T_1, \ldots, T_n] & \longrightarrow & \{\mathit{functions}, \mathbb{A}^n \longrightarrow k\} \\ & f & \longmapsto & \tilde{f} \end{array}$$

is a k-algebra homomorphism.

1.1.1 Affine varieties

As seen aboven the affine space of dimension n over k is simply the set k^n. *It will be denoted by* $\mathbb{A}^n_k$ *or simply by* $\mathbb{A}^n$. *The elements (also called points)* $\mathbb{A}^n$ *are then n-uples* $(a_1, \ldots, a_n)$, *where* $a_i \in k$ *for* $i = 1, \ldots, n$. *Algebraic sets in the affine space are defined by means of subsets* $S \subseteq k[T_1, \ldots, T_n]$. *For such a subset, we let by* (S) *be the ideal of* $k[T_1, \ldots, T_n]$ *generated by S.*

---

* *A field k is algebraically closed if every non-constant polynomial (on one indeterminate and with coefficients in k) has a root in k. It follows that every polynomial of degree n can be uniquely factorized (up to permutation of the factors) as*

$$P = c\prod_{i=1}^{n}(X - a_i)$$

where c and the a_i *are elements of k.*

Definition 1.1.1 *Let $S \subseteq k[T_1, \ldots, T_n]$ be any subset. The set*

$$Z(S) := \{(a_1, \ldots, a_n) \in \mathbb{A}^n \mid f(a_1, \ldots, a_n) = 0, \text{for all} f(T_1, \ldots, T_n) \in S\}$$

is called the algebraic set (of $\mathbb{A}^n$) defined by S.

Remarks 1.1.1 *i) It is not hard to see that if the set of polynomials is larger, the set of common zeros is smaller, i.e.,*

$$S \subseteq S' \Longrightarrow Z(S') \subseteq Z(S)$$

ii) If I is the ideal generated by the polynomials in S, then we have $Z(I) = Z(S)$. So algebraic sets can be defined $Z(I)$ for ideals $I \subseteq k[T_1, \ldots, T_n]$. Recall that all ideals in $k[T_1, \ldots, T_n]$ are finitely generated by the Hilbert Basis Theorem.

Examples 1.1.1 *1) Affine n-space itself is an algebraic set, since $\mathbb{A}^n = Z(0)$. Similarly, the empty set $\emptyset = Z(1)$ is an algebraic set.*

2) Any single point in $\mathbb{A}^n$ is an algebraic set. Indeed, we have $\{(a_1, \ldots, a_n)\} = Z(T_1 - a_1, \ldots, T_n - a_n)$.

3) The special linear group, $SL(n, k)$ which is the set of all matrices $A = (a_{ij})_{1 \le i,j \le n}$ with entries in k and such that $det(A) = 1$, can be viewed as a subset of $\mathbb{A}^{n^2}$ by the correspondence

$$(a_{ij}) \quad \longmapsto \quad (a_{11}, \ldots, a_{1n}, \ldots, a_{21}, \ldots, a_{2n}, \ldots, a_{n1}, \ldots, a_{nn})$$

This is an algebraic set because the determinant of a matrix is a polynomial function of the matrix-elements, so that $SL(n, k)$ is the set of zeros of the polynomial, $det(A) - 1$ for $A \in \mathbb{A}^{n^2}$.

Here are some basic properties of algebraic sets and the ideals that generate them :

Proposition 1.1.1 *Let I, J be ideals of $k[T_1, \ldots, T_n]$. Then*

1) $I \subseteq J$ implies $Z(J) \subseteq Z(I)$.

2) $Z(IJ) = Z(I \cap J) = Z(I) \cup Z(J)$.

3) $Z(\sum I_i) = \bigcap Z(I_i)$.

Proof. *1) For $a \in Z(J)$, we have $f(a) = 0$, for all $f \in J$, so in particular for all $f \in I$. So $a \in Z(I)$.*

2) Plainly, we have $IJ \subseteq I \cap J \subseteq I, J$, so $Z(I \cap J) \subseteq Z(I) \cup Z(J)$. For the reserve inclusions, let $a \notin Z(I) \cup Z(J)$, then there exists $f \in I$ and $g \in J$ such that $f(a) \neq 0$ and $g(a) \neq 0$. Then $fg(a) \neq 0$, so $a \notin Z(IJ)$.

3) For all j, we have $I_j \subseteq \sum I_j$ then $Z(\sum I_j) \subseteq Z(I_i)$, hence $Z(\sum I_i) \subseteq \cap Z(I_i)$. Conversely, for $a \in \bigcap Z(I_i)$, we have $a \in Z(I_i)$, for all i. For each $f \in \sum I_i$, we can write $f = \sum_{k=1}^{r} f_k$, where $f_k \in I_k$, $k = 1, \ldots, r$. So, $f(a) = \sum_{k=1}^{r} f_k(a) = 0$, therefore $a \in Z(\sum I_i)$

It follows that the algebraic sets in $\mathbb{A}^n$ satisfy the axioms of the closed sets in a topology.

Definition 1.1.2 *The Zariski topology on $\mathbb{A}^n$ is the topology for which the closed sets are algebraic sets of $\mathbb{A}^n$.*

Notation. *For a subset $X \subseteq \mathbb{A}^n$, define $I(X) := \{f \in k[T_1, \ldots, T_n] \mid f(x) = 0, \forall x \in X\}$. The set $I(X)$ is an ideal in $k[T_1, \ldots, T_n]$.*

Example 1.1.1 *Let $a = (a_1, \dots, a_n) \in \mathbb{A}^n$ be a point, then the ideal of the one-point set $\{a\}$ is $I(a) := I(\{a\}) = (T_1 - a_1, \dots, T_n - a_n)$.*

We have now constructed operations

$$\begin{array}{ccc} \{\text{Algebraic sets in } \mathbb{A}^n\} & \longleftrightarrow & \{\text{ideals in } k[T_1,\dots,T_n]\} \\ X & \longrightarrow & I(X) \\ Z(J) & \longleftarrow & J \end{array}$$

and should check whether they actually give a bijective correspondence between ideals of $k[T_1, \dots, T_n]$ and algebraic sets.

Lemma 1.1.1 *Let S and $S^{'}$ be a subsets of $k[T_1, \dots, T_n]$ and let X and $X^{'}$ be a subsets of $\mathbb{A}^n$*

i) If $X \subseteq X^{'}$ then $I(X^{'}) \subseteq I(X)$.

ii) $X \subseteq Z(I(X))$ and $S \subseteq I(Z(S))$.

iii) The Zariski closure of X is exactly $Z(I(X))$. So, if X is an algebraic set, then $Z(I(X)) = X$.

iv) $I(X \cup X^{'}) = I(X) \cap I(X^{'})$.

Proof. *i) Clear.*

ii) Clear.

iii) By ii), we have $X \subseteq Z(I(X))$ and so $\overline{X} \subseteq Z(I(X))$. Conversely, let $W \subseteq \mathbb{A}^n$ be an algebraic set containing X and write $W = Z(S)$ for some $S \subseteq k[T_1, \dots, T_n]$. Then, again by ii), we have $S \subseteq I(Z(S)) = I(W) \subseteq I(X)$ and so $Z(I(X)) \subseteq Z(S) = W$, as required.

iv) We have $X, X^{'} \subseteq X \cup X^{'}$, so by i) we get $I(X \cup X^{'}) \subseteq I(X) \cap I(X^{'})$. Conversely for $f \in I(X) \cap I(X^{'})$, we have $f(x) = 0$, for all $x \in X \cup X^{'}$. So $f \in I(X \cup X^{'})$.

By this lemma, the only thing left that would be needed for a bijective correspondence between ideals of $k[T_1, \dots, T_n]$ and algebraic sets $\mathbb{A}^n$ would be $I(Z(J)) \subset J$ for any ideal J (so that then $I(Z(J)) = J$ by part ii). Unfortunately, the following example shows that why this is not true in general.

Example 1.1.2 *Let J be a nonzero ideal $\mathbb{C}[X]$. As $\mathbb{C}[X]$ is a principal ideal domain and $\mathbb{C}$ is algebraically closed, we have*

$$J = ((X - b_1)^{m_1} \cdots (X - b_n)^{m_n})$$

for some $n \in \mathbb{N}$, distinct elements $b_1, \dots, b_n \in \mathbb{C}$, and $m_1, \dots, m_n \in \mathbb{N}$. Obviously, the zero locus of this ideal in $\mathbb{A}^1$ is $Z(J) = \{b_1, \dots, b_n\}$. The polynomials vanishing on this set are precisely those that contain each factor $X - b_i$ for $i = 1, \dots, n$ at least once, i. e. we have

$$I(Z(J)) = ((X - b_1) \cdots (X - b_n)) \neq J.$$

If at least one of the numbers $m_1, \dots, m_n$ is greater than 1, this is a bigger ideal than J.

In what follows we will see that a bijective correspondence does however exist between algebraic sets in $\mathbb{A}^n$ and some special ideals (radical ideals) of $k[T_1, \dots, T_n]$.

Definition 1.1.3 *Let R be a commutative ring and let $J \subseteq R$ be an ideal. Then the set of $a \in R$ with the property that $a^m \in J$ for some $m > 0$ is an ideal of R, called the radical of J and denoted $rad(J)$. We say that J is a radical ideal if $rad(J) = J$.*
We say that the ring R is reduced if the zero ideal (0) is a radical ideal (in other words, if $a \in R$ with that $a^m = 0$, for some positive integer m, then $a = 0$).

Lemma 1.1.2 *If A and B are integral domains, with B integral over A, then B is a field if and only if A is a field.*

Proof. *Let $b \in B$ be a nonzero element. Since B is an integral over A, then we can write*

$$b^m + a_{m-1}b^{m-1} + \ldots + a_0 = 0 \tag{1.1}$$

with $m \in \mathbb{N}$ a nonzero natural integer, $a_i \in A$ $(1 \leq i \leq m)$. Moreover, Since A is integral domain, we can suppose that $a_0 \neq 0$.
Suppose that A is a field, then a_0 has an inverse in A. By (1.1), we have :

$$\begin{aligned} a_0 &= -(b^m + a_{m-1}b^{m-1} + \ldots + a_1 b) \\ &= -(b^{m-1} + a_{m-1}b^{m-2} + \ldots + a_1)b \end{aligned}$$

$1 = -a_0^{-1}(b^{m-1} + a_{m-1}b^{m-2} + \ldots + a_1)b$*, which shows that b is a unit of B. Conversely, suppose B is a field and $r \in A$. Then $r^{-1} \in B$ and we can write r :*

$$r^{-n} + a_{n-1}r^{-(n-1)} + \ldots + a_0 = 0$$

for some positive integer n and some elements $a_i \in A$. If we multiply this equality by r^{n-1}, we get

$$r^{-1} + a_{n-1} + \ldots + a_0 r^{n-1} = 0.$$

Hence $r^{-1} = -(a_{n-1} + ... + a_0 r^{n-1}) \in A$.

Theorem 1.1.1 *Let A be a finitely generated algebra over k. If A is a field, then A is an algebraic extension of k.*

Proof. *See [6, Lemma 9.1.2, p.**454**].*

Corollary 1.1.1 *(Hilbert's Nullstellensatz) (weak form). Let k be an algebraically closed field. The maximal ideals of $k[T_1, \ldots, T_n]$ are precisely the ideals*

$$I(a_1, \ldots, a_n) = (T_1 - a_1, T_2 - a_2, \ldots, T_n - a_n)$$

for all points $(a_1, \ldots, a_n) \in \mathbb{A}^n$.

Proof. *Let $\mathfrak{m}$ be a maximal ideal of $k[T_1, \ldots, T_n]$ and $A := \frac{k[T_1,\ldots,T_n]}{\mathfrak{m}}$. Plainly, obvious that A is a finitely generated algebra over k (generated by the elements $T_i + \mathfrak{m}$ of A); moreover by theorem 1.1.1, A is an algebraic field extension of k. Since k is algebraically closed, embedding $\phi : k \longrightarrow A(= \frac{k[T_1,\ldots,T_n]}{\mathfrak{m}})$, $a \longmapsto a + \mathfrak{m}$ is an isomorphism (of fields). In particular there exists $a_i \in k$ such that $T_i + \mathfrak{m} = \phi(a_i)$ (for all $1 \leq i \leq n$). This means that $T_i - a_i \in \mathfrak{m}$, so the ideal $(T_1 - a_1, \ldots, T_n - a_n)$ is contained in $\mathfrak{m}$. Conversely, for any $f \in \mathfrak{m}$ considering f as a polynomial in T_1 and taking the Euclidean division of f by $T_1 - a_1$, we get $f = f_1(T_1, \ldots, T_n)(T_1 - a_1) + r(T_2, \ldots, T_n)$, where $f_1(T_1, \ldots, T_n), r(T_2, \ldots, T_n) \in k[T_1, \ldots, T_n]$, with $\deg r(T_2, \ldots, T_n) = 0$ i.e., T_1 not appearing in $r(T_2, \ldots, T_n)$*
Once again, taking the Euclidean division of $r(T_2, \ldots, T_n)$ by $T_2 - a_2$, we get

$$f = f_1(T_1, \ldots, T_n)(T_1 - a_1) + f_2(T_2, \ldots, T_n)(T_2 - a_2) + r_3(T_3 \ldots, T_n)$$

Continuing in this way, we get

$$f = f_1(T_1, \ldots, T_n)(T_1 - a_1) + \ldots + f_n(T_n)(T_n - a_n) + a.$$

We have $T_i - a_i \in \mathfrak{m}$, so necessarily $a = 0$ (for $a \in \mathfrak{m}$ and $\mathfrak{m}$ is a maximal ideal of $k[T_1, \ldots, T_n]$). Therefore $f \in (T_1 - a_1, \ldots, T_n - a_n)$. So $\mathfrak{m} = (T_1 - a_1, T_2 - a_2, \ldots, T_n - a_n)$.

Corollary 1.1.2 *Let k be k an algebraically closed field. For every proper ideal J in $k[T_1, \ldots, T_n]$, there is a point $x \in Z(J)$.*

Proof. *Let J be a proper ideal in $k[T_1, \ldots, T_n]$ J and let $\mathfrak{m}$ be a maximal ideal of $k[T_1, \ldots, T_n]$ containing J. By corollary 1.1.1, we can write $\mathfrak{m} = (T_1 - a_1, \ldots, T_n - a_n)$. As $J \subseteq \mathfrak{m}$, we may conclude that $(a_1, \ldots, a_n) \in Z(J)$.*

Theorem 1.1.2 *(Hilbert's Nullstellensatz). Let k be an algebraically closed field. Then for every ideal J of $K[T_1, \ldots, T_n]$ we have $I(Z(J)) = rad(J)$*

Proof. *Let $f \in rad(J)$, then there is some positive integer n such that $f^n \in J$, so f^n vanishes on $Z(J)$, hence f vanishes on it too. Thus, $I(Z(J)) \supset rad(J)$. For the reverse inclusion, let's introduce a new auxiliary indeterminate is to introduce a new auxiliary variable T_{n+1}. Let's also consider some $g \in I(Z(J))$ and let L be the ideal of the polynomial ring $k[T_1, \ldots, T_{n+1}]$ given by*

$$L = J \cdot k[T_1, \ldots, T_{n+1}] + t(1 - T_{n+1} \cdot g)$$

In geometric terms the zero-locus $Z(L) \subseteq \mathbb{A}^{n+1}$ is the intersection of the the subset $Z = Z(1 - T_{n+1}, g)$ and the inverse image $\pi^{-1}(Z(J))$ of $Z(J)$ under the projection $\pi : \mathrm{A}^{n+1} \to \mathbb{A}^n$ that forgets the auxiliary coordinate T_{n+1}. This intersection is empty since obviously g does not vanish along Z, but vanishes identically on $\pi^{-1}(Z(J))$. The corollary 1.1.1 therefore gives that $1 \in L$, and there are polynomials f_i in J and h_i and h in $k[T_1, \ldots, T_{n+1}]$ satisfying a relation like

$$1 = \sum_{i=1}^{m} f_i(T_1, \ldots, T_n) h_i(T_1, \ldots, T_{n+1}) + h(1 - T_{n+1} \cdot g)$$

We substitute $T_{n+1} = \frac{1}{g}$ and multiply through by a sufficiently high power g^N of g to obtain

$$g^N = \sum f(T_1, \ldots, T_n) H_i(T_1, \ldots, T_n)$$

where $H_i(T_1, \ldots, T_n) = g^N \cdot h_i(T_1, \ldots, T_n, g^{-1})$. Hence $g \in rad(J)$.

Hilbert's Nullstellensatz† *precisely describes the correspondence between algebra and geometry :*

Corollary 1.1.3 *Let k be an algebraically closed field.*

i) The map $J \longmapsto Z(J)$ defines a one-to-one correspondence between the set of radical ideals in $k[T_1, \ldots, T_n]$ and the set of algebraic subsets of $\mathbb{A}^n$. Its inverse is given by $X \mapsto I(X)$, for any algebraic set in $\mathbb{A}^n$ i.e

$$\left\{ \begin{array}{c} \text{algebraic sets} \\ \text{in } \mathbb{A}^n \end{array} \right\} \underset{Z}{\overset{I}{\rightleftarrows}} \left\{ \begin{array}{c} \text{radical ideals in} \\ k[T_1, \ldots, T_n] \end{array} \right\}. \tag{1.2}$$

ii) There is a one-to-one correspondence

$$\begin{array}{ccc} \{\text{points of } \mathbb{A}^n\} & \longleftrightarrow & \{\text{maximal ideals of } k[T_1, \ldots, T_n]\} \\ p & \longmapsto & m_p \end{array}$$

where $m_p := (T_1 - p_1, \ldots, T_n - p_n)$.

† *Hilbert's Nullstellensatz is a theorem that establishes a fundamental relationship between geometry and algebra. This relationship is the basis of algebraic geometry, a branch of mathematics. It connects algebraic sets to ideals in polynomial rings on algebraically closed fields. This relation was discovered by David Hilbert who proved the Nullstellensatz and several other important related theorems named after him (such as Hilbert's basic theorems).*

Proof. *i) This follows from the fact that $I(Z(J)) = J$ and $Z(I(X)) = X$, for every radical ideal J of $k[T_1, \ldots, T_n]$ and every algebraic set X in $\mathbb{A}^n$.*

ii) Let J be a maximal ideal of $k[T_1, \ldots, T_n]$, then by corollary 1.1.1 there exists $a_1, ..., a_n \in k$ such that $J = (T_1 - a_1, \ldots, T_n - a_n) = m_p$, hence $J = m_p$, where $p = (a_1, ..., a_n)$.
Then prove that $p \longmapsto m_p$ is a surjective map from $\mathbb{A}^n$ onto the set of maximal ideals of $k[T_1, \ldots, T_n]$. This map is also injective, indeed let p_1 and $p_2 \in \mathbb{A}^n$, and suppose $m_{p_1} = m_{p_2}$, then $Z(m_{p_1}) = Z(m_{p_2})$, but we have $Z(m_{p_i}) = \{p_i\}$ $(1 \leq i \leq n$. So, $p_1 = p_2$.

Corollary 1.1.4 *The radical of an ideal of $k\,[T_1, \ldots, T_n]$ is equal to the intersection of the maximal ideals containing it.*

Remark 1.1.1 *The radical of an ideal is the intersections of all prime ideals that contain it (see corollary 1.1.4). The statement given here is true in the above context, where the basic field is algebraically closed.*

Proof. *Let a $J \subseteq k[T_1, \ldots, T_n]$ be an ideal. Because maximal ideals are radical, every maximal ideal containing J also contains $rad(J)$, so*

$$rad(J) \subset \bigcap_{\mathfrak{m} \supset J} \mathfrak{m}$$

For each $P = (a_1, \ldots, a_n) \in k^n, \mathfrak{m}_P = (T_1 - a_1, \ldots, T_n - a_n)$ is a maximal ideal in $k[T_1, \ldots, T_n]$ and

$$f \in \mathfrak{m}_P \Leftrightarrow f(P) = 0$$

so

$$\mathfrak{m}_P \supset J \Leftrightarrow P \in Z(J)$$

If $f \in \mathfrak{m}_P$ for all $P \in Z(J)$, then f vanishes on $Z(J)$, so $f \in I(Z(J)) = rad(J)$. It follows that

$$rad(J) \supseteq \bigcap_{P \in Z(J)} \mathfrak{m}_P.$$

The coordinate ring of an algebraic set

The (affine) coordinate ring is one of the central concepts of algebraic geometry, particularly the theory of affine algebraic sets. It is the ring of algebraic functions on an algebraic set.

Definition 1.1.4 *Let $X \subset \mathbb{A}^n$ be an algebraic set. The quotient ring*

$$k[X] := k\,[T_1, \ldots, T_n]\,/I(X)$$

is called the affine coordinate ring of X. It is a finitely generated algebra over k.
Two polynomials f and g on the indeterminates $T_1, \ldots, T_n$ restrict to the same function on X precisely when their difference $f - g$ belongs to the ideal $I(X)$. Hence it is natural to interpret elements in $k[X]$ as being polynomial functions from X into k, i.e., k-valued functions on X that are restrictions of a polynomials.

Example 1.1.3 *Let $X \subset \mathbb{A}^2$ be the hyperbola defined by $XY - 1 = 0$, so the coordinate ring is*

$$k[X, Y]/(XY - 1) = k[X, X^{-1}].$$

the ring of so-called Laurent polynomials.

If X is an algebraic set of $\mathbb{A}^n$ and if Y is an algebraic set contained in X, then as previously seen, we have $I(X) \subseteq I(Y)$. Conversely if $I(Y)$ contains $I(X)$, then $Y (= Z(I(Y)) \subseteq (Z(I(X) =)X$. Moreover, in such a case, $I(Y)/I(X)$ is a radical ideal of $k[X]$. It follows that there is a one-to-one correspondence between radical ideals in the coordinate ring $k[X]$ and algebraic subsets contained in X. If $\mathfrak{a}$ is an ideal in $k[X]$, we denote by $Z(\mathfrak{a})$ the corresponding closed subset of X, i.e., $Z(\mathfrak{a}) := Z(\phi^{-1}(\mathfrak{a}))$, where $\phi : k[T_1, \ldots, T_n] \to k[X]$ is the canonical epimorphism. Also, for a subset Y of X, we let $I_X(Y) := I(Y)/I(X)(\in k[X])$. In particular, for a point $a = (a_1, \ldots, a_n) \in X$, we let to be $I_X(a)$. Note that if f, g are polynomials of $k[T_1, \ldots, T_n]$ with $f + I(X) = g + I(X)$ in $k[X]$, then for any $x \in X$, we have $f(x) = g(x)$, so $f + I(X)$ defines a k-valued function on X. One can then see that $Z_X(Y) = \{f + I(X) \in k[X] \mid f(y) = 0 \text{ for all } y \in Y\}$.

Proposition 1.1.2 *The coordinate ring, $k[X]$ of an algebraic set X, has the following properties :*

1) *The points of X are in a one-to-one correspondence with the maximal ideals of $k[X]$.*

2) *The closed sets of X are in a one-to-one correspondence with the radical ideals of $k[X]$.*

3) *If $f \in k[X]$ and $p \in X$ with corresponding maximal ideal $\mathfrak{m}_p$, then $k[X]/\mathfrak{m}_p$ is isomorphic (as a field to k) and under this identification we have $f(p) = \pi(f)$, where $\pi : k[X] \to k[X]/\mathfrak{m}_p$ is the canonical epimorphism.*

For the proof of the previous proposition we need some lemmas.

Lemma 1.1.3 *Let R be a ring and let I of R be an ideal and let*

$$p : R \to R/I$$

Then p induces a one-to-one correspondence between ideals of R/I and ideals J of R that contain I addition, for any ideal I of R and any ideal K of R/I,

a) *$p(I)$ is prime or maximal in R/I if and only if I is prime or maximal in R.*

b) *$p^{-1}(K)$ is prime or maximal in R if and only if K is prime or maximal in R/I.*

Proof. *See [26, Lemma A.1.24, p.***335***].*

We will also need to know the effect of multiple quotients :

Lemma 1.1.4 *Let $I \subset J$ be ideals of a ring R and let*

i) *$f : R \to R/I$*

ii) *$g : R \to R/J$ and*

iii) *$h : R/I \to (R/I)/f(J)$ be the canonical projections. Then $(R/I)/f(J) = R/J$ and the diagram*

$$\begin{array}{ccc} R & \xrightarrow{\quad f \quad} & R/I \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ R/J & \longrightarrow & (R/I)/f(J) \end{array}$$

commutes.

Proof. *See [26, Lemma A.1.25, p.***337***].*

Proof. *Let $X \subset \mathbb{A}^n$ be an algebraic set. If*

$$\pi : k[T_1, \ldots, T_n] \to k[X]$$

is the canonical projection, and $J \subset k[X]$ is an ideal, then lemma 1.1.3 implies that

$$J \mapsto \pi^{-1}(J)$$

is a bijection from the set of ideals of $k[X]$ onto the set of ideals of $k[T_1, \ldots, T_n]$ containing $I(X)$. Prime, and maximal ideals in $k[X]$ correspond to prime, and maximal ideals in $k[T_1, \ldots, T_n]$ containing $I(X)$. The fact that radical ideals are intersections of maximal ideals (see corollary 1.1.4) implies that this correspondence respects radical ideals too. If $p = (a_1, \ldots, a_n) \in X \subset \mathbb{A}^n$ is a point, the maximal ideal of functions in $k[T_1, \ldots, T_n]$ that vanish at p is

$$L = (T_1 - a_1, \ldots, T_n - a_n) \subset k[T_1, \ldots, T_n]$$

and this gives rise to the maximal ideal $\pi(L) \subset k[X]$.
Clearly

$$Z(\pi^{-1}(J)) = Z(J) \subseteq X$$

So $J \mapsto Z(J)$ is a bijection between the set of radical ideals in $k[X]$ and the algebraic sets contained X. To see that $f(p) = \pi(f)$, it suffices to apply lemma 1.1.4.

Irreducible topological spaces

The algebraic set $X = \{xy = 0\} \subset \mathbb{A}^2$ can be written as the union of the two coordinate axes $X_1 = \{x = 0\}$ and $X_2 = \{y = 0\}$, which are themselves algebraic sets. However, X_1 and X_2 cannot be decomposed further into finite unions of smaller algebraic sets. We now want to generalize this idea. It turns out that this can be done completely in the language of topological spaces. This has the advantage that it applies to more general cases, i.e., open subsets of algebraic sets.

Definition 1.1.5 *i) Topological space X is said to be reducible if it can be written as a union $X = X_1 \cup X_2$, where X_1 and X_2 are (nonempty) closed subsets of X not equal to X. It is called irreducible otherwise. A subset Y of X is irreducible if it is an irreducible topological space with respect to the induced topology.*

ii) A topological space X is called disconnected if it can be written as a disjoint union $X = X_1 \cup X_2$ of (nonempty) closed subsets of X not equal to X. It is called connected otherwise.

Remark 1.1.2 *Note that a Hausdoroff topological space is always reducible unless it consists of at most one point. Thus the notion of irreducibility is relevant only for non-Hausdoroff spaces. Also one should compare it with the notion of a connected space.*

Proposition 1.1.3 *Let X be a topological space. Then :*

1) X is irreducible if and only if the intersection of any two nonempty open subsets is nonempty.

2) If X is irreducible, then every nonempty open subset U of X is dense and irreducible.

Proof. *1) Assume first that X is irreducible and let U_1 and U_2 be two open subsets of X. If $U_1 \cap U_2 = \varnothing$, it would follow, when taking complements, that $X = U_1^c \cup U_2^c$, and X being irreducible, we would have that $U_i^c = X$ for either $i = 1$ or $i = 2$, hence $U_i = \varnothing$ for one of the i's. To prove the other implication, assume that X is expressed as a union $X = X_1 \cup X_2$ with the X_i 's being closed. Then $X_1^c \cap X_2^c = \varnothing$; hence either $X_1^c = \varnothing$ or $X_2^c = \varnothing$, and therefore either $X_1 = X$ or $X_2 = X$.*

2) *Let U be a nonempty open subset of X. We have $X = \overline{U} \cup (X \setminus U)$, where $\overline{U}$ is the closure of U in X, since X is irreducible and $X \setminus U \neq U$, then $\overline{U} = X$. Now that U is irreducible, let U_1, U_2 be two nonempty open subsets of U. Since X is irreducible, then by 1) above the open subsets. $U \cap U_1$ and $U \cap U_2$ of X are nonempty. Hence, again by 1) are tow nonempty open subsets of X, since X is irreducible, by 1) $(U \cap U_1) \cap (U \cap U_2)$ is nonempty. Therefore $U_1 \cap U_2$ is nonempty, which yields (by 1)) U is irreducible.*

Lemma 1.1.5 *Let X be a topological space. A subspace $Y \subseteq X$ in X is irreducible if and only if its closure $\overline{Y}$ is irreducible.*

Proof. *By proposition 1.1.3 a subset Z of X is irreducible if and only if for any two open subsets U and V of X which meet Z, $U \cap V$, also meet Z, i.e., if $Z \cap U \neq \emptyset$ and $Z \cap V \neq \emptyset$ we have $Z \cap (U \cap V) \neq \emptyset$. Therefore, to conclude, it suffices to notice that an open subset of X meets Y if and only if it meets $\overline{Y}$.*

Definition 1.1.6 *A maximal irreducible subset of a topological space X is called an irreducible component of X.*

Let X be a topological space. Lemma 1.1.5 shows that every irreducible component is closed. The set of irreducible subsets of X is ordered inductively, as for every chain of irreducible subsets their union is again irreducible. Thus Zorn's lemma‡ implies that every irreducible subset is contained in an irreducible component of X. In particular, every point of X is contained in an irreducible component. This shows that X is the union of its irreducible components.
For later use, we record one more lemma.

Lemma 1.1.6 *Let X be a topological space and let $X = \bigcup_{i \in I} U_i$ be an open covering of X by connected open subsets U_i.*

1) *If X is not connected, then there exists a nonempty subset J of I such that for all $j \in J$, $i \in I \setminus J$, $U_j \cap U_i = \emptyset$.*

2) *If X is connected, I is finite, and all the U_i are irreducible, then X is irreducible.*

Proof. *To prove 1), note that if we can write $X = V_1 \cup V_2$ as a disjoint union of open and closed subsets V_1, V_2, than each U_i is be contained in either V_1 or V_2, so we can set $J = \{i \in I;\, U_i \subseteq V_1\}$.*
For the second part, recall that every irreducible subset is contained in an irreducible component, so the assumption implies that X has only finitely many irreducible components, say $X_1, \ldots, X_n$. Assume $n > 1$. Since the X_i are closed, and X is connected, X_1 must intersect another irreducible component, say X_2 and let $x \in X_1 \cap X_2$. Let $i \in I$ with $x \in U_i$. Then $U_i \cap X_1$ is open and hence dense in X_1, and similarly for X_2, so that the closure of U_i in X contains $X_1 \cup X_2$, a contradiction.

Next proposition relates irreducible algebraic sets in $\mathbb{A}^n$ to prime ideals of $k[T_1, \ldots, T_n]$.

Proposition 1.1.4 *An affine algebraic set $X \subseteq \mathbb{A}^n$ is irreducible if and only if $I(X)$ is a prime ideal of $k[T_1, \ldots, T_n]$ (which is equivalent to the fact that $k[X]$ is a domain).*

Proof. *Suppose X is irreducible and let $f, g \in k[T_1, \ldots, T_n]$ be such that $fg \in I(X)$. Then $X \subseteq Z(fg) = Z(f) \cup Z(g)$. Since X is irreducible, then X is contained in $Z(f)$ or in $Z(g)$. So $f \in I(X)$ or $g \in I(X)$, proving that $I(X)$ is a prime ideal.*
Conversely, suppose that X is the union of two closed subsets X_1 and X_2 that are both different from X. Then, for $i = 1, 2$, there exist $f_i \in I(X_i) \setminus I(X) (i = 1, 2)$ It is clear that $f_1 f_2$ vanishes on $X_1 \cup X_2 = X$, so that $f_1 f_2 \in I(X)$. Thus, $I(X)$ is not a prime ideal of $k[T_1, \ldots, T_n]$.

‡*Zorn's lemma, also known as Kuratowski-Zorn lemma originally called maximum principle, is a statement in the language of set theory, equivalent to the axiom of choice, that is often used to prove the existence of a mathematical object when it cannot be explicitly produced.*

Example 1.1.4 *1) The affine space $\mathbb{A}^n$ is irreducible (and thus connected) by proposition 1.1.4, since its coordinate ring $k[\mathbb{A}^n] = k[T_1, \dots, T_n]$ is an integral domain.*

2) The union $X = V(x_1x_2) \subset \mathbb{A}^2$ of the two coordinate axes $X_1 = V(x_2)$ and $X_2 = V(x_1)$ is not irreducible, since $X = X_1 \cup X_2$. But X_1 and X_2 themselves are irreducible. This gives a decomposition of X into a union of two irreducible spaces.

Remark 1.1.3 *The correspondence of corollary 1.1.3 induces a bijection*

$$\{\text{irreducible algebraic sets of } \mathbb{A}^n\} \longleftrightarrow \{\text{prime ideals in } k[T_1, \dots, T_n]\}$$

From the Nullstellensatz, we obtain the following relations between algebraic objects and and geometric one :
Let $A = k[T_1, \dots, T_n]$ with k algebraically closed field. Then the mappings $X \longmapsto I(X)$ and $J \longmapsto Z(J)$ give a one-to-one inclusion reversing correspondence between the objects in the left and right-hand columns in the following table :

Algebra	*Geometry*
maximal ideals of A	*points of $\mathbb{A}^n$*
prime ideals of A	*irreducible algebraic sets of $\mathbb{A}^n$*
radical ideals of A	*algebraic sets $\mathbb{A}^n$*

(1.3)

Definition 1.1.7 *An affine algebraic variety is an irreducible algebraic sets of $\mathbb{A}^n$.*

In what follows we introduce the concept of a Notherian (topological) space. As will be seen, these spaces allow nice decomposition into irreducible components.

Noetherian topological spaces

Definition 1.1.8 *A topological space X is called Noetherian if it is satisfies the descending chain condition for closed subsets : For any sequence closed subsets of X if :*

$$Y_1 \supseteq Y_2 \supseteq \dots$$

, is a such sequence, then there is an integer r such that $Y_r = Y_j$, for all $j \geq r$.

Lemma 1.1.7 *Let X be a topological space that has a finite covering $X = \bigcup_{i=1}^r X_i$ by Noetherian subspaces. Then X itself is Noetherian.*

Proof. *Let $X \supseteq Y_1 \supseteq Y_2 \supseteq \dots$ be a descending chain of closed subsets of X. Then $(Y_j \cap X_i)_j$ is a descending chain of closed subsets in X_i. Therefore there exists an integer $N_i \geq 1$ such that $Y_j \cap X_i = Y_{N_i} \cap X_i$ for all $j \geq N_i$. For $N := \max\{N_1, \dots, N_r\}$, we have $Y_j = Y_N$ for all $j \geq N$.*

Lemma 1.1.8 *Let X be a Noetherian topological space.*

i) Every subspace of X is Noetherian.

ii) Every open subset of X is compact (in particular, X is compact).

Proof. *i) Let $(Z_i)_i$ be a descending chain of closed subsets of a subspace Y. Then the closures $\overline{Z}_i$ of Z_i in X form a descending chain of closed subsets of X which becomes stationary by hypothesis. As we have $Z_i = Y \cap \overline{Z}_i$, this shows that the chain $(Z_i)_i$ becomes stationary as well.*

ii) By i) it suffices to show that X is compact. Let $(U_i)_i$ be an open covering of X and let $\mathcal{U}$ be the set of those open subsets of X that are finite unions of the subsets U_i. As X is Noetherian, $\mathcal{U}$ has a maximal element V. Clearly $V = X$, otherwise there existed an U_i such that $V \subsetneq V \cup U_i \in \mathcal{U}$. This shows that $(U_i)_i$ has a finite sub-covering.

Example 1.1.5 *$\mathbb{A}^n$ is a Noetherian topological space. Indeed, If $Y_1 \supseteq Y_2 \supseteq \ldots$ is a descending chain of closed subsets, then $I(Y_1) \subseteq I(Y_2) \subseteq \ldots$ is an ascending chain of ideals in $A := k[T_1, \ldots, T_n]$. Since A is a Noetherian ring, this chain of ideals is eventually stationary. But for each i, $Y_i = Z(I(Y_i))$, so the chain Y_i is also stationary.*

Proposition 1.1.5 *If X is an algebraic subset of $\mathbb{A}^n$, then X is a Noetherian space.*

Proof. *Let X be an algebraic subset of $\mathbb{A}^n$, by lemma 1.1.8 i) and example 1.1.5, then X is a Noetherian space.*

Theorem 1.1.3 *Let X be a Noetherian topological space. Then X is a union of finitely many irreducible closed subsets X_k of X. Furthermore, if $X_i \not\subset X_j$ for any $i \neq j$, then the subsets X_k are unique, up to a permutation of the indices.*

Proof. *Let us prove the first part of this result. If X is irreducible, then the assertion is obvious. Otherwise, $X = X_1 \cup X_2$, where X_i are proper closed subsets of X. If both of them are irreducible, the assertion is true. Otherwise, one of them, say X_1 is reducible. Hence $X_1 = X_1^{'} \cup X_2^{'}$ as above. Continuing in this way, we either stop somewhere and get the assertion or obtain an infinite strictly decreasing sequence of closed subsets of X. But the later case is impossible because X is Noetherian. To prove the second assertion, we assume that*

$$X = X_1 \cup \cdots \cup X_s = W_1 \cup \cdots \cup W_t$$

where no one of the X_i (resp. W_j) is contained in another $X_{i'}$ (resp. $W_{j'}$). We can assume that $s \leq t$. Obviously, we have :

$$X_1 = (X_1 \cap W_1) \cup \cdots \cup (X_1 \cap W_t)$$

Since X_1 is irreducible, one of the subsets $X_1 \cap W_j$ is equal to X_1, i.e., $X_1 \subseteq W_j$. We may assume that $j = 1$. Similarly, we show that $W_1 \subseteq X_i$ for some i. Hence $X_1 \subseteq W_1 \subseteq X_i$. This contradicts the assumption $X_i \not\subseteq X_j$ for $i \neq j$, so necessarily $i = j$, hence $X_1 = W_1$ repeating this argument for $X_2, \ldots, X_s$, we may assume that $X_i = W_i$, for all $1 \leq i \leq s$. It will follow that necessarily $t = s$.

Remark 1.1.4 *Compare this proof with the proof of the theorem on factorization of integers into prime factors. Irreducible components play the role of prime factors.*

In view of proposition 1.1.5, we can apply the previous terminology to affine algebraic sets X.

Corollary 1.1.5 *Every algebraic set in $\mathbb{A}^n$ can be expressed uniquely -up to a permutation of the indices- as a union of varieties, no one containing another.*

Example 1.1.6 *Let $f = f_1^{a_1} \cdots f_r^{a_r}$ be a decomposition of f into a product of irreducible polynomials. Then*

$$Z(f) = Z(f_1) \cup \cdots \cup Z(f_r)$$

since the ideal (f_i) of $k[T_1, \ldots, T_n]$, generated by f_i is prime, then $Z(f_i)$ is a variety, therefore the above gives the decomposition of $Z(f)$ into a union of varieties.

1.1.2 Projective varieties

We fix a ground field k, which we will always assume to be algebraically closed (we will nevertheless recall this fact in the statement of the main theorems). Let $\mathbb{P}^n$ denote the projective space consisting of lines passing through the origin, but without including the origin the vector space k^{n+1}. An element of $\mathbb{P}^n$ represented by the line generated by the nonzero vector $x = (x_0, \ldots, x_n) \in k^{n+1}$ will be denoted by $[x] = (x_0 : \ldots : x_n)$. The elements (k is not necessarily a number field) $x_0, \ldots, x_n$ are not all zero, and they are defined only up to a common scalar multiple. They are called the homogeneous coordinates of the point $[x] \in \mathbb{P}^n$.
Let $f \in k[T_0, \ldots, T_n]$ be a polynomial of degree d with homogeneous decomposition

$$f = f_0 + \ldots + f_d.$$

Given a point $x = (x_0 : \ldots : x_n) \in \mathbb{P}^n$, we cannot define the expression $f(x)$ as $f(x_0, \ldots, x_n)$, since it clearly depends on the choice of a vector representing x. Indeed, a general representative for x will have the form $(\lambda x_0, \ldots, \lambda x_n)$ (with $\lambda \neq 0$) and then $f((\lambda x_0, \ldots, \lambda x_n)) = f_0(\lambda x_0, \ldots, \lambda x_n) + \ldots f_d(\lambda x_0, \ldots, \lambda x_n) = f_0(x_0, \ldots, x_n) + \ldots + \lambda^d f_d(x_0, \ldots, x_n)$, which clearly varies when λ varies. However, if f is homogeneous of degree d, we have $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$.
Even if then $f(x)$ is not defined neither, it makes sense at least to say when it is zero, since obviously $f(\lambda x_0, \ldots, \lambda x_n) = 0$ for any $\lambda \neq 0$ if and only if $f(x_0, \ldots, x_n) = 0$.

Lemma 1.1.9 *Let k be an infinite field, $f \in k[T_0, \ldots, T_n], f_0, \ldots, f_d$ be forms with deg $(f_i) = i$, such that $f = \sum_{i=0}^{d} f_i$. $P \in \mathbb{P}^n(k)$ is a root of f if and only if P is a root of f_i for all $0 \leq i \leq d$.*

Proof. *If P is a root of every f_i, then obviously it is also a root of f. Conversely, let $(x_0 : \ldots : x_n)$ be a fixed tuple of homogeneous coordinates of P. We consider the polynomial*

$$g(\lambda) = f(\lambda x_0, \ldots, \lambda x_n) = \sum_{i=0}^{d} \lambda^i f_i(x_0, \ldots, x_n)$$

For P to be a root of f, the polynomial g must vanish on all $\lambda \in k \backslash \{0\}$. Since k is infinite, this is only possible if $g = 0$, i.e., $f_i(x_0, \ldots, x_n) = 0$ for all $0 \leq i \leq d$.

The main objects we are going to study will be the subsets of a projective space defined as zeros of homogeneous polynomials. More precisely :

Definition 1.1.9 *A projective algebraic set $X \subset \mathbb{P}^n$ is a subset for which there exists a set of homogeneous polynomials $\{f_j \mid j \in J\}$ such that*

$$X = \{p \in \mathbb{P}^n \mid f_j(p) = 0 \text{ for all } j \in J\}$$

For practical reasons, and in view of the previous lemma, we will say that $f(x) = 0$ for a point $x \in \mathbb{P}^n$ and an arbitrary polynomial $f \in k[T_0, \ldots, T_n]$ if and only if any homogeneous component of f vanishes at x. With this convention we can make the following definitions :

Definition 1.1.10 *i) The projective algebraic set defined by a subset $M \subseteq k[T_0, \ldots, T_n]$ will be*

$$Z(M) := \{x \in \mathbb{P}^n \mid f(x) = 0, \text{ for any } f \in M\}.$$

ii) The homogeneous ideal of a subset $X \subseteq \mathbb{P}^n$ will be the ideal

$$I(X) := \{f \in k[T_0, \ldots, T_n] \mid f(x) = 0 \text{ for any } x \in X\}.$$

iii) The graded ring of a projective algebraic set X is the ring

$$S(X) := k[T_0, \ldots, T_n] / I(X).$$

Remarks 1.1.2 *i) If we want to distinguish these projective constructions from the affine ones in definition 1.1.9 and definition 1.1.1, we will denote them by $Z_p(M)$ and $I_p(X)$, and the affine ones by $Z_a(S)$ and $I_a(X)$, respectively.*

ii) An ideal I of $k[T_0, \ldots, T_n]$ is said to be homogeneous if, for every $f = \sum_{i=0}^{d} f_i \in I$, f_i form of degree i also $f_i \in I$ for $0 \leq i \leq d$. So, as one can easily see, $X \subseteq \mathbb{P}^n$, the ideal $I(X)$ is homogeneous.

Example 1.1.7 *1) As in the affine case, the empty set $\emptyset = Z_p(1)$, and the whole space $\mathbb{P}^n = Z_P(0)$ are projective algebraic sets.*

2) Let $x \in \mathbb{P}^n$ be a point. Then the one-point set $\{x\} = Z_p(T_0 - x_0, \ldots, T_n - x_n)$, with $(x_0, \ldots, x_n)$ the homogeneous coordinates of x is a projective algebraic set.

Proposition 1.1.6 *The operators Z_p and I_p satisfy the following properties :*

1) *$I(\mathbb{P}^n) = \{0\}$ (k is assumed to be infinite), $I_p(\emptyset) = k[T_0, \ldots, T_n]$, $Z_p(\{0\}) = \mathbb{P}^n$, and $Z_p(\{1\}) = \emptyset$.*

2) *If $M \subset k[T_0, \ldots, T_n]$ and (M) is the ideal generated by M, then $Z_p(M) = Z_p((M))$. In particular, any projective algebraic set can be defined by a finite number of equations.*

3) *If $M \subset M' \subset k[T_0, \ldots, T_n]$, then $Z_p(M') \subset Z_p(M) \subset \mathbb{P}^n$.*

4) *If $\{M_j\}_{j \in J}$ is a collection of subsets of $k[T_0, \ldots, T_n]$, then $Z_p\left(\bigcup_{j \in J} M_j\right) = \bigcap_{j \in J} Z_p(M_j)$.*

5) *If $\{I_j\}_{j \in J}$ is a collection of ideals of $k[T_0, \ldots, T_n]$, then $Z_p\left(\sum_{j \in J} I_j\right) = \bigcap_{j \in J} Z_p(I_j)$.*

6) *If $I \subset k[T_0, \ldots, T_n]$ is any homogeneous ideal, then $Z_p(I) = Z_p(rad(I))$.*

7) *If $I, I' \subset k[T_0, \ldots, T_n]$ are two homogeneous ideals, then $Z_p(I \cap I') = Z_p(II') = Z_p(I) \cup Z_p(I')$.*

8) *If $X \subset X' \subset \mathbb{P}^n$, then $I_p(X') \subset I_p(X)$.*

9) *If $\{X_j\}_{j \in J}$ is a collection of subsets of $\mathbb{P}^n$, then $I_p(\cup_{j \in J} X_j) = \bigcap_{j \in J} I_p(X_j)$.*

10) *For any $X \subset \mathbb{P}^n, X \subset Z_p(I(X))$, with equality holding if and only if X is a projective algebraic set.*

Proof. *We will just prove the first part of 1), leaving the rest since it can be proved by analogous arguments as we saw in the affine case. So we just need to prove that a homogeneous polynomial vanishing at $\mathbb{P}^n$ is necessarily the zero polynomial. We will prove it by induction on n, the case $n = 0$ being trivial. So assume $n > 1$ and write $f = f_0 + f_1 T_1 + \ldots + f_d T_n^d$, with $f_0, f_1, \ldots, f_d \in k[T_0, \ldots, T_{n-1}]$ and $f_d \neq 0$. We thus know by induction hypothesis that we can find $(x_0 : \ldots : x_{n-1})$ such that $f_d(x_0, \ldots, x_{n-1}) \neq 0$. But then the polynomial $f(x_0, \ldots, x_{n-1}, T_n) \in k[T_n]$ is nonzero, so it has a finite number of roots. Hence the fact that k in infinite implies that we can find a point $(x_0 : \ldots : x_{n-1} : x_n)$ not vanishing on f.*

Definition 1.1.11 *Part 1), 4) and 7) of proposition 1.1.6 show that the set of projective algebraic sets satisfy the axioms needed to be the closed sets of a topology in $\mathbb{P}^n$. This topology (in which the closed sets are exactly the projective algebraic sets) is called the Zariski topology on $\mathbb{P}^n$. The intersection of a projective algebraic set with an open set will be called a quasi-projective algebraic set. The topology induced by the Zariski topology on any quasi-projective algebraic set will be still called Zariski topology on that quasi-projective algebraic set.*

Recall the following : Let I be a homogeneous ideal of $k[T_0, \ldots, T_n]$. We say that I homogeneous prime (or graded prime) if for any forms (i.e., homogeneous polynomials) f and g of $k[T_0, \ldots, T_n]$, if $fg \in I$, then $f \in I$ or $g \in I$. The (homogeneous) ideal I is said to be prime if the above implication holds but for arbitrary polynomials (non necessarily homogeneous) f and g of $k[T_0, \ldots, T_n]$.

Lemma 1.1.10 *i) A homogeneous ideal I of $k[T_0, \ldots, T_n]$ is prime if and only if*

$$fg \in I \text{ implies } f \in I \text{ or } g \in I$$

for arbitrary forms $f, g \in k[T_0, \ldots, T_n]$.

ii) If I is homogeneous, then also $rad(I)$ is homogeneous.

Proof. *i) We have to show that a homogeneous ideal I of $k[T_0, \ldots, T_n]$ is prime if and only if it is homogeneous prime. One sense of this implication is clear. Remains to prove that I is prime when it is homogeneous prime. To see this, assume that there exists polynomials f, g such that*

$$fg \in I, \text{ but } f, g \notin I$$

Let f, g be such that $deg(fg)$ is least with this property. Write

$$f = f_k + \ldots + f_0$$
$$g = g_l + \ldots + g_0$$

where f_i, g_i are forms of degree i, and both f_k and g_l are nonzero. Since I contains fg, is must also contain its highest degree form $f_k g_l$, and therefore either f_k or g_l. Assume $f_k \in I$. Then also $(f_{k-1} + \ldots + f_0)\, g = fg - f_k g \in I$, and it is of lower degree than fg. So either $(f_{k-1} + \ldots + f_0) \in I$, and therefore $f \in I$, or $g \in I$.

ii) Let $f = f_0 + \ldots + f_k$ be a polynomial of $k[T_0, \ldots, T_n]$ with $f_0, \ldots, f_k$ being forms with increasing degrees. It suffices to show that $f \in rad(I)$ implies $f_k \in rad(I)$. From $f \in rad(I)$ we get $f^m = f_k^m +$ lower degree forms $\in I$ for some m, so $f_k^m \in I$, and therefore $f_k \in rad(I)$.

Theorem 1.1.4 *An ideal I of $k[T_1, \ldots, T_n]$ is homogeneous if and only if it is generated by a (finite) set of forms.*

Proof. *A homogeneous ideal is clearly generated by forms (i.e., by homogeneous polynomials). Conversely, an ideal that is generated by forms is plainly a homogeneous ideal. Indeed, these facts are true in general for any ideal of a graded ring. The fact that such a generating subset can be finite follows from the fact that the polynomial ring $k[T_0, \ldots, T_n]$ is noetherian.*

As for affine algebraic sets, we call a projective algebraic set $X \subseteq \mathbb{P}^n$ irreducible if it is so when endowed with its Zariski topology, i.e., if it cannot be written as the union of two algebraic subsets.
An irreducible projective algebraic set is called a projective variety. Analogously to the affine case one proofs that every projective algebraic set can be decomposed uniquely into a union of finitely many projective varieties. These coincide with the irreducible components of the projective algebraic set.
Furthermore, in analogy to the affine case, one shows (using lemma 1.1.10 i)) that the projective algebraic set X is irreducible if and only if $I_p(X)$ is prime.
In what follows, we want to show that $\mathbb{A}^n$ can be considered as a topological subspace of $\mathbb{P}^n$. To do this, we need the following definition :

Definition 1.1.12 *i) Let* $f = \sum_{i_1,\cdots,i_n \in \mathbb{N}} a_{i_1,\cdots,i_n} T_1^{i_1} \cdots T_n^{i_n}$ *be a (nonzero) polynomial of degree d of* $k[T_1, \ldots, T_n]$*. We define its homogenization to be the polynomial*

$$f^h := T_0^d f\left(\frac{T_1}{T_0}, \ldots, \frac{T_n}{T_0}\right)$$
$$= \sum_{i_1,\cdots,i_n \in \mathbb{N}} a_{i_1,\ldots,i_n} T_0^{d-i_1-\cdots-i_n} T_1^{i_1} \cdots T_n^{i_n} \text{ of } k[T_0, \ldots, T_n]$$

obviously this is a homogeneous polynomial of degree d.

ii) The homogenization of an ideal I of $k[T_1, \ldots, T_n]$ *is defined to be the ideal* I^h *of* $k[T_0, \ldots, T_n]$ *generated by all* f^h *for* $f \in I$.

Remark 1.1.5 *In the above the homogenization* f^h *would be called the homogenization with respect to the (new) indeterminate* T_0*. The same homogenization could be made with respect to any other (new) indeterminate, e.g., when a polynomial* $f \in k[R, S]$*, then for any new indeterminate* V*, one can define a homogenization of f with respect to V and have a polynomial* $f^h \in k[R, S, V]$.

Example 1.1.8 *For* $f = T_1^2 - T_2^2 - 1 \in k[T_1, T_2]$*, we have* $f^h = T_1^2 - T_2^2 - T_0^2 \in k[T_0, T_1, T_2]$.

Remark 1.1.6 *If* $f, g \in K[T_1, \ldots, T_n]$ *are polynomials of degree d and e, respectively, then fg has degree* $d + e$*, and so we get*

$$(fg)^h = T_0^{d+e} f(\frac{T_1}{T_0}, \ldots, \frac{T_n}{T_0}) \cdot g(\frac{T_1}{T_0}, \ldots, \frac{T_n}{T_0}) = f^h \cdot g^h.$$

However, $(f + g)^h$ *is clearly not equal to* $f^h + g^h$ *in general.*

Notation. *Let* $f_i = T_i \in k[T_0, \ldots, T_n]$ *and consider the open subset* $U_i = \mathbb{P}^n \setminus Z_p(T_i)$ *of* $\mathbb{P}^n$*. We define the map*

$$\phi_i : U_i \to \mathbb{A}^n, (x_0 : \ldots : x_n) \longmapsto (\frac{x_0}{x_i} : \ldots : \frac{x_n}{x_i})$$

As one can easily see, ϕ *is a bijective map, with inverse*

$$\psi_i : \mathbb{A}^n \to U_i, (a_0, \ldots, \hat{a}_i, \ldots, a_n) \longmapsto (a_0 : \ldots : 1 : \ldots : a_n)$$

Proposition 1.1.7 *For* $i \in \{0, \ldots, n\}$ *the map*

$$\phi_i : U_i \to \mathbb{A}^n, (x_0 : \ldots : x_n) \mapsto (\frac{x_0}{x_i} : \ldots : \frac{x_n}{x_i})$$

is a homeomorphism§ *when* U_i *and* $\mathbb{A}^n$ *are endowed with their Zariski topologies.*

Proof. *We will show this result for* $i = 0$ *and (the other cases follow in the same way). Let* $X \subseteq \mathbb{A}^n$ *be an algebraic set of* $\mathbb{A}^n$ *and write* $X = Z(f_1, \ldots, f_r)$ *with* $f_1, \ldots, f_r \in k[T_1, \ldots, T_n]$*. One can easily see that* $\phi^{-1}(X) = Z_p(g_1, \ldots, g_r) \cap U_0$*, where* $g_j = f_j^h$*, for all j (recall here that* f_j^h *denotes the homogenization of* f_j*). So,* $\phi^{-1}(X)$ *is closed* U_0*. Conversely, let Y be an algebraic set of* U_0*, then we can write* $Y = Z_p(g_1, \ldots, g_r) \cap U_0$ *with* $g_1, \ldots, g_r$ *the homogeneous polynomials in* $k[T_0, \ldots, T_n]$*. One can see that* $\phi(Y) = Z_a(Q_1, \ldots, Q_r)$*,* $Q_i(T_1, \ldots, T_n) = g_i(1, \ldots, T_n)$.

Remark 1.1.7 *We have :*

$$\mathbb{P}^n = \cup_{i=0}^n U_i$$

where $U_i = \mathbb{P}^n \setminus Z_p(T_i)$ *and by the above* $U_i \simeq \mathbb{A}^n$*, i.e.,* U_i *and* $\mathbb{A}^n$ *are homeomorphic. Thus* $\mathbb{P}^n$ *has a covering by open subsets all homeomorphic to* $\mathbb{A}^n$.

§*A homeomorphism between two topological spaces X and Y is a bijection* $f : X \longrightarrow Y$ *both f and* f^{-1} *are continuous.*

1.2 Dimension of a variety

In this section, we will introduce the notion of dimension of a topological space, and we will give some of its elementary properties. Before this we will recall some facts concerning the (Krull) dimension of a (commutative) ring since will apply this in the study of the dimension of an algebraic variety (projective or affine).

1.2.1 Dimension of rings

Definition 1.2.1 *Let R be a commutative ring and P a prime ideal of R.*

i) The height of P is the greatest integer n when there exists a family

$$P_0 \subsetneq \cdots \subsetneq P_n = P$$

with all P_i being prime ideals of R. We write in this case $ht(P) = n$. If such (greatest) integer does not exist, such a large integer does not exist we write $ht(p) = \infty$.

ii) The (Krull) dimension of the ring R is

$$dim(R) := sup\{ht(P) \mid P \subseteq R \, prime\}.$$

Examples 1.2.1 *1) Fields are of dimension 0.*

2) If R is a principal ideal ring which is not a field, then $dim(R) = 1$.

3) For any field k, $dim(k[X]) = 1$.

1.2.2 Transcendence Degree

We can describe the size of a field extension k/E using the idea of dimension from linear algebra

$$[k : E] = dim_E(k)$$

But this doesn't say enough about the size of really big field extensions.

$$[k(T_1) : k] = [k(T_1, \dots, T_n) : k] = \infty$$

Another notion of the size of a field extension k/E, called transcendence degree is widely used in field theory and linear algebra. It has the following two important properties.

$$tr.deg_k(k(T_1, \dots, T_n)) = n$$

and if k/E is algebraic, $tr.deg_E(k) = 0$.

Algebraic (In)dependence

Definition 1.2.2 *A subset S of k said to be algebraically independent over E, if for all nonzero polynomials $f(T_1, \dots, T_n) \in E[T_1, \dots, T_n]$, and $s_1, \dots, s_n \in S$ (all distinct), we have $f(s_1, \dots, s_n) \neq 0$. Otherwise, we say that S is algebraically dependent over E.*

Example 1.2.1 *1) If k/E is an algebraic extension and $\alpha \in k$ then $\{\alpha\}$ is algebraically dependent over E.*

2) In $k(T_1, \dots, T_n)/k$, $\{T_1, \dots, T_n\}$ is algebraically independent.

Lemma 1.2.1 *If $S \subseteq k$ is algebraically independent, then S is maximal if and only if k is algebraic over $E(S)$.*

Proof. *See [30, Section 030D].*

Theorem 1.2.1 *(Exchange Lemma). Let k/E be a field extension. If k is algebraic over $E(a_1, \dots, a_n)$, and $\{b_1, \dots, b_m\}$ is an algebraically independent set, then $m \leq n$.*

Proof. *See [30, Section 030D].*

Corollary 1.2.1 *If k/E has a maximal, finite, algebraically independent set $\{s_1, \dots, s_n\}$, then any other maximal algebraically independent set also has size n.*

Remarks 1.2.1

i) In fact it is true that if k/E has two maximal algebraically independent sets S and T then $|S| = |T|$. This is analogous to the fact that the cardinality of a vector space basis is unique, even when it is infinite. The proof of this fact is difficult, and we will not need this result. We refer the read to [30, Ch 09FA, Section 030D].

ii) Every extension k/E has a maximal algebraically independent subset.

Definition 1.2.3

1) A maximal algebraically independent subset $S \subseteq k$ is called a transcendence base for k/E. So by the above lemma, S is a transcendence base for k/E if and only if S is algebraically independent and k is algebraic over $E(S)$.

2) The transcendence degree of k/E is the size of a transcendence base. It is denoted $tr.deg(k/E)$.

Example 1.2.2 $tr.deg_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = 0$.

Theorem 1.2.2 *Let k be a field and A be a finitely generated algebra over k. Assume that A is an integral domain and let F be its field of fractions. Then $dim(A) = tr.deg_k(F)$.*

Proof. *See [6, Theorem, 8.9.11, p.282].*

Example 1.2.3 *We have $tr.deg_k(k(T_1, \dots, T_n)) = n$, so $dim(k[T_1, \dots, T_n]) = n$.*

1.2.3 Dimension of a topological space

Definition 1.2.4 *Let X be a nonempty topological space. Considering a strictly increasing chain of irreducible closed subsets of X :*

$$X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_d.$$

We call d the length of this chain (that is, the number of inclusions in the chain). The Krull dimension of X is the supremum of the lengths of such chains, denote it by $dim(X)$. We then write $dim(X) = d$.

Remarks 1.2.2

1) This notion has no interest if X is a Hausdorff space. Indeed, in such a case we have $dim(X) = 0$.

2) By convention we assume that the dimension of the empty set is equal -1.

3) Note that the dimension of X may be equal to ∞.

Lemma 1.2.2 *Let X be a nonempty topological space and Y be a nonempty subspace of X. Then $dim(Y) \leq dim(X)$. In particular, if $dim(X)$ is finite, then also $dim(Y)$ is so (in this case, the integer $dim(X) - dim(Y)$ is called the co-dimension of Y in X).*

Proof. *Let $S_0 \subsetneq \cdots \subsetneq S_d$ a family of irreducible closed subsets of Y and for each i, let $\overline{S}_i$ be the closure of S_i in X, then by lemma 1.1.5, $\overline{S}_0 \subseteq \cdots \subseteq \overline{S}_d$ is a family of (increasing) irreducible closed subsets of X. Moreover, for any $i \in \{1, \ldots, d\}$, we have $S_i = \overline{S}_i \cap Y$, so $\overline{S}_{i-1} \neq \overline{S_i}$, hence $dim(Y) \leqslant dim(X)$.*

Proposition 1.2.1 *Let X be a nonempty topological space. The following statements hold :*

1) *If $X = \bigcup_{i \in I} U_i$ is an open of X, then $dim(X) = sup\{dim(U_i)\}$.*

2) *If X is Noetherian, and $X_1, \ldots, X_d$ are its irreducible components, then $dim(X) = sup_i\{dim(X_i)\}$.*

3) *If $Y \subseteq X$ is closed, X is irreducible, $dim(X)$ is finite and $dim(X) = dim(Y)$, then $Y = X$.*

Proof. 1) *Let $X_0 \subsetneq \cdots \subsetneq X_d$ be a chain of irreducible closed subsets of X and let x_0 be a point of X_0, then of X. Let $x \in X_0$ be a point there exists an index $i \in I$ such that $x \in U_i$. Plainly, for all $j \in \{0, \ldots, d\}$, $X_j \cap U_i$ is nonempty; moreover this last set is an irreducible closed subset of U_i. Consider*

$$X_0 \cap U_i \subseteq X_1 \cap U_i \subseteq \cdots \subset X_d \cap U_i$$

of irreducible closed subsets of U_i. It is a chain of length d. We check that for any $0 \leq j \leq d-1$, we have $X_j \cap U_i \neq X_j \cap U_{j+1}$. This shows that $dim(X) \leq dim(U_i)$. Thus, $dim(X) \leq sup_i\{dim(U_i)\}$. The reverse inequality follows by lemma 1.2.2.

2) *Any chain of irreducible closed subsets of X is completely contained in an irreducible component of X. Therefore, $dim(X) \leq sup_i\{dim(X_i)\}$. As in 1) above the equality follows by lemma 1.1.5.*

3) *Let Y be a proper closed subset of X and let $Y_0 \subsetneq \cdots \subsetneq Y_d$ be a chain of irreducible closed subsets of X. Considering the following chain*

$$Y_0 \subsetneq \cdots \subsetneq Y_d \subsetneq X$$

of irreducible closed subsets of X, we see that $dim(Y) < dim(X)$.

In what follows, we restrict our attention to the case of varieties. We recall that k denotes an algebraically closed field.

Dimension of an affine variety

Let $X \subseteq \mathbb{A}^n$ be a quasi-affine variety.

Theorem 1.2.3 *LetX be an affine variety. Then*

$$dim(X) = dim(k[X])$$

where $K[X]$ is the affine coordinate ring of X.

Proof. *Let $X_0 \subsetneq \cdots \subsetneq X_m$ be a family of irreducible closed subsets of X (i.e., of affine varieties contained in X), then*

$$P_0 = I(X_m) \subsetneq \cdots \subsetneq P_m = I(X_0)$$

and $P_0, \ldots, P_m$ are prime ideals of $k[T_1, \ldots, T_n]$. For any $i \in \{1, \ldots, m\}$, we have $X_i \subseteq X$, so $I(X) \subseteq I(X_i)$. Thus, P_i are prime ideals which contain $I(X)$. It follows that $P_i + I(X)$ are distinct prime ideals of $k[X]$. Therefore, $dim(X) \leq dim(k[X])$. The reverse inequality follows in the same way by noticing that any prime ideal of $k[X]$ corresponds to a well defined irreducible closed subset of X.

Corollary 1.2.2 *Let X be an affine variety. Then*

$$dim(X) = tr.deg\big(Frac(k[X])\big)$$

Proof. *Since X is an affine variety, then $k[X]$ is a finitely generated k-algebra that is an integral domain, so $dim(k[X]) = tr \cdot deg_k(Frac(k[X]))$. The corollary follows then by theorem 1.2.2.*

Corollary 1.2.3

$$dim(\mathbb{A}^n) = n.$$

Proof. *Indeed, we have $dim(\mathbb{A}^n) = dim(k[T_1, \ldots, T_n]) = n$.*

Corollary 1.2.4 *The dimension of an affine variety is finite.*

Proof. *Let $X \subseteq \mathbb{A}^n$ be an affine variety. Then by lemma 1.2.2, we have*

$$dim(X) \leq n.$$

1.3 Regular functions and morphisms

In this section, we will define regular functions on both affine and projective varieties and also morphisms between varieties. We show at the end of this section that there is an equivalence of categories between the category of affine varieties (over the base field k) and the category of finitely generated (integral) domains over k.

1.3.1 Regular functions

Definition 1.3.1 *Let $X \subseteq \mathbb{A}^n$ be a quasi-affine variety and let $x \in X$.*

i) A function $f : X \longrightarrow k$ is said to be regular at x if there exists an open subset $U \subseteq X$ containing x and polynomials $g, h \in k[T_1, \ldots, T_n]$, with $h(y) \neq 0$ for all $y \in U$, such that for all $y \in U$, we have

$$f_{|U}(y) = \frac{g(y)}{h(y)}$$

ii) A function $f : X \longrightarrow k$, is called a regular function if f is regular at all points of X.

Example 1.3.1 *Let $f \in k[T_1, \ldots, T_n]$, then the polynomial function defined is a regular function on any quasi-affine variety X of $\mathbb{A}^n$.*

Proposition 1.3.1 *Let X be a quasi-affine variety.*

1) If $f : X \longrightarrow k$ is a regular function, then f is continuous for the Zariski topologies on X and k.

2) If f and g are regular functions on X that restrict to the same function on some nonempty open subset $U \subseteq X$, then $f = g$.

Proof. *1) As continuity is a local notion, it suffices to consider the case where $f = \frac{g}{h}$ for some polynomial functions g and h with h nowhere vanishing. Recall that the proper closed subsets of k (for its Zariski topology) are the finite subsets of k, so continuity of f then follows from the fact that, for $a \in k$, we have $f^{-1}(a) = Z(g - ah)$, which is a closed subset of X.*

2) The set $Z = \{x \in X \,|\, f(x) = g(x)\}$ is the inverse image of 0 ($\in k$ under the regular function $f - g$, so by 1) Z a closed subset of X. Suppose that if $f_{|U} = g_{|U}$, then it follows from the fact that U is dense in X (see proposition 1.1.3) that $Z = X$.

Definition 1.3.2 *Let $X \subseteq \mathbb{P}^n$ be a quasi-projective variety and let $x \in X$*

i) A function $f : X \longrightarrow k$, is said to be regular at the point x if there exists an open subset $U \subseteq X$ containing x and homogeneous polynomials of the same degree $g, h \in k[T_0, \ldots, T_n]$ with $h(y) \neq 0$ for all $y \in U$, such that for all $y \in X$, we have

$$f_{|U}(y) = \frac{g(y)}{h(y)}.$$

ii) A function $f : X \longrightarrow k$ is called a regular function if it is regular at all points of X.

Proposition 1.3.2 *Let $f : X \longrightarrow k$, be a regular function. Then f is continuous when both X and k are endowed with their Zariski topologies.*

Proof. *As in the affine case, it is enough to prove that for any element $a \in k$, $f^{-1}(a)$ is closed in X, $a \in k$. For all $x \in X$, a convenient an open neighbourhood U of x, and homogeneous polynomials of the some degree g, h with $h(y) \neq 0$, for all $y \in U$ such that*

$$f_{|U}(y) = \frac{g(y)}{h(y)}.$$

Then

$$f^{-1}(a) = \{y \in U \,|\, g(y) - ah(y) = 0\} = U \cap Z_p(g - ah)$$

, which is clearly closed in U. The proposition then the following lemma.

Lemma 1.3.1 *Let Y be a topological space, $Y = \bigcup_{i \in I} U_i$ be an open covering of Y and Z a subset of Y. Then Z is a closed subset of Y if and only if $Z \cap U_i$ is closed in U_i for all i.*

Proof. *If Z is closed in Y, then clearly $Z \cap U_i$ is a closed subset of U_i for all $i \in I$. Conversely, the fact that each $Z \cap U_i$ is closed in U_i implies the existence of a collection of closed subsets Z_i of X such that $U_i \cap Z = U_i \cap Z_i$. We then have :*

$$\begin{aligned} Y \setminus Z &= \bigcup_{i \in I}(U_i \setminus Z) \\ &= \bigcup_{i \in I}(U_i \cap Y \setminus Z) \\ &= \bigcup_{i \in I}(U_i \cap Y \setminus Z_i) \end{aligned}$$

which implies that Z is a closed subset of Y.

Terminology : *In what follows, the word variety will be used to mean a quasi-affine or a quasi-projective variety (which includes affine and projective varieties).*

1.3.2 Morphisms of varieties

Definition 1.3.3 *Let X and Y be varieties. A morphism of varieties $\phi : X \longrightarrow Y$ is a continuous map such that for all nonempty open subset V of Y, and for any regular function $f : V \longrightarrow k$, the map $f \circ \phi : \phi^{-1}(V) \longrightarrow k$ is a regular function.*

Notation. *Let X and Y be tow varieties. We denote by $Hom_{Var}(X, Y)$ the set of morphisms from X to Y.*

Remark 1.3.1 *The composition of two morphisms is a morphism. Indeed, one can consider the category of varieties whose morphisms are those defined in above.*

Let $U_i = \mathbb{P}^n \setminus Z_p(T_i)$, we previously saw that U_i is homeomorphic to $\mathbb{A}^n$. The next proposition shows that the canonical homeomorphism between U_i and $\mathbb{A}^n$ is an isomorphism of varieties.

Proposition 1.3.3 *Let $U_i = \mathbb{P}^n \setminus Z_p(T_i)$. Then the map*

$$\phi_i : U_i \longrightarrow \mathbb{A}^n, (x_0 : \ldots : x_n) \longmapsto (\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}).$$

is an isomorphism of varieties

Proof. *We have already shown in proposition 1.1.7 that ϕ is a homeomorphism.*
To simplify the notation we take $i = 0$ and denote U_0 and ϕ_0 simply by U and ϕ, respectively. To show that ϕ is a morphism of varieties, let V be a nonempty open subset of $\mathbb{A}^n$ and let $f : V \longrightarrow k$ be a regular function. Locally, f is a quotient of two polynomials functions, so without losing the generality we can assume that f is a quotient on the whole V i.e., there exist polynomials g and $h \in k[T_1, \ldots, T_n]$, such that for all $y \in V$, $h(y) \neq 0$ and $f = \frac{g}{h}$. One can then easily deduce that $f \circ \phi : \phi^{-1}(V) \longrightarrow k$ is a regular function. Indeed, we have :

$$(f \circ \phi)(y) = (\frac{g}{h} \circ \phi)(y) = \frac{g \circ \phi(y)}{h \circ \phi(y)} = \frac{T_0^d f^h(y)}{T_0^e g^h(y)}, \text{ for all } y \in \phi^{-1}(V)$$

where $e = deg(f)$ and $d = deg(g)$.
Conversely, Recall $\phi^{-1} : \mathbb{A}^n \longrightarrow U$ is defined by $(b_1, \ldots, b_n) \longmapsto (1 : b_1 : \ldots : b_n)$. Let W be a nonempty open subset of U and $g : W \longrightarrow k$ a regular function. $g \circ \phi^{-1} : \phi(W) \longrightarrow k$ is a regular function. Then, locally g is a quotient of two homogeneous polynomials of the same degree. Also here without losing the generality we can suppose that on whole W g is a quotient of such polynomial functions, say $\frac{P}{Q}$ where $P, Q \in k[T_0, \ldots, T_n]$ i.e $\forall y \in W$, $Q(y) \neq 0$ and $g(y) = \frac{P(y)}{Q(y)}$.
$g \circ \phi^{-1} : \phi(W) \longrightarrow k$, is then defined as follows :

$$g \circ \phi^{-1}(x) = \frac{s(P)(x)}{s(Q)(x)}, \forall x \in \phi(W), \text{ where } s(P) := P(1, T_1, \ldots, T_n).$$

This shows that $g \circ \phi^{-1} : \phi(W) \longrightarrow k$ is a regular function. This shows that ϕ is an isomorphism of varieties.

Remark 1.3.2 *We previously saw that $\mathbb{P}^n = \bigcup_{i=0}^n U_i$. Moreover, we saw that U_i is homeomorphic to $\mathbb{A}^n$, so $dim(U_i) = n$. It follows that $dim(\mathbb{P}^n) = sup_i(dim(U_i)) = n$.*

Lemma 1.3.2 *Let X be an affine variety and $\phi : X \longrightarrow k$ $(= \mathbb{A}^1)$ be a map. Then, ϕ is a morphism of varieties if and only if ϕ be a regular function.*

Proof. *Straightforward.*

Proposition 1.3.4 *Let X be an arbitrary variety and let $Y \subseteq \mathbb{A}^m$ be an affine variety. A map of sets $\psi : X \longrightarrow Y$ is a morphism if and only if $t_i \circ \psi$ is a regular function on X for each i, where $t_1, \ldots, t_m$ are the coordinate functions on $\mathbb{A}^m$.*

Proof. *By lemma 1.3.2, for all $i \in \{1, \ldots, m\}$, t_i is a morphism. So, assuming that ψ is a morphism, it follows that $t_i \circ \psi$ is also a morphism. Conversely, suppose that for all i, $t_i \circ \psi$ is a regular function, then for any polynomial function $f : Y \longrightarrow k$, $f \circ \psi$ is regular function. So, for any algebraic set $Z(P_1, \ldots, P_r) \subseteq Y$, it follows from the equality*

$$\psi^{-1}(P_1, \ldots, P_r) = \bigcap_{i=1}^{r} (P_i \circ \psi)^{-1}(\{0\})$$

that ψ is continuous. Let $g : Y \longrightarrow k$ be a regular function, then there exists a nonempty open subset $U \subseteq Y$ and polynomials g_1, g_2 such that $g_{|U} = \frac{g_1}{g_2}$. Thus, for any $x \in \psi^{-1}(U)$:

$$g_{|U}(\psi(x)) = \frac{g_1(\psi(x))}{g_2(\psi(x))}$$

and we know $g_i \circ \psi$ is regular functions for $i = 1, 2$. So, $g \circ \psi : \psi^{-1}(U) \longrightarrow k$ is a regular function.

Now, we introduce some rings of functions associated with any varieties.

Definition 1.3.4 *Let X be a variety. We denote by $\mathcal{O}(X)$ the set of all regular functions on X. One can easily see that endowed with the natural addition and multiplication, $\mathcal{O}(X)$ is in fact a (commutative) ring we call the ring of regular functions on X. For all $x \in X$, we define the local ring of X at x, denoted $\mathcal{O}_{X,x}$, or simply by $\mathcal{O}_x$, as being the ring of germs of regular functions at x. $\mathcal{O}_x$ can be defined as follows : the set of all pairs (U, f), where U is an open subset of X containing x and $f : U \longrightarrow k$ is a regular function, and we consider on this set of pairs the following relation :*

$$(U, f) \sim (V, g) \text{ if } f_{|U\cap V} = g_{|U\cap V}$$

One can easily see that this is an equivalence relation. We define $\mathcal{O}_x$ to be the corresponding to quotient set. Usually, when there is no risk of confusion, we just write f for the class of some pair (U, f). For a convenient set of polynomials S and regular function g defined on some open subset $U \setminus Z(S)$ of U, we will write $g_{|\complement Z(S)}$ or $g_{|U\setminus Z(S)}$, for the class defined by the pair $(U \setminus Z(S), g)$. Note that $\mathcal{O}_x$ is indeed a local ring for the canonical addition and multiplication laws. Its maximal ideal $\mathfrak{m}_x$ is the set of germs of regular functions, which vanish at x (for if for a regular function f, we have $f(x) \neq 0$, then $\frac{1}{f}$ is regular function in some neighborhood of x). One can easily see that the residue field $\mathcal{O}_x/\mathfrak{m}_x$ is isomorphic to k.

Remarks 1.3.1 1) *In what follows, we will need to consider the (canonical) structure of $\mathcal{O}(X)$ as a k-algebra. We precise that this structure is given by the following operations :*
Let $f : X \longrightarrow k$ and $g : X \longrightarrow k$ be two regular functions on X, then.

- $*$ $f + g : X \longrightarrow k$, *is defined by* $x \longmapsto f(x) + g(x)$.
- $*$ $fg : X \longrightarrow k$, *is defined by* $x \longmapsto f(x)g(x)$.
- $*$ $\lambda f : X \longrightarrow k$, *is defined by* $x \longmapsto \lambda f(x)$, *for all* $\lambda \in k$.

2) *Similarly, it is easily verified that $\mathcal{O}_x$ is a k-algebra when equipped by the following operations :*

- $*$ $< U, f > + < V, g > = < U \cap V, f_{|U\cap V} + g_{|U\cap V} >$.
- $*$ $< U, f > \times < V, g > = < U \cap V, f_{|U\cap V} \times g_{|U\cap V} >$.
- $*$ $\lambda\cdot < U, f > = < U, \lambda f >$.

Definition 1.3.5 *Let X be a variety, we define the function field $k(X)$ of X as follows : an element of $k(X)$ is an equivalence class of pairs (U, f) where U is a nonempty open subset of X, f is a regular function on U, and where we identify two pairs (U, f) and (V, g) when $f = g$ on $U \cap V$.*

Remark 1.3.3 *Note that $k(X)$ is indeed a field, for :*

- $*$ *Let $< U, f >$ and $< V, g >$ two elements of $k(X)$. Since X is irreducible, any two nonempty open subsets have a nonempty intersection (see proposition 1.1.3). We define :*

$$< U, f > + < V, g > := < U \cap V, f_{|U\cap V} + g_{|U\cap V} > .$$

We show that this defines an abelian group structure on $k(X)$. In the same way we define the product of two elements of $k(X)$ and the product of an element of $k(X)$ by a scalar of k. We can easily see that this gives a (commutative) ring structure on $k(X)$.

- $*$ *If $< U, f > \in k(X)$ with $f \neq 0$, we can restrict f to the open set $W = U \setminus Z(f)$ it does not vanish, so that $\frac{1}{f}$ is regular function on W, hence $< U, f >$ is invertible in $k(X)$ with inverse $< W, \frac{1}{f} >$.*

Relation between $k[X]$ and $\mathcal{O}(X)$ when X is an affine variety

Considering an affine variety $X \subseteq \mathbb{A}^n$, the algebraic object $k[X] := k[T_1, \ldots, T_n]/I(X)$ consists of all polynomials $k[T_1, \ldots, T_n]$ modulo the equivalence relation $\sim$ (i.e., $f \sim g$ if $f - g \in I(X)$). We can identify each element of $k[X]$ with a function defined on X i.e., if $P \in k[T_1, \ldots, T_n]$, then we let $f_{P+I(X)} : X \longrightarrow k$ be the map defined by $f_{P+I(X)}(x) := P(x)$ for all $x \in X$. It is clear that $f_{P+I(X)}$ is a regular function on X. Thus we have a map :

$$\begin{array}{rccc} \gamma : & k[X] & \longrightarrow & \mathcal{O}(X) \\ & P + I(X) & \longmapsto & f_{P+I(X)} \end{array} \tag{1.4}$$

It is easy to verify that γ is a homomorphism of k-algebras. Moreover, by proposition 1.3.1 2) γ is injective.

Theorem 1.3.1 *Let $X \subseteq \mathbb{A}^n$, be an affine variety with affine coordinate ring $k[X]$. Then :*

i) The k-algebras $k[X]$ and $\mathcal{O}(X)$ are isomorphic (a canonical isomorphism is given by the map γ in above).

ii) For each point $x \in X$, let $\mathfrak{m}_x \subseteq k[X]$ be the ideal of functions vanishing at x. Then $x \longmapsto \mathfrak{m}_x$ gives a 1-1 correspondence between the points of X and the maximal ideals of $k[X]$.

iii) For any point $x \in X$ we have $k[X]_{\mathfrak{m}_x} = (T_1 - x_1, \ldots, T_n - x_n)$ is isomorphic to $\mathcal{O}_x$ and we have $dim(\mathcal{O}_x) = dim(X)$.

iv) $Frac(k[X])$ is isomorphic (as a field) to $k(X)$ and the transcendence degree of the finitely generated extension $k(X)/k$ is equal to $dim(X)$.

Proof. *i) We have seen above that the map $\gamma : k[X] \to \mathcal{O}(X)$ is a k-algebra monomorphism. We will see below that it is also surjective, hence an algebra isomorphism.*

ii) By proposition 1.1.2 $x \longmapsto \mathfrak{m}_x$ is a one-to-one correspondence between the points of X and the maximal ideals of $k[X]$.

iii) Let $f \in k[T_1, \ldots, T_n]$ be a polynomial, and let's denote its image in $k[X]$ by $\overline{f}$. For a point $x = (x_1, \ldots, x_n) \in X$ such that $\overline{f}(x) \neq 0$, $\gamma(\overline{f})$ is a unit with inverse $1/\gamma(\overline{f})_{|X \setminus Z(f)}$. Thus, we obtain an algebra homomorphism

$$k[X]_{\mathfrak{m}_x} \longrightarrow \mathcal{O}_x$$

induced by γ, which is injective (since any polynomial functions that coincide on a nonempty subset of X are actually equal). Moreover, this is surjective by definition of a regular function. We previously saw that $dim(X) = tr.deg_k(Frac(k[X]))$. Moreover, we have $dim(\mathcal{O}_x) = tr.deg_k(Frac(\mathcal{O}_x))$. We have also $Frac(k[X]) = Frac(k[X]_{\mathfrak{m}_x})$, so $dim(X) = dim(\mathcal{O}_x)$.

iv) Any nonzero element $f \in k[X]$ maps under γ to a unit with inverse $(\frac{1}{f})_{|X \setminus Z(f)}$. Thus we obtain an injective map

$$Frac(k[X]) \hookrightarrow k(X)$$

In fact, this map is also surjective : for each nonzero $< U, f > \in k(X)$, we have $< U, f > \in \mathcal{O}_x$ for some $x \in X$ This follows by the already established isomorphism in iii) and the fact that the following diagram commutes :

$$\begin{array}{ccc} k[X]_{\mathfrak{m}_x} & \xrightarrow{\sim} & \mathcal{O}_x \\ \big\downarrow & & \big\downarrow \\ Frac(k[X]) & \hookrightarrow & k(X) \end{array}$$

By theorem 1.2.2 $dim(k(X)) = tr.deg_k(k(X))$ and that $dim(X) = dim(k[X])$. Hence $k(X)$ is an algebraic extension of k with transcendence degree equal to $dim(X)$.

To end the proof of i), let's show that the homomorphism γ is surjective. It suffices to see that, up to identification, we have :

$$\begin{array}{rcl} k[X] & \subseteq & \mathcal{O}(X) \\ & \subseteq & \bigcap_{x\in X} \mathcal{O}_x \\ & \subseteq & \bigcap_{x\in X} k[X]_{\mathfrak{m}_x} \end{array}$$

Surjectivity now follows from the general fact that for an integral domain R, we have $\bigcap_m R_m = R$ (where the intersection is considered inside the fractions field of R).

Remark 1.3.4 *Let U be a nonempty open set of X. We can define a homomorphism of algebras over k, h from $k[X]$ into $k[U]$ by*

$$< V, f > \longmapsto < V \cap U, f_{|V\cap U} > .$$

One can easily see that h is isomorphism of algebras over k. So $k[U] \simeq k[X]$. Let X be an arbitrary variety and Y an affine variety and let $\phi : X \longrightarrow Y$ be a morphism. Then there is induced map

$$\begin{array}{rccc} \phi^* : & \mathcal{O}(Y) & \longrightarrow & \mathcal{O}(X) \\ & f & \longmapsto & \phi^*(f) := f \circ \phi \end{array}$$

We have also already seen that $k[Y] \simeq \mathcal{O}(Y)$ (see theorem 1.3.1). We get then a map $k[Y] \longrightarrow \mathcal{O}(X)$, which is a homomorphism of algebras over k, and so get a map

$$\begin{array}{rccc} \beta : & Hom_{var}(X, Y) & \longrightarrow & Hom_{k-alg}(k[Y], \mathcal{O}(X)) \\ & \phi & \longmapsto & \phi^* \end{array}$$

The following proposition shows that this map is bijective.

Proposition 1.3.5 *The map β defined previously is bijective.*

Proof. *We describe an inverse to β. Let $h : k[Y] \longrightarrow \mathcal{O}(X)$ be a homomorphism of algebras over k and let $y_i : Y \longrightarrow k$ be the coordinate functions. We previously saw that $k[Y]$ can be (canonically) identified with $\mathcal{O}(Y)$. Under this identification, the functions y_i plainly generate the k-algebra of $k[Y]$ (we can also take $y_i = T_i + I(Y) \in k[Y]$). Let $\mathfrak{z}_i = h(y_i) \in \mathcal{O}(X)$, so that $\mathfrak{z}_i : X \longrightarrow k$ is a regular function. Suppose that Y is a variety in $\mathbb{A}^n$, and consider the map*

$$\begin{array}{rccc} \phi_h : & X & \longrightarrow & \mathbb{A}^n \\ & x & \longmapsto & (\mathfrak{z}_1(x), \dots, \mathfrak{z}_n(x)) \end{array}$$

For each $P \in I(Y)$, i.e., $P + I(Y) = 0$ in $k[Y]$, we have $P(\phi_h(x)) = P(\mathfrak{z}_1(x), \dots, \mathfrak{z}_n(x)) = P(h(y_1)(x), \dots, h(y_n$ Since h is a homomorphism we have $P(h(y_1)(x), \dots, h(y_n)(x)) = h(P + I(Y))(x) = 0$, and so $\phi_h(x) \in Z(I(Y)) = Y$, which shows that $\phi_h(X) \subseteq Y$. If we write t_i for the coordinate function of $\mathbb{A}^n$ (so that $y_i = t_{i_{|Y}}$), then we have $t_i \circ \phi_h = \mathfrak{z}_i$ for all i. It follows from proposition 1.3.4 that ϕ_h is a morphism (of varieties). We have then

$$\begin{array}{rccc} \alpha : & Hom_{k-alg}(k[Y], \mathcal{O}(X)) & \longrightarrow & Hom_{var}(X, Y) \\ & h & \longmapsto & \phi_h \end{array}$$

Let's show that α and β are mutually inverse to each other. We have $\beta(\phi_h) = \phi_h^* : f \longmapsto f \circ \phi_h$, for all $f \in k[Y]$. Let $x \in X$, then $f \circ \phi_h(x) = f(h(y_1)(x), \dots, h(y_n)(x))$. So, writing $f = Q + I(Y)$, for some $Q \in k[T_1, \dots, T_n]$. We have $f \circ \phi_h(x) = h(f)(x)$. This shows that $\phi^*(f) = h(f)$. So $\beta(\phi_h) = h$, i.e $\beta \circ \alpha(h) = h$. It follows that $\beta \circ \alpha = id_{Hom_{k-alg}}(k[Y], \mathcal{O}(X))$. Similarly, given $\psi : X \longrightarrow Y$, and we have $\alpha \circ \beta(\psi) = \alpha(\psi^*) = \phi_{\psi^*} : X \longrightarrow Y, x \longmapsto (t_1 \circ \psi(x), \dots, t_n \circ \psi(x)) = \psi(x)$. which shows that $\alpha \circ \beta(\psi) = \psi$. It follows that $\alpha \circ \beta = id_{Hom_{var}(X,Y)}$.

Corollary 1.3.1 *If X and Y are two affine varieties, then X and Y are isomorphic if and only if $k[X]$ and $k[Y]$ are isomorphic as algebras over k.*

Proof. *Immediate from proposition 1.3.5.*

Remark 1.3.5 *In the language of categories, we can express the above result as follows :*

Corollary 1.3.2 *The functor $X \longrightarrow k[X]$ induces an arrow-reversing equivalence of categories between the category of affine varieties over k and the category of finitely generated integral domains over k.*

Proof. *Immediate from proposition 1.3.5.*

1.4 Rational functions

In Algebraic Topology, the notion of homeomorphism is relaxed to homotopy equivalence which leads to significant theorems (Whitehead's Theorem)[¶] relating topology to algebra. Similarly, rational functions are a relaxation of morphisms of varieties. We continue in this section, we explore how this notion interacts with algebra. We continue in this to assume that k is an algebraically closed field.

Let X and Y be two varieties. We consider the set $S_{X,Y}$ of all pairs (U, ϕ), where U is a nonempty open subset of X, and $\phi : U \longrightarrow Y$ is a morphism of varieties. On $S_{X,Y}$, we define the following equivalence relation

$$(U, \phi) \sim (V, \psi) \text{ if and only if } \phi_{U\cap V} = \psi_{U\cap V}$$

The equivalence class of (U, ϕ) by this relation will be denoted $< U, \phi >$.

Definition 1.4.1 *i) A rational function of varieties $X \longrightarrow Y$ is an equivalence class (with respect to the above equivalence relation) of a pair (U, ϕ), where $U \subseteq X$ is an open subset, and $\phi : U \longrightarrow Y$ a morphism.*

ii) We say that a rational function $X \longrightarrow Y$ is dominant if for some (or equivalently, any) representative pair (U, ϕ), $\phi(U)$ is dense in Y.

Remark 1.4.1 *Let $\phi : X \longrightarrow Y$, and $\psi : Y \longrightarrow Z$ be two rational functions. Suppose that $\phi = (U, \phi)$, and $\psi = (V, \psi)$, and that $\phi(U) \cap V$ is nonempty. Then we may define the composition of ϕ, and ψ by taking the pair $(\psi \circ \phi, \phi^{-1}(V))$.*
Note that in general, we cannot compose rational functions. The problem might be that the image of the first function might lie in the locus, where the second function is not defined. However there will never be a problem when ϕ is dominant.

Lemma 1.4.1 *Let $f : X \longrightarrow Y$ be a continuous map and U an open subset of Y. Then $\overline{f^{-1}(U)} \subseteq f^{-1}(\overline{U})$.*

Proof. *This follows from the fact that f is continuous and $f^{-1}(U) \subseteq f^{-1}(\overline{U})$.*

Lemma 1.4.2 *Let X be a variety, Y be an affine variety, $\phi : X \longrightarrow Y$ be a morphism of varieties and $\phi^* : \mathcal{O}(Y) \to \mathcal{O}(X)$ be the corresponding algebra homomorphism. Then*

$$\overline{\phi(X)} = Y \text{ if and only if } \phi^* \text{ is injective .}$$

[¶]*In homotopy theory, the Whitehead theorem states that if a continuous mapping f between CW complexes X and Y induces isomorphisms on all homotopy groups, then f is a homotopy equivalence. This result was proved by **J. H. C. Whitehead** in two landmark papers from 1949, and provides a justification for working with the concept of a CW complex that he introduced there.*

Proof. *Suppose that* $\overline{\phi(X)} = Y$, *and let* $f \in k[Y]$ *such that* $\phi^*(f) = 0$, *i.e* $f \circ \phi = 0$, *then* $f(\phi(X)) = 0$ *or equivalently* $\phi(X) \subseteq f^{-1}(0)$. *By identifying* $k[Y]$ *with* $\mathcal{O}(Y)$, *one can see that* f *is continuous, so* $f^{-1}(\{0\})$ *is a closed subset in* Y. *Moreover, by assumption,* $Y = \overline{\phi(X)}$, *so* $Y = f^{-1}(0)$, *or equivalently* $f = 0$. *This shows that* ϕ^* *is injective. Conversely, suppose that* $\overline{\phi(X)} \neq Y$, *so that there exists* $P \in I(\overline{\phi(X)})$ *with* $P \notin I(Y)$. *Let* $f = P + I(Y)$, *then we have* $\phi^*(f) = 0$, *but* $f \neq 0$, *because* $P \notin I(Y)$.

Remark 1.4.2 *In particular, if* $\phi : X \longrightarrow Y$ *is a rational function, and* (U, ϕ) *is one representative of* ϕ *and if we assume that* Y *is an affine variety, then*

$$\overline{\phi(U)} = Y \text{ if and only if } \phi^* : k[Y] \longrightarrow \mathcal{O}(U) \text{ is injective.}$$

Consequently

$$\phi \text{ is dominant if and only if for any representative } (U, \phi) \text{ of } \phi,\ \phi^* : k[Y] \longrightarrow \mathcal{O}(U) \text{ is injective.}$$

Proposition 1.4.1 *Let* $\phi : X \longrightarrow Y$ *be a rational function between two varieties, with* ϕ *dominant. Then* ϕ *induces a homomorphism of field extensions of* k.

$$\phi^{\perp} : k(Y) \longrightarrow k(X)$$

Proof. *Let* (U, ϕ) *one representative of* ϕ. *The fact that* ϕ *is dominant implies that* $\phi(U) \cap W$ *is nonempty for any nonempty open subset* W *of* Y. *This yields that* $\phi^{-1}(W)$ *is nonempty in* X, *and hence dense.*
Let $< V, f >$ *be an element of* $k(Y)$, *then* $f \circ \phi$ *is defined on* $\phi^{-1}(V)$, *and hence gives an element* $< \phi^{-1}(V), f \circ \phi >$ *of* $k(X)$.
$\phi^{\perp}$ *is a homomorphism of fields. One can easily see that this construction yields a homomorphism if field extension of* k $\phi^{\perp} : k(Y) \longrightarrow k(X)$.

Proposition 1.4.2 *Let* X *and* Y *be an arbitrary variety and* Y *be an affine variety. Any homomorphism of fields over* k, $h : k(Y) \longrightarrow k(X)$ *is induced by a dominant rational function* $\phi : X \longrightarrow Y$.

Proof. *Let* $h : k(Y) \longrightarrow k(X)$ *be a nonzero homomorphism field extensions of* k. *We want to show that* h *is induced by a rational function* $\phi_h : X \longrightarrow Y$. *For that, consider the restriction* $h_{|k[Y]} : k[Y] \longrightarrow \mathcal{O}(X)$. *Since* h *is a homomorphism of fields, then in particular,* $h_{|k[Y]}$ *is injective.*
Let $y_i := T_i + I(Y)$ *be the canonical generators of the* k*-algebra* $k[Y]$. *We have* $h(y_i) \in k(X)$, *so we can write* $h(y_i) =< U_i, f_i >$, *where* U_i *is a nonempty open subset of* X, *and* $f_i : U_i \longrightarrow k$ *is a regular function. Since* X *is a variety, then* $U := \cap_{i=1}^{n} U_i$ *is nonempty. We have* $< U_i, f_i >=< U, f_{i|U} >$, *we can write* $h(y_i) =< U, g_i >$, *where* $g_i = f_{i|U}$. *It follows that* $h(y_i) \in \mathcal{O}(U)$ *for all* i. *Thus,* $h(y_i) \in \mathcal{O}(U)$. *By proposition 1.3.5,* $h_{|k[Y]}$ *corresponds to a morphism of varieties*

$$\begin{array}{rccc} \phi_{h_{|k[Y]}} : & U & \longrightarrow & Y \\ & x & \longmapsto & (h(y_1)(x), \ldots, h(y_n)(x)) \end{array}$$

We have $h_{|k[Y]}$ *is injective and* $h_{|k[Y]} = (\phi_{h_{|k[Y]}})^*$, *so by lemma 1.4.2* $\overline{\phi_{h_{|k[Y]}}(U)} = Y$. $< U, \phi_h >$ *is a dominant rational function from* X *to* Y *and as one can easily see* h *is induced by this (dominant) rational function.*

Notation. *Let* X *and* Y *be varieties. We will consider the following notation :*

1) ***RF****(X,Y):=* $\{$*The set of all rational functions from* X *to* $Y\}$.

2)

$$\begin{array}{rccc} \gamma : & \mathbf{FR}(X, Y) & \longrightarrow & Hom(k(Y), k(X)) \\ & \phi & \longmapsto & \phi^{\perp} \end{array}$$

3)

$$\begin{array}{rcl} \lambda : Hom_{k-alg}(k(Y), k(X)) & \longrightarrow & \boldsymbol{FR}(X,Y) \\ h & \longmapsto & \phi_h \end{array}$$

Theorem 1.4.1 *Let X and Y be two affine varieties, then there is a bijection between* $\boldsymbol{FR}(X,Y)$ *and* $Hom_{k-alg}(k(Y), k(X))$.

Proof. *Similar to the proof of proposition 1.3.5.*

Definition 1.4.2 *We say that a dominant rational function* $\phi : X \longrightarrow Y$ *of varieties is bi-rational if it has an inverse. In this case we say that X and Y are bi-rational (or bi-rationally equivalent) and we write by* $X \sim_{bir} Y$.

Proposition 1.4.3 *Let X and Y be two varieties. Then the following statements are equivalent*

1) *X and Y are bi-rational.*

2) *X and Y contain isomorphic open subsets.*

3) *The function fields of X and Y are isomorphic.*

Proof. *One can derive from theorem 1.4.1 that 1)⇔ 3) and clearly 2) implies 1). It remains to prove that if X and Y are bi-rational, then they contain isomorphic open subsets. Let* $\phi : X \longrightarrow Y$ *be a bi-rational function with inverse* $\psi : Y \longrightarrow X$. *Suppose that* ϕ *is defined on U, and* ψ *is defined on V. Let* $W := \phi^{-1}(V) \subseteq U$ *and let* $f := \phi_{|W}$. *Then* $f : W \longrightarrow f(W) \subseteq V$. *Note that* $\psi \circ f : W \longrightarrow W$ *is the identity morphism. Therefore* $f(W) = \psi^{-1}(W)$ *is an open and so* $\psi : f(W) \longrightarrow W$ *is the inverse of f.*

Example 1.4.1 *The projective space* $\mathbb{P}^n$, *and the affine space* $\mathbb{A}^n$ *are bi-rationally equivalent.*

Corollary 1.4.1 *The correspondence* $X \longmapsto k(X)$ *defines an equivalence between the category of varieties over k with morphisms the dominant rational functions and the category of finitely generated field extensions of k.*

1.5 Tangent spaces and singularities

We continue to assume in this section that k is an algebraically closed.

1.5.1 Tangent spaces

In Differential Geometry, tangent spaces at least for smooth manifolds, arise very naturally. The tangent space at a single point is best described as the collection of possible starting directions one can take when travelling from that point along the manifold. We will sees in this section that a similar notion does exist for algebraic varieties. For this, we will start with the definition for affine varieties, and build from that towards a more general formulation.

Notation. *For* $f \in k[T_1, \ldots, T_n]$ *and* $x = (x_1, \ldots, x_n) \in \mathbb{A}^n$. *The linear map* $k^n \longmapsto k$ *given by*

$$d_x f(a) := \sum_{j=1}^{n} \frac{\partial f}{\partial T_j}(x) a_j, \forall a = (a_1, \ldots, a_n) \in k^n \tag{1.5}$$

sends a vector $a \in k^n$ *to the "directional derivative" of f at x along that vector. Thus, for a geometric interpretation,* $d_x f(a) = 0$ *precisely for those directions in which f is stationary at x.*

Definition 1.5.1 *Let X be a nonempty affine algebraic set, $x \in X$. Let $v \in k^n$, we say that v is tangent to a X at x if $d_x g(v) = 0$, for all $g \in I(X)$. The set of all vectors v of k^n which verifies this condition is called the tangent space to X at x. We denote it by $T_x X$.*

Remarks 1.5.1 *1) Let $f_1, \ldots, f_r \in k[T_1, \ldots, T_n]$ be such that $I(X) = (f_1, \ldots, f_r)$ and let $g \in k[T_1, \ldots, T_n]$. For $x \in X$, we have :*

$$\frac{\partial (f_i g)}{\partial T_j}(x) = f_i(x)\frac{\partial g(x)}{\partial T_j} + g(x)\frac{\partial f_i}{\partial T_j}(x) = g(x)\frac{\partial f_i}{\partial T_j}(x). \tag{1.6}$$

Note that an element of $I(X)$ is of the form $\sum_{j=1}^{r} f_j h_j$ where $h_j \in k[T_1, \ldots, T_n]$. So, using (1.6) we can restrict ourselves in definition 1.5.1 to the case where g describes only the elements $f_1, \ldots, f_r$.

2) Also, we can see the tangent space to X at x as

$$T_x X = \bigcap_{g \in I(X)} ker(d_x g) \subseteq k^n.$$

So, clearly $T_x X$ is $k-$ vector subspace of k^n.

3) The tangent space is sometimes called the Zariski tangent space, when it is necessary to distinguish it from other kinds of tangent.

4) $T_x X = \{(v_1, \ldots, v_n) \in k^n \mid \sum_{i=1}^{n} \frac{\partial f}{\partial T_i}(x) v_i = 0$, for all $f \in I(X)\} = ker(J_x)$, where J_x is the Jacobian matrix

$$J_x = \left(\frac{\partial f_i}{\partial T_j}(x)\right)_{1 \leq i \leq r,\ \ 1 \leq j \leq n} \tag{1.7}$$

so, we have $dim(T_x X) = n - rank(J_x)$.

Example 1.5.1 *Let $X \subseteq \mathbb{A}^2$ be the affine algebraic set defined by the polynomial*

$$f(T_1, T_2) = T_2^2 - T_1^3$$

we have $\frac{\partial f}{\partial T_1} = -3T_1^2$, and $\frac{\partial f}{\partial T_2} = 2T_2$. So

$$\frac{\partial f}{\partial T_1}(0,0) = \frac{\partial f}{\partial T_2}(0,0) = 0.$$

Hence $d_{(0,0)} f$ is the zero map. Thus

$$T_{(0,0)} X = \mathbb{A}^2.$$

We have another definition of tangent space in terms of derivations.

Tangent space in terms of derivations

Recall that if M is a real manifold, and $p \in M$, a tangent vector X_p in $T_p M$ defines a derivation of the $\mathbb{R}$-algebra $\mathcal{C}_p(M)$:

$$\begin{array}{ccc} \mathcal{C}_p(M) & \longrightarrow & \mathbb{R} \\ f & \longmapsto & X_p(f) := d_p f(X_p) \end{array} \tag{1.8}$$

In particular, we have

$$X_p(fg) = X_p(f)g(p) + f(p)X_p(g)$$

The derivation is actually an $\mathbb{R}$-derivation, since $X_p(\alpha) = 0$ for all constant functions $\alpha \in \mathbb{R}$. Using Taylor's formula can prove that the tangent space of M at p is actually isomorphic to the vector space of derivations of $\mathcal{C}_p(M)$ with values in $\mathbb{R}$ (Cf., [28]) :

$$T_p M \simeq Der_{\mathbb{R}}(\mathcal{C}_p(M), \mathbb{R})$$

We will see below how algebraic tangent spaces are defined in a similar way :

Definition 1.5.2 *Let $X \subseteq \mathbb{A}^n$ be a nonempty affine algebraic set and $D : k[X] \longrightarrow k$ be a homomorphism of k-vector spaces. We say that D is a derivation of $k[X]$ at x if for all $f, g \in k[X]$, we have:*

$$D(fg) = f(x)D(g) + g(x)D(f).$$

We denote by $Der_x(k[X])$ the set of derivations of $k[X]$ at x.

Remark 1.5.1 *One can easily see that $Der_x(k[X])$ is k-vector space.*

Note that if $\mathfrak{m}_x$ is the maximal ideal of $k[X]$ corresponding to a point x of X i.e., $\mathfrak{m}_x = \{P + I(X) \mid P(x) = 0\}$, then up to a field isomorphism, $k[X]_{\mathfrak{m}_x}$, for $k[X]/\mathfrak{m}_x$ is a field and k is algebraically closed. Note also, that if we identify $k[X]$ with its canonical image in the localized algebra $k[X]_{\mathfrak{m}_x}$ and so $\mathfrak{m}_x$ the maximal ideal of $k[X]_{\mathfrak{m}_x}$, then for the same reason, we have $k[X]_{\mathfrak{m}_x}/\mathfrak{m}_x = k$.

Remark 1.5.2 *Let $(R, \mathfrak{m})$ be a Noetherian local ring and $k = R/\mathfrak{m}$, then $\mathfrak{m}/\mathfrak{m}^2$ is a finitely generated k-vector space. By Nakayama's Lemma, $dim_k(\mathfrak{m}/\mathfrak{m}^2)$ is the minimal number of generators of $\mathfrak{m}$.*

In particular, if we take, $R = k[X]_{\mathfrak{m}_x}$, then $\mathfrak{m}_x/\mathfrak{m}_x^2$ is a k-vector space. We will denote its dual space, i.e., $Hom(\mathfrak{m}_x/\mathfrak{m}_x^2)$ by $(\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee$.

Lemma 1.5.1 *Let $X \subseteq \mathbb{A}^n$ be an affine algebraic set and x be a point of X. Then there exists a homomorphism of k-vector spaces from T_xX into $Der_x(k[X])$.*

Proof. *Let $v = (v_i)_{1 \le i \le n})$ be a vector of $\in T_xX$ and consider the map*

$$\begin{array}{rccc} D_v: & k[T_1, \dots, T_n] & \longrightarrow & k \\ & f & \longmapsto & \sum_{i=1}^n \frac{\partial f}{\partial T_i}(x)v_i \end{array}$$

It is clear that D_v is a homomorphism of k-vector spaces Moreover, we have $D_v(fg) = f(x)D_v(g) + g(x)D_v(f)$ for all $f, g \in k[T_1, \dots, T_n]$. Also, by definition, for all $f \in I(X)$, we have $D_v(f) = 0$. So D_v induces a homomorphism of k-vector spaces from $k[X]$.

$$\begin{array}{rccc} D_v: & k[X] & \longrightarrow & k \\ & \overline{f} & \longmapsto & \sum_{i=1}^n \frac{\partial f}{\partial T_i}(x)v_i \end{array}$$

which is an element of $Der_x(K[X])$.
The map

$$\begin{array}{rccc} D: & T_xX & \longrightarrow & Der_x(k[X]) \\ & v & \longmapsto & D_v \end{array}$$

is a homomorphism of k-vector spaces. Indeed, we have :

$$D(v + \lambda w)(f) = \sum_{i=1}^n \frac{\partial f}{\partial T_i}(x)(v_i + \lambda w_i) = \sum_{i=1}^n \frac{\partial f}{\partial T_i}(x)v_i + \lambda \sum_{i=1}^n \frac{\partial f}{\partial T_i}(x)w_i = D_v(f) + \lambda D_w(f), f \in k[X].$$

Lemma 1.5.2 *Let $X \subseteq \mathbb{A}^n$ be an affine algebraic set, $x \in X$. Then there exists a homomorphism of k-vector spaces from $Der_x(k[X])$ into $(\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee$.*

Proof. *Plainly, any $\Delta \in Der_x(k[X])$ induces a homomorphism of k-vector spaces that we denote also by Δ*

$$\Delta : \mathfrak{m}_x \longrightarrow k$$

Let $f, g \in \mathfrak{m}_x$, then we have

$$\Delta(fg) = f(x)\Delta(g) + g(x)\Delta(g) = 0.$$

So Δ induces a homomorphism k-vector spaces :

$$\Delta_x : \mathfrak{m}_x/\mathfrak{m}_x^2 \longrightarrow k.$$

It's clear that $\Delta_x \in (\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee$. Moreover, one can easily see that

$$\begin{array}{rccc} \Theta : & Der_x(k[X]) & \longrightarrow & (\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee \\ & \Delta & \longmapsto & \Delta_x \end{array}$$

is a homomrphism of k-vector spaces.

Lemma 1.5.3 *Let $X \subseteq \mathbb{A}^n$ be an affine algebraic set and x be an element of X. $x \in X$. Then there exists a homomorphism of k-vector spaces from $(\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee$ into T_xX.*

Proof. *Let $\Gamma \in (\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee$ and let $v_i := \Gamma(T_i - x_i + \mathfrak{m}_x^2)$, then put $v = (v_i)_{1\le i\le n}$. Let us show that $v \in T_xX$. For $f \in I(X)$ using taylor's development, we have*

$$f \equiv f(x) + \sum_{i=1}^{n} \frac{\partial f}{\partial T_i}(x)(T_i - x_i)[\mathfrak{m}_x^2] \tag{1.9}$$

hence $f + \mathfrak{m}_x^2 = \sum_{i=1}^{n} \frac{\partial f}{\partial T_i}(x)(T_i - x_i) + \mathfrak{m}_x^2$.
On the other hand we have

$$f + I(X) = 0 \text{ in } k[X].$$

Then

$$f + \mathfrak{m}_x^2 = 0 \text{ in } \mathfrak{m}_x/\mathfrak{m}_x^2.$$

Therefore,

$$\begin{array}{rcc} 0 & = & \Gamma(f + \mathfrak{m}_x^2) \\ & = & \Gamma(\sum_{i=1}^{n} \frac{\partial f}{\partial T_i}(x)(T_i - x_i) + \mathfrak{m}_x^2) \\ & = & \sum_{i=1}^{n} \frac{\partial f}{\partial T_i}(x)\Gamma((T_i - x_i) + \mathfrak{m}_x^2) \\ & = & \sum_{i=1}^{n} \frac{\partial f}{\partial T_i}(x)v_i \end{array}$$

which means that $v \in T_xX$. We get then a the map

$$\begin{array}{rccc} \Lambda : & \mathfrak{m}_x/\mathfrak{m}_x^2 & \longrightarrow & T_xX \\ & \Gamma & \longmapsto & (v_i)_{1\le i\le n} \end{array}$$

where $v_i = \Gamma(T_i - x_i + \mathfrak{m}_x^2)$. One can easily Λ is a k-vector spaces homomorphism.

Proposition 1.5.1 *Let X be a nonempty affine algebraic set of $\mathbb{A}^n$. Then for any $x \in X$, we have*

$$T_xX \simeq Der_x(k[X]) \simeq (\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee$$

Proof. *It suffices to verify that homomorphisms Θ, D and Λ defined in the preceding lemmas are isomorphisms of k-vector spaces.*

We aim in what follows to define and study the tangent space of any (algebraic) variety.

Definition 1.5.3 *Let X be a projective quasi-variety, x be a point of X and $\mathfrak{m}_x$ be the maximal ideal of $\mathcal{O}_x$. The tangent space of X at $x \in X$ is as*

$$T_xX := Hom_k(\mathfrak{m}_x/\mathfrak{m}_x^2, k) := (\mathfrak{m}_x/\mathfrak{m}_x^2)^\vee$$

Remarks 1.5.2 *Let X and Y be two varieties, then we have the following :*

1) *For any morphism $\phi : X \longrightarrow Y$ of varieties and any $x \in X$, there is an induced homomorphism of algebras*
$$\phi^* : \mathcal{O}_{\phi(x)} \longrightarrow \mathcal{O}_x$$
which sends the maximal ideal $\mathfrak{m}_{\phi(x)}$ of $\mathcal{O}_{\phi(x)}$ inside the maximal ideal $\mathfrak{m}_x$ of $\mathcal{O}_x$, i.e., $\phi^*(\mathfrak{m}_{\phi(x)}) \subseteq \mathfrak{m}_x$. Indeed, let $f \in \mathfrak{m}_{\phi(x)}$, then $\phi^*(f) = f \circ \phi$. So, $\phi^*(f)(x) = f(\phi(x)) = 0$. We get then an induced algebra homomorphism
$$\mathfrak{m}_{\phi(x)}/\mathfrak{m}^2_{\phi(x)} \longrightarrow \mathfrak{m}_x/\mathfrak{m}^2_x$$
which dually yields a k-homomorphism of vector spaces
$$T_x\phi : T_xX \longrightarrow T_{\phi(x)}Y$$

2) *If $g : Y \longrightarrow Z$ is a morphism and $z = g(f(x))$, then*
$$T_zg \circ T_xf = T_x(g \circ f)$$

3) $T_x(id_X) = id_{T_xX}$.

4) *If ϕ is an isomorphism, then we have a corresponding (induced) homomorphism of k-vector spaces*
$$T_x\phi : T_xX \longrightarrow T_{\phi(x)}Y$$
is an isomorphism. Indeed, let φ be the inverse of ϕ,
$$T_{\phi(x)}\varphi : T_{\phi(x)}Y \longrightarrow T_xX.$$
Moreover, we have $T_{\phi(X)}\varphi \circ T_x\phi = T_x(\varphi \circ \phi) = T_x(id_X) = id_{T_xX}$, and $T_x\phi \circ T_{\phi(x)}\varphi = T_{\phi(x)}(\phi \circ \varphi) = T_{\phi(X)}(id_Y) = id_{T_{\phi(x)}Y}$. This shows that $T_x\phi$ is an isomorphism.

Lemma 1.5.4 *If R is a Noetherian local ring with maximal ideal $\mathfrak{m}$ and let $k := R/\mathfrak{m}$, then $dim(R) \leq dim_k(\mathfrak{m}/\mathfrak{m}^2)$.*

Proof. *See [3, Corollary 11.15].*

Proposition 1.5.2 *Let X be a variety and x be a point of X. Then*
$$dim_k(T_xX) \geq dim(X).$$

Proof. *Let $\mathcal{O}_x$ be the local ring of X at x and $\mathfrak{m}_x$ be the maximal ideal of $\mathfrak{O}_x$. We previously saw that $dim(X) = dim(\mathcal{O}_x)$. Also, by lemma 1.5.4, we have $dim_k(\mathfrak{m}_x/\mathfrak{m}_x^2) \geq dim(\mathcal{O}_x)$. So, $dim_kT_x(X) = dim_k(\mathfrak{m}_x/\mathfrak{m}_x^2) \geq dim(X)$.*

Definition 1.5.4 *Let R be a Noetherian ring with maximal ideal $\mathfrak{m}$ and let $k := R/\mathfrak{m}$. We say that R is regular if $dim_k(\mathfrak{m}/\mathfrak{m}^2) = dim(R)$.*

Definition 1.5.5 *Let X be an algebraic set. The dimension of X at a point x, denoted by $dim_x(X)$, is the maximum of the dimensions of irreducible components of X containing x.*

Corollary 1.5.1 *Let X be an algebraic set and and $x \in X$. Then*
$$dim_k(T_xX) \geq dim_x(X).$$

Proof. *Let Z be an irreducible component of X containing x. Obviously $T_xZ \subseteq T_xX$. So*
$$dim_x(Z) \leq dim_k(T_xZ) \leq dim_k(T_xX).$$
Hence
$$dim_k(T_xX) \geq dim_x(X).$$

1.5.2 Singularities

Definition 1.5.6 *Let $X \subseteq \mathbb{A}^n$ be an affine variety of dimension d, and $x \in X$.*

i) We say that X is nonsingular (or regular or smooth) in x if rank $J_x = n - d$.

ii) We say that X is nonsingular it it is nonsingular at all its points.

Notation. *We will write $\textbf{Sing}(X) := \{x \in X \,|\, x \text{ singular } \}$.*

Example 1.5.2 *Let $X = Z(f)$, where $f \in k[T_1, T_2]$. Then X is nonsingular at $x \in X$ if and only if*

$$(\frac{\partial f}{\partial T_1}(x), \frac{\partial f}{\partial T_2}(x)) \neq (0, 0).$$

For example let $f = T_1^3 - T_2^2$ and $x = (a, b)$. We have $J_{(a,b)} = \begin{pmatrix} 3a^2 & -2b \end{pmatrix}$, so X is nonsingular at x if and only if $(a, b) \neq (0, 0)$.

Definition 1.5.7 *Let X be a variety and $x \in X$.We say that X is nonsingular at x if the local ring $\mathcal{O}_x$ is regular ring. We say that X is nonsingular if it is nonsingular at every point.*

Lemma 1.5.5 *Let X be an affine algebraic set of $\mathbb{A}^n$. For any integer d, the set $X_d := \{x \in X \,|\, dim_k(T_x X) \geq d\}$ is a closed subset of X.*

Proof. *Let $f_1, \ldots, f_r \in k[T_1, \ldots, T_n]$ be such that $I(X) = (f_1, \ldots, f_r)$.
By remarks 1.5.1, we have $T_x X = \bigcap_{i=1}^r ker(d_x f_i) = ker(J_x)$, where*

$$J_x = \left(\frac{\partial f_i}{\partial T_j}(x)\right)_{1 \leq i \leq r, \quad 1 \leq j \leq n}$$

So $dim(T_x X) = n - rank(J_x)$. Hence

$$X_d = \{x \in X \,|\, rank(J_x) < n - d\}$$

We know that $rank(J_x) < n - d$ is equivalent the fact that : every $(n - d) \times (n - d)$ sub-matrix of J_x has determinant zero. The determinant of a sub-matrix of J_x is a polynomial function, so X_d is a closed subset of X.

Corollary 1.5.2 *Let x be an affine algebraic set of $\mathbb{A}^n$. Then the following statements are equivalent :*

i) X is singular at x.

ii) $dim(T_x X) > dim(X)$.

iii) The Jacobian matrix J_x does not have full rank.

Proposition 1.5.3 *Let X an be an affine algebraic set of $\mathbb{A}^n$. The set $\textbf{Sing}(X)$ of singular points of X is a closed subset of X.*

Proof. *By lemma 1.5.4, and proof of lemma 1.5.5 the set of singular points is the set of points where the **rank** of the Jacobian matrix is $< n - d$, where $d = dim(X)$. Thus, $\textbf{Sing}(X)$ is an algebraic set defined by the ideal generated by $I(X)$ together with all determinants of $(n - d) \times (n - d)$ sub-matrices of the matrix J_x.*

By the above, $\textbf{Sing}(X)$ is a closed subset of X. In what follows, we want that to show that it is a proper subset of X.

Lemma 1.5.6 *Let X, Y be two varieties and $\phi : X \longrightarrow Y$ be a bi-rational function. If X admits a nonsingular point, then so does Y.*

Proof. *By the above, $\textbf{Sing}(X)$ is a closed subset of X if X has a nonsingular points, then there exists an open dense subset $U \subsetneq X$ containing only nonsingular points. Since $X \sim_{bir} Y$, then by proposition 1.4.3, there exists two open sets $W \subseteq X$ and $V \subseteq Y$ so that $\phi_{|W} : W \longrightarrow V$ is an isomorphism. So Y has a nonsingular points as well (any point of $\phi(W \cap U)$ well do).*

Lemma 1.5.7 *Let X be a variety of dimension d. Then X is bi-rationally equivalent to a hypersurface $\mathbb{A}^{d+1}$.*

Proof. *See [12, proposition 4.9].*

Lemma 1.5.8 *Let X be an affine hypersurface, then $\textbf{Sing}(X)$ is a proper closed subset of X.*

Proof. *Assume that X is an affine subvariety of $\mathbb{A}^{n+1}$ and write $X = Z(f)$, with f is irreducible. We have $x \in \textbf{Sing}(X)$ if and only if $\frac{\partial f}{\partial T_i}(x) = 0$, for all $i \in \{1, \ldots, n+1\}$.*
$\textbf{Sing}(X) = X$, $\frac{\partial f}{\partial T_i} \in I(X)(= (f))$. Note that (f) a prime ideal of $k[T_1, \ldots, T_{n+1}]$ and and $\frac{\partial f}{\partial T_i}$ has smaller degree (than f). So, $\textbf{Sing}(X) = X$ if and only if $\frac{\partial f}{\partial T_i}$ is the zero polynomial for all i, which means that So f is constant, a contradiction.

Theorem 1.5.1 *Let X be an affine variety. Then the set $\textbf{Sing}(X)$ of singular points proper closed subset of X.*

Proof. *By lemma 1.5.7, X is bi-rationally equivalent to hypersurface H in $\mathbb{A}^{d+1}$, so by proposition 1.4.3 there exist open subsets $U \subseteq X$ and $W \subseteq H$ which $U \simeq W$. As seen in lemma 1.5.8, $\textbf{Sing}(H)$ is a proper closed subset of H. Therefore $\textbf{Sing}(W)$ is proper subset of W.*

1.6 Prevarieties

Affine varieties are special objects in the category $\mathcal{TA}$ of topological spaces with distinguished algebras of regular functions. In order to define (abstract) algebraic varieties, we have to replace $\mathcal{TA}$ with the category of spaces (space of functions) over k, where one has not only a distinguished sub-algebra $\mathcal{O}_X$ on the entire space X, but for every open subset U of X. In this section, we define this more general category that we denote by $\mathcal{TA}_k$. We recall that throughout k is an algebraically closed field.

Notation. *Let X be a topological space. For any open subset U of X. We pose*

$$\mathcal{M}ap(U, k) := \{f : U \longrightarrow k\}$$

the set of all maps defined on U and with values in k.
$\mathcal{M}ap(U, k)$ is a k-algebra equipped with the usual laws.

Definition 1.6.1 *A space of functions over k is a topological space X together with a family $\mathcal{O}_X$ of sub-algebras over k, $\mathcal{O}_X(U) \subseteq \mathcal{M}ap(U, k)$ for every open subset U of that satisfy the following properties:*

i) If W, U are two open subsets of X such that $W \subseteq U$, then for any $f(\in \mathcal{O}_X(U))$, the restriction $f_{|W} \in \mathcal{M}ap(W, k)$ is an element of $\mathcal{O}_X(W)$.

ii) Given an open subset U of X and an open cover $(U_i)_{i \in I}$ of U, i.e., U_i are open subsets of X such that $U = \cup_{i \in I} U_i$, together with $f_i \in \mathcal{O}_X(U_i)$ such that

$$f_{i|U_i \cap U_j} = f_{j|U_i \cap U_j}$$

for all $i, j \in I$. There exists a unique $f \in \mathcal{O}_X(U)$ such that $f_{|U_i} = f_i$, for all i.

Remark 1.6.1 *The space of functions* $(X, \mathcal{O}_X)$ *will often be simply denoted by* X.

Examples 1.6.1 1) *Let* X *be a* $\mathcal{C}^\infty$*-manifold. For any open subset* U *of* X *define*

$$\mathcal{O}_X(U) := \{f : U \longrightarrow \mathbb{R} \mid f \text{ is } \mathcal{C}^\infty\}$$

with restriction maps given by restrictions of functions. Then $(X, \mathcal{C}^\infty)$ *is a space of functions over* $\mathbb{R}$.

2) *Let* X *be a quasi-affine variety, for an arbitrary open subset* U *of* X, *let*

$$\mathcal{O}_X(U) := \{f : U \longrightarrow k \mid f \text{ being a regular function}\}.$$

Then $(X, \mathcal{O}_X)$ *is a space of functions.*

Definition 1.6.2 *(Morphism of space with functions) A morphisms* $(X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ *of spaces with functions is a continuous map* $f : X \longrightarrow Y$ *such that for any open subset* V *of* Y, *and any* $\psi \in \mathcal{O}_Y(V)$, *we have* $\psi \circ f \in \mathcal{O}_X(f^{-1}(V))$.

Notation. *We will denote* $\psi \circ f$ *by* $f^*\psi$.

Proposition 1.6.1 *Let* X, Y *and* Z *be spaces of functions over* k. *Then*

1) *For any open subset of* X, *the inclusion map* $\imath : U \longrightarrow X$ *is a morphism of spaces of functions.*

2) *The identity is a morphism.*

3) *If* $f : X \longrightarrow Y$ *and* $g : Y \longrightarrow Z$ *are morphisms of spaces of functions, then* $g \circ f$ *is a morphism.*

Proof. 1) *By definition of the induced topology on* U, $\imath$ *is continuous. For any open subset* V *of* X *and for any* $\psi \in \mathcal{O}_X(V)$ *we have for every* $x \in \imath^{-1}(V)$, $\imath(x) = x$, *so* $\psi \circ \imath(x) = \psi(x)$. *Therefore,* $\psi \circ \imath \in \mathcal{O}_U(\imath^{-1}(V))$.

2) *By 1) It suffices to take* $U = X$, *and we have* $id_X = \imath$.

3) *It is clear that* $g \circ f$ *is continuous. Let* W *be an open subset of* Z, *and* $\psi \in \mathcal{O}_Z(W)$. *Then*

$$g^*\psi \in \mathcal{O}_Y(g^{-1}(W)).$$

So

$$f^*g^*\psi \in \mathcal{O}_X\big(f^{-1}(g^{-1}(W))\big)$$

Therefore, we get

$$(g \circ f)^*\psi \in \mathcal{O}_X\big((g \circ f)^{-1}(W)\big).$$

Definition 1.6.3 *We define the category* $\mathcal{TA}_k$ *as follows :*

* *Objects :* $(X, \mathcal{O}_X)$ *where* X *is a topological space.*
* *Morphisms : morphisms of spaces with functions.*

Remarks 1.6.1 i) *If* $X = \bigcup_{i \in I} U_i$ *is an open cover of* X, $\beta_i : U_i \longrightarrow X$ *are the inclusions, and* $f : X \longrightarrow Y$ *is any map, then* f *is a morphism if and only if* $f \circ \beta_i$ *is a morphism for all* i.

ii) $f : (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ *is an isomorphism if and only if* f *is a homeomorphism and for any open* $V \subseteq Y$

$$\psi : V \longrightarrow k \text{ is in } \mathcal{O}_Y(V) \text{ if and only if } f^*\psi \in \mathcal{O}_X\big(f^{-1}(V)\big).$$

iii) *If $X \subseteq \mathbb{A}^n$, $Z \subseteq \mathbb{A}^m$ are two affine varieties, one can easily see that a map $h : X \longrightarrow Z$ is a morphism in the new sense of definition 1.6.2 if and only if it is a morphism in the sense definition 1.3.3.*

Definition 1.6.4 *An element $(X, \mathcal{O}_X)$ in $\mathcal{TA}_k$ is an affine variety if it isomorphic in $\mathcal{TA}_k$ to certain $(Y, \mathcal{O}_Y)$, where Y is an algebraic set of some $\mathbb{A}^m$.*

Notation. *Let X be a space with functions and let $U \subseteq X$ be an open subspace. We denote by $(U, \mathcal{O}_{X|U})$ the space U of functions $\mathcal{O}_U(W) := \mathcal{O}_{X|U}(W) := \mathcal{O}_X(W)$, for any open subset W of U.*

Definition 1.6.5 *A prevariety is a connected space with functions X with a finite open cover by affine varieties. This is a topological space X with an open cover $(U_i)_{i \in I}$ such that $(U_i, \mathcal{O}_{U_i})$ is isomorphic to an affine variety.*

Remark 1.6.2 *Morphisms of prevarieties are just morphisms in $\mathcal{TA}_k$.*

Lemma 1.6.1 *Let X be a topological space, and $X = U_1 \cup \cdots \cup U_r$ be an open cover of X with all U_i nonempty. Then X is irreducible if and only if U_i is irreducible for all i, and $U_i \cap U_j$ is irreducible for all i, j.*

Proof. *See [26, A.119, p.**357**].*

Proposition 1.6.2 *Every prevariety X is an irreducible topological space.*

Proof. *Immediate, by lemma 1.6.1.*

Proposition 1.6.3 *Let $(X, \mathcal{O}_X)$ be a space with functions. If $(X, \mathcal{O}_X)$ is a prevariety, then X is a Noetherian topological space.*

Proof. *Write $X = U_1 \cup \cdots \cup U_r$, where $(U_i, \mathcal{O}_{U_i})$ are affine. Then U_i is Noetherian for all i. Note that any chain*

$$S_1 \supseteq S_2 \supseteq \cdots$$

of closed subsets in X gives a chain

$$S_1 \cap U_i \supseteq S_2 \cap U_i \supseteq \cdots$$

of closed subsets in U_i, so there exists m_i such that $S_j \cap U_i = S_{j+1} \cap U_i$ for $j > m_i$, whence $S_j = S_{j+1}$ for $j > max\{m_1, \ldots, m_r\}$.

Properties 1.6.1 *Let $(X, \mathcal{O}_X)$ be a space with functions*

i) *If $(X, \mathcal{O}_X)$ is a prevariety, then $\mathcal{O}_X$ is subspace of the $\mathcal{C}_X(U)$ of continuous functions to k, i.e.,*

$$\mathcal{C}_X(U) = \{f : U \longrightarrow k \,|\, f \text{ continuous } \}.$$

ii) *If $(X, \mathcal{O}_X)$ is a prevariety and $\psi \in \mathcal{O}_X(X)$, then $U := \{x \in X \,|\, \psi(x) \neq 0\}$ is an open subset of X, and we have $\frac{1}{\psi} \in \mathcal{O}_X(U)$.*

iii) *All statements about dimensions of quasi-affine varieties to prevarieties.*

iv) *If $(X, \mathcal{O}_X)$ is a prevariety, then the open subsets of X that are affine form a basis for the topology of X.*

Proof. *i)* *Immediate.*

iii) *Immediate.*

iv) *Let $\{X_i\}$ be any open affine covering of X. If $U \subseteq X$ is an open subset of X, the sets $U_i := U \cap X_i$ form an open covering of U. The U_i's will not necessarily be affine, but we know that the principals open sets in X_i form a basis for its topology, so are affine varieties. Hence we can cover each of the U_i's, and thereby U, by affine opens.*

1.7 Normal varieties

In this section, we define the notion of a normal variety that corresponds to normal domains in algebra. In particular, we show that any nonsingular variety is normal. Along this section, we continue to assume that k is an algebraically closed field.

Normal rings

Definition 1.7.1 *Let R be an integral domain with quotient field K. We say that R is normal if R coincides with its integral closure in K.*

Remark 1.7.1 *For more details on normal domains one can see e.g., [3, Chapter 5].*

Example 1.7.1 *1) A UFD is a normal domain. ([20, Vol I, p.**261**].)*

2) Any DVR is a normal domain.

Proposition 1.7.1 *Let R be a domain and K its field of fractions. Then, the following statements are equivalent.*

1) R is normal.

2) $S^{-1}R$ is normal for any multiplicative set of R.

3) $R_{\mathfrak{p}}$ is normal for all $\mathfrak{p} \in Spec(R)$.

4) $R_{\mathfrak{m}}$ is normal for all $\mathfrak{m} \in Spm(R)$.

Proof. *See [23, Proof of theorem 4.1].*

Normal varieties

Definition 1.7.2 *Let X be an algebraic variety over k and $x \in X$. We say that x is normal if the local ring $\mathcal{O}_x$ is a normal domain. We say that X is normal if all points of X are normal.*

Proposition 1.7.2 *Let X be an affine variety, then X is a normal if and only if the coordinate ring $k[X]$ is a normal domain.*

Proof. *If X is normal, then for all $x \in X$, $\mathcal{O}_x$ is normal domain. By theorem 1.3.1, we have $k[X]_{\mathfrak{m}_x} \simeq \mathcal{O}_x$, so $k[X]_{\mathfrak{m}_x}$ is a normal domain. Recall that $\mathfrak{m}_x$ describe all possible maximal ideals of $k[X]$ when x describes all points of X, therefore by proposition 1.7.1 $k[X]$ is a normal domain. Conversely, if $k[X]$ is a normal domain, then by proposition 1.7.1 $k[X]_{\mathfrak{m}_x}$ is normal for all $x \in X$, hence $\mathcal{O}_x(\simeq k[X]_{\mathfrak{m}_x})$ is normal for all $x \in X$. So X is normal.*

Examples 1.7.1 *1) $k[T_1, \dots, T_n]$ is a UFD so as seen above. Recall that $k[T_1, \dots, T_n] = K[X]$, where $X = \mathbb{A}^n$, so by proposition 1.7.2 $\mathbb{A}^n$ is normal.*

2) Let $X = Z(T_2^2 - T_1^3) \subseteq \mathbb{A}^2$, then X is not normal, indeed we have $k[X] = k[T_1, T_2]/(T_2^2 - T_1^3) \simeq k[T^2, T^3]$ which is not an integrally closed domain in its field of fractions $k(T^2, T^3) = k(T)$. Indeed, $X^2 - T^2 = 0$ is an equation of integral dependence of T over $k[T^2, T^3]$, but $T \notin k[T^2, T^3]$. In fact, the integral closure of $k[T^2, T^3]$ in $k(T)$ is $k[T]$.

Theorem 1.7.1 *Let X be a normal variety. Then the ring of regular functions $\mathcal{O}(X)$ is a normal domain.*

Proof. *We know that* $\mathcal{O}(X) = \bigcap_{x \in X} \mathcal{O}_x$. *(intersection taken in* $k(X)$*). Thus, the integral closure of* $\mathcal{O}(X)$ *in* $k(X)$ *is contained in* $\bigcap_{x \in X} \mathcal{O}_x$ *(as each* $\mathcal{O}_x$ *is normal), which is equal to* $\mathcal{O}(X)$.

Remark 1.7.2 *Even if* $\mathcal{O}(X)$ *is a normal domain,* X *need not be normal for general varieties. Indeed, in example 1.7.1, let* $\overline{X}$ *to be the projetive closure of* X. *It is a projective variety, and thus* $\mathcal{O}(X) = k$, *whence it is a normal domain. But, as* X *not a normal variety, then* $\overline{X}$ *cannot be normal.*

Theorem 1.7.2 *Let* X *be nonsingular variety, then* X *is normal.*

Proof. *Let* $x \in X$, *by definition the local ring* $\mathcal{O}_x$ *regular, hence a UFD, hence by example 1.7.1.*

Remark 1.7.3 *There are varieties which have singular points but are still normal. For example* $X := Z(T_1T_2 - T_3^2)$ *is normal and* $\mathcal{O}_{(0,0,0)}$ *is not a regular ring.*

1.8 Divisors in algebra

In this section, we introduce the basic definitions and results concerning divisors in terms of places on rational fields. This will prepare necessary background to give Riemann-Roch result on curves in the next section. Throughout this section k *denotes a field and* E *an extension field of* k.

1.8.1 Places

Definition 1.8.1 *Let* E *be a field and* k *be a subfield of* E. *We say* E/k *is a function field if there is at least one element* $x \in E$ *that is transcendental over* k. *The field* k *is called in this case a constant field of* E. *In case* $E = k(x)$, *we say that* E *is a rational function field (over* k*).*

Notation. *For any field* F *and any vector space* V *over* F, *we denote by* $dim_F(V)$ *or also by* $[V : F]$ *the dimension of* V *over* F.

Definition 1.8.2 *Let* E/k *be a field extension. We say that* E/k *is an algebraic function field in one variable if there exists a transcendental element* x *of* E *over* k *such that* $E/k(x)$ *is a finite extension, i.e.,* $[E : k(x)] < +\infty$. *We call* k *the full constant field of* E.

Now, we introduce the notions of valuation rings and places in this restricted case of a function field extension.

Definition 1.8.3 *Let* E/k *be a function field extension. A valuation ring of the function field* E/k *is a ring* $\mathcal{O} \subseteq E$ *with the following properties :*

i) $k \subsetneq \mathcal{O} \subsetneq E$.

ii) For every $x \in E$, *we have* $x \in \mathcal{O}$ *or* $x^{-1} \in \mathcal{O}$.

Example 1.8.1 *If we take* $E = k(T)$, *i.e., the quotient field of the polynomial ring* $k[T]$, *then given an irreducible monic polynomial* $q(T) \in k[T]$, *we consider the set*

$$\mathcal{O}_{q(T)} := \{\frac{f(T)}{g(T)} \mid f(T), g(T) \in k[T], q(T) \nmid g(T)\}$$

then it is easy to see $\mathcal{O}_{q(T)}$ *is a valuation ring of* $k(T)/k$.

Proposition 1.8.1 *Let* $\mathcal{O}$ *be a valuation ring of a function field extension* E/k *and let* $\tilde{k}$ *be the algebraic closure of* k *in* E. *Then the following hold :*

1) $\mathcal{O}$ *is a local with maximal ideal* $\mathcal{M} := \mathcal{O} \setminus \mathcal{O}^{\times}$*, where* $\mathcal{O}^{\times}$ *the group of units of* $\mathcal{O}$*.*

2) *For every nonzero element* x *of* E*, we have* $x \in \mathcal{M}$ *if and only if* $x^{-1} \in \mathcal{O}$*.*

3) *For the field* $\tilde{k}$*, we have* $\tilde{k} \subseteq \mathcal{O}$ *and* $\tilde{k} \cap \mathcal{M} = 0$*.*

Proof. 1) *It suffices to see that* $\mathcal{O} \setminus \mathcal{O}^{\times}$ *is an ideal of* $\mathcal{O}$ *(so* $\mathcal{O} \setminus \mathcal{O}^{\times}$ *is the unique maximal ideal of* $\mathcal{O}$*).*

2) *Assume that* $x \in \mathcal{M}$*. If* $x^{-1} \in \mathcal{O}$*, then we would have* $1 = xx^{-1} \in \mathcal{M}$*, which is not true. Conversely, if* $x^{-1} \notin \mathcal{O}$*, then* $x \in \mathcal{O}$ *and* x *is not invertible in* $\mathcal{O}$*, so by the above* $x \in \mathcal{M}$*.*

3) *Let* x *be a nonzero element of* $\tilde{k}$*, and suppose that* $x \notin \mathcal{O}$*, then* $x^{-1} \in \mathcal{O}$*. Since* x^{-1} *also algebraic over* k*, there are elements* $\alpha_1, \ldots, \alpha_m \in k$ *with* $1 + \ldots + \alpha_m(x^{-1})^m = 0$*. Hence* $x^{-1}(\alpha_m(x^{-1})^{m-1} + \ldots + \alpha_1) = -1$*, which implies that* $x = \left(\alpha_m(x^{-1})^{m-1} + \ldots + \alpha_1\right) \in k[x^{-1}] \subseteq \mathcal{O}$ *. So* $x \in \mathcal{O}$*, a contradiction. Therefore,* $\tilde{k} \subseteq \mathcal{O}$*. Since all nonzero invertible elements of* $\tilde{k}$ *are then invertible in* $\mathcal{O}$*, then* $\tilde{k} \cap \mathcal{M} = 0$*.*

Definition 1.8.4 *A valuation of* E/k *is a map* $\mathcal{V} : E \longrightarrow \mathbb{R} \cup \{\infty\}$ *satisfying the following conditions.*

i) $\mathcal{V}(x) = \infty$ *if and only if* $x = 0$*.*

ii) $\mathcal{V}(xy) = \mathcal{V}(x) + \mathcal{V}(y)$ *for all* $x, y \in E$*.*

iii) $\mathcal{V}(x + y) \geq min\{\mathcal{V}(x), \mathcal{V}(y)\}$ *for all* $x, y \in E$*.*

iv) $\mathcal{V}(E^*) \neq \{0\}$*.*

v) $\mathcal{V}(a) = 0$ *for all* $a \in k^*$*.*

Remarks 1.8.1 i) *The symbol* ∞ *means some element not in* $\mathbb{R}$ *such that* $\infty + \infty = \infty + m = m + \infty = \infty$*, and* $\infty > n$ *for all* $m, n \in \mathbb{R}$*.*

ii) *Note that if* $\mathcal{V}(x) \neq \mathcal{V}(y)$*, we have* $\mathcal{V}(x + y) = min\{\mathcal{V}(x), \mathcal{V}(y)\}$*.*

iii) *If the image* $\mathcal{V}(E^*)$ *is a discrete set in* $\mathbb{R}$*, then* $\mathcal{V}$ *is called discrete valuation. If* $\mathcal{V}(E^*) = \mathbb{Z}$*, then* $\mathcal{V}$ *is called normalized.*

Two discrete valuations $\mathcal{V}$ *and* $\mathcal{V}'$ *of* E/k *are called equivalent if there exists a constant* $\lambda > 0$ *such that*

$$\mathcal{V}(x) = \lambda \mathcal{V}'(x) \text{ for all } x \in E^*.$$

One can easily to see that this an equivalence relation between the discrete evaluations of E/k*. An equivalence class of discrete valuation of* E/k *is called a place of* E/k*.*

If $\mathcal{V}$ *is a discrete valuation of* E/k*, then* $\mathcal{V}(E^*)$ *is a nonzero discrete subgroup of* $(\mathbb{R}, +)$*, and so we have* $\mathcal{V}(E^*) = c\mathbb{Z}$ *for some positive* $c \in \mathbb{R}$*. Thus, there exists a uniquely determined normalized valuation of* E *that is equivalent to* $\mathcal{V}$*. In other words, every place* P *of* E/k *contains a uniquely determined normalized valuation of* E/k*, which is denoted by* $\mathcal{V}_P$*. Thus, we can identify places of* E/k *and (discrete) normalized valuations of* E/k*.*

For the normalized valuation $\mathcal{V}_P$ *of* E/k *we have* $\mathcal{V}_P(E^*) = \mathbb{Z}$*. Thus, there exists an element* $\alpha \in E$ *satisfying* $\mathcal{V}_P(\alpha) = 1$*. Such an element* α *is called a local parameter (or uniformizing parameter) of* E *at the place* P*.*

Definition and Notation 1.8.1 1) $\mathbb{P}_E := \{P \mid P \text{ is a place of } E/k\}$*.*

2) *For a place P of E/k, we set*

$$\mathcal{O}_P := \{x \in E \,|\, \mathcal{V}_P(x) \geq 0\}.$$

We call $\mathcal{O}_P$ the valuation ring of the place P.

Proposition 1.8.2 *Let $P \in \mathbb{P}_E$, the valuation ring $\mathcal{O}_P$ has a unique maximal ideal given by*

$$\mathcal{M}_P := \{x \in E \,|\, \mathcal{V}_P(x) \geq 1\}$$

Proof. *One can easily see that $\mathcal{M}_P$ is an ideal of $\mathcal{O}_P$. Since $1 \in \mathcal{O}_P \setminus \mathcal{M}_P$, we obtain that $\mathcal{M}_P$ is a proper ideal. It remains to show that any proper ideal I of $\mathcal{O}_P$ is contained in $\mathcal{M}_P$. Let $x \in I$ and suppose that $\mathcal{V}_P(x) = 0$. Then $\mathcal{V}_P(x^{-1}) = -\mathcal{V}_P(x) = 0$, and so $x^{-1} \in \mathcal{O}_P$. Thus, $1 = xx^{-1} \in I$ and, hence, $I = \mathcal{O}_P$ a contradiction. Therefore, $\mathcal{V}_P(x) \geq 1$ and $I \subseteq \mathcal{M}_P$.*

*It is also necessary to understand some of the next result to recall that every valuation of a function field in one variable is discrete (see [19, Theorem 1.5.12, p.**19**]).*

Definition 1.8.5 *Let $P \in \mathbb{P}_E$, $\mathcal{O}_P$ its corresponding valuation ring and $\mathcal{M}_P$ the maximal ideal of $\mathcal{O}_P$. The field $E_P := \mathcal{O}_P/\mathcal{M}_P$ is called the residue class field of P. The canonical map, denoted $x \longmapsto \overline{x}_P$ (make this notation throughout the rest for the residue map images), from E to E_P is called the residue class map with respect to P. The degree of P, denoted $deg(P)$, is the dimension $[E_P : k]$. We say that P is a rational place of E/k if $deg(P) = 1$.*

Lemma 1.8.1 *For any place P of E/k, the residue field E_P is a finite extension of k, hence the degree of P is finite.*

Proof. *See [19, Theorem 1.5.13, p.**20**].*

Corollary 1.8.1 *The field $\tilde{k}$ of constants of E/k is a finite field extension of k.*

Proof. *Choose some $P \in \mathbb{P}_E$. Since $\tilde{k}$ can be embedded into E_P via the residue class map, then $[\tilde{k} : k] \leq [E_P : k] < \infty$.*

Proposition 1.8.3 *Let E/k be a function field, R be a subring of E with $k \subsetneq R$ and J a nonzero ideal of R. Suppose that J is a proper ideal of R, then there is a place $P \in \mathbb{P}_E$ that $J \subseteq \mathcal{M}_P$ and $R \subseteq \mathcal{O}_P$.*

Proof. *See [29, Theorem 1.1.19, p.**7**].*

Remark 1.8.1 *Recall that if E/k is a function field in one variable, then by proposition 1.8.3 above that the set $\mathbb{P}_E$ is nonempty.*

Definition 1.8.6 *Let $P \in \mathbb{P}_E$ and $x \in E$.*

i) *We say that P is a zero of x if $\mathcal{V}_P(x) > 0$.*

ii) *We say that P is a pole of x if $\mathcal{V}_P(x) < 0$.*

iii) *If $\mathcal{V}(x) = n > 0$, we say that P is a zero of x of order n.*

iv) *If $\mathcal{V}_P(x) = -n < 0$, we say that P is a pole of x of order n.*

Corollary 1.8.2 *Let E/k be a function field and x an element of E that is transcendental over k. Then x has at least one zero and one pole.*

Proof. *Let $x \in E$. Let $R = k[x]$, and the ideal $J = xk[x]$. By proposition 1.8.3 there exists a place $P \in \mathbb{P}_E$ with $x \in \mathcal{M}_P$, hence P is a zero of x. The same argument proves that x^{-1} has a zero $P' \in \mathbb{P}_E$. So P' is a pole of x.*

Lemma 1.8.2 *(Approximation Theorem). Let E/k be a function field in one variable, $P_1, \dots, P_m$ be distinct places of E/k, $x_1, \dots, x_m \in E$ and $n_1, \dots, n_m$ be integers. Then there is some $x \in E$ such that*

$$\mathcal{V}_{P_i}(x - x_i) = n_i \text{ for } i = 1, \dots, m.$$

Proof. *See [19, Theorem 1.5.18, p.22].*

Corollary 1.8.3 *Let E/k be a function field in one variable. Then E/k has infinitely many places.*

Proof. *Suppose there are only finitely many places, say $P_1, \dots, P_m$. By lemma 1.8.2 we can find a nonzero element $x \in E$ with $\mathcal{V}_{P_i}(x) > 0$ for $i = 1, \dots, m$. Then x is transcendental over x, since it has zeros. But x has no pole, this is a contradiction to Corollary 1.8.2.*

1.8.2 Divisors

As previously said in the introduction, divisors in algebraic geometry are in extension of divisors in number field theory. They reveal a large amount of information about the variety in question. In this section, we define a divisor in terms of places of the considered function field in one variable. In the next section, considering a curve over an algebraically closed field, the function field of this curve will be a function field in one variable, and hence one can translate the definitions and results given here to this geometric case. Many results in the rest of this chapter will allow to retrieve information about zeros, poles and the structure of functions defined on the variety through the use of divisors. In this paragraph, E/k will always denote an algebraic function field in (always replace in the rest function field of one variable by function field in one variable) one variable such that k is the full constant field of E/k.

Definition 1.8.7 *The divisor group of E/k is defined as the (additively written) free abelian group which is generated by the places of E/k, it is denoted by $Div(E)$. The elements of $Div(E)$ are called divisors of E/k. In other words, a divisor is a formal sum*

$$D = \sum_{P \in \mathbb{P}_E} n_P P.$$

where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many n_P.
A divisor of the form $D = P$ with $P \in \mathbb{P}_E$ is called a prime divisor.

Remarks 1.8.2 *i) The addition of divisors is defined component-wise :*

$$\sum_{P \in \mathbb{P}_E} n_P P + \sum_{P \in \mathbb{P}_E} m_P P = \sum_{P \in \mathbb{P}_E} (n_P + m_P) P.$$

ii) For $Q \in \mathbb{P}_E$ and $D = \sum_{Q \in \mathbb{P}_E} n_Q Q \in Div(E)$, we define $\mathcal{V}_Q(D) := n_Q$.

Definition 1.8.8 *(Support of a divisor) Let D be a divisor of E/k. The support of D is defined as*

$$supp(D) := \{P \in \mathbb{P}_E \,|\, n_P \neq 0\}.$$

It is more convenient to write $D = \sum_{P \in supp(D)} n_P P$.

Definition 1.8.9 *(Degree of a divisor) The degree of a divisor is defined as*

$$deg(\sum_{P \in \mathbb{P}_E} n_P P) = \sum_{P \in \mathbb{P}_E} n_P \cdot deg(P) \in \mathbb{Z}.$$

Obviously, the degree is a group homomorphism $deg : Div(E) \longrightarrow \mathbb{Z}$. Its kernel is denoted by

$$Div^0(E) = \{D \in Div(E) \,|\, deg(D) = 0\}.$$

Note that a partial ordering on $Div(E)$ is defined by

$$D \leq D' \Leftrightarrow \mathcal{V}_P(D) \leq \mathcal{V}_P(D') \text{ for all } P \in \mathbb{P}_E.$$

The reflexivity, antisymmetry and transitivity follow directly from the definition.

Remark 1.8.2 *Note that this partial ordering on $Div(E)$ is not total in general. Indeed, If we take $E = \mathbb{F}_q(x)$ and*

$$\begin{cases} P_\infty = \{\frac{f(x)}{g(x)}, f(x), g(x) \in \mathbb{F}_q[x], deg(f(x)) < deg(g(x))\} \\ P_\alpha = P_{x-\alpha} = \{\frac{f(x)}{g(x)}, f(x), g(x) \in \mathbb{F}_q[X], X - \alpha \nmid g(x) \text{ and } X - \alpha | f(x)\} \end{cases}$$

Then $D = 4P_\alpha - 2P_\infty$ and $D' = P_\alpha$ are not comparable

Theorem 1.8.1 *Let E/k be a function field in one variable, $x \in E \setminus k$ and let $P_1, \ldots, P_m$ be zeros of x. Then*

$$\sum_{i=1}^{m} \mathcal{V}_{P_i}(x) \cdot deg(P) \leq [E : k(x)].$$

Proof. *Set $n := [E : k(x)]$. Suppose that*

$$\sum_{i=1}^{m} \mathcal{V}_{P_i}(x) \cdot deg(P_i) > n$$

We have $x \notin k$, so x is not algebraic over k (since k is a full constant subfield of E). We set $n_i = \mathcal{V}_{P_i}(x)$ and $\mathcal{V}_j = \mathcal{V}_{P_i}$ for $1 \leq i \leq m$. Put $\mathcal{O} := \bigcap_{i=1}^{m} \mathcal{O}_i$ where $\mathcal{O}_i = \mathcal{O}_{P_i}$. By lemma 1.8.2 we can choose an element $y_i \in E$ such that $\mathcal{V}_i(y_i) = -1$ with $\mathcal{V}_i(y_i) = 0$ for all j with $1 \leq j \leq m$ with $i \neq j$. Since $[E_{P_i} : k]$ is finite (as k-vector space), then there exist $z_{it} \in \mathcal{O}$, $1 \leq t \leq deg(P_i)$ such that $\{z_{it}(P_i)\}_{1 \leq t \leq deg(P_i)}$ forms a $k-$basis of the residue class field E_{P_i}. In order to arrive at a contradiction, it suffices to show that $z_{it} y_i^j \in E$ $(1 \leq t \leq deg(P_i), 1 \leq j \leq n_i, 1 \leq i \leq m)$ are linearly independent over $k(x)$. Suppose there is a nontrivial combination, then it can be written as :

$$\sum_{i=1}^{m} \sum_{j=1}^{n_i} \eta_{ij} y_i^j + x \sum_{i=1}^{m} \sum_{j=1}^{n_i} \alpha_{ij} y_i^j = 0 \tag{1.10}$$

where $\eta_{ij}, \alpha_{ij} \in \mathcal{O}$, either $\eta_{ij} = 0$ or $\mathcal{V}_{P_i}(\eta_{ij}) = 0$ and the latter case occurs for at least one pair (i, j). Now, let d such that

$$\mathcal{V}_{P_d}(\eta_{ij}) = 0, \text{ for some } j \text{ with } 1 \leq j \leq n_d.$$

Then

$$\mathcal{V}_{P_d}(\sum_{i=1}^{m} \sum_{j=1}^{n_i} \eta_{ij} y_i^j) < 0.$$

and

$$\mathcal{V}_{P_d}(x \sum_{i=1}^{m} \sum_{j=1}^{n_i} \alpha_{ij} y_i^j) \geq 0$$

a contradiction.

Corollary 1.8.4 *Let E/k be a function field in one variable. Then every nonzero element $x \in E$ has only finitely many zeros and poles.*

Proof. *Let x be a nonzero element of E. If $x \in k$, x has neither zeros nor poles. If $x \in E \setminus k$, then x is transcendental over k, so by theorem 1.8.1, the number of zeros is finite. The same argument shows that x^{-1} has only a finite number of zeros, so x has a finite number of poles.*

Definition 1.8.10 *(Effective divisor) A divisor $D = \sum_{P \in \mathbb{P}_E} n_P P$ is called effective (or positive) at P if $n_P \geq 0$ and D is called effective if it is effective at each P.*

Definition 1.8.11 *(Zero divisor, pole divisor and principal divisor) Let $0 \neq x \in E$ and denote by $\mathcal{Z}$ (resp. $\mathcal{P}$) the set of zeros (resp. poles) of x in $\mathbb{P}_E$. Then we define*

i) The zero divisor $(x)_0$ of x by

$$(x)_0 = \sum_{P \in \mathcal{Z}} \mathcal{V}_P(x) P.$$

ii) The pole divisor $(x)_\infty$ of x by

$$(x)_\infty = \sum_{P \in \mathcal{P}} (-\mathcal{V}_P(x)) P.$$

iii) The principal divisor of x by

$$(x) = (x)_0 - (x)_\infty.$$

Remark 1.8.3 *Clearly $(x)_0 \geq 0$, $(x)_\infty \geq 0$ and*

$$(x) = \sum_{P \in \mathbb{P}_E} \mathcal{V}_P(x) P. \tag{1.11}$$

Sometimes the principal divisor of x is denoted by $div(x)$. Obviously, div is a group homomorphism $div : E^* \longrightarrow Div(E)$.

Definition 1.8.12 *The group*

$$\mathcal{P}rinc(E) := \{div(x) \,|\, 0 \neq x \in E\}$$

is called the group of principal divisors of E/k. The quotient group

$$\mathcal{C}l(E) := Div(E)/\mathcal{P}rinc(E)$$

is called the divisor class group of E/k. Two divisors D and D' belonging to the same residue class of $\mathcal{C}l(E)$ are said to be equivalent, we write $D \sim D'$. This means that $D' = D + div(x)$ for some $x \in E \setminus \{0\}$.

1.9 Curves and Riemann-Roch Theorem

In this section we introduce a fundamental space attached to the study of divisors on a function field in one variable, the so-called Riemann-Roch space. A space that is in particular well known in modern geometric coding theoryand also in cryptography. We also introduce the notion of an adèle space and genus of such function field and Weil differentials. As the reader can see, all these notions are part of algebraic number field theory and apply very well in the case of a (smooth) algebraic affine curve via its rational function field.

1.9.1 Curves

Let us start by giving the definition of algebraic curves. Unless otherwise mentioned, we continue to assume in the rest of this chapter that k is an algebraically closed field.

Definition 1.9.1 *Let X be an algebraic variety over k. We say that X is an affine (resp. projective) algebraic curve if $dim(X) = 1$.*

Notation. *Sometimes we will denoted the algebraic curve X over a field k by X/k.*

Example 1.9.1 *Let $f(X, Y)$ be an irreducible polynomial in two indeterminates coefficients in k Then the graph in k^2 which is defined by the equation $f(X, Y) = 0$ is an algebraic curve.*

Let R be a local domain of dimension one with maximal ideal $\mathfrak{m}$ and let $h := R/\mathfrak{m}$. Recall that R is a discrete valuation ring if and only if $dim_h(\mathfrak{m}/\mathfrak{m}^2) = 1$.

Proposition 1.9.1 *Let $X \subseteq \mathbb{A}^n$ be an affine algebraic curve and $x \in X$. Then X is smooth at x if and only if $\mathcal{O}_x$ is a discrete valuation ring.*

Proof. *Note that X is nonsingular at x if and only if the local ring $\mathcal{O}_x$ is regular ring . Moreover, since X is an affine curve, then $dim(\mathcal{O}_x) = dim(X) = 1$ (see theorem 1.3.1 iii)). So X is smooth at x if and only if $\mathcal{O}_x$ is a valuation ring.*

Proposition 1.9.2 *Let X be an affine algebraic curve. Then the set of singular points is a finite proper closed subset of X.*

Proof. *We already saw in theorem 1.5.1 that the set of singular points of X is a proper closed subset of X. It is finite by [19, Theorem 3.1.7, p.**71**].*

Remark 1.9.1 *For more details on nonsingular curves, we refer to [19, Chapter 3].*

1.9.2 Riemann-Roch Theorem

In this subsection, we fix an algebraic function field in one variable E/k. As the reader can see, most results in this section do not need the field k to be algebraically closed. Nevertheless, since k is a full constant field of E, then k is algebraically closed in E.

The vector space $\mathcal{L}(D)$

Let D be a divisor of E/k, let

$$\mathcal{L}(D) := \{x \in E^* \mid div(x) + D \geq 0\} \cup \{0\}.$$

One can easily see that $\mathcal{L}(D)$ is a k-vector space. This space is called Riemann-Roch Space. It dimension over k will be denoted by $l(D)$, i.e., $l(D) := dim_k(\mathcal{L}(D))$.
For any divisor of E, we have $x \in \mathcal{L}(D)$ if and only if $\mathcal{V}_P(x) \geq -\mathcal{V}_P(D)$ for all $P \in \mathbb{P}_E$.

Proposition 1.9.3 *Let D, $D^{'}$ be two divisor of E/k. Then :*

1) *For the zero divisor 0, we have $\mathcal{L}(0) = k$, and $l(0) = 1$.*

2) *If $D \leq D^{'}$, then $\mathcal{L}(D)$ is a subspace of $\mathcal{L}(D^{'})$ and $dim_k(\mathcal{L}(D^{'})/\mathcal{L}(D)) \leq deg(D^{'}) - deg(D)$.*

3) *If $D \geq 0$, then $l(D) \geq 1$.*

4) *$l(D)$ is finite for all D.*

5) *For any element $x \in E$, we have $l(D + div(x)) = l(D)$.*

Proof. 1) *For any $x \in k^*$, we have $div(x) = 0$. So $div(x) + 0 \geq 0$, then $k \subseteq \mathcal{L}(D)$. Conversely, if $x \in \mathcal{L}(D) \setminus \{0\}$, then $div(x) \geq 0$. This means that has no pole, so $x \in k$ by corollary 1.8.2. Moreover, $l(0) = dim_k(\mathcal{L}(0)) = dim_k(k) = 1$.*

2) *Assume that $D \leq D'$, let $x \in \mathcal{L}(D)$, then $div(x) + D' = div(x) + D + (D' - D) \geq 0$. So $x \in \mathcal{L}(D')$. For the second assertion we can assume that $D' = D + P$ for some $P \in \mathbb{P}_E$, the general case follows then by induction. Choose an element $x_0 \in E$ with $\mathcal{V}_P(x_0) = \mathcal{V}_P(D') = \mathcal{V}_P(D) + 1$. For $x \in \mathcal{L}(D')$ we have $\mathcal{V}_P(x) \geq -\mathcal{V}_P(D') = -\mathcal{V}_P(x_0)$, so $xx_0 \in \mathcal{O}_P$. Thus we obtain a k-linear map*

$$\begin{array}{rccc} \Phi : & \mathcal{L}(D') & \longrightarrow & E_P \\ & x & \longmapsto & \overline{xx_0}_P \end{array}$$

For an element $x \in E$, we have $x \in ker(\Phi)$ if and only if $\mathcal{V}_P(xx_0) > 0$, i.e., $\mathcal{V}_P(x) \geq -\mathcal{V}_P(D)$. Hence $ker(\Phi) = \mathcal{L}(D)$ and Φ induce a k-linear injective mapping from$\mathcal{L}(D')/\mathcal{L}(D)$ to E_P. So $dim_k(\mathcal{L}(D')/\mathcal{L}(D)) \leq dim(E_P) = deg(P) = deg(D') - deg(D)$.

3) *By 1) and 2) we know that $k = \mathcal{L}(0)$ is a subspace of $\mathcal{L}(D)$. So $1 = l(0) \leq l(D)$.*

4) *Assume that $D \geq 0$. Then applying 1) and 2), we get $l(D) = dim_k(\mathcal{L}(D)/\mathcal{L}(0)) + 1 \leq deg(D) + 1$. So $l(D) < +\infty$. If D is arbitrary, then it suffices to consider some positive divisor D' such that $D \leq D'$ and to conclude.*

5) *Let $D \in Div(E)$ and let $x \in E$. Then one can easily see that $\mathcal{L}(D) = x\mathcal{L}(D + div(x))$. Since $x\mathcal{L}(D + div(x))$ and $\mathcal{L}(D + div(x))$ have the same dimension over k, then we have $l(D + div(x)) = l(D)$.*

Remark 1.9.2 *5) implies that if D' is a divisor equivalent to D, then $l(D) = l(D')$.*

Lemma 1.9.1 *Let $D \in div(E)$, if $D = D_+ - D_-$ with positive divisors D_+ and D_-, then*

$$l(D) \leq deg(D_+) + 1$$

Proof. *Since $\mathcal{L}(D) \subseteq \mathcal{L}(D+)$, it is sufficient to show that*

$$l(D_+) \leq deg(D_+) + 1.$$

But this by what we have already shown (See the proof of 4) in proposition 1.9.3.

Remark 1.9.3 *It follows by the above lemma that if $D \geq 0$, then we have*

$$l(D) \leq deg(D) + 1 \tag{1.12}$$

Proposition 1.9.4 *All principal divisors have degree zero. More precisely, let $x \in E \setminus k$, then we have*

$$deg((x)_0) = deg((x)_\infty) = [E : k(x)]$$

Proof. *Set $m := [E : k(x)]$ and $D := (x)_\infty = \sum_{i=1}^r -\mathcal{V}_{P_i}(x)P_i$ where $P_1, \ldots, P_r$ are all the pole of x. Then $deg(D) = \sum_{i=1}^r \mathcal{V}_{P_i}(x^{-1}) \cdot deg(P_i) \leq [E : k(x)]$ (see theorem 1.8.1). Conversely, let $m := [E : k(x)]$ and let's show that $m \leq deg(D)$. For this let's choose a basis $\beta_1, \ldots, \beta_m$ of $E/k(x)$ and a divisor $G \geq 0$ such that $div(\beta_i) \geq -G$ for $i = 1, \ldots, m$. We have*

$$l(tD + G) \geq m(t + 1) \text{ for all } t \geq 0.$$

which follows immediately from the fact $x^i\beta_j \in \mathcal{L}(tD+G)$ *for* $i = 0,\ldots,r$, $j = 0,\ldots,m$. *Set* $d = deg(G)$, *we get* $m(t+1) \leq l(tD+G) \leq tdeg(D) + d + 1$ *by lemma 1.9.1. Thus*

$$t(deg(D) - m) \geq m - d - 1 \tag{1.13}$$

for all $t \in \mathbb{N}$, *the right hand side of (1.13) is independent of* t, *therefore (1.13) is possible only when* $deg(D) \geq m$. *We have thus proved that* $deg((x)_\infty) = [E : k(x)]$. *Since* $(x)_0 = (x^{-1})_\infty$, *we conclude that* $deg((x)_0) = deg((x^{-1})_\infty) = [E : k(x^{-1})] = [E : k(x)]$.

Corollary 1.9.1 *If* $deg(D) < 0$, *then* $l(D) = 0$.

Proof. *Assume that* $deg(D) < 0$ *and suppose that there is some nonzero* $x \in \mathcal{L}(D)$, *then by definition* $deg(div(x) + D) \geq 0$, *but by applying proposition 1.9.4 and the fact that deg is a group homomorphism, we have* $deg(div(x) + D) = deg(D)(< 0)$. *It follows then that* $\mathcal{L}(D) = \{0\}$, *so* $l(D) = 0$.

Adèles

Most results here are true for an arbitrary function field E/k.

Definition 1.9.2 *An adèle of* E/k *is a mapping*

$$\begin{array}{rccc} \beta : & \mathbb{P}_E & \longrightarrow & E \\ & P & \longmapsto & \beta_P \end{array}$$

such that $\beta_P \in \mathcal{O}_P$ *for all but a finite number of* $P \in \mathbb{P}_E$. *We may regard an adèle as an element of the direct product* $\prod_{P\in\mathbb{P}_E} E$ *and therefore use the notation* $\beta = (\beta_P)_{P\in\mathbb{P}_E}$.
The set

$$\mathbb{A}_E := \{\beta \,|\, \beta \text{ is an adèle of } E/k\}$$

is called the adèle space of E/K. *The principal adèle of an element* $x \in E$ *is the adèle whose components are equal to* x. *This gives the diagonal embedding* $x \longmapsto (x, x, x, \ldots)$, *from* E *to* $\mathbb{A}_E$.

Remarks 1.9.1 *i)* $\mathbb{A}_E$ *is a vector space over* k.

ii) The valuations $\mathcal{V}_P$ *of* E/k *extend naturally to* $\mathbb{A}_E$ *by setting* $\mathcal{V}_P(\beta) := \mathcal{V}_P(\beta_P)$ *(where* β_P *is the* P*-component of the adèle* β*). By definition 1.9.2* $\mathcal{V}_P(\beta) \geq 0$ *for all but finitely many* $P \in \mathbb{P}_E$.

Definition 1.9.3 *For any divisor* $D = \sum_{P\in\mathbb{P}_E} n_P P$, *we define*

$$\mathbb{A}_E(D) := \{\beta \in \mathbb{A}_E \,|\, \mathcal{V}_P(\beta) + \mathcal{V}_P(D) \geq 0 \text{ for all } P \in \mathbb{P}_E\}.$$

Obviously this is a k-subspace of $\mathbb{A}_E$.

For divisors $D = \sum_{P\in\mathbb{P}_E} n_P P$ *and* $D' = \sum_{P\in\mathbb{P}_E} m_P P$, *we define* $min\{D, D'\} := \sum_{P\in\mathbb{P}_E} min\{n_P, m_P\}P$, *and* $max\{D, D'\} := \sum_{P\in\mathbb{P}_E} max\{n_P, m_P\}P$

Proposition 1.9.5 *Let* $D = \sum_{P\in\mathbb{P}_E} n_P P$ *and* $D' = \sum_{P\in\mathbb{P}_E} m_P P$. *Then, the following statements hold:*

1) *If* $D \leq D'$, *then* $\mathbb{A}_E(D) \subseteq \mathbb{A}_E(D')$ *and*

$$dim_k(\mathbb{A}_E(D')/\mathbb{A}_E(D)) = deg(D') - deg(D).$$

2) $\mathbb{A}_E(min\{D, D'\}) = \mathbb{A}_E(D) \cap \mathbb{A}_E(D')$.

3) $\mathbb{A}_E(max\{D, D'\}) = \mathbb{A}_E(D) + \mathbb{A}_E(D')$.

Proof. 1) *If $D \leq D'$, then by definition, $m_P \geq n_P$ for all P. Let $(\beta_P)_{\mathbb{P}_E} \in \mathbb{A}_E(D)$ then*

$$\mathcal{V}_P(\beta_P) + m_P \geq \mathcal{V}_P(\beta_P) + n_P \geq 0, \text{ for all } P \in \mathbb{P}_E.$$

Thus $(\beta_P)_{P\in\mathbb{P}_E} \in \mathbb{A}_E(D')$, which shows that $\mathbb{A}_E(D) \subseteq \mathbb{A}_E(D')$. Let's prove the rest by induction on $deg(D') - deg(D)$.

- *If $deg(D') = deg(D)$, then necessarily $D = D'$ (for $D \leq D'$), so $\mathbb{A}_E(D') = \mathbb{A}_E(D)$, hence $\mathbb{A}_E(D')/\mathbb{A}_E(D) = \{0\}$.*
- *For the rest of the induction, it suffices to consider the case where $deg(D') - deg(D) = 1$, $D' = D + P$ for some place P. Choose $x_0 \in E$, with $\mathcal{V}_P(x_0) = \mathcal{V}_P(D') = \mathcal{V}_P(D) + 1$ and consider the $k-$linear map $\Phi : \mathbb{A}_E(D') \longrightarrow E_P$ defined by $\beta \longmapsto \overline{x_0\beta_P}_P$, which is surjective with kernel $ker(\Phi) = \mathbb{A}_E(D)$, and so*

$$dim_k(\mathbb{A}_E(D')/\mathbb{A}_E(D)) = dim_k(E_P) = deg(P) = 1.$$

2) *Since $min\{D, D'\} \leq D, D'$, then by 1), $\mathbb{A}_E(min\{D, D'\}) \subseteq \mathbb{A}_E(D) \cap \mathbb{A}_E(D')$. Conversely, if $(\beta) \in \mathbb{A}_E(D)$ and $(\beta_P) \in \mathbb{A}_E(D')$, then for any $P \in \mathbb{P}_E$,*

$$\mathcal{V}_P(\beta_P) + n_P \geq 0 \text{ and } \mathcal{V}_P(\beta_P) + m_P \geq 0$$

Thus, we have

$$\mathcal{V}_P(\beta_P) + min\{n_P, m_P\} \geq 0.$$

Therefore

$$\mathbb{A}_E(D) \cap \mathbb{A}_E(D') = \mathbb{A}_E(min\{D, D'\}).$$

3) *We have $D, D' \leq max\{D, D'\}$, so by 1), $\mathbb{A}_E(D) + \mathbb{A}_E(D') \subseteq \mathbb{A}_E(max\{D, D'\})$. Conversely, for $(\beta_P) \in \mathbb{A}_E(D)$, $(\alpha_P) \in \mathbb{A}_E(D')$, if $\beta_P = -\alpha_P$ then one can conclude easily. For arbitrary case, we have $\mathcal{V}_P(\beta_P + \alpha_P) \geq min\{\mathcal{V}_P(\beta_P), \mathcal{V}_P(\alpha_P)\}$. Thus for all places P,*

$$\mathcal{V}_P(\beta_P + \alpha_P) + max\{n_P, m_P\} \geq min\{\mathcal{V}_P(\beta_P), \mathcal{V}_P(\alpha_P)\} + max\{n_P, m_P\}$$

and

$$min\{\mathcal{V}_P(\beta_P), \mathcal{V}_P(\alpha_P)\} + max\{n_P, m_P\} \geq 0.$$

Lemma 1.9.2 *Let D, D' be two divisor of E/k, if $D \leq D'$. Then*

$$dim_k\big((\mathbb{A}_E(D') + E)/(\mathbb{A}_E(D) + E)\big) = \big(deg(D') - l(D')\big) - \big(deg(D) - l(D)\big).$$

Proof. *We have an exact sequence of linear mappings*

$$0 \longrightarrow \mathcal{L}(D')/\mathcal{L}(D) \xrightarrow{\gamma_1} \mathbb{A}_E(D')/\mathbb{A}_E(D) \xrightarrow{\gamma_2} (\mathbb{A}_E(D') + E)/(\mathbb{A}_E(D) + E) \longrightarrow 0$$

γ_1, γ_2 are defined in the obvious manner. The only nontrivial assertion is that the kernel of γ_2 is contained in the image of γ_1. In order to prove this let $\beta \in \mathbb{A}_E(D')$ with $\gamma_2(\beta + \mathbb{A}_E(D)) = 0$. Then $\beta \in \mathbb{A}_E(D) + E$, so there is some $x_0 \in E$ with $\beta - x_0 \in \mathbb{A}_E(D)$. As $\mathbb{A}_E(D) \subseteq \mathbb{A}_E(D')$. We conclude that $x_0 \in \mathbb{A}_E(D') \cap E = \mathcal{L}(D')$. Therefore $\beta + \mathbb{A}_E(D) = x_0 + \mathbb{A}_E(D) = \gamma_1(x_0 + \mathcal{L}(D))$ lies in the image of γ_1. From the exactness of the above sequence, we get that

$$\begin{aligned} dim_k\big((\mathbb{A}_E(D') + E)/\mathbb{A}_E(D) + E)\big) &= dim_k\big(\mathbb{A}_E(D')/\mathbb{A}_E(D)\big) - dim_k\big(\mathcal{L}(D')/\mathcal{L}(D)\big) \\ &= \big(deg(D') - l(D')\big) - \big(deg(D) - l(D)\big). \end{aligned}$$

In the second equality here, we used proposition 1.9.5 1).

For any divisor D of E/k, we define

$$r(D) := deg(D) - l(D).$$

We obtain a map $r : Div(E) \longrightarrow \mathbb{Z}$. We have then the following lemma :

Lemma 1.9.3 *Let $x \in E^*$ and D, D' be two divisors on E. The following statements hold :*

i) *If $D \leq D'$, then $r(D) \leq r(D')$*

ii) *$r(div(x) + D) = r(D)$.*

Proof. i) *This follows from lemma 1.9.2.*

ii) *By proposition 1.9.3 5)*

$$l(D + div(x)) = l(D).$$

Moreover, we have $deg(div(x) + D) = deg(D) + deg(div(x))$ and by proposition 1.9.4 $deg(div(x)) = 0$. So $r(div(x) + D) = deg(D) - l(D)$.

Proposition 1.9.6 *Let E/k be an algebraic function field, $r(D)$ has an upper bound, when D describes the divisors of E/k.*

Proof. *See [22, Theorem 4.10, p.**15**].*

Genus and the Riemann's theorem

Definition 1.9.4 *(genus) Let E/k be a function field in one variable, the genus of E is defined as*

$$g := 1 + max_D(r(D)).$$

i.e., g is the last integer for which

$$deg(D) - l(D) \leq g - 1.$$

holds for any divisor D of E/k.

Proposition 1.9.6 (with this definition) gives a proof to the following famous Riemann's Theorem.

Theorem 1.9.1 *Let E/k be an algebraic function field, then there exists a nonnegative integer g depending only on E such that*

$$l(D) \geq deg(D) + 1 - g \tag{1.14}$$

for every divisor D of E.

Proof. *Clear.*

Corollary 1.9.2 *There exists an integer c depending only on E such that*

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

for any divisor D of E/k satisfying $deg(D) \geq c$.

Proof. *Let D and D_0 be two divisors of E/k with $g = 1 + r(D_0)$. Set $c := deg(D_0) + g$. If $deg(D) \geq c$ and applying theorem 1.9.1 we obtain*

$$l(D - D_0) \geq deg(D - D_0) + 1 - g \geq c - deg(D_0) + 1 - g = 1.$$

Thus there exists a non-zero element z in $\mathcal{L}(D - D_0)$. Let the divisor $D' := div(z) + D$, which $\geq D_0$. We have

$$\begin{aligned} deg\ (D) - l(D) &= deg(D) - l(D') \\ &\geq deg(D_0) - l(D_0) = g - 1 \end{aligned}$$

Hence $l(D) \leq deg\ (D) + 1 - g$.

Corollary 1.9.3 *Let D be a divisor such that $deg(D) \geq c$ where c is the constant in corollary 1.9.2, we have*

$$\mathbb{A}_E(D) + E = \mathbb{A}_E.$$

Proof. *By lemma 1.9.2*

$$dim_k\big((\mathbb{A}_E(D^{'}) + E)/\mathbb{A}_E(D) + E)\big) = r(D^{'}) - r(D)$$

for any divisors $D^{'} \geq D$, by corollary 1.9.2 $deg(D) \geq c$ implies $r(D) = g - 1$. Thus if $deg(D^{'})$, $deg(D^{''}) \geq c$, then

$$\mathbb{A}_E(D^{''}) + E = \mathbb{A}_E(D^{'}) + E$$

For any divisor $D = \sum_P n_P P$ with $deg(D) \geq c$ and for any adèle (β_P), define $G := max\big(D, -div(\beta_P)\big)$. Therefore, $G \geq D$, $deg(G) \geq deg(D) \geq c$. By the above we get $\mathbb{A}_E(G) + E = \mathbb{A}_E(D) + E$. We have also $(\beta_P) \in \mathbb{A}_E(-div(\beta_P)) \subseteq \mathbb{A}_E(G) \subseteq \mathbb{A}_E(G) + E = \mathbb{A}_E(D) + E$. If $deg(D)$ is large enough, then any adèle is in $\mathbb{A}_E(D) + E$ and we have $\mathbb{A}_E \supseteq \mathbb{A}_E(D) + E$ since $\mathbb{A}_E(D)$ and E are both subsets of the adèles under the diagonal embedding. Thus

$$\mathbb{A}_E(D) + E = \mathbb{A}_E.$$

In the case of an algebraic function field E/k, we already defined its genus, so by the same way we define the genus of an algebraic nonsingular projective curve as :

Definition 1.9.5 *The genus of a nonsingular projective curve X over k is defined to be the genus of its k-rational function field $k(X)$.*

Chapter 2

Introduction to Schemes

In this chapter we aim to present basic background of scheme theory. The material developed her covers elementary definitions and properties and is oriented in order to prepare necessary tools to understand the meaning of Severi-Brauer varieties in the third chapter. In particular, we will study some local and global properties of schemes like the notions of reduced, integral, regular, normal, separated, proper, projective schemes. We will also study modules over schemes, some cohomological interpretations in scheme theory and introduce Weil and Cartier divisors.

2.1 Generalities on sheaf theory

Sheaves are tools which allow us to keep track of local information on a topological space in a single mathematical object. Their use is ubiquitous throughout algebraic geometry. In this section, we will study their basic theory. We present the notions of presheaf and sheaf on a topological space, that of morphisms of presheaves, as well as their first properties : injectivity and surjectivity, exact sequences. We then study the direct image and inverse image functors, which allow to pass from a sheaf on a topological space to a sheaf on another space and which play a fundamental role in the study of the schemes. Finally, we end with the study of the gluing of bundles

Notation. *Let X be a topological space. We will denote by $\mathcal{T}_X$ the category having for objects the open subsets of X and for morphisms identity maps and inclusions. Also, $\mathcal{C}$ will denote a category, which can be the category of sets (also denoted by $\mathcal{S}et$), that of groups (also denoted by $\mathcal{G}p$), that of R-modules (also dented by $\mathcal{R}$-$\mathcal{M}od$), that of R-algebras (also dented by R-$\mathcal{A}lg$), for some ring R.*

2.1.1 Presheaves

Definition 2.1.1 *Let X be a topological space. A presheaf $\mathcal{F}$ (of sets) on X consists of the following deta:*

i) For every open subset U of X, a set $\mathcal{F}(U)$.

ii) Whenever $U \subseteq V$ are two open subsets of X, a map

$$res_{V,U} : \mathcal{F}(V) \longrightarrow \mathcal{F}(U)$$

called the restriction map, which satisfies the following conditions :

a) $res_{U,U} = id_{\mathcal{F}(U)}$.

b) Having three open subsets $U \subseteq V \subseteq W$ of X, then $res_{V,U} \circ res_{W,V} = res_{W,U}$

Remarks 2.1.1 *1) We will mostly write $s_{|U}$ for s when $s \in \mathcal{F}(U)$. The elements of $\mathcal{F}(U)$ are usually called sections of (the presheaf $\mathcal{F}$) over U.*

2) By considering $\mathcal{F}(U)$ as an object in some category $\mathcal{C}$ and assuming that $res_{V,U}$ is a morphism between the objects $\mathcal{F}(V)$ and $\mathcal{F}(U)$, we may define more generally a presheaf $\mathcal{F}$ on X into $\mathcal{C}$. Note that we can state definition 2.1.1 in the following way : Let X be a topological space. A presheaf $\mathcal{F}$ on X (into a category $\mathcal{C}$) is a contravariant functor from $\mathcal{T}_X$ into $\mathcal{C}$.

$$\begin{array}{rccc} \mathcal{F}: & \mathcal{T}_X & \longrightarrow & \mathcal{C} \\ & U & \longmapsto & \mathcal{F}(U) \end{array}$$

Examples 2.1.1 *1) For a topological space, a presheaf $\mathcal{C}_X$ of $\mathbb{R}$-algebras on X is defined by assigning to every open $U \subseteq X$ the set of continuous functions $U \longrightarrow \mathbb{R}$.*

2) *Let X be a variety, we previously considered the presheaf of k-algebras $\mathcal{O}_X$. For any open $U \subseteq X$, $\mathcal{O}_X(U)$ is the k-algebra of regular functions. If X be an affine variety we have $\mathcal{O}_X(U) = k[U]$.*

3) *Let X be a topological space, the formula :*

$$U \longmapsto \begin{cases} \mathbb{Z} & \text{if} \quad U = X \\ \{0\} & \text{otherwise} \end{cases}$$

defines a presheaf of abelian groups on X.

Although it is possible to define a presheaf of a topological space X into an arbitrary category $\mathcal{C}$, we will be interested in what follows only in cases where the objects of $\mathcal{C}$ are sets (that could have an additional structure) and the morphisms $res_{V,U}$ are maps (which are morphisms for the extra structure on $\mathcal{F}(V)$ and $\mathcal{F}(U)$.

Definition 2.1.2 *Let $\mathcal{F}$ be a presheaf on X, a subpresheaf $\mathcal{G}$ (of $\mathcal{F}$) is a presheaf on X such that $\mathcal{G}(U) \subseteq \mathcal{F}(U)$ for every open $U \subseteq X$, and such that the restriction maps of $\mathcal{G}$ are induced by those of $\mathcal{F}$.*

Example 2.1.1 *If U is an open subset of X, every presheaf $\mathcal{F}$ on X induces, in an obvious way, a presheaf $\mathcal{F}_U$ on U by setting $\mathcal{F}_{|U}(V) = \mathcal{F}(V)$ for every open subset V of U. This is the restriction of $\mathcal{F}$ to U.*

Morphisms of presheaves

Definition 2.1.3 *Let $\mathcal{F}$ and $\mathcal{G}$ be two presheaves on X. A morphism of presheaves ψ from $\mathcal{F}$ to $\mathcal{G}$ consists of the datum, for all open U of X, of a morphism $\psi(U)$ from $\mathcal{F}(U)$ to $\mathcal{G}(U)$, so that the diagram*

$$\begin{array}{ccc} \mathcal{F}(V) & \xrightarrow{\psi(V)} & \mathcal{G}(V) \\ \downarrow{\scriptstyle res_{V,U}} & & \downarrow{\scriptstyle res_{V,U}} \\ \mathcal{F}(U) & \xrightarrow[\psi(U)]{} & \mathcal{G}(U) \end{array}$$

commutes for any pair (U, V) of open subsets of X such that $U \subseteq V$.

Remarks 2.1.2 *i) The commutativity of the diagram is written : $\psi(V)(s)_{|U} = \psi(U)(s_{|U})$, for every $s \in \mathcal{F}(V)$.*

ii) *Morphisms of presheaves can be composed. So that presheaves on the topological space X form a category, that we will denote by $\mathcal{P}reSh_X$.*

iii) *A morphism $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ between two presheaves $\mathcal{F}$ and $\mathcal{G}$ is an isomorphism if it has a two-sided inverse i.e, a morphism $\phi : \mathcal{G} \longrightarrow \mathcal{F}$ such that $\psi \circ \phi = id_{\mathcal{G}}$ and $\phi \circ \psi = id_{\mathcal{F}}$.*

Definition 2.1.4 *Assume $\mathcal{C}$ has direct limits. The stalk of a presheaf $\mathcal{F}$ at a point $x \in X$ is*

$$\mathcal{F}_x := \varinjlim_{x \in U} \mathcal{F}(U)$$

The direct limit is taken over open neighborhoods of x, and restriction maps between them. Given a section $s \in \mathcal{F}(U)$, and a point $x \in U$, we let $s_x \in \mathcal{F}_x$ denote the image of s under the natural morphism

$$\begin{array}{ccc} \mathcal{F}(U) & \longrightarrow & \mathcal{F}_x \\ s & \longmapsto & s_x \end{array}$$

An element of the stalk is called a germ.
More generally, if $Y \subseteq X$ is a closed and irreducible subset. Then, we set

$$\mathcal{F}_Y := \varinjlim_{U \cap Y \neq \emptyset} \mathcal{F}(U)$$

Notation. *Let X be a topological space and $x \in X$, we denote by $\mathcal{V}$ the set of open neighborhoods of x, which is filtering for the opposite order to inclusion i.e, for all $U, V \in \mathcal{V}$ we have*

$$U \leq V \Longleftrightarrow V \subseteq U.$$

Remark 2.1.1 *We can identify $\mathcal{F}_x$ as the quotient of the set of pairs (U, s), where $U \in \mathcal{V}$ and where s is a section of $\mathcal{F}$ on U, by the relation of equivalence defined as follows :*

$(U, s) \sim (V, t)$ *if and only if there exists an open neighborhood W of x in $U \cap V$ such that $s_{|W} = t_{|W}$.*

Moreover, we can see $\mathcal{F}_x$ as the set of sections of $\mathcal{F}$ defined in the neighborhood of x. Two sections belonging to $\mathcal{F}_x$ being considered as equal if they coincide in some neighborhood of x.

Example 2.1.2 *Let $\mathcal{F}(U) = \{$ continuous functions $U \longrightarrow \mathbb{R}\}$. Then $\mathcal{F}_x$ the set of germs of continuous functions at x.*

Proposition 2.1.1 *Let $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ be a morphism of presheaves, then ψ induces for every point $x \in X$ a morphism $\psi_x : \mathcal{F}_x \longrightarrow \mathcal{G}_x$ between the stalks, where ψ_x is defined by $\psi_x(s_x) = \big(\psi(U)(s)\big)_x$ for any open subset U of X, $s \in \mathcal{F}(U)$, and $x \in U$.*

Proof. *If $s \in \mathcal{F}(U)$ and $t \in \mathcal{F}(V)$ are such that $s_x = t_x$, then there exists an open neighborhood W of x such that $s_{|W} = t_{|W}$. So $\psi(U)(s)_{|W} = \psi(W)(s_{|W})$ and $\psi(V)(t)_{|W} = \psi(V)(t_{|W})$. Hence $\big(\psi(U)(s)\big)_x = (\psi(V)(t))_x$.*

Note that if $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ and $\phi : \mathcal{G} \longrightarrow \mathcal{Z}$ are two morphisms of sheaves we have $(\psi \circ \phi)_x = \psi_x \circ \phi_x$ and $(id_{\mathcal{F}})_x = id_{\mathcal{F}_x}$. Moreover, $\psi \longrightarrow \psi_x$ define a functor from the category of sheaves over X to the category $\mathcal{C}$.

Definition 2.1.5 *Let $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ be a morphism of presheaves*

i) *We say that ψ is injective if for any open subset U of X, $\psi(U) : \mathcal{F}(U) \longrightarrow \mathcal{G}(U)$ is injective.*

ii) *We say that ψ is surjective if for all $x \in X$, $\psi_x : \mathcal{F}_x \longrightarrow \mathcal{G}_x$ is surjective.*

2.1.2 Sheaves

Definition 2.1.6 *We say that a* ***presheaf*** $\mathcal{F}$ *is a sheaf if we have the following properties :*

i) *(Uniqueness) Let U be an open subset of X, $s \in \mathcal{F}(U)$, $\{U_i\}_{i\in I}$ a covering of U by open subsets U_i. If $s_{|U_i} = 0$ for every $i \in I$, then $s = 0$.*

ii) *(Gluing axiom) If $U = \bigcup_{i\in I} U_i$, and if $s_i \in \mathcal{F}(U_i)$ is a collection of sections matching on the overlaps; that is, they satisfy*
$$s_{i|U_i\cap U_j} = s_{j|U_i\cap U_j}$$
for all $i, j \in I$, then there exists a section $s \in \mathcal{F}(U)$ so that $s_{|U_i} = s_i$, for all $i \in I$

Remarks 2.1.3 *1) When $\mathcal{F}$ is a presheaf of groups or of an algebraic structure that is in particular a group, we can replace i) by : for all $s, t \in \mathcal{F}(U)$ such that for $i \in I$, $s_{|U_i} = t_{|U_i}$ then $s = t$.*

2) The section s in ii) is unique by condition i).

Examples 2.1.2 *1) Let X be a topological space and $\mathcal{F} : U \longmapsto \mathcal{C}^0(U, \mathbb{R})$ the correspondence that assigns to $\mathcal{U}$ the $\mathbb{R}$-algebra of continuous maps from U to $\mathbb{R}$, then $\mathcal{F}$ a sheaf of $\mathbb{R}$-algebras over X.*

2) In example 2.1.1, if moreover, $\mathcal{F}$ is a sheaf then $\mathcal{F}_{|U}$ is still a sheaf.

Morphisms of sheaves

Definition 2.1.7 *A morphism of sheaves is just a morphism of the underlying presheaves.*

Remarks 2.1.4 *1) The sheaves of X form a full subcategory $\mathcal{S}h_X$ of the category of the presheaves on X.*

2) The notions injective, surjective and isomorphism for sheaves are defined in the same way as for presheaves.

Lemma 2.1.1 *Let X be a topological space and let U be an open subset of X.*

i) *Let $\mathcal{F}$ be a sheaf on X and let $s, t \in \mathcal{F}(U)$ be two sections such that $s_x = t_x$ for every $x \in U$. Then $s = t$.*

ii) *Let $\mathcal{F}, \mathcal{G}$ be presheaves on X and let $\psi, \phi : \mathcal{F} \longrightarrow \mathcal{G}$ be morphisms of presheaves on X such that $\mathcal{F}_x = \mathcal{G}_x$ for every $x \in X$. If $\mathcal{G}$ is a sheaf, then $\mathcal{F} = \mathcal{G}$.*

Proof. *i) Let $x \in U$, since $s_x = t_x$, there exists an open subset W_x of U containing x such that $s_{|W_x} = t_{|W_x}$. Since $(W_x)_x$ is an open covering of U, according to condition i) in definition 2.1.6, it comes that $s = t$.*

ii) Let W be an open subset of X and let $s \in \mathcal{F}(W)$. We need to prove that s has the same image under the maps $\psi(W)$ and $\phi(W)$, let $t = \psi(U)(s)$ and $l = \phi(U)(s)$. For all $x \in W$, we have $t_x = \psi_x(s_x) = \phi_x(s_x) = l_x$. Since $\mathcal{G}$ is a sheaf, then by i) we get that $t = l$.

In what follows, we consider (pre)sheaves of objects with algebraic structures which in particular are groups.

Proposition 2.1.2 *Let $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ be a morphism of sheaves. Then ψ is injective if and only if $\psi_x : \mathcal{F}_x \longrightarrow \mathcal{G}_x$ is injective for every $x \in X$.*

Proof. *Suppose ψ is injective. Let $x \in X$ and $s_x \in \mathcal{F}_x$ such that $\psi_x(s_x) = 0$, where $s \in \mathcal{F}(U)$ and U is an open neighborhood of x, so $\big(\psi(U)(s)\big)_x = 0$. Then, there exists an open neighborhood W of x such that $\psi(U)(s)_{|W} = 0$ or that $\psi(W)(s_{|W}) = 0$. From the injectivity of ψ it comes that $s_{|W}$, thus $s_x = 0$. Conversely, suppose that for all $x \in X$, ψ_x is injective, we fix an open subset V of X and $s \in \mathcal{F}(V)$ such that $\psi(V)(s) = 0$, locally we have, for all $x \in V$, $\psi_x(s_x) = \big(\psi(U))(s)\big)_x = 0$, it comes from local injectivity, that for all $x \in V$, $s_x = 0$. Hence $s = 0$.*

Remark 2.1.2 *Proposition 2.1.2 gives a local characterization of the injectivity.*

Theorem 2.1.1 *Let $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ be a morphism of sheaves. The following assertions are equivalent :*

i) ψ is an isomorphism.

ii) For every $x \in X$, $\psi_x : \mathcal{F}_x \longrightarrow \mathcal{G}_x$ is an isomorphism.

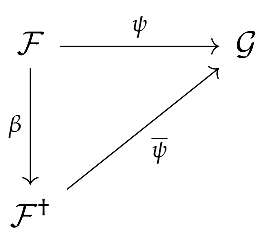
iii) ψ is both injective and surjective.

Proof. *i) $\Rightarrow$ ii) Let ϕ be the inverse morphism of ψ. Plainly, for every $x \in X$, we have $\phi_x \circ \psi_x = id_{\mathcal{F}_x}$ and $\psi_x \circ \phi_x = id_{\mathcal{G}_x}$. So ψ_x is an isomorphism.*
ii) $\Rightarrow$ iii) Immediate, according to proposition 2.1.2 and definition 2.1.5 ii)
iii) $\Rightarrow$ i) We will construct the inverse ϕ of ψ. Let W be an open subset of X and $t \in \mathcal{G}(W)$, for every $x \in W$, there exists U_x an open neighborhood of x and $s^x \in \mathcal{F}(U_x)$ such that $t_x = \psi_x(s^x_x) = \big(\psi(U_x)(s^x)\big)_x$. Hence there exists $V_x \subseteq U_x \cap W$ neighborhood of x such that $t_{|V_x} = \big(\psi(V_x)(s^x_{|V_x})\big)_{|V_x}$. If $y \in W$, then $\psi(V_x \cap V_y)(s^x_{|V_x\cap V_y}) = \psi(V_x \cap V_y)(s^y_{|V_x\cap V_y})$, so $s^x_{|V_x\cap V_y} = s^y_{|V_x\cap V_y}$, as the family $(V_x)_{x\in U}$ forms a covering of U, then $(s^x)_x$ rises to a section s of $\mathcal{F}$ on U, and we have $\psi(U)(s) = t$, the uniqueness of s follows from the injectivity of ψ. We set $\phi(U)(t) = s$, then ϕ is the inverse of ψ.

Sheafification

In this paragraph, we answer the following question : How to build a sheaf from a presheaves?

Definition 2.1.8 *Let $\mathcal{F}$ be a presheaf on a topological space X. We call associated sheaf with $\mathcal{F}$ any sheaf $\mathcal{F}^\dagger$ equipped with a morphism of presheaves $\beta : \mathcal{F} \longrightarrow \mathcal{F}^\dagger$ satisfying the following universal property : For any morphism of presheaves $\psi : \mathcal{F} \longrightarrow \mathcal{G}$, where $\mathcal{G}$ is a sheaf, there exists a unique morphism of sheaves $\overline{\psi} : \mathcal{F}^\dagger \longrightarrow \mathcal{G}$ such that the following diagram is commutative :*



Remark 2.1.3 *The uniqueness of $\mathcal{F}^\dagger$ when it exists is an immediate consequence of the universal property.*

Proposition 2.1.3 *Let $\mathcal{F}$ be a presheaf on a topological space X. Then the sheaf $\mathcal{F}^\dagger$ associated with $\mathcal{F}$ exists and is a unique up to isomorphism. Moreover, using the above notation, all $x \in X$, the induced morphism $\beta : \mathcal{F}_x \longrightarrow \mathcal{F}^\dagger_x$ is an isomorphism.*

Proof. *Let $\mathcal{F}$ be a presheaf on X. Consider $Z := \coprod_{x\in X} \mathcal{F}_x$ (disjoint union) and consider the map $\pi : Z \longrightarrow X$ defined by : for all s_x, $\pi(s_x) = x$. For any open V of X and $s \in \mathcal{F}(V)$, let π_s be the map $\pi_s : V \longrightarrow X$ defined by $\pi_s(x) = s_x$. Note that $\pi\big(\pi_s(x)\big) = x$ i.e $\pi \circ \pi_s = id_V$ (π_s is a section and π*

is a retraction). We now endow Z with the topology which makes all maps $\pi_s : V \longrightarrow Z$, V open subset of X and $s \in \mathcal{F}(V)$, continuous.
For any open subset V of X, we define $\mathcal{F}^{\dagger}(V) := \{g : V \longrightarrow Z / g$ continuous and $\pi \circ g = id_V\}$ it is the set of sections of Z on V.

- *For every $W \subseteq V$, the restriction $\mathcal{F}^{\dagger}(V) \longrightarrow \mathcal{F}^{\dagger}(W)$ is the usual restriction, i.e $g \longrightarrow g_{|W}$. In particular $\mathcal{F}^{\dagger}$ is a presheaf.*
- *Condition i) in definition 2.1.6 is immediate.*
- *If $(W_j)_j$ is a covering of V and $g_j \in \mathcal{F}^{\dagger}(W_j)$ are such that for all i, j, $g_{i|W_i \cap W_j} = g_{j|W_i \cap W_j}$, then as the g_j are continuous, and coincide on the intersections, there exists $g : V \longrightarrow X$ which is continuous such that for all j, $g_{|W_j} = g_j$. Moreover g is a section in fact : for all $x \in V$, there is some j such that $x \in W_j$, $\pi \circ g(x) = \pi(g(x)) = \pi(g_j(x)) = x$.*
  $\mathcal{F}^{\dagger}$is a sheaf.
- *Definition of $\beta : \mathcal{F} \longrightarrow \mathcal{F}^{\dagger}$: For any open subset V of X and $s \in \mathcal{F}(V)$, we define $\beta(V)(s) := \pi_s \in \mathcal{F}^{\dagger}(V)$.*
- *Compatibility with restrictions : let $W \subseteq V$ two open subsets of X, $s \in \mathcal{F}(V)$ and $x \in W$, we have $\beta(V)(s)_{|W}(x) = \pi_s(x) = s_x = (s_{|W})(x) = \pi_{s|W}(x)$. So $\beta(V)(s)_{|W} = \beta(W)(s_{|W})$.*
- *Let $\mathcal{G}$ be a sheaf, and $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ be a morphism of presheaves. We cut a section g of $\mathcal{F}^{\dagger}(V)$ into small sections (sections of $\mathcal{F}$) on a covering W_j of V, then by sending them to the $\mathcal{G}(W_j)$, then we stick back into $\mathcal{G}$. Sections of $\mathcal{F}^{\dagger}$ are obtained by gluing sections of $\mathcal{F}$, so $\mathcal{F}_x = \mathcal{F}^{\dagger}_x$.*

Remark 2.1.4 *If $\mathcal{F}$ is a sheaf, it follows from the universal property that $\mathcal{F} \simeq \mathcal{F}^{\dagger}$.*

Example 2.1.3 *(Constant sheaves) Let A be a group (or a ring, an algebra,. . .), then*

$$U \longmapsto \begin{cases} A & \text{if} \quad U \neq \emptyset \\ \{0\} & \text{otherwise} \end{cases}$$

is a presheaf and the associated sheaf is called the constant sheaf associated to A. We denoted by $\underline{A}$. For any $x \in X$, we have $\underline{A}_x = A$.

Subsheaves and Quotient sheaves

Throughout, we fix a category of objects that have an algebraic structure which are in particular groups, say e.g., $\mathcal{C} = \mathcal{G}p$ or R-$\mathcal{M}od$.

Subsheaves

Definition 2.1.9 *Let $\mathcal{F}$ and $\mathcal{G}$ be two sheaves on X, we say that $\mathcal{F}$ is a subsheaf of $\mathcal{G}$, if for any open subset U of X, $\mathcal{F}(U) \subseteq \mathcal{G}(U)$ and such that we have compatibility with the restrictions induced from $\mathcal{F}$ and $\mathcal{G}$, i.e., For every open subsets $U \subseteq V$ of X, the following diagram is commutative :*

$$\begin{array}{ccc} \mathcal{F}(V) & \hookrightarrow & \mathcal{G}(V) \\ \downarrow res_{V,U} & & \downarrow res_{V,U} \\ \mathcal{F}(U) & \hookrightarrow & \mathcal{G}(U) \end{array}$$

Remark 2.1.5 *$\mathcal{F}$ is a subsheaf of $\mathcal{G}$ if, the canonical injection $\imath : \mathcal{F} \longrightarrow \mathcal{G}$ is a morphism of sheaves.*

Definition 2.1.10 *Let $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ a morphism of presheaves on X. We define the presheaf $ker(\psi)$ by the formula :*

$$U \longrightarrow ker(\psi(U))$$

for any open subset U of X. $ker(\psi)$ is said to be the kernel of ψ, it's a subpresheaf of $\mathcal{F}$.

Using the notation of definition 2.1.10, one can easily see that ψ is injective if and only if its kernel is the trivial presheaf.

Lemma 2.1.2 *Let $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ be a morphism of sheaves. Then the presheaf $ker(\psi)$ is a sheaf.*

Proof. *Let U be an open of X , $(U_j)_j$ be a covering of U and $s_j \in ker(\psi(U_j))$ such that for i, j, $s_{i|U_i \cap U_j} = s_{j|U_i \cap U_j}$. Since $s_j \in \mathcal{F}(U_j)$, then $(s_j)_j$ rises to a section s of $\mathcal{F}$ over U, but for every $x \in U$, there exists j such that $x \in U_j$, and we have $(\psi(U))(s)_x = (\psi(U_j))(s_j)_x = 0$. So $\psi(U)(s) = 0$. Hence $s \in ker(\psi(U))$. On the other hand, if $s \in ker(\psi(U))$ such that for every j, $s_{|U_j} = 0$, then $s = 0$ (because $s \in \mathcal{F}(U)$ and $\mathcal{F}$ is a sheaf).*

Definition 2.1.11 *Let $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ be a morphism of presheaves on X. We define the $im(\psi)$ presheaf by the formula :*

$$U \longmapsto im(\psi(U))$$

for any open set U of X. One can easily see that $im(\psi)$ is indeed a subpresheaf of $\mathcal{G}$. We say that $im(\psi)$ is the image presheaf of ψ.

Remark 2.1.6 *Note that the presheaf $im(\psi)$ is not in general a sheaf.*

Definition 2.1.12 *Let $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ be a morphism of sheaf. The sheaf associated with the image presheaf called the image sheaf of ψ is denoted $Im(\psi)$. In the same way we define the cokernel sheaf and that we denote by $Coker(\psi)$.*
Note that in general $(Im(\psi))(U) \neq Im(\psi(U))$. The first term is section of the sheaf $Im(\psi)$ on the open set U, while the second is the image of the morphism $\psi(U)$. More precisely, we have :

Theorem 2.1.2 *Let $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ be a morphism of sheaves. Then, the following assertions hold :*

i) For any open subset U of X, and $s \in \mathcal{G}(U)$. $s \in (im(\psi)(U))$ if and only if there exists an open covering (U_j) of U and $t_j \in \mathcal{F}(U_j)$ such that, for any j, $s_{|U_j} = \psi(U_j)(t_j)$.

ii) ψ is surjective if and only if, for any open subset U of X and $s \in \mathcal{G}(U)$, there exists an open covering $(U_j)_j$ of U and $t_j \in \mathcal{F}(U_j)$ such that, for any j, $s_{|U_j} = \psi(U_j)(t_j)$.

iii) ψ is surjective if and only if $\mathcal{G} = im(\psi)$.

Proof. *i) $Im(\psi)$ is a the sheaf associated with presheaf $U \longmapsto Im(\psi(U))$, hence the result.*

ii) If ψ is surjective, let U an open subset of X and $s \in \mathcal{G}(U)$, for all $x \in U$, by theorem 2.1.1, the map ψ_x is surjective. So there exists $t_x \in \mathcal{F}_x$ such that $\psi_x(t_x) = s_x$. Therefore, there there exists an open neighborhood $U_x \subseteq U$, and $t^x \in U_x$ such that $s_{|U_x} = \psi(U_x)(t^x)$. The covering $(U_x)_{x \in U}$ answers the question. Conversely, let $x \in X$ and $s \in \mathcal{G}(U)$. Let $(U_j)_j$ be covering of U and $t_j \in \mathcal{F}(U_j)$ such that $s_{|U_j} = \psi(U_j)(t_j)$ for all j. Since $\mathcal{F}$ is a sheaf then there is $t \in \mathcal{F}(U)$ such that $t_{|U_j} = t_j$ for all j. In particular, for every j such that $x \in U_j$, $s_x = (s_{|U_j})_x = \left(\psi(U_j)(t_j)\right)_x = \psi_x(t_x)$. Hence ψ is surjective.

iii) Immediate from i) and ii).

Quotients sheaves

Assume that $\mathcal{F}$ is a subsheaf of the sheaf $\mathcal{G}$. Then we can define a presheaf whose sections over U are the quotient $\mathcal{G}(U)/\mathcal{F}(U)$. The restriction maps of $\mathcal{F}$ and $\mathcal{G}$ are compatible the inclusions $\mathcal{F}(U) \subseteq \mathcal{G}(U)$ and hence pass to the quotient $\mathcal{G}(U)/\mathcal{F}(U)$. This presheaf, i.e., $U \longmapsto \mathcal{G}(U)/\mathcal{F}(U)$, is called quotient presheaf of $\mathcal{G}$ by $\mathcal{F}$.

Definition 2.1.13 *The quotient sheaf $\mathcal{G}/\mathcal{F}$ is the sheafification of the quotient presheaf of $\mathcal{G}$ by $\mathcal{F}$.*

Proposition 2.1.4 *Let $\mathcal{F}$ be a subsheaf of $\mathcal{G}$, $x \in X$. Then $(\mathcal{G}/\mathcal{F})_x = \mathcal{G}_x/\mathcal{F}_x$.*

Proof. *$\mathcal{G}/\mathcal{F}$ is the sheaf associated with the presheaf $U \longmapsto \mathcal{G}(U)/\mathcal{F}(U)$ whose stalks at x is clearly isomorphic to $\mathcal{G}_x/\mathcal{F}_x$.*

Continuous maps and sheaves

So far, we have only talked about sheaves defined on a single topological space. We are going to study in this paragraph some transformations of sheaves via continuous mappings between topological spaces.
Let $f : X \longrightarrow Y$ be a continuous map of topological spaces. We will define the pushforward and pullback functors for presheaves and sheaves.

Pushforward

Definition 2.1.14 *Let $f : X \longrightarrow Y$ be a continuous map between topological spaces. Let $\mathcal{F}$ be a presheaf on X. We define the pushforward of $\mathcal{F}$ by the formula :*

$$f_*\mathcal{F}(V) = \mathcal{F}\big(f^{-1}(V)\big)$$

for any open $V \subseteq Y$.
Given opens $W \subseteq V$ of Y the restriction map is given by the commutativity of the diagram

$$\begin{array}{ccc} f_*\mathcal{F}(V) & = & \mathcal{F}\big(f^{-1}(V)\big) \\ \downarrow & & \downarrow{\scriptstyle res_{f^{-1}(V),f^{-1}(W)}} \\ f_*\mathcal{F}(W) & = & \mathcal{F}\big(f^{-1}(W)\big) \end{array}$$

It is clear that this defines a presheaf on Y.

Remark 2.1.7 *The construction is clearly functorial in the presheaf $\mathcal{F}$ and hence we obtain a functor*

$$\begin{array}{rccc} f_* : & \mathcal{P}re\mathcal{S}h_X & \longrightarrow & \mathcal{P}re\mathcal{S}h_Y \\ & \mathcal{F} & \longmapsto & f_*\mathcal{F} \end{array}$$

Proposition 2.1.5 *Let $f : X \longrightarrow Y$ be a continuous map and $\mathcal{F}$ be a sheaf on X. Then $f_*\mathcal{F}$ is a sheaf on Y.*

Proof. *This immediately follows from the fact that if $(W_j)_j$ is an open covering of some open subset W of Y then, $(f^{-1}(W_j))_j$ is an open covering of the open $f^{-1}(W)$. Consequently, we obtain a functor*

$$f_* : \mathcal{S}h_X \longrightarrow \mathcal{S}h_Y$$

This is compatible with composition in the following strong sense :

Lemma 2.1.3 *Let $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ be continuous maps of topological spaces. Then, the functors $(g \circ f)_*$ and $g_* \circ f_*$ are equal.*

Proof. *Immediate.*

Pullback

We saw in example 2.1.1 that if $\mathcal{F}$ is a sheaf on X, then for any open subset U of X $\mathcal{F}_{|U}$ is a sheaf on U. Now if we take an arbitrary subset Z of X. the restriction of $\mathcal{F}$ on Z is not necessarily a sheaf because an open set W of Z is not necessarily an open set of X.
Next definition gives the meaning of $\mathcal{F}_{|Z}$, when Z is a closed subset of X. This will be generalized in definition 2.1.16 to give the meaning of the pullback presheaf defined by a continuous map. For this purpose, note that if $f : X \longrightarrow Y$ is a continuous map between topological spaces and V is an open of Y, then the family $(U)_{f(U)\subseteq V}$ consisting of all open subsets U of X satisfying $f(U) \subseteq V$, is an inductive system for the inverse of the inclusion relation.

Definition 2.1.15 *If $\imath : Z \longrightarrow X$ is the inclusion of a closed subset Z of X, and V is an open subset of Z. We define the restriction $\mathcal{F}_{|Z}$ as the sheafification of the following presheaf*

$$V \longmapsto \varinjlim_{V\subseteq U} \mathcal{F}(U)$$

Definition 2.1.16 *Let $f : X \longrightarrow Y$ be a continuous map between topological spaces and $\mathcal{G}$ be a presheaf on Y. We define the pullback presheaf of $\mathcal{G}$ by the formula :*

$$f_p\mathcal{G}(U) = \varinjlim_{f(U)\subseteq V} \mathcal{G}(V).$$

Remark 2.1.8 *In the language of categories. The pullback presheaf $f_p\mathcal{G}$ of $\mathcal{G}$ is defined as the left adjoint of the pushforward f_* on presheaves. In other words, $f_p\mathcal{G}$ will be a presheaf on X such that*

$$Mor_{\mathcal{P}reSh_X}(f_p\mathcal{G}, \mathcal{F}) = Mor_{\mathcal{P}reSh_Y}(G, f_*\mathcal{F})$$

Proposition 2.1.6 *Let $f : X \longrightarrow Y$ be a continuous map between topological spaces, x be a point of X and $\mathcal{G}$ be a presheaf on $\mathcal{Y}$. Then, up to an isomorphism, we have $(f_p\mathcal{G})_x = \mathcal{G}_{f(x)}$.*

Proof.

$$\begin{aligned}(f_p\mathcal{G})_x &= \varinjlim_{x\in U} f_p\mathcal{G}(U)\\ &= \varinjlim_{x\in U}\varinjlim_{f(U)\subseteq V} \mathcal{G}(V)\\ &= \varinjlim_{f(x)\in V} \mathcal{G}(V)\\ &= \mathcal{G}_{f(x)}\end{aligned}$$

Definition 2.1.17 *Let $f : X \longrightarrow Y$ be a continuous map between topological spaces and $\mathcal{G}$ be a sheaf on Y. The pullback sheaf $f^{-1}\mathcal{G}$ is defined by the formula :*

$$f^{-1}\mathcal{G} = (f_p\mathcal{G})^\dagger$$

$f^{-1}\mathcal{G}$ is also called the inverse image along the map f.

Remark 2.1.9 *f^{-1} defines a functor :*

$$\begin{array}{rccc} f^{-1} : & \mathcal{S}h_Y & \longrightarrow & \mathcal{S}h_X \\ & \mathcal{G} & \longmapsto & f^{-1}\mathcal{G} \end{array}$$

The pullback f^{-1} is a left adjoint of pushforward on sheaves.

$$Mor_{\mathcal{S}h_X}(f^{-1}\mathcal{G}, \mathcal{F}) = Mor_{\mathcal{S}h_Y}(\mathcal{G}, f_*\mathcal{F}).$$

For more details see [9, 1.12.1, p.38].

Example 2.1.4 *Let $\mathcal{F}$ be a sheaf on X and $x \in X$. Let $\imath : \{x\} \longrightarrow X$ be the inclusion map, then $\imath^{-1}\mathcal{F} = \mathcal{F}_x$*

Lemma 2.1.4 *Let $f : X \to Y$ be a continuous map between topological spaces, $x \in X$ and $\mathcal{G}$ be a sheaf on Y, then the stalks $(f^{-1}\mathcal{G})_x$ and $\mathcal{G}_{f(x)}$ are equals.*

Proof. *This a combination of proposition 2.1.3 and proposition 2.1.6.*

Lemma 2.1.5 *Let $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ be continuous maps of topological spaces. The functors $(g \circ f)^{-1}$ and $f^{-1} \circ g^{-1}$ are canonically isomorphic. Similarly, $(g \circ f)_p = f_p \circ g_p$, for presheaves.*

Proof. *This follows from the fact that adjoint functors are unique up to unique isomorphism, and Lemma 2.1.3.*

Exact sequences of sheaves

In this paragraph, we will define what is an exact sequence of sheaves, and we will study some of their properties. For this we will restrict our study to the case of sheaves of groups.

Definition 2.1.18 *A sequence of presheaves with presheaves morphisms*

$$\cdots \longrightarrow \mathcal{F}^{j-1} \xrightarrow{\psi^{j-1}} \mathcal{F}^{j} \xrightarrow{\psi^{j}} \mathcal{F}^{j+1} \xrightarrow{\psi^{j+1}} \cdots$$

is said to be exact if for all i, $Im(\psi^{j-1}) = ker(\psi^j)$. In particular the following exact sequence is call a short exact sequence when it is exact :

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow 0$$

Remark 2.1.10 *Let $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ be a morphism of sheaves. Then,*

i) *ψ is injective if and only if*

$$0 \longrightarrow \mathcal{F} \xrightarrow{\psi} \mathcal{G}$$

is an exact sequence.

ii) *ψ is surjective if and only if*

$$\mathcal{F} \xrightarrow{\psi} \mathcal{G} \longrightarrow 0$$

is an exact sequence.

Example 2.1.5 *Let $X = \mathbb{C}$, and $\mathcal{O}_X$ the sheaf of holomorphic functions and consider the map $d : \mathcal{O}_X \longrightarrow \mathcal{O}_X$, sending $f(z)$ to $f'(z)$. There is an exact sequence*

$$0 \longrightarrow \mathbb{C}_X \longrightarrow \mathcal{O}_X \xrightarrow{d} \mathcal{O}_X \longrightarrow 0$$

Indeed, this follows by the following facts :

- *A function whose derivative vanishes identically is locally constant, so $ker(d)$ is the constant sheaf $\mathbb{C}_X$.*
- *In small open disks any holomorphic function is a derivative.*

Lemma 2.1.6 *Let $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ be a morphism of sheaves on X. Then for any $x \in X$, we have $(ker\psi)_x = ker(\psi_x)$ and $(im\psi)_x = im(\psi_x)$.*

Proof. *Let $s_x \in \big(ker(\psi)\big)_x$, and let U an open neighborhood of x such that $s \in \big(ker(\psi)\big)(U) = ker\big(\psi(U)\big)$, so $\psi(U)(s) = 0$, hence $\psi_x(s_x) = \big(\psi(U)(s)\big)_x = 0$, so $s_x \in ker(\psi_x)$. Conversely, if $\psi_x(s_x) = 0$, then $\big(\psi(U)(s)\big)_x = 0$ (U is an open neighborhood of x and $s \in \mathcal{F}(U)$), then there exists an open neighborhood $W \subseteq U$ of x such that $\psi(U)(s)_{|W} = 0$, i.e., $\psi(W)(s_{|W}) = 0$ and therefore $s_{|W} \in ker\big(\psi(W)\big)$ whence $s_x = (s_{|W})_x \in \big(ker(\psi)\big)_x$. One can proceed similarly for the image.*

Theorem 2.1.3 *A sequence of sheaves with sheaves morphisms*

$$\cdots \longrightarrow \mathcal{F}^{j-1} \xrightarrow{\psi^{j-1}} \mathcal{F}^{j} \xrightarrow{\psi^{j}} \mathcal{F}^{j+1} \xrightarrow{\psi^{j+1}} \cdots$$

is an exact sequence if and only if for any $x \in X$

$$\cdots \longrightarrow \mathcal{F}_x^{j-1} \xrightarrow{\psi_x^{j-1}} \mathcal{F}_x^{j} \xrightarrow{\psi_x^{j}} \mathcal{F}_x^{j+1} \xrightarrow{\psi_x^{j+1}} \cdots$$

is an exact sequence.

Proof.

$$\cdots \longrightarrow \mathcal{F}^{j-1} \xrightarrow{\psi^{j-1}} \mathcal{F}^{j} \xrightarrow{\psi^{j}} \mathcal{F}^{j+1} \xrightarrow{\psi^{j+1}} \cdots$$

is an exact sequence if and only if, for any j, $im(\psi^{j-1}) = ker(\psi^j)$ if and only if, for any $x \in X$ and for any j, $im(\psi_x^{j-1}) = ker(\psi_x^j)$ if and only if,

$$\cdots \longrightarrow \mathcal{F}_x^{j-1} \xrightarrow{\psi_x^{j-1}} \mathcal{F}_x^{j} \xrightarrow{\psi_x^{j}} \mathcal{F}_x^{j+1} \xrightarrow{\psi_x^{j+1}} \cdots$$

is an exact sequence.

Proposition 2.1.7 *Let $\mathcal{F}$ be a subsheaf of $\mathcal{G}$ on X. Then*

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{G}/\mathcal{F} \longrightarrow 0$$

is an exact sequence.

Proof. *By proposition 2.1.4, for any $x \in X$,*

$$0 \longrightarrow \mathcal{F}_x \longrightarrow \mathcal{G}_x \longrightarrow \mathcal{G}_x/\mathcal{F}_x = (\mathcal{G}/\mathcal{F})_x \longrightarrow 0$$

is an exact sequence. Hence the result.

Remark 2.1.11 *If*

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow 0$$

is an exact sequence over X, then $\mathcal{F}$ can be identified with a sub-sheaf of $\mathcal{G}$ and $\mathcal{G}/\mathcal{F} \simeq \mathcal{H}$.

Corollary 2.1.1 *Let $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ be a morphism of sheaves. Then*

1) *$Im(\psi) \simeq \mathcal{F}/ker(\psi)$.*

2) *$Coker(\psi) \simeq \mathcal{G}/Im(\psi)$.*

Proof. 1) *It is easy to check that for all $x \in X$, we have*

$$0 \longrightarrow (ker(\psi))_x \longrightarrow \mathcal{F}_x \longrightarrow im(\psi)_x \longrightarrow 0$$

It follows by theorem 2.1.3, that

$$0 \longrightarrow ker(\psi) \longrightarrow \mathcal{F} \longrightarrow im(\psi) \longrightarrow 0$$

is an exact sequence. Also by remark 2.1.11 we have $im(\psi) \simeq \mathcal{F}/ker(\psi)$

2) *Similar to 1).*

2.1.3 Glueing sheaves

In this section, we fix a topological space X, and we consider an open covering $(U_i)_{i\in I}$ of X with a sheaf $\mathcal{F}_i$ on each subset U_i. Our goal is to "glue" the $\mathcal{F}_i$ together, that is we search for a global sheaf $\mathcal{F}$ such that $\mathcal{F}_{|U_i} = \mathcal{F}_i$ for all $i \in I$. For this, we consider the following notion:

Notation. i) *For $i, j \in I$, we denote by U_{ij} the intersection $U_i \cap U_j$.*

ii) *For $i, j, k \in I$, we denote by U_{ijk} the intersection $U_i \cap U_j \cap U_k$.*

Definition 2.1.19 *A Gluing Data consists of a family of sheaves $\mathcal{F}_i$ over U_i and a family of morphisms $\delta_{ij} : \mathcal{F}_{i|U_{ij}} \longrightarrow \mathcal{F}_{j|U_{ij}}$ such that*

i) $\delta_{ii} = id_{\mathcal{F}_i}$.

ii) $\delta_{ji} = \delta_{ij}^{-1}$.

iii) $\delta_{ik} = \delta_{jk} \circ \delta_{ij}$ *on* U_{ijk}.

A morphism of gluing data $(\mathcal{F}_i, \delta_{ij}) \longrightarrow (\mathcal{G}_i, \eta_{ij})$ is a family of morphism of sheaves $\psi_i : \mathcal{F}_i \longrightarrow \mathcal{G}_i$ such that the following diagram

$$\begin{array}{ccc} \mathcal{F}_i & \xrightarrow{\psi_i} & \mathcal{G}_i \\ \downarrow{\scriptstyle \delta_{ij}} & & \downarrow{\scriptstyle \delta_{ij}} \\ \mathcal{F}_j & \xrightarrow{\psi_j} & \mathcal{G}_j \end{array}$$

is commutative.

Theorem 2.1.4 *(Gluing sheaves) There exists a sheaf $\mathcal{F}$ on X, unique up to ismorphism such that there are isomorphisms $\theta_i : \mathcal{F}_{U_i} \longrightarrow \mathcal{F}_i$ satisfying*

$$\theta_j = \delta_{ij} \circ \theta_i.$$

Proof. *Let W be an open subset of X. We write $W_i = U_i \cap W$, and $W_{ij} = U_{ij} \cap W$. We are going to define the sections of $\mathcal{F}$ over W by gluing sections of the $\mathcal{F}_i'$s over W_i's along the W_{ij}'s using the isomorphisms δ_{ij}. We define*

$$\mathcal{F}(W) := \{(s_i)_{i\in I} \mid \delta_{ji}(s_{i|W_{ij}}) = \delta_{j|W_{ij}}(s_{j|W_{ij}})\} \subseteq \prod_{i\in I} \mathcal{F}_i(W_i). \tag{2.1}$$

The δ_{ij}'s are morphisms of sheaves and therefore are compatible with all restrictions maps (see definition 2.1.3). So if $V \subseteq W$ is another open subset we have

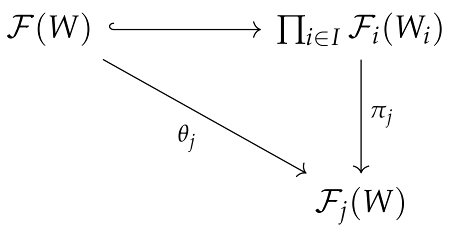
$$\delta_{ij}(s_{i|V_{ij}}) = s_{j|V_{ij}}.$$

Because of this, the defining condition (2.1) is compatible with componentwise restrictions, and they can therefore be used as the restriction maps in $\mathcal{F}$. We get then a presheaf on X. To finish the proof we have to complete the following steps:

- ***First step** : We need to establish an isomorphisms $\theta_i : \mathcal{F}_{|U_i} \longrightarrow \mathcal{F}_i$. To avoid getting confused by the indices, we shall work with a fixed index $j \in I$. Suppose $W \subseteq U_j$ is an open set. We have $W = W_j$, and projecting from the product $\prod_{i \in I} \mathcal{F}_i(W_i)$ onto the component*

  $$\mathcal{F}_j(W) = \mathcal{F}_j(W_j)$$

  gives us a map $\theta_j : \mathcal{F}_{|U_j} \longrightarrow \mathcal{F}_j$. Moreover, $\theta_j\big((s_i)_{i \in I}\big) = s_j$. The situation is summarized in the following commutative diagram



Now, we want to show that θ_j's give the desired isomorphisms. We note that on the restrictions $W_{jj'}$, the requirement in the proposition, that

$$\theta_{j'} = \eta_{j'j} \circ \theta_j$$

is fulfilled. This follows directly from the (2.1) since we have

$$s_{j|W_{jj'}} = \delta_{jj'}(s_{j'|W_{jj'}}).$$

- *θ_j is surjective : Let α be a section of $\mathcal{F}_j(W)$ over some $W \subseteq U_j$, and let $s = (\delta_{ij}(\alpha_{|W_{ij}}))_{i \in I}$. Then s satisfies (2.1) and is therefore an element $\mathcal{F}(W)$. As $\delta_{jj}(\alpha_{|W_{jj}}) = \alpha$ by the first gluing request, the element s projects to the section α of $\mathcal{F}_j$.*

- *θ_j is injective : Suppose that $s_j = 0$, then $s_{i|W_{ij}} = \delta_{ij}(s_j) = 0$ for each $i \in I$. Now $\mathcal{F}_j$ is a sheaf, and the $((W_{ij}))_{i \in I}$ is an open covering of W_j. So $s = 0$.*

- ***Final step** : We have to show $\mathcal{F}$ is a sheaf. Let $\{W_j\}_{j \in I}$ be an open covering of $W \subseteq U$, and $s_j \in \mathcal{F}(W_j)$ is a bunch of sections matching on the intersections $W_{jj'}$. Since $\mathcal{F}_{|U_i \cap W}$ is a sheaf patch together to give sections s_i in $\mathcal{F}_{U_i \cap W)}$ matching on the overlaps $U_{ij} \cap W$. This last condition means that $\delta ij(s_i) = s_j$. By definition $(s_i)i \in I$, then is a section in $\mathcal{F}(W)$ restricting to s_i. Hence the result.*
  The Gluing axiom (see definition 2.1.6) is easier : Let $s = (s_i)_{i \in I}$ in $\mathcal{F}(W)$, and a covering $\mathcal{L} = \{V_j\}_{j \in J}$ of W such that $s_{|V_j} = 0$ for all $j \in J$, then also $s_{|V_j \cap W_i} = 0$, and since $\{V_j \cap W_i\}_{j \in J}$ forms a covering of W_i, we must have $s_{|W_i} = 0$ as well, since $\mathcal{F}_{W_i} = \mathcal{F}_i$ is a sheaf. But from the (2.1) we thus see that $s = 0$.

2.2 Spectrum of a ring and ringed spaces

2.2.1 Spectrum of ring

In this section, for a commutative ring R, we will define Zariski topology on the spectrum $Spec(R)$ of R and study some of the basic properties of this topological space. One can already notice the analogy with Zariski topology defined on affine algebraic sets, indeed, this last one is fully inspired from the first one in an attempt to make our work on varieties free from the assumption that the base field k is algebraically closed (even free from working on varieties defined only on field). We define then and study some basic facts concerning ringed spaces for which we make intensive call to sheaf theory. All this is made to prepare necessary tools to define schemes of rings which will generalize the notion of (classical) algebraic sets.

Definition 2.2.1 *Let R be a commutative ring. The set of all prime ideals of R is called the spectrum of R. It will be denoted by $Spec(R)$.*

Remark 2.2.1 *Plainly, the set of all maximal ideals of R is a subset of $Spec(R)$, it is denoted by $Spm(R)$. By Krull theorem, for any (nonzero) commutative ring R, then R has a maximal ideal, so $Spec(R)$ is nonempty.*

Examples 2.2.1 *1) If R be a field, then $Spec(R) = \{0\}$.*

2) $Spec(\mathbb{Z}) = \{p\mathbb{Z} \mid p \text{ prime number }\} \cup \{0\}$.

3) By corollary 1.1.1, if R is an algebraically closed field, then for any positive integer n, $Spec(R[T_1, \ldots, T_n]) = \{(T_1 - a_1, \ldots, T_n - a_n) \mid \text{where } a_i \in R\}$

Notation. *Let R be a ring and S be a subset of R.*

- *We define*
$$V(S) = \{P \in Spec(R) \mid S \subseteq P\}.$$
- *For any $f \in R$, we denote by $D(f)$ the complement of $V(\{f\})$ i.e,*
$$D(f) = \{P \in Spec(R) \mid f \notin P\}.$$

Remark 2.2.2 *One can easily see that $V(1) = \emptyset$ and $V(0) = Spec(R)$.*

Proposition 2.2.1 *Let R be a ring, S, M be subsets of R, I, J be ideals of R and $f \in R$. Then, the following statements hold :*

1) If $S \subseteq M$, then $V(M) \subseteq V(S)$.

2) Let (S) be the ideal generated by S, then we have $V(S) = V((S))$.

3) $V(J) = V(rad(J))$.

4) $V(I) = \emptyset$ if and only if $I = R$.

5) $V(I) = V(J)$ if and only if $rad(I) = rad(J)$.

6) $V(I) \cup V(J) = V(I \cap J) = V(IJ)$.

7) If $\{I_j\}$ is a family of ideals of R, then
$$\bigcap_j V(I_j) = V(\bigcup_j I_j).$$

Proof. *1) Clear.*

2) *Plainly, we have $V((S)) \subseteq V(S)$. Conversely, let $P \in V(S)$ and $g \in (S)$, we need to show that $g \in P$. We can write $g = \sum_{j=1}^{r} f_j h_j$, $f_j \in S$, $h_j \in R$. Since $S \subseteq P$, then for all $j \in \{1, \ldots, r\}$, $f_j \in P$. So $f_j h_j \in P$. Thus, $\sum_{j=1}^{r} f_j h_j \in P$ which means that $g \in P$.*

3) *Since $J \subseteq rad(J)$, then clearly $V(rad(J)) \subseteq V(J)$. Conversely, $P \in V(J)$, then we have $J \subseteq P$, so $rad(J) \subseteq rad(P) = P$. Thus $P \in V(rad(J))$.*

4) *As seen above, we have $V(R) = \emptyset$. Suppose that $I \neq R$, then there exists a maximal ideal $\mathcal{M}$ of R such that $I \subseteq \mathcal{M}$. By 1) we have $V(\mathcal{M}) \subseteq V(I)$. Since $\mathcal{M}$ is prime, then $\mathcal{M} \in V(\mathcal{M})$. So $V(I) \neq \emptyset$.*

5) *If $rad(I) = rad(J)$, then by 3), $V(I) = V(J)$. Conversely, suppose that $V(I) = V(J)$, then $\bigcap_{I \subseteq P} P = \bigcap_{J \subseteq P} P$, which means that $rad(I) = rad(J)$.*

6) *We have $I \cap J \subseteq I, J$, so by 1) $V(I) \cup V(J) \subseteq V(I \cap J)$. Conversely, let $P \in V(I \cap J)$, i.e., $I \cap J \subseteq P$. Since P is prime, then necessarily $I \subseteq P$ or $J \subseteq P$, so $P \in V(I) \cup V(J)$. The rest is clear.*

7) *Note that $P \in \bigcap_j V(I_j)$ if and only if P contains all I_j if and only if P contains $\bigcup_j I_j$ if and only if $P \in V(\bigcup_j I_j)$.*

Remark 2.2.3 *Proposition 2.2.1 shows that we can consider a topology on $Spec(R)$ by taking the subsets $V(S)$ to be the closed subsets of $Spec(R)$.*

Definition 2.2.2 *Let R be a commutative ring. The topology on $Spec(R)$ whose closed sets are the sets $V(S)$, where S describes all subsets of R, is called the Zariski topology of $Spec(R)$. For $f \in R$, $D(f)$ is plainly an open subset of $Spec(R)$. These open sets are called the principal open subsets of $Spec(R)$.*

Remarks 2.2.1 *i) Let $P \in Spec(R)$, then P is a closed point of $Spec(R)$ (i.e., $\{P\}$ is a closed subset of $Spec(R)$) is closed if and only P is a maximal ideal of R.*

ii) $(0)(= \{0\}) \in Spec(R)$ if and only if R has a nonzero divisors.

Proposition 2.2.2 *For a commutative ring R, the following statements hold :*

1) *$D(f) = \emptyset$, if and only if $f \in N(R)$, the nilradical of R.*

2) *$D(f) = Spec(R)$, if and only if $f \in U(R)$, the group of invertible elements of $\mathcal{R}$.*

3) *For all $f, g \in R$, $D(fg) = D(f) \cap D(g)$.*

4) *For every $m \in \mathbb{N}$, $D(f^m) = D(f)$.*

Proof. *1) Clearly, if $D(f) = \emptyset$, then $f \in P$ for all prime ideals P of R, thus $f \in N(R)$. The converse is straightforward.*

2) *If $D(f) = Spec(R)$, then f is not in any prime ideal of R, and so it is not in any maximal ideal. Since every non-unit is contained in some maximal ideal, f must be a unit. The converse is clear.*
3) and 4) Clear.

Theorem 2.2.1 *The sets $D(f)$ form a basis for the Zariski topology.*

Proof. *Indeed, to show for any Ideal J of R we have $Spec(R) \setminus V(J) = \bigcup_{f \in J} D(f)$.*

Notation. *For any $Y \subseteq Spec(R)$, let $j(Y) := \{f \in R \mid Y \subseteq V(f)\}$. One has $j(Y) = \bigcap_{P \in Y} P$. In particular, $j(Y)$ is a radical ideal of R.*

Lemma 2.2.1 *1) If Y_1 and Y_2 are subsets of $Spec(R)$ such that $Y_1 \subseteq Y_2$, then $j(Y_2) \subseteq j(Y_1)$.*

2) If $(Y_t)_{t\in T}$ is a family of subsets of $Spec(R)$, then $j(\bigcup_{t\in T} Y_t) = \bigcap_{t\in T} j(Y_t)$.

3) For every subset Y of $Spec(R)$, we have $Y \subseteq V(j(Y))$.

4) For every subset S of R, we have $S \subseteq j(V(S))$.

Proof. *1) and 2) clear.*

3) Let $P \in Y$. Since $j(Y) = \bigcap_{P\in Y} P \subseteq P$, then $P \in V(j(Y))$.

4) Clear.

The following result gives a characterization of the closure of a subset of $Spec(R)$.

Proposition 2.2.3 *Let Y be a subset of $Spec(R)$. Then $\overline{Y} = V(j(Y))$.*

Proof. *By lemma 2.2.1 3) $Y \subseteq V(j(Y))$, so $\overline{Y} \subseteq V(j(Y))$. Conversely, it suffices to show that any closed set containing Y must contain $V(j(Y))$. If $Y \subseteq V(S)$, then for any $P \in Y$, we have $S \subseteq P$, and this yields $S \bigcap_{P\in Y} P = j(Y)$. So $V(j(Y)) \subseteq V(S)$.*

Remark 2.2.4 *Let X be a topological space, if X is Hausdorff, then for every $x \in X$, we have $\{x\}$ is closed. So, $X = Spec(\mathbb{Z})$ is not Hausdoroff. Indeed, we have $j(\{0\}) = \bigcap_{P\in X} P$ and by proposition 2.2.3, we have $\overline{\{0\}} = V(j(\{0\})) = V(0) = Spec(\mathbb{Z})$. So $\{0\}$ is not closed.*

In the chapter 1, we gave a one-to-one correspondence between the set of algebraic sets of $\mathbb{A}^n$ and the set of radical ideals of $k[T_1, \ldots, T_n]$, when k is algebraically closed. This was defined by the maps $X \mapsto I(X)$ and $J \mapsto Z(J)$. The following result gives a similar correspondence when replacing $\mathbb{A}^n$ by $Spec(R)$ and $k[T_1, ..., T_n]$ by R.

Theorem 2.2.2 *Let R be a commutative ring. Then*

i) For every ideal I of R, we have $j(V(I)) = rad(I)$.

ii) The maps $S \longrightarrow V(S)$ and $Y \longrightarrow j(Y)$ induce bijections, inverse one of the other, between the set of radical ideals of R and the set of closed subsets of $Spec(R)$.

Proof. *i) We have $j(V(I)) = \bigcap_{P\in V(I)} P = \bigcap_{I\subseteq P} P = rad(I)$.*

ii) This follows directly from i) and proposition 2.2.3.

Proposition 2.2.4 *1) Let $\psi : R \longrightarrow A$ be a homomorphism of rings. Then ψ induces a continuous map $\psi^* : Spec(A) \longrightarrow Spec(R)$ given by $\psi^*(Q) = \psi^{-1}(Q)$.*

2) Let J be an ideal of R and $\pi : R \longrightarrow R/J$ be the canonical homomorphism. Then π^* is a homeomorphism from $Spec(R/J)$, to the subspace $V(J)$ of $Spec(R)$.

Proof. *1) It is clear that for any $Q \in Spec(A)$, $\psi^{-1}(Q) \in Spec(R)$. One can easily see that*

$$(\psi^*)^{-1}(V(J)) = V(\psi(J)).$$

This shows that ψ^* is continuous.

2) *We know that the prime ideals of R/J are the ideals I/J where I is a prime ideal of R containing J. The rest of the proof is straightforward.*

Corollary 2.2.1 *Let R be a commutative ring, then $Spec(R)$ is homeomorphic to $Spec(R/N(R))$ where $N(R)$ denotes the nilradical of R.*

Proof. *It suffices to see that $V(N(R)) = Spec(R)$.*

Remark 2.2.5 *Let S be a multiplicatively stable subset of $R\backslash\{0\}$. By [3, Proposition, 3.11, p.**41**], there is one-to-one correspondence between prime ideals of $S^{-1}R$, and prime ideals of R disjoint from S. One deduce then the following result.*

Proposition 2.2.5 *Let $\Omega := \{P \in Spec(R) \mid P \cap S = \emptyset\}$, then the map $\theta : \Omega \longrightarrow Spec(S^{-1}R)$, defined by $\theta(P) = S^{-1}P$ is a homeomorphism.*

Proposition 2.2.6 *Let R be a commutative ring. Then $Spec(R)$ is compact.*

Proof. *It suffices to show that any cover of $Spec(R)$ by basic open sets, has a finite sub-cover. Assume $Spec(R) \subseteq \bigcup_{t\in T} D(f_t)$ and let $J := (\{f_t, t \in T\})$, be the ideal of R generated by the f_t. For any $P \in Spec(R)$, we have $P \in D(f_t)$ for some $t \in T$. Thus, J cannot be contained in any prime ideal of R, and so cannot be contained in any maximal ideal of R. Write $1 = \sum_{j=1}^{r} h_j f_j$. For any $P \in Spec(R)$, we have $1 \notin P$, so $f_{t_j} \notin P$, for some $j \in \{1, \ldots, r\}$. Hence $f \in D(f_{t_j})$. Therefore, $Spec(R) \subseteq \bigcup_{j=1}^{r} D(f_{t_j})$.*

Corollary 2.2.2 *Let R be a commutative ring and let $f \in R$. Then $D(f)$ is compact with respect to the subspace topology induced from $Spec(R)$.*

Theorem 2.2.3 *Let R be a Noetherian ring, then $Spec(R)$ is a Noetherian topological space.*

Proof. *Let*

$$V(J_1) \supseteq V(J_2) \supseteq \cdots$$

be a descending chain of closed sets in $Spec(R)$, where J_i are ideals of R, then we have a corresponding ascending sequence

$$rad(J_1) \subseteq rad(J_2) \subseteq \cdots$$

of ideals of R. Since R is a Noetherian ring, then there exists $d \in \mathbb{N}$ such that, for all $r \geq d$, $rad(J_r) = rad(J_d)$. It follows that $V(J_r) = V(J_d)$, for all $r \geq d$ showing $Spec(R)$ is Noetherian.

Irreducibility

We give in this section a characterization of the irreducible closed subsets of $Spec(R)$.

Lemma 2.2.2 *Let R be a commutative ring and P be a prime ideal of R. Then $V(P)$ is irreducible in $Spec(R)$.*

Proof. *Suppose that $V(P) = V(J_1) \cup V(J_2)$, where J_1, J_2 are ideals of R. Since $P \in V(P)$, then $P \in V(J_1)$ or $P \in V(J_2)$. Assume that $P \in V(J_1)$, i.e., $J_1 \subseteq P$. , then for any $Q \in V(P)$, we have $J_1 \subseteq P \subseteq Q$, so $Q \in V(J_1)$. Consequently, $V(P) = V(J_1)$.*

Proposition 2.2.7 *Let J be an ideal of R. If $V(J)$ is irreducible, then $rad(J)$ is a prime ideal of R.*

Proof. *Let $f, g \in R$ with $fg \in rad(J)$ and suppose that $f, g \notin rad(J)$. Then there exist two prime ideals P, Q such that $J \subseteq P, Q$ with $f \notin P$ and $g \notin Q$. We then have $P \in V(J) \cap D(f)$ and $Q \in V(J) \cap D(g)$ and clearly $V(J) \cap D(f)$, $V(J) \cap D(g)$ are nonempty open subset of $V(J)$. Since $V(J)$ is irreducible, by proposition 1.1.3 we have $W := \big(V(J) \cap D(f)\big) \cap \big(V(J) \cap D(g)\big) \neq \emptyset$. Let L be the intersection of all elements of W. We have:*
$L \subseteq V(J) = V(rad(J))$, so $rad(J) \subseteq L$ and $L \subseteq D(f) \cap D(g) = D(fg)$, so $fg \notin L$ which contradicts the fact that $fg \in rad(J) \subseteq L$. Hence $rad(J)$ is a prime ideal.

Remark 2.2.6 *If $rad(J)$ is a prime ideal, by lemma 2.2.2 then $V(J)$ is irreducible.*

Proposition 2.2.8 *Let $\mathcal{Y}$ be a closed subset Y of $Spec(R)$, then Y is irreducible if and only if Y is of the form $Y = V(P)$ for some ideal $P \in Spec(R)$.*

Proof. *This follows from the above since for any ideal J of R, we have $V(J) = V(rad(J))$.*

Theorem 2.2.4 *Let R be a commutative ring. Then $Spec(R)$ is irreducible if and only if $N(R)$ is a prime ideal of R.*

Proof. *For any $P \in Spec(R)$, we have $N(R) \subseteq P$, so $P \in V(N(R))$. Thus, $Spec(R) = V(N(R))$, hence by remark 2.2.6 $Spec(R)$ is irreducible when $N(R)$ is a prime ideal of R. Conversely, suppose that $Spec(R)$ is irreducible. Let $fg \in N(R)$. By proposition 2.2.2 3) we have $D(fg) = D(f) \cap D(g)$, moreover, if f and g are not nilpotent, then by proposition 2.2.2, $D(f)$ and $D(g)$ are nonempty. Since $Spec(R)$ is irreducible then $D(fg)(= D(f) \cap D(g))$ is nonempty. This implies that fg is not nilpotent a contradiction.*

Generic points

Definition 2.2.3 *Let X be a topological space, Y be a closed subset of X and $x \in Y$. We say that x is a generic point for Y if Y is the closure of the singleton $\{x\}$, i.e., $Y = \overline{\{x\}}$.*

Examples 2.2.2 1) *Let P be a prime ideal of R, then $\overline{P} = V(P)$ and P is the only generic point of $V(P)$.*

2) *For an integral domain R, the zero ideal $N(R)$ $(= (0))$ is prime, and $\overline{\{(0)\}} = Spec(R)$. Then (0) is a generic point of $Spec(R)$.*

2.2.2 Ringed spaces

Definition 2.2.4 *A ringed topological space is a pair $(X, \mathcal{O}_X)$ consisting of a space and a sheaf of rings $\mathcal{O}_X$ called the structure sheaf.*

Examples 2.2.3 1) *Let X be a topological space and $\mathcal{O}_X (= \mathcal{C}^0(., \mathbb{R}))$ be a sheaf of continuous real functions on X. Then $(X, \mathcal{O}_X)$ is a ringed space.*

2) *Let M be a $\mathcal{C}^\infty$-manifold, then the sheaf $\mathcal{C}^\infty(., \mathbb{R})$ of smooth functions is a sheaf of rings on M.*

Remark 2.2.7 *Let $(X, \mathcal{O}_X)$ be a ringed space and U an open subset of X, then $(U, \mathcal{O}_{X|U})$ is a ringed space, the structure sheaf $\mathcal{O}_{X|U}$ will be denoted simply by $\mathcal{O}_U$.*

Definition 2.2.5 *A morphism of ringed spaces is pair $(f, f^\sharp) : (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$, where $f : X \longrightarrow Y$ is* ***continuous*** *map, and $f^\sharp : \mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X$ is a morphism of sheaves of rings on Y.*

Remark 2.2.8 *For every open subset U of Y :*

1) $f^\sharp(U) : \mathcal{O}_Y(U) \longrightarrow \mathcal{O}_X(f^{-1}(U))$ is a ring homomorphism.

2) We have

$$\begin{array}{ccc} \mathcal{O}_Y(U) & \xrightarrow{f^\sharp(U)} & \mathcal{O}_X(f^{-1}(U)) \\ \downarrow{\scriptstyle res_{U,V}} & & \downarrow{\scriptstyle res_{f^{-1}(U),f^{-1}(V)}} \\ \mathcal{O}_Y(V) & \xrightarrow[f^\sharp(V)]{} & \mathcal{O}_X(f^{-1}(V)) \end{array}$$

for any open subsets $V \subseteq U$ of Y

3) Let's denote the set of morphisms of ringed spaces from X to Y by $Hom((X, \mathcal{O}_X), (Y, \mathcal{O}_Y))$. Then we have a canonical categorical isomorphism : $Hom((X, \mathcal{O}_X), (Y, \mathcal{O}_Y)) \cong \{f : X \longrightarrow Y$ (a continuous map) and $f^\flat : f^{-1}\mathcal{O}_Y \longrightarrow \mathcal{O}_X$ (a morphism of sheaves) $\}$

(see [9, Lemma 1.45])

Notation. Let $(f, f^\sharp) : (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ be a morphism of ringed spaces. We will simply write f instead of $(f, f^\sharp)$.

Examples 2.2.4 1) Let $\psi : U \longrightarrow V$ be a morphism of varieties, then ψ induces a canonical morphism of ringed spaces

$$(U, \mathcal{O}_U) \longrightarrow (V, \mathcal{O}_V)$$

where $\mathcal{O}_U$ (respectively $\mathcal{O}_V$) is the sheaf of regular functions on U (resp V).
We take $f = \psi : U \longrightarrow V$ to be the corresponding continuous map and $f^\sharp : \mathcal{O}_V \longrightarrow f_*\mathcal{O}_U$ to be defined by : For each open set $W \subseteq V$

$$\begin{array}{ccc} \mathcal{O}_V(W) & \longrightarrow & \mathcal{O}_U(f^{-1}(W)) \\ h & \longmapsto & f^\sharp(h) := h \circ \psi. \end{array}$$

2) Let $(X, \mathcal{O}_X)$ be a ringed space, $W \subseteq X$ be an open subset and let $j : W \longrightarrow X$ be the canonical injection. Then $(j, j^\sharp) : (W, \mathcal{O}_W) \longrightarrow (X, \mathcal{O}_X)$ is a morphism of ringed spaces, where for every open U of X, $j^\sharp(U) : \mathcal{O}_X(U) \longrightarrow j_*\mathcal{O}_W(U)(= \mathcal{O}_W(U \cap W))$ is the restriction morphism.

Remarks 2.2.2 1) Let $f : (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ be a morphism of ringed spaces. For any $x \in X$, f induces a morphism of the stalks $f^\sharp_x : \mathcal{O}_{Y,f(x)} \longrightarrow \mathcal{O}_{X,x}$

2) Let $(f, f^\sharp) : (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$, and $(h, h^\sharp) : (Y, \mathcal{O}_y) \longrightarrow (Z, \mathcal{O}_Z)$ be morphisms of ringed spaces. It is clear that $h \circ f$ is a continuous map and by lemma 2.1.3, we have $(h \circ f)_* = h_* \circ f_*$, then $(h \circ f)_*\mathcal{O}_X = h_*(f_*\mathcal{O}_X)$, since $f_*\mathcal{O}_X$ is a sheaf on Y then $h_* \circ f_*\mathcal{O}_X$ is a sheaf on Z.

Definition 2.2.6 Let $(f, f^\sharp) : (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ and $(h, h^\sharp) : (Y, \mathcal{O}_Y) \longrightarrow (Z, \mathcal{O}_Z)$ be morphisms of ringed spaces. The composition of these morphisms is given by the map $h \circ f$ and the morphism of sheaves $h^\sharp$ given by

$$\mathcal{O}_Z \longrightarrow h_*\mathcal{O}_Y \longrightarrow h_*f_*\mathcal{O}_X$$

We denote this composition of morphisms(of ringed spaces) as follows :

$$(h, h^\sharp) \circ (f, f^\sharp) = (h \circ f, f^\sharp \circ h^\sharp).$$

We get in this way a category $\mathcal{RS}$ of ringed spaces. An isomorphism of ringed spaces is a morphism which has an inverse. If X is a ringed space with structure sheaf $\mathcal{O}_X$, Z a topological space and $f : Z \longrightarrow X$ a continuous map, then $f^{-1}\mathcal{O}_X$ can be considered as a structure sheaf on Z. In particular any subspace of a ringed space is a ringed space.

Locally ringed spaces

Definition 2.2.7 *i) A locally ringed space is a ringed space $(X, \mathcal{O}_X)$ with the property that the stalk of each point is a local ring. In other words for all $x \in X$, $\mathcal{O}_{X,x} = \varinjlim_{x \in U} \mathcal{O}_X(U)$ is a local ring.*

ii) Given a locally ringed space $(X, \mathcal{O}_X)$, we say that $\mathcal{O}_{X,x}$ is the local ring of X at x. We denote by $\mathfrak{m}_{X,x}$ or simply by $\mathfrak{m}_x$ the maximal ideal of $\mathcal{O}_{X,x}$. The residue field of X at x is $\mathcal{O}_{X,x}/\mathfrak{m}_x$. We denote it by $k(x)$.

Example 2.2.1 *Let X be a complex analytic manifold and $\mathcal{O}_X$ the sheaf of holomorphic functions on X, then $(X, \mathcal{O}_X)$ is a locally ringed spaces.*

Definition 2.2.8 *A morphism of locally ringed spaces $(X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ is a morphism of ringed topological spaces $(f, f^\sharp)$ such that for all $x \in X$ the induced map*

$$f_x^\sharp : \mathcal{O}_{Y,f(x)} \longrightarrow \mathcal{O}_{X,x}$$

is a local homomorphism i.e., $f^\sharp(\mathfrak{m}_{f(x)}) \subseteq \mathfrak{m}_x$. Recall that we have $\mathcal{O}_{Y,f(x)} = (f^{-1}\mathcal{O}_Y)_x$ (see lemma 2.1.4).

Example 2.2.2 *Let M be a manifold on which we consider the sheaf $\mathcal{C}^\infty(M)$. Then $(M, \mathcal{C}^\infty(M))$ is a locally ringed space. Moreover, any morphism $f : M \longrightarrow N$ of manifolds induces a morphism of locally ringed spaces $(M, C^\infty(M)) \to (N, C^\infty(N))$.*

Let $(X, \mathcal{O}_X)$ be a locally ringed space and $x \in X$. We have a canonical surjection $\mathcal{O}_{X,x} \xrightarrow{\phi} k(x)$, called evaluation at x. For $h \in O_{X,x}$, denoting $\phi(x)$ by $h(x)$, $h(x) \neq 0$ if and only if h is invertible in $\mathcal{O}_{X,x}$. Let U be an open subset of X and $x \in U$. The composition morphism $\mathcal{O}_X(U) \longrightarrow \mathcal{O}_{X,x} \longrightarrow k(x)$ will also be denoted by $h \longmapsto h(x)$. In particular, if h is an invertible element of $\mathcal{O}_X(U)$, then $h(x)$ it is a nonzero element of $k(x)$.

2.3 Affine schemes and varieties

As we have seen, one can view a differentiable manifold of dimension m as a locally ringed space. Grothendieck defined a scheme in roughly the same way, with the important difference that, rather than one local model $\mathbb{R}^m$ in each dimension, one needs to use all the ringed spaces $Spec(R)$ for the local models.*

2.3.1 Affine schemes

In section 2.1, we introduced the notion of sheaf on an arbitrary topological space. In this section, we are interested in a very particular space, the spectrum of a commutative ring. We continue to assume that R denotes a ring commutative a unit.

**Alexander Grothendieck, (French 28 March 1928-13 November 2014) was a stateless and then French mathematician who became the leading figure in the creation of modern algebraic geometry. His research extended the scope of the field and added elements of commutative algebra, homological algebra, sheaf theory, and category theory to its foundations, while his so-called "relative" perspective led to revolutionary advances in many areas of pure mathematics. He is considered by many to be the greatest mathematician of the twentieth century.*

The Structure Sheaf on $Spec(R)$

Definition 2.3.1 *Let R be a ring, $X = Spec(R)$. We define a sheaf of rings on $Spec(R)$ as follows. For any open subset U of X, let*

$$\mathcal{O}_X(U) := \{s : U \longrightarrow \coprod_{Q\in X} R_Q \mid \text{for all } Q \in U, \text{ we have } s(Q) \in R_Q, \text{ there exist } a, f \in R, \text{ and an open subset } V \text{ of } U \text{ such that } V \subseteq D(f) \text{ and } s(L) = \tfrac{a}{f} \text{ for all } L \in V\}.$$

This formula clearly defines a sheaf of rings on X.

Remark 2.3.1 *1) Note the similarity in the above definition the definition of regular functions on a variety. The difference is that we consider functions into various local rings, instead of to a field.*

2) It is clear that sums and products of such functions are again such, and that the element 1 which gives 1 in each R_P is an identity. Hence $\mathcal{O}_X(U)$ is a commutative ring with identity.

3) If $V \subseteq U$ are open subsets of X, then the restriction map $\mathcal{O}_X(U) \longrightarrow \mathcal{O}_X(V)$, $s \longmapsto s_{|V}$ is a homomorphism of rings.

Proposition 2.3.1 *Let $X = Spec(R)$. Then :*

1) For all $f \in R$, we have a canonical isomorphism $\mathcal{O}_X(D(f)) \simeq R_f$, where R_f the localization of R by $S = \{1, f, f^2, \ldots\}$.

2) If $g \in R$ and $g \in (f)$, then there is commutative diagram

$$\begin{array}{ccc} \mathcal{O}_X(D(f)) & \longrightarrow & \mathcal{O}_X(D(g)) \\ \downarrow \simeq & & \downarrow \simeq \\ R_f & \longrightarrow & R_g \end{array}$$

where the vertical isomorphisms come from 1).

3) For any $P \in Spec(R)$, there is a natural isomorphism $\mathcal{O}_{X,P} \cong R_P$ which fits in a commutative diagram

$$\begin{array}{ccc} \mathcal{O}_{X,P} & \xrightarrow{\simeq} & R_P \\ \uparrow & & \uparrow \\ \mathcal{O}_X(X) & \xrightarrow[\simeq]{} & R \end{array}$$

Here the vertical morphisms are the natural ones and the lower horizontal one comes from 1).

Proof. *1) Let $f \in R$, and let $\psi : R_f \longrightarrow \mathcal{O}_X(D(f))$ be the map defined by :*

$$\psi(\frac{a}{f^n}) := \text{ the map } s : D(f) \longrightarrow \coprod_{P\in X} R_P \text{ which sends any } P \in D(f) \text{ to the image of } \frac{a}{f^n} \text{ in } R_P$$

One can easily see that ψ is a homomorphism of rings. We wish to show that ψ is an isomorphism.

- *ψ is injective :*
  We have $ker(\psi) = \{\frac{a}{f^n} \in R_f \mid \psi(\frac{a}{f^n}) = 0\} = \{\frac{a}{f^n} \in R_f | s(P) := \frac{a}{f^n} = 0$, in R_P, for all $P\}$ Suppose that $\frac{a}{f^n} \in ker(\psi)$ and $\frac{a}{f^n} \neq 0$, and let $Ann(\frac{a}{f^n}) := \{g \in R_f \mid g \cdot \frac{a}{f^n} = 0\}$. Since $\frac{a}{f^n}$, since $\frac{a}{f^n} \neq 0$, then $Ann(\frac{a}{f^n}) \neq R_f$, so there exists a maximal ideal $\mathfrak{m}$ of R_f such that $Ann(\frac{a}{f^n}) \subseteq \mathfrak{m}$. It follows that the image of $\frac{a}{f^n}$ in $R_{\mathfrak{m}}$ does not vanish, a contradiction.

* ψ *is surjective :*
  Let $s \in \mathcal{O}_X(D(f))$. *We know that in the neighbourhood of every point of* $D(f)$, s *is represented by a fraction. Since* $\mathcal{B} := \{D(g), g \in R\}$ *is a basis of* X *(see theorem 2.2.1) and* $D(f)$ *is compact (see proposition 2.2.2), then there are* $f_1, \ldots, f_r \in R$ $D(f) = \bigcup_{j=1}^{r} D(f_j)$. *There are* $g_1, \ldots, g_r \in R$ *such that* s *is represented on* $D(f_j)$ *by* $\frac{g_j}{f_j}$. *By proposition 2.2.2 we have* $D(f_i) \cap D(f_j) = D(f_i f_j)$. *Using the fact that* ψ *is injective, we get* $\frac{g_i}{f_i} = \frac{g_j}{f_j}$. *Hence for some* m

$$(f_i f_j)^m f_j g_i = (f_i f_j)^m f_i g_j.$$

Using the assumption and proposition 2.2.1, there are $h_1, \ldots, h_r \in R$ *and* $d \geq 1$ *such that* $f^d = \sum_{j=1}^{r} h_j f_j^{m+1}$. *Let* $\beta := \sum_{j=1}^{r} h_j f_j^m g_j$, *it easy to check that* $\beta f_i^{m+1} = f^d f_i^m g_i$. *Then*

$$\frac{\beta}{f^d} = \frac{g_i}{f_i}$$

in R_{f_i}. *In other words,* $\frac{\beta}{f^d}$ *is an element of* $D(f)$ *whose image in* $\mathcal{O}_X(D(f))$ *is* s.

2) *Immediate, using the fact that if* $D(g) \subseteq D(f)$ *if and only if* $g \in rad((f))$ *if and only if* $g^m = fc$, *for some positive integer* m. *So* f *is invertible in* R_g, *and we have a homomorphism of rings*

$$\theta : \begin{array}{ccc} R_f & \longrightarrow & R_g \\ \frac{a}{f^n} & \longmapsto & \frac{ac^n}{g^{mn}} \end{array}$$

3) *We have a natural isomorphism* $\mathcal{O}_{X,P} \cong \varinjlim_{f \in R, f \notin P} \mathcal{O}_X(D(f))$. *By 1) and 2), last ring is naturally isomorphic to* $\varinjlim_{f \in R, f \notin P} R_p$, *which can be identified with* R_P $(*)$.

Remark 2.3.2 *Let* R *be a ring and* $P \in Spec(R)$. *There is a natural isomorphism*

$$\varinjlim_{f \in R, f \notin P} R_P \simeq R_P$$

Here the arrows in the inductive system are defined as follows. If g *is a multiple of* f *then the arrow is the natural map. Otherwise there is no arrow. This justifying* $(*)$

Theorem 2.3.1 *Let* R *and* T *be two rings, and let* $\psi : R \longrightarrow T$ *be a homomorphism of rings. Then :*

i) $\left(X = Spec(R), \mathcal{O}_X\right)$ *is a locally ringed space.*

ii) ψ *induces a natural morphism of locally ringed spaces*

$$(\psi, \psi^\sharp) : \quad (Z := Spec(T), \mathcal{O}_Z) \quad \longrightarrow \quad (X := Spec(R), \mathcal{O}_X)$$

iii) *Any morphism of locally ringed spaces from* Z *to* X *is induced by a homomorphism of rings* $\psi : R \longrightarrow T$ *as in ii).*

Proof. i) *This follows from proposition 2.3.1.*

ii) *By proposition 2.2.4* ψ *induces a continuous map* $\psi^* : Z \longrightarrow X$, *we can localize* ψ *to obtain a local homomorphism of local rings* $\psi_Q : R_{\psi^{-1}}(Q) \longrightarrow T_Q$. *Now, for any open subset* U *of* X, *we have a homomorphism of rings* $(\psi^*)^\sharp : \mathcal{O}_X(U) \longrightarrow \mathcal{O}_Z\left((\psi^*)^{-1}(U)\right)$. *One can see that* $\left(\psi^*, (\psi^*)^\sharp\right)$ *is a morphism of locally ringed spaces.*

iii) *Let* $(f, f^\sharp) : (Z, \mathcal{O}_Z) \longrightarrow (X, \mathcal{O}_X)$ *be a morphism of locally ringed spaces. By definition we have for any open subset* V *of* X*, we have a homomorphism of rings* $f^\sharp(V) : \mathcal{O}_X(V) \longrightarrow \mathcal{O}_Z(\psi^{-1}(V))$. *In particular, for* $V = X$*, we have* $\mathcal{O}_X(X) = R$*, and* $\mathcal{O}_Z\big(f^{-1}(X)\big) = \mathcal{O}_Z(Z) = T$. *So we get a homomorphism of rings* $\psi := f^\sharp(X) : R \longrightarrow T$. *Let* $Q \in Spec(T)$*, we have an induced local homomorphism on the stalks,* $f^\sharp : \mathcal{O}_{X,f(Q)} \longrightarrow \mathcal{O}_{Z,Q}$ *such that the following diagram*

$$\begin{array}{ccc} R & \xrightarrow{\quad \psi \quad} & T \\ \big\downarrow & & \big\downarrow \\ R_{f(Q)} & \xrightarrow{\quad f^\sharp_Q \quad} & T_Q \end{array}$$

commutes. The assumption that $f^\sharp_Q$ *is local then gives* $\psi^{-1}(Q) = f(Q)$*, which shows that* f *coincides with the map* $Z \longrightarrow X$ *induced by* ψ. *It is immediate that* $f^\sharp$ *also is induced by* ψ. *So that* $(f, f^\sharp)$ *does indeed come from* ψ.

Corollary 2.3.1 *Let* R, T *be a two rings. Then the map*

$$\begin{array}{rccc} \chi : & Hom_{rings}(R, T) & \longrightarrow & Hom\big((Z, \mathcal{O}_Z), (X, \mathcal{O}_X)\big) \\ & \psi & \longmapsto & (\psi^*, (\psi^*)^\sharp) \end{array}$$

is a bijection.

Proof. *This follows from theorem 2.3.1 ii) and iii).*

Now, we come to the definition of a scheme.

Definition 2.3.2 *Let* X *be a locally ringed space. We say that* X *is an affine scheme if there exists a ring* R *such that* X *is isomorphic to the spectrum of* R*, i.e.,* X *is an affine scheme if and only if* $(X, \mathcal{O}_X) \simeq (Spec(R), \mathcal{O}_{Spec(R)})$*, where* $\simeq$ *is an isomorphism of locally ringed spaces as defined in section 2.2.2.*

Examples 2.3.1 1) *For a field* k*,* $Spec(k)$ *consists of one single point, with structural sheaf* k.

2) $Spec(k[T_1, \ldots, T_n])$ *is the affine space* $\mathbb{A}^n$ *over* k. *More generally, an affine variety over a field* k *is an affine scheme* $Spec(R)$*, where the ring* R *is a finitely generated* k*-algebra.*

3) *Let* X *be an affine scheme and let* $f \in R$*, then* $\big(D(f), \mathcal{O}_{X|D(f)}\big)$ *is also an affine scheme. Indeed, the canonical ring homomorphism*

$$R \longrightarrow R_f$$

induces a continuous map

$$h : \quad Spec(R_f) \quad \longrightarrow \quad Spec(R)$$

which is a homeomorphism onto its, image $D(f)$ *(see proposition 2.2.5). Moreover,* $h^\sharp$ *is an isomorphism. Indeed, for any* $Q \in Spec(R_f)$

$$h^\sharp_Q : R_{h(Q)} \longrightarrow (R_f)_Q$$

since $f \notin Q \cap R$. *Thus*

$$\big(D(f), \mathcal{O}_{X|D(f)}\big) \simeq \big(Spec(R_f), \mathcal{O}_{Spec}\big)$$

4) *Let* $(X, \mathcal{O}_X)$ *be an affine scheme,* $V \subseteq X$ *be an open subset and set* $\mathcal{O}_V := \mathcal{O}_{X|V}$*, then* $(V, \mathcal{O}_V)$ *is not necessarily an affine scheme (see [9, 4.1]).*

Now, we come to the general definition of a scheme :

Definition 2.3.3 *A scheme is a locally ringed space $(X, \mathcal{O}_X)$ such that every point x in X has an open neighbourhood U, which is isomorphic to an affine scheme as a locally ringed space. For each point x of a scheme X, one defines its residue field $k(x)$ as the quotient of the local ring $\mathcal{O}_{X,x}$, by its maximal ideal $\mathfrak{m}_x$.*

Remarks 2.3.1 *1) Equivalently, X is a scheme if there exists an open covering $\{U_i\}_{i\in I}$ of X such that $(U_i, \mathcal{O}_{X|U_i})$ is isomorphic to an affine scheme $(Spec(R_i), \mathcal{O}_{Spec_i(R_i)})$ for some rings R_i.*

2) We say that an open subset U of a scheme $(X, \mathcal{O}_X)$ is affine if $(U, \mathcal{O}_{X|U})$ is an affine scheme.

Proposition 2.3.2 *Any scheme has a basis of affine open subsets.*

Proof. *Let X be a scheme. By remarks 2.3.1, there exists an open covering $\{U_i\}_{i\in I}$ of X such that $(U_i, \mathcal{O}_{X|U_i})$ is an affine scheme, i.e., For any $i \in I$ there is a ring R_i, a homeomorphism*

$$\psi : U_i \longrightarrow Spec(R_i)$$

and a sheaf ismorphism

$$\psi_i : \mathcal{O}_{Spec_i(R_i)} \longrightarrow \psi_i^*(\mathcal{O}_{X|U_i})$$

For each i, we know that $\{D(f_i) \subseteq Spec(R_i) \,|\, f_i \in R_i\}$ is a basis for the topology of $Spec(R_i)$ (see theorem 2.2.1). Moreover, these $D(f_i)$ again define affine schemes by examples 2.3.1 3)

$$\left(D(f_i), \mathcal{O}_{Spec_i(R_i)\,|\,D(f_i)}\right) \simeq \left(Spec(R), \mathcal{O}_{Spec_i(R_i)}\right).$$

Let $V_i := \psi^{-1}(D(f_i)) \subseteq U_i$, so that

$$(V_i, \mathcal{O}_{X|V_i}) \simeq (D(f_i), \mathcal{O}_{Spec_i|D(f_i)})$$

is an affine schemes and $\mathcal{B}_i := \{V_i \subseteq U_i \,|\, f_i \in R_i\}$ is a basis of the topology on $U_i \subseteq X$. Then $\mathcal{B} = \bigcup_{i\in I} \mathcal{B}_i$ is a basis of the topology of X consisting of affine open subsets.

We now describe the morphisms between schemes.

Morphisms of Schemes

Definition 2.3.4 *A morphism of schemes is just a morphism of the underlying locally ringed spaces.*

Remarks 2.3.2 *1) Observe that if $f : Z \longrightarrow X$ is a morphism of schemes, then for each $z \in Z$, with image $x = f(z)$, there is an induced homomorphism $\mathcal{O}_{X,x} \longrightarrow \mathcal{O}_{Z,z}$, hence also a homomorphism between the residue fields $k(x) \longrightarrow k(y)$.*

2) For $x \in X$, by proposition 2.3.1 we have a natural isomorphism $\mathcal{O}_{X,x} = R_P$, for some prime ideal P of R. Moreover, we have $\mathfrak{m}_x = PR_P$, and $k(x) = R_P/PR_P$.

3) The schemes form a category (which is a full subcategory of the category of locally ringed spaces), we shall denote it by $\mathcal{S}ch$.

4) We shall denoted by $A\mathcal{S}ch$ the category of affine schemes.

Theorem 2.3.2 *There is an equivalence of categories*

$$\begin{array}{rccc} Spec : & (\mathcal{R}ing)^{op} & \longrightarrow & A\mathcal{S}ch \\ & R & \longmapsto & (Spec(R), \mathcal{O}_{Spec(R)}) \end{array}$$

Proof. *One can easily see that Spec is a morphism of categories. It suffices then to show that it is fully faithful.*
Let R, T be rings. We define the maps :

$$\begin{array}{rccc} \chi : & Hom_{rings}(R,T) & \longrightarrow & Hom((Z,\mathcal{O}_Z),(X,\mathcal{O}_X)) \\ & \psi & \longmapsto & (\psi^*, \psi^\sharp) \end{array}$$

which is a bijection (see corollary 2.3.1). Let $X = Spec(R)$, $Z = Spec(T)$, we define :

$$\begin{array}{rccc} \Psi : & Hom_{\mathcal{A}Sch}(Z,X) & \longrightarrow & Hom_{Rings}(R,T) \\ & (f,f^\sharp) & \longmapsto & f^\sharp(X) \end{array}$$

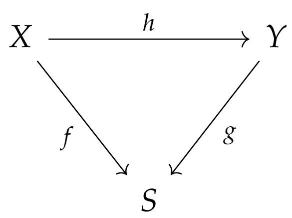
where as previously seen, $f^\sharp : \mathcal{O}_X(X)(= R) \longrightarrow \mathcal{O}_Z(Z)(= T)$. It is easy to see that $\chi \circ \Psi = id$, and using theorem 2.3.1 iii), we also have $\Psi \circ \chi = id$.

Relative schemes

Grothendieck has also introduced the relative viewpoint, whose idea is to study morphisms of schemes and how they behave instead of studying a scheme by itself.

Definition 2.3.5 *i) Let S be a (fixed) scheme. An S-scheme (or a scheme over S) is a scheme X, equipped with a morphism $f : X \longrightarrow S$.*

ii) A morphism from $(X, f : X \longrightarrow S)$ to $(Y, g : Y \longrightarrow S)$ is a morphism of schemes $h : X \longrightarrow Y$ such that the following diagram



is commutative. We also call such a morphism h an S-morphism.

Remarks 2.3.3 *1) The schemes over S form a category $\mathcal{S}ch/S$, and the set of morphisms as defined above will be denoted by $Hom_S(X,Y)$.*

2) We will say X is a scheme over over (a ring) R if X is a scheme over $Spec(R)$.

Examples 2.3.2 *1) Let S be a scheme that we view as an S-scheme with $id : S \to S$, and let X with $f : X \longrightarrow S$ an S-scheme. The S-morphism f is called an S-section.*

2) Every affine scheme is a scheme over $\mathbb{Z}$. Indeed, for any ring R, we have the natural map

$$\begin{array}{rccc} \phi : & \mathbb{Z} & \longrightarrow & R \\ & n & \longmapsto & n \cdot 1 \end{array}$$

which induces such structure.

3) An affine variety X over an algebraically closed field k comes with an inclusion $k \longrightarrow k[X]$. Applying Spec to this map, we see that the canonically associated scheme to X is a scheme over k.

Now, we come to special classes of morphisms.

Open subschemes and closed subschemes

Definition 2.3.6 *i) An open subscheme U of a scheme X is an open subset, equipped with the restriction of the sheaf $\mathcal{O}_X$ to U.*

ii) An open immersion is a morphism of schemes $X \longrightarrow Y$ which induces an isomorphism from X to an open subscheme of Y.

The notion of closed subscheme is more complicated, because you have to define a locally ringed space structure on the closed subset, and there is no canonical one. First we have to define closed immersions.

Definition 2.3.7 *A closed immersion is a morphism $f : X \longrightarrow Y$ of schemes such that :*

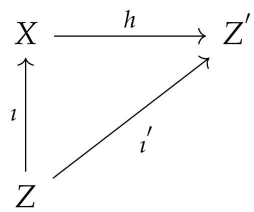
i) f induces a homeomorphism (a bicontinuous map) from X to a closed subset of Y.

ii) The morphism of sheaves $f^\sharp : \mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X$ is surjective.

Example 2.3.1 *Let R be a ring, J an ideal of R, $X = Spec(R)$ and $Z = Spec(R/J)$. By proposition 2.2.4 $\pi^* : Z \longrightarrow X$ is a homeomorphism from Z to $V(J)$, and $(\pi^*)^\sharp : \mathcal{O}_X \longrightarrow \pi^*_*\mathcal{O}_Z$ is surjective because it is surjective on the stalks.*

Definition 2.3.8 *(closed subscheme) Let X be a scheme. A closed subscheme of X is an equivalence class of closed immersions into X.*

Remark 2.3.3 *More precisely, A closed subscheme of a scheme X is a scheme Z, equipped with a closed immersion $\imath : Z \longrightarrow X$, where one identifies the pairs $(Z, \imath)$ and $(Z', \imath')$ if there exists an isomorphism of schemes $h : Z \longrightarrow Z'$ such that the following diagram*



is commutative.

Example 2.3.2 *$Spec(R/J)$ is a closed subscheme of $Spec(R)$ with underlying topological space $V(J)$.*

Gluing schemes

Given a family $\{X_i\}_{i \in I}$ of schemes indexed by a set I. Assume that in each of the schemes X_i we are given a collection of open subschemes X_{ij}, where the indices i and j run through I.

Notation. *Let $X_{ij} \subseteq X_i$ be open subschemes, and $\delta_{ij} : X_{ij} \longrightarrow X_{ji}$ be isomorphisms of schemes for all $i, j \in I$. We require also that*

i) $\delta_{ii} = id$.

ii) $\delta_{ij}(X_{ij} \cap X_{ik}) = X_{ji} \cap X_{jk}$.

iii) $\delta_{ik} = \delta_{ik} \circ \delta_{ij}$ on $X_{ij} \cap X_{ik}$.

Proposition 2.3.3 *Given gluing data X_i, δ_{ij} as above, there exists a scheme X with open immersions $\delta_i : X_i \longrightarrow X$ such that*

$$\begin{array}{ccccc} X_{ij} & \hookrightarrow & X_i & & \\ \downarrow{\scriptstyle \delta_{ij}} & & & \searrow^{\delta_i} & \\ X_{ji} & \hookrightarrow & X_j & \xrightarrow{\delta_j} & X \end{array} \tag{2.2}$$

The scheme X has the universal property : For every scheme Z and any family of morphisms of schemes $\eta_i : X_i \longrightarrow Z$ satisfying

$$\begin{array}{ccccc} X_{ij} & \hookrightarrow & X_i & & \\ \downarrow{\scriptstyle \delta_{ij}} & & & \searrow^{\eta_i} & \\ X_{ji} & \hookrightarrow & X_j & \xrightarrow{\eta_j} & Z \end{array} \tag{2.3}$$

there exists a unique morphism $\eta : X \longrightarrow Z$ such that

$$\begin{array}{ccc} X_i & \xrightarrow{\delta_i} & X \\ & \searrow^{\eta_i} & \downarrow{\scriptstyle \eta} \\ & & Z \end{array}$$

is commutative.

Remarks 2.3.4 *1) In (2.2), we have $\delta_{|X_{ij}} = \delta_{|X_{ji}} \circ \delta_{ij}$.*

2) In (2.3), we have $\eta_{|X_{ij}} = \eta_{j|X_{ij}} \circ \delta_{ij}$.

Proof. *Let $X := \coprod_i X_i / \sim$, where $x \in X_i \sim y \in X_j$ if and only if $y = \delta_{ij}(x)$. This makes a topological space X with open subsets $X_i \subseteq X$. We have a sheaf $\mathcal{O}_{X_i}$ on each X_i, and we glue them to get $\mathcal{O}_X$ (see theorem 2.1.4). For more details for the proof we refer to [9, Section 4.3, p.**91**].*

Example 2.3.3 *Let $X_1 = X_2 = \mathbb{A}^1_k$, $X_{12} = X_{21} = \mathbb{A}^1_k \setminus \{0\}$. Write $X_{12} = Spec(k[X, X^{-1}])$, $X_{21} = Spec(k[Y, Y^{-1}])$. Gluing them by $X \longmapsto Y^{-1}$, we get the projective line $\mathbb{P}^1$.*

2.3.2 Varieties

The goal of this section is to

* *describe how schemes are a generalization of varieties*

* *or more precisely that how there is a fully faithful functor.*

$$\tau : Var(k) \longrightarrow \mathcal{S}ch_k$$

from the category of varieties over an algebraically closed field k to the category of schemes over $Spec(k)$.

If you feel like a physicist, you might want to regard this as a way of understanding observables like positions in terms of spectra of certain operators. The starting point is the basic observation that the information contained in ordinary spaces may be encoded in the (rings and / or algebras of) functions on these spaces.

Notation. *Let X be a topological space and denote by $t(X)$ the set of nonempty irreducible closed subsets of X. Hence if $Z \subseteq X$ is closed, then $t(Z) \subseteq t(X)$. Moreover t has the following properties :*

i) $t(Z_1 \cup Z_2) = t(Z_1) \cup t(Z_2)$ *if* $Z_1, Z_2 \subseteq X$ *are closed*

ii) For a family of closed subsets $\{Z_i\}_i$, *we have* $t(\bigcap_i Z_i) = \bigcap_i t(Z_i)$.

i) and ii) define a topology on the set $t(X)$ by saying that $Y \subseteq X$ is closed if and only if $Y = t(Z)$ for some closed subset $Z \subseteq X$.
In addition, a continuous map $f : X_1 \longrightarrow X_2$ induces a continuous map $t(f) : t(X_1) \longrightarrow t(X_2)$ given by

$$t(f) : Z \longrightarrow \overline{f(Z)}.$$

$t(f)$ is well-defined since for an irreducible closed subset Z of X, $f(Z)$ is irreducible, so its closure $\overline{f(Z)}$ is also irreducible.
Thus t defines a functor $\mathcal{T}op \longrightarrow \mathcal{T}op$. Furthermore we have a continuous map

$$\begin{array}{rccc} \gamma : & X & \longrightarrow & t(X) \\ & x & \longmapsto & \overline{\{x\}} \end{array}$$

This map γ is the tool we have to use to add generic points in order to construct a scheme from a variety. We will only sketch the proof of the following theorem. A more detailed proof can e.g. be found in [12].

Theorem 2.3.3 *Let k be an algebraically closed field. Then there exists a fully faithful functor $\tau : Var(k) \longrightarrow \mathcal{S}ch_k$ from the category of varieties over k to the category of schemes over $Spec(k)$.*

***The idea of the proof* :** *Let X be a variety over k and denote by $\mathcal{O}_X$ its sheaf of regular functions. We set*

$$\tau(X) := (t(X), \gamma_* \mathcal{O}_X).$$

One has to show that this is indeed a scheme over $Spec(k)$. One first proves that $(t(X), \beta_* \mathcal{O}_X)$ is a scheme if X is an affine variety. Then, by examples 2.3.2, we know that giving a morphism of schemes $t(X) \longrightarrow Spec(k)$ is equivalent to endowing the sheaf $\gamma_* \mathcal{O}_X$ with the structure of a vector space over k. This is done by using theorem 2.3.2 : Since $\gamma^{-1}(t(X)) = X$, we have

$$Hom_{\mathcal{S}h}\big((t(X), \gamma_* \mathcal{O}_X), (Spec(k), \mathcal{O}_k)\big) \simeq Hom_{rings}\big(k, \gamma_*(t(X))\big) = Hom_{rings}\big(k, \mathcal{O}_X(X)\big).$$

We define this ring homomorphism $k \longrightarrow \mathcal{O}_X(X)$ by mapping $a \in k$ to the constant function λ_a on X. It follows that $\tau(X)$ is a scheme over $Spec(k)$. Now if X and Y are two varieties, one also checks that the natural map induced by τ

$$Hom_{var(k)}(X, Y) \longrightarrow Hom_{\mathcal{S}h_k}\big(\tau(Y), \tau(X)\big).$$

is a bijection.
The functor τ being fully faithful, it follows again that we may identify the category of varieties over k with a full subcategory of the category of schemes over $Spec(k)$ in the case of an algebraically closed field. Thus we may see varieties as being "embedded" into the category of schemes. In particular, that $\tau(X) \simeq \tau(Y)$ as schemes if and only if $X \simeq Y$ as varieties.

New definition of a variety

Definition 2.3.9 *Let k be an algebraically closed field. We say that a scheme X over $Spec(k)$ is an affine variety over k if it is isomorphic to the spectrum of the coordinate ring of an affine variety. In other words, $X = Spec(R)$, where R is a finitely generated k-algebra with no zero divisors.*

Examples 2.3.3 *The schemes*

1) $\mathbb{A}^1_{\mathbb{C}} = Spec(\mathbb{C}[t])$ *and* $Spec\big(\mathbb{C}[X,Y]/(X^2 - Y^3)\big)$ *are affine varieties.*

2) $Spec\big(\mathbb{C}[X,Y]/(XY)\big)$ *is not affine variety.*

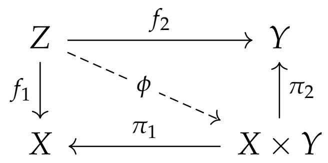
2.4 Fiber products and dimension of schemes

2.4.1 Fiber products

In classical geometry (The theory of algebraic varieties). We know that we can construct the Cartesian product $X \times Y$ of two varieties X and Y. The identification $\mathbb{A}^n_k \times \mathbb{A}^m_k = \mathbb{A}^{n+m}_k$ shows that this is a reasonable thing to do. Indeed, If $X = Z(f_1, \dots, f_r) \subseteq \mathbb{A}^n_k$ and $Y = Z(g_1, \dots, g_s) \subseteq \mathbb{A}^m_k$ are two affine varieties, then their product $X \times Y$ is the affine variety $Z(f_1, \dots, f_r, g_1, \dots, g_s) \subseteq \mathbb{A}^{m+n}_k$, and departing from this, the general case is handled by a gluing process. However, with schemes we redefine

$$\mathbb{A}^n_k = Spec(k[T_1, \dots, T_n])$$

and the cartesian product no longer works even as sets!
We have to understand what the product really means in the categorical language. Let us start with sets X, Y, the product is a new set $X \times Y$ with projections $\pi_1 : X \longrightarrow X \times Y$ and $\pi_2 : X \longrightarrow X \times Y$ which is universal in the sense that given any other set Z with projections $f_1 : Z \longrightarrow X$, $f_2 : Z \longrightarrow Y$, we have a unique map $\phi : Z \longrightarrow X \times Y$, namely $\phi(z) = (f_1(z), f_2(z))$, such that

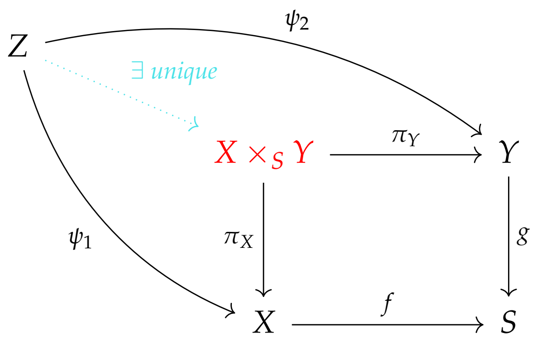


commutes. This can be used to define the product in any category. Note that there is no guarantee that the product exists in an arbitrary category, but it will be unique up to isomorphism if it does.
In this subsection, for any scheme S and any two S-schemes $X \longrightarrow S$ and $Y \longrightarrow S$ we will construct a new scheme, denoted $X \times_S Y$, equipped with projection morphisms $\pi_X : X \times_S Y \longrightarrow X$ and $\pi_Y : X \times_S Y \longrightarrow Y$ satisfying a certain universal property.

Let $\mathcal{C}$ be category and S be a fixed object in $\mathcal{C}$.

Definition 2.4.1 *(Fiber product) The fiber product of $f : X \longrightarrow S$, $g : Y \longrightarrow S$ (if it exists) is an object $X \times_S Y \in \mathcal{C}$ with morphism π_X, π_Y to X, Y. For any $Z \in \mathcal{C}$ with morphisms ψ_1, ψ_2 to X, Y respectively (commuting with f and g as indicated in the diagram below), there exists a unique morphism*

$Z \to X \times Y$ such that the whole diagram is commutative.



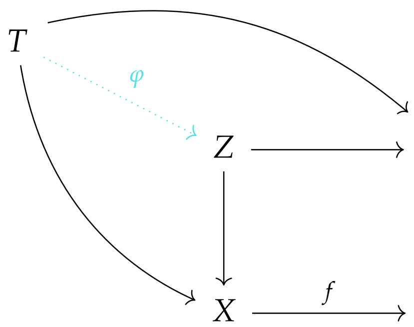
Notation and convention *1) We note the unique morphism $Z \longrightarrow X \times_S Y$ by $(\psi_1, \psi_2)_S$.*

2) We call $\pi_X : X \times_S Y \longrightarrow X$ the first projection, and $\pi_Y : X \times_S Y \longrightarrow Y$ the second projection.

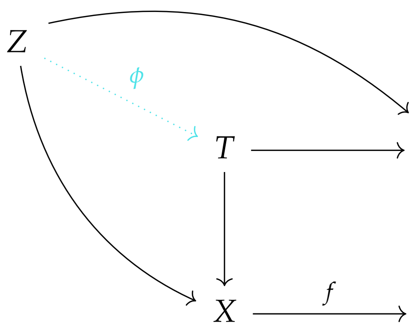
Example 2.4.1 *For sets or topological spaces $X \times_S Y = \{(x, y) \in X \times Y \mid f(x) = g(y)\}$.*

Theorem 2.4.1 *The fiber product $X \times_S Y$ is unique if it exists. In other words, if Z and T are two fiber products satisfying the above characteristic property, then Z and T are canonically isomorphic.*

Proof. *Let Z and T be two fiber products satisfying the above characteristic property. In particular T comes together with morphisms to X and Y. As Z is a fiber product, we get a morphism $\varphi : T \longrightarrow Z$*



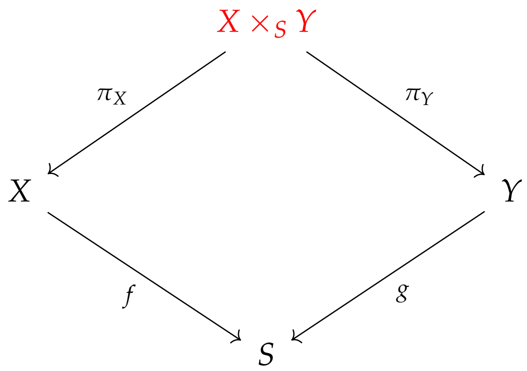
So that this diagram commutes. By symmetry we get a morphism $\phi : Z \longrightarrow T$ as well. The diagram



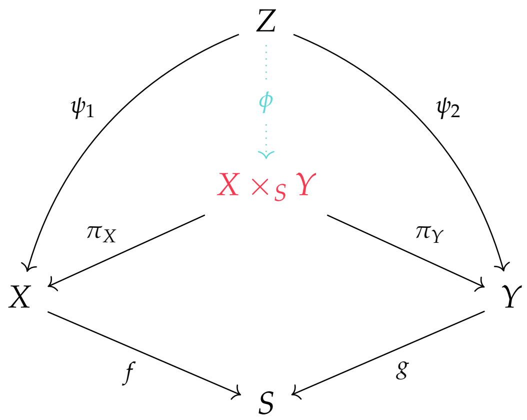
is then commutative by construction. But the same diagram is commutative too if we replace $\varphi \circ \phi$ by id_Z. The universal property when considering Z as a fiber product, we have $\varphi \circ \phi = id_Z$. Moreover, by symmetry $\phi \circ \varphi = id_T$. So Z and T are canonical isomorphic.

In particular, the fiber product is defined in the category of schemes, i.e., by taking $\mathcal{C} = \mathcal{S}h$, is defined in the following way :

Definition 2.4.2 *Let X, Y, S be schemes with morphisms $f : X \longrightarrow S$, and $g : Y \longrightarrow S$. The fiber product of X and Y over S is a scheme $X \times_S Y$ with morphisms π_X, π_Y*



making the diagram commutative, along with the universal property that for any scheme Z with morphisms ψ_1, ψ_2 to X and Y, respectively, such that $f \circ \psi_1 = g \circ \psi_2$, there exists a unique morphism $\phi : Z \longrightarrow X \times_S Y$ such that $\psi_1 = \pi_X \circ \phi$ and $\psi_2 = \pi_Y \circ \phi$



Proposition 2.4.1 *Fibre products exist in the category of schemes.*

Proof. *See [12, Theorem 3.3, p.**87**].*

Consequence. 2.4.1 *If $X = Spec(A)$, $Y = Spec(T)$ and $S = Spec(R)$, where A, T and R are commutative rings, f, g make A and T into R-algebras, and we have $X \times_S Y = Spec\big(A \otimes_R T\big)$*

Remark 2.4.1 *Observe that if $S \subseteq T$ is an open subscheme, then $X \times_T Y = X \times_S Y$ as if $j : S \longrightarrow T$ is the natural inclusion morphism, then $f \circ \psi_1 = g \circ \psi_2$ if and only if $j \circ f \circ \psi_1 = j \circ g \circ \psi_2$. Also observe that if V is an open subset of X, then $U \times_S Y = \pi_X^{-1}(V) \subseteq X \times_S Y$. Indeed, $U \times_S Y$ is an open subscheme of $X \times_S Y$.*

Proposition 2.4.2 *Let $f : X \longrightarrow S$ and $g : Y \longrightarrow S$ be morphisms of schemes. Suppose that $U \subseteq S$, $V \subseteq X$, $W \subseteq Y$ are opens subschemes such that $f(V) \subseteq U$ and $g(W) \subseteq U$. Then the canonical morphism $V \times_U W \longrightarrow X \times_S Y$ is an open immersion which identifies $V \times_U W$ with $\pi_X^{-1}(V) \cap \pi_Y^{-1}(W)$.*

Proof. *Let Z be a scheme. Suppose that $\varphi_1 : Z \longrightarrow V$ and $\varphi_2 : Z \longrightarrow W$ are morphisms such that $f \circ \varphi_1 = g \circ \varphi_2$ as morphisms into U. Then they agree as morphisms into S. By the universal property of fibre product we get a unique morphism $\phi : Z \longrightarrow X \times_S Y$. Moreover, ϕ has image contained in the open $\pi_X^{-1}(V) \cap \pi_Y^{-1}(W)$. Thus $\pi_X^{-1}(V) \cap \pi_Y^{-1}(W)$ is a fibre product of V and W over U. The result follows from the uniqueness of the fibre product.*

Basic properties of the fibre product

Proposition 2.4.3 *Let X, Y and Z be schemes over S. Then :*

i) *(Reflectivity) $X \times_S S \simeq X$.*

ii) *(Symmetry) $X \times_S Y \simeq Y \times_S X$.*

iii) *(Associativity) $(X \times_S Y) \times_S Z \simeq X \times_S (Y \times_S Z)$.*

If $S^{'}$ is a scheme over S and we assume that Y is as well a scheme over $S^{'}$, then

iv) *(Transitivity) $X \times_S S^{'} \times_{S^{'}} Y \simeq X \times_S Y$, where $X \times_S S^{'}$ is a scheme over $S^{'}$ via the projection onto $S^{'}$ and Y is a scheme over S via the map $S^{'} \longrightarrow S$.*

v) *Let $f_1 : X_1 \longrightarrow X$ and $g_1 : Y_1 \longrightarrow Y$ two S-morphisms. There is a unique morphism $f_1 \times g_1 : X_1 \times_S Y_1 \longrightarrow X \times_S Y$ such that the two squares in the diagram commute*

$$\begin{array}{ccccc} X_1 & \xleftarrow{\pi_{X_1}} & X_1 \times_S Y_1 & \xrightarrow{\pi_{Y_1}} & Y_1 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_1 \times g_1} & & \downarrow{\scriptstyle g_1} \\ X & \xleftarrow{\pi_X} & X \times_S Y & \xrightarrow{\pi_Y} & Y \end{array}$$

Proof. *All there properties follow from the universal property of the fiber product.*

Fibres

Definition 2.4.3 *Let $f : X \longrightarrow S$ be a morphism of scheme and $s \in S$ be a point. The scheme theoretic fibre X_s of f over s, or simply the fibre of f over s, is the scheme fitting in the following fibre product diagram*

$$\begin{array}{ccc} X_s = Spec(k(s)) \times_S X & \longrightarrow & X \\ \downarrow & & \downarrow \\ Spec(k(s)) & \longrightarrow & S \end{array}$$

In particular, the fibre X_s is a scheme over $k(s)$.

Proposition 2.4.4 *The map $\pi_X : X_s \longrightarrow X$ is a homeomorphism between X_s and $f^{-1}(s)$.*

Proof. *Without loss of generality, we may assume $S = Spec(R)$, $X = Spec(T)$, and f is induced by $\psi : R \longrightarrow T$. Let $s \in S$ be defined by the prime ideal $\mathfrak{q}$. We have $k(s) = k(\mathfrak{q}) = R_{\mathfrak{q}}/\mathfrak{q}R_{\mathfrak{q}}$. So $X_s = Spec(k(s)) \times_S X = Spec\big(R_{\mathfrak{q}}/\mathfrak{q}R_{\mathfrak{q}} \otimes_R T\big) = Spec\big(T_{\mathfrak{q}}/\mathfrak{q}T_{\mathfrak{q}}\big)$. Elements of $Spec(T_{\mathfrak{q}}/\mathfrak{q}T_{\mathfrak{q}})$ correspond bijectively to primes $\mathfrak{p}$ of T such that $\psi(\mathfrak{q}) \subseteq \mathfrak{p}$, and $\mathfrak{p}$ does not intersect $\psi(R \setminus \mathfrak{q})$. This is equivalent to $\psi^{-1}(\mathfrak{p}) = \mathfrak{q}$. So the map $\pi_X : X_s \longrightarrow f^{-1}(s)$ is a bijection. Since $Spec(T_{\mathfrak{q}}/\mathfrak{q}T_{\mathfrak{q}}) \longrightarrow Spec(T_{\mathfrak{q}}) \longrightarrow Spec(T)$ are successive embeddings, and $f^{-1}(s)$ is endowed with the subspace topology, π_X is a homeomorphism.*

Remark 2.4.2 *We may view a morphism $f : X \longrightarrow S$ as family of fibers X_s parameterized by $s \in S$.*

Example 2.4.2 *Let $X := Spec(\frac{k[X,Y,Z]}{(ZY-X^2)})$ and $S := Spec(k[Z])$. We have the inclusion $k[Z] \hookrightarrow \frac{k[X,Y,Z]}{(ZY-X^2)}$ so we get a continuous map $g : X \longrightarrow S$. By identifying the closed point of S with elements of k, for $b \in k$, $b \neq 0$, X_b= is the plane curve defined by $bY = X^2$.*

Base change

Definition 2.4.4 *Let X, S, and $S^{'}$ be schemes. We define $X_S := X \times_{S'} S$, the following diagram*

$$\begin{array}{ccc} X_S & \xrightarrow{\pi_X} & X \\ \downarrow{\scriptstyle \pi_S} & & \downarrow{\scriptstyle g} \\ S & \xrightarrow{f} & S^{'} \end{array}$$

*is called the **base change** of g to S via f.*

Remarks 2.4.1 *1) The above definition generalises the idea of changing the "base coefficients".*

2) Let $h : Y \longrightarrow S$, and let $\psi : X \longrightarrow Y$ be a S-morphism, then there is an induced morphism $\psi_{S'} = \psi \times id_{S'}$ from $X_{S'}$ to $Y_{S'}$ over $S^{'}$, making the following diagram

$$\begin{array}{ccccc} X_{S'} & \xrightarrow{\psi_{S'}} & Y_{S'} & \xrightarrow{\pi_{S'}} & S^{'} \\ \downarrow{\scriptstyle \pi_X} & & \downarrow{\scriptstyle \pi_Y} & & \downarrow{\scriptstyle g} \\ X & \xrightarrow{\psi} & Y & \xrightarrow{h} & S \end{array}$$

commutative.

Example 2.4.3 *Let $S = Spec(R)$, then $\mathbb{A}^m_S := \mathbb{A}^m_{\mathbb{Z}} \times_{Spec(\mathbb{Z})} S$ is a base change of $\mathbb{A}^m_{\mathbb{Z}}(:= Spec(\mathbb{Z}[T_1, \ldots, T_m]) \longrightarrow$ $Spec(\mathbb{Z})$ to X via $S \longrightarrow Spec(\mathbb{Z})$.*

Definition 2.4.5 *We say that a property $\mathcal{P}$ of morphism of schemes is stable under base change if for any morphism $X \longrightarrow S$ verifying $\mathcal{P}$, $X \times_S S^{'}$ also verifies $\mathcal{P}$ for every S-scheme $S^{'}$.*

2.4.2 Dimensions of schemes

Recall that the Krull dimension of a ring R is defined as the supernum of length of all strictly ascending chains of prime ideals in R.
Recall also that the dimension of a topological space X is the supernum of all integers d such that there exists a chain

$$Z_0 \subsetneq \ldots \subsetneq Z_n$$

of distinct irreducible closed subsets of X.

Definition 2.4.6 *Let X be a scheme. We define the dimension of X to be the dimension of its underlying topological space.*

Proposition 2.4.5 *Let $X = Spec(R)$ be an affine scheme. The dimension of X equals the Krull dimension of R.*

Proof. *Let $Z_0 \subsetneq \cdots \subsetneq Z_r$ be a chain of distinct irreducible closed subsets of X. By proposition 2.2.8, the Z_i are the form $V(P_i)$, for some $P_i \in Spec(R)$. Moreover, by theorem 2.2.2 i), we have $j\big(V(P_i)\big) = rad(P_i) = P_i$ for all i. Also, for all i, the fact that $Z_i \subsetneq Z_{i+1}$ implies $j(Z_{i+1}) = P_{i+1} \subsetneq j(Z_i) = P_i$. Hence, we get a chain of strictly ascending prime ideals of R*

$$P_r \subsetneq \cdots \subsetneq P_0.$$

Let $Q_i = P_{r-i}$, then we have

$$Q_0 \subsetneq \cdots \subsetneq Q_r.$$

Hence $dim(X) \leq dim(R)$. Conversely, let $P_0 \subsetneq \cdots \subsetneq P_n$ be a strictly ascending chain of prime ideals of R. Applying $V(.)$, we get a chain of irreducible closed subsets of X

$$V(P_n) \subsetneq \cdots \subsetneq V(P_0).$$

Set $Z_i = V(P_{n-i})$, we get a strictly ascending chain

$$Z_0 \subsetneq \cdots \subsetneq Z_n$$

of irreducible closed subsets of X. Hence $dim(R) \leq dim(X)$.

Remark 2.4.3 *Recall that, if R is a Noetherian ring, then $dim(R[T]) = dim(R) + 1$.*

Examples 2.4.1 1) *If R is a Noetherian ring, then the dimension of $\mathbb{A}^m_R = Spec(R[T_1, \ldots, T_n])$ equals $m + dim(R)$.*

2) *$dim(Spec(\mathbb{Z})) = 1$. all maximal chain have the form $V(P) \subsetneq V(0) = Spec(\mathbb{Z})$.*

3) *If k is a field, then we $dim(k) = 0$. So $dim(Spec(k)) = 0$.*

Remark 2.4.4 *Let X be a scheme.*

i) *If $Y \subseteq X$ is an open or a closed subscheme, then $dim(Y) \leq dim(X)$.*

ii) *Let $X = \bigcup_{i \in I} Spec(R_i)$ be a scheme $dim(X) = Sup_i(dim(Spec(R_i))$ (see proposition 1.2.1 1)).*

Codimension

Let X be a topological space, and let $Z \subseteq X$ be an irreducible closed subset of X.

* *The codimension $codim(Z, X)$ of Z is defined to be*

  $Sup\{m \mid$ *there exists a strictly ascending chain* $Z = Z_0 \subsetneq \cdots \subsetneq Z_m$, *of irreducible closed subsets of* $X\}$.

* *If Z is an arbitrary closed subset, we define its codimension as*

$$inf\{codim(Z', X) \mid Z' \text{ is an irreducible and closed subset of } X\}.$$

By the correspondence between closed subsets and prime ideals (see theorem 2.2.2), the codimension of $V(P)$ in $Spec(R)$ is the height of the prime ideal P of R.

Proposition 2.4.6 *Let X be scheme, $x \in X$ be a point and set $Z = \overline{\{x\}}$. Then $dim(\mathcal{O}_{X,x}) = codim(Z, X)$*

Proof. *Let $Z \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_r$ be a chain of distincts irreducible closed subsets of X, then for any open neighborhood V of x the generic points $y_1, \ldots, y_r$ of Z_i' are contained in V. We can assume that $V = Spec(R)$ is an affine open of x, then the generic points correspond to prime ideals (of R) $P_r \subsetneq \cdots \subsetneq P_0 = P$, where P is the prime ideal corresponding to $x (\in V)$. in R. Therefore, $dim(\mathcal{O}_{X,x}) = codim(Z, X)$.*

2.5 Local and global properties of schemes

In this section, we survey some of the main geometric properties of schemes.

2.5.1 Noetherian schemes

Definition 2.5.1 *i) A scheme X is called locally Noetherian if X admits an affine open covering $X = \bigcup_{i \in I} X_i$ such that $\mathcal{O}_X(X_i)$ is a Noetherian ring for all i.*

ii) A scheme X is called Noetherian if it is compact and locally Noetherian, where X is compact means that every open covering of X has a finite subcovering.

Remarks 2.5.1 *1) Recall from lemma 2.2.6, that for any commutative ring R, $Spec(R)$ is compact. So an affine scheme is compact.*

2) In general a scheme is Noetherian if and only it can be covered by finitely many open affine schemes $Spec(R_i)$, where each R_i is Noetherian.

Lemma 2.5.1 *Let R be a Noetherian ring and S be a multiplicatively closed subset of R. Then $S^{-1}R$ is a Noetherian ring.*

Proof. *See [3, Proposition 7.3, p.**80**].*

Theorem 2.5.1 *Let X be a scheme. Then X is locally Noetherian if and only if for any open subset U of X, which is isomorphic to an affine scheme $(Spec(R), \mathcal{O}_{Spec(R)})$ as locally ringed space, the ring R is Noetherian.*

Proof. *By simple logical reductions using lemma 2.5.1 and proposition 2.2.2, the statement of the theorem can be shown to be equivalent to the following statement in commutative algebra. Let R be a ring, let $g_1, \dots, g_r \in R$ be such that $1 \in (g_1, \dots, g_r)$ i.e $R = (g_1, \dots, g_r)$. If R_{g_i} is Noetherian for all i, then R is Noetherian. This is what we shall prove.*
Let $\psi_i : R \longrightarrow R_{g_i}$ be the natural homomorphism and J be an ideal of R. Then we have

$$J = \bigcap_{i \in \{1,\dots,r\}} \psi^{-1}(\psi_i(J)R_{g_i}) \tag{2.4}$$

where $\psi_i(J)R_{g_i}$ is the ideal in R_{g_i} generated by $\psi_i(J)$. Now, from the assumption that $(g_1, \dots, g_r) = R$, and by proposition 2.2.1 5) we seen that there are element $b_i \in R$ such that

$$\sum_i b_i g_i^{m+n} = 1$$

Thus $c \in J$. Now consider an ascending chain of ideals of R

$$J_1 \subseteq J_2 \subseteq \cdots$$

For all $i \in \{1, \dots, r\}$

$$\psi_i(J_1)R_{g_i} \subseteq \psi_i(J_2)R_{g_i} \subseteq \cdots \tag{2.5}$$

is an ascending chain of ideals of R_{g_i}, which must become stationary because R_{g_i} is Noetherian, since there are only finite many R_{g_i}, we conclude from the above that $J_1 \subseteq J_2 \subseteq \cdots$ is stationary. Hence R is Noetherian.

Proposition 2.5.1 *Let R be a commutative ring. Then $Spec(R)$ is Noetherian if and only if R is Noetherian.*

Proof. *$\Rightarrow$) You should think of this as a purely algebraic fact : Refining the cover, we can assume that for each i, we have $X_i = R_{f_i}$. As in the proof of theorem 2.5.1 R is Noetherian provided that each localization R_{f_i} is Noetherian, and $1 \in (f_1, \dots, f_r)$.*

$\Leftarrow$) This follows from theorem 2.2.2.

Proposition 2.5.2 *Let X be a Noetherian scheme, then its underlining topological space is Noetherian.*

Proof. *Since X is compact, then we can write* $X = \bigcup_{i=1}^{r} X_i$, *where* $(X_i, \mathcal{O}_{X_i}) \simeq (Spec(R_i), \mathcal{O}_{Spec_i(R_i)})$. *A descending chain*

$$Z_1 \supseteq Z_2 \supseteq \cdots \tag{2.6}$$

gives rise to a chain for all $i \in \{1, \ldots, r\}$

$$Z_1 \cap X_i \supseteq Z_2 \cap X_i \supseteq \cdots \tag{2.7}$$

of closed subsets in X_i. *Since* X_i *are Noetherian, this last chain is stationary. Since we have only a finite number of indices i, this implies that X is Noetherian.*

Proposition 2.5.3 *Let X be a locally Noetherian scheme. Then any closed or open subscheme of X is also locally Noetherian.*

Proof. *Without loss of generality, we may assume that X is Noetherian. We can consider an open covering* $(X_i)_{i \in I}$ *of X such that* $\forall i$, $X_i = Spec(R_i)$, *where each* R_i *is Noetherian.*
Let $Z \subseteq X$ *be an open or closed subset, we will show that* $Z \cap X_i$ *is Noetherian. Since* $Z \cap X_i$ *is an open or a closed subset of an affine scheme, we reduce our statement to considering the case where* $X = Spec(R)$.
If Z is open, by theorem 2.2.1, there are elements $f_1, \ldots, f_r \in R$ *such that* $Z = \bigcup_{i=1}^{r} D(f_i) = \bigcup_{i=1}^{r} Spec(R_{f_i})$. *Since R is Noetherian, then by lemma 2.5.1, for all i,* R_{f_i} *are Noetherian, and so by proposition 2.5.1,* $Spec(R_{f_i})$ *is Noetherian. It follows that Z is also Noetherian.*
If Z is closed, we have $Z = V(J)$ *for some ideal* $J \subseteq R$. *We know that if R is Noetherian then* R/J *is also Noetherian. So* $Spec(R/J)$ *is Noetherian, and by proposition 2.2.4,* $Spec(R/J)$ *is homeomorphic to* $V(J)$. *Hence Z is Noetherian.*

Definition 2.5.2 *Let* $f : X \longrightarrow Y$ *be a morphism of schemes.*

i) *f is called locally of finite type if for every affine open* $U = Spec(R) \subseteq Y$, $f^{-1}(U) = \bigcup_j V_j$ *with each* $V_j = Spec(A_j)$ *affine open subset of X, with* A_j *a finitely generated R-algebra.*

ii) *f is called compact if* $Y = \bigcup_i Y_i$ *with* Y_i *open affine subschemes of Y that* $f^{-1}(Y_i)$ *is compact for all i.*

iii) *f is called of finite type if f is locally of finite type and compact.*

iv) *f is called finite if* $Y = \bigcup_i Y_i$ *with each* $Y_i = Spec(R_i)$ *affine open subschemes of Y where* A_i *is a finite* R_i*-algebra.*

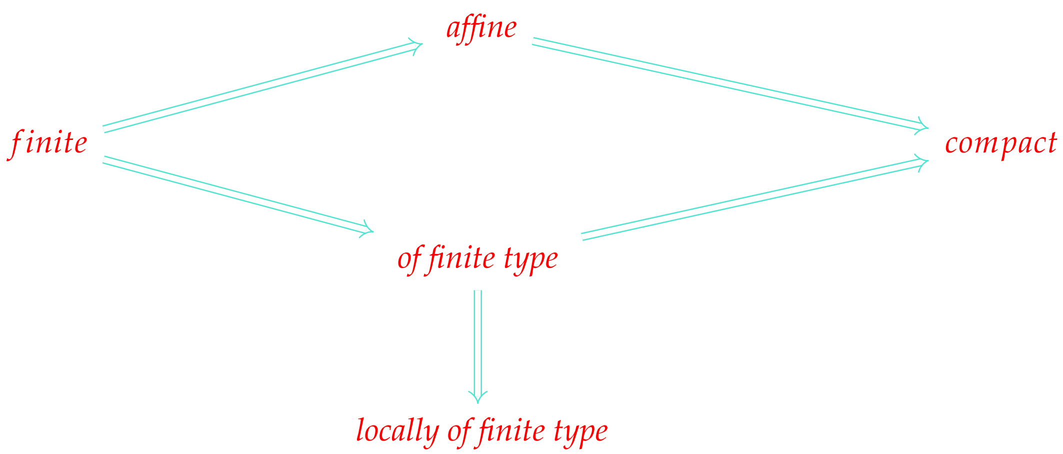
v) *f is called affine if* $Y = \bigcup_i U_i$ *with* $U_i = Spec(R_i)$, *an affine open subscheme of Y such that* $f^{-1}(U_i)$ *is also affine.*

Remarks 2.5.2 1) *Recall that an R-algebra A is finite if A is finitely generated as an R-module.*

2) *Finiteness is transitive : The composition of finite morphisms is finite. This follows from the fact that finite generation of modules is transitive.*

3) *The base change of a morphism which is locally of finite type is locally of finite type. The same is true for morphisms of finite type (see [30]).*

4) We have the following implications :



Examples 2.5.1 *1) $Spec(\mathbb{Q}) \longrightarrow Spec(\mathbb{Z})$ is not locally of finite type.*

2) Let R be a ring. Then $\mathbb{A}^n \longrightarrow Spec(R)$, and $\mathbb{P}^n \longrightarrow Spec(R)$ are both of finite type.

2.5.2 Irreducible schemes

Definition 2.5.3 *A nonempty scheme is connected if its underlying topological space is connected, i.e cannot be written as a disjoint union of two nonempty open sets.*

Proposition 2.5.4 *Let $X = Spec(R)$ be an affine scheme. The following assertions are equivalent :*

1) X is connected.

2) The only idempotents of R are 0 and 1.

Proof. *1) $\Rightarrow$ 2) Assume that X is connected. If R contains an idempotent element r such that $r \neq 1, 0$, then we have $R = r \cdot R \times (1 - r) \cdot R$ and both rR and $(1 - r) \cdot R$ are non trivial subrings of R. Hence $Spec(R) = Spec(rR) \times Spec\big((1 - r) \cdot R\big) \simeq Spec(rR) \coprod Spec\big((1 - r) \cdot R\big)$. So X is not connected. 2) $\Rightarrow$ 1) Assume that $0, 1$ are the only idempotent of R. If X is not connected, then $X = X_1 \coprod X_2$ with $X_i \subsetneq X$ nonempty opens. We then have $\mathcal{O}_X(X) = \mathcal{O}_X(X_1) \times \mathcal{O}_X(X_2)$. As X_i are nonempty, then $\mathcal{O}_X(X_i)$ are non trivial rings. In particular, $(1, 0)$ is a non trivial idempotent of R. A contradiction.*

Definition 2.5.4 *Let X be a scheme, we say that X is irreducible if its underlying topological space is irreducible.*

Remark 2.5.1 *Plainly, irreducible topological spaces are connected.*

Examples 2.5.2 *1) Let k be an algebraically closed field. $\mathbb{A}^m_k = Spec(k[T_1, \ldots, T_n])$ is irreducible.*

2) $X = k[X, Y]$, $Z = V(XY) = V(X) \cup V(Y)$. Then Z is not irreducible.

Proposition 2.5.5 *Let $X = Spec(R)$ be an affine scheme. Then X is irreducible if and only if $N(R)$ is a prime ideal.*

Proof. *See proof of theorem 2.2.4.*

Recall again the following terminology : Let X be a topological space and let $x, y \in X$, we say that x is a generic point if $\overline{\{x\}} = X$ (see definition 2.2.3). An irreducible component of X is maximal irreducible closed subset of X. y is a specialization of x (x specializes to y) if $y \in \overline{\{x\}}$.

Examples 2.5.3 *1) Let X be an affine scheme, and let $P \in X$, then $\overline{P} = V(P)$. Moreover, P is the only generic point of $V(P)$.*

2) Let R be a domain, then (0) is only generic point of $Spec(R)$.

Proposition 2.5.6 *Let X be a scheme. Then :*

1) Every irreducible closed subset of X has a unique generic point.

2) For any generic point $x \in X$, $\overline{\{x\}}$ is an irreducible component of X. Moreover, there exists a bijection between the set of irreducible components of X and the set of generic points of X.

3) For any $x \in X$, there exists a bijection between the set of irreducible component of $Spec(\mathcal{O}_{X,x})$ and the set of irreducible components of X containing x.

Proof. *1) Let Z be an irreducible closed of X. Assume that X is affine scheme i.e $X = Spec(R)$ for some ring R. By proposition 2.2.8 Z is irreducible if and only if Z is of the form $Z = V(P)$, for some prime ideal P of R. By example 2.5.3, P is the only generic point of Z.*
Now, for X an arbitrary scheme, let the only $x \in Z$, then x has an affine neighborhood V in X. Since Z is irreducible then $Z \cap V \subseteq Z$ is irreducible and dense i.e $\overline{Z \cap V} = Z$. By the above, $Z \cap V$ contains a generic point x_o, which is also a generic point of Z. If $y_0 \in Z$ with $\overline{\{y_0\}} = Z$, then $y_0 \in Z \cap V$ and it follows immediately (from the affine case above) that $x_0 = y_0$.

2) Let Z be an irreducible component of X, and $x_0 \in Z$ be its generic point. We claim that x_0 is a generic point of X, that is no point other then x_0 can specialize to x_0 : if y_0 specialize to x_0 then $x_0 \in \overline{\{y_0\}}$, hence $Z = \overline{\{x_0\}} \subseteq \overline{\{y_0\}}$. Since Z is a maximal irreducible closed subset of X, then $\overline{\{x_0\}} = \overline{\{y_0\}}$, hence $x_0 = y_0$. This shows that x_0 is a generic point of X. It is easy to check that $x \longmapsto \overline{\{x\}}$ is a bijection from X onto the set of irreducible components of X.

3) We may assume that $X = Spec(R)$, with $x \in X$ corresponding to a prime ideal P_x of R. By the correspondence between irreducible closed subsets and the prime ideals of R (see lemma 2.2.2 and proposition 2.2.8), an irreducible component of X corresponds to a minimal prime ideal of R. Hence the irreducible components of X containing x are in one-to-one correspondence with minimal prime ideals of R which are contained in P_x, or still with the minimal prime ideals of $R_{P_x} = \mathcal{O}_{X,x}$, that is the irreducible component of $Spec(\mathcal{O}_{X,x})$.

2.5.3 Regular schemes

Recall that, a local Noetherian ring $(R, \mathfrak{m})$ is said to be regular if $dim(R) = dim_k(\mathfrak{m}/\mathfrak{m}^2)$, where $k := R/\mathfrak{m}$. Recall also that R is regular if and only if every local ring R_P of R is regular. For more details we refer to [3, Theorem 11.22].

Definition 2.5.5 *Let X be a locally Noetherian scheme, and let $x \in X$ be a point.*

i) We say that X is regular at x, or x is a regular point of X if $\mathcal{O}_{X,x}$ is regular.

ii) We say that X is regular if X is regular at all points.

iii) A point $x \in X$ which is not regular is called a singular point of X.

iv) A scheme that is not regular is said to be singular.

Remark 2.5.2 *For i) equivalently, X is regular at x if there exists an affine open neighbourhood $U \subseteq X$ of x such that the rings $\mathcal{O}_X(U)$ is Noetherian and regular.*

Proposition 2.5.7 *Let X be a scheme. The following are equivalent :*

1) *X is regular.*

2) *For every open $U \subseteq X$, the ring $\mathcal{O}_X(U)$ is Noetherian and regular.*

3) *There exists an affine open covering $X = \bigcup_{i\in I} U_i$ such that each $\mathcal{O}_X(U_i)$ is Noetherian and regular.*

4) *There exists an affine open covering $X = \bigcup_i X_i$ such that each open subscheme X_i is regular.*

Proof. *1) ⇒ 2) Let U be an open subset of X. By theorem 2.5.1 $\mathcal{O}_X(U) \simeq (Spec(R), \mathcal{O}_{Spec(R)})$ as locally ringed space for some Noetherian ring. By theorem 2.2.3 $Spec(R)$ is Noetherian. So $\mathcal{O}_X(U)$ is Noetherian. Since X is regular, then in particular it is regular at all point of $\mathcal{U}$, so necessarily for any prime ideal Q of R, R_Q is regular, so R is regular.*
2) ⇒ 3) Clear.
3)⇒ 4) Immediate.
4) ⇒ 1) Assume that $X = \bigcup_j X_j$ with X_j regular for all j. Let j_0 such that $x \in X_{j_0}$. Since X_{j_0} is regular at x, then x is a regular point of X.

Corollary 2.5.1 *If X is a regular scheme, then every open subscheme is regular.*

Corollary 2.5.2 *Let X be a Noetherian scheme, then X is regular if and only if X is regular at all its closed points.*

Proof. *If X is regular, then X is regular at all points of X. In particular, X is regular at all closed points. Conversely, note that, as X is Noetherian any closed subset of X admits a closed point. One can deduce that X is regular.*

Definition 2.5.6 *Let X be a locally Noetherian scheme. We denote the set of regular points of X by **Reg**(X), and we denote the set of singular points by **Sing**(X).*

Remark 2.5.3 *Let $X = Spec(R)$ be a Noetherian affine scheme. Then $Spec(R)$ is regular if and only if for all $P \in Spec(R)$, $\mathcal{O}_{X,P} \simeq R_P$ is regular if and only if R is regular.*

2.5.4 Reduced and integral schemes

Reduced schemes

Recall that a commutative ring R is said to be reduced if it has no nilpotent elements, i.e the only nilpotent element of R is 0. Recall also that R is called integral if for any $a, b \in R$ such that $ab = 0$, we have $a = 0$ or $b = 0$.

Definition 2.5.7 *Let X be a scheme.*

i) *X is called reduced at point x, if the local ring $\mathcal{O}_{X,x}$ is reduced.*

ii) *X is called reduced, if it is reduced at all points.*

Proposition 2.5.8 *Let X be a scheme. Then X is reduced if and only if for each nonempty open $U \subseteq X$, the ring $\mathcal{O}_X(U)$ is reduced.*

Proof. *Assume that X is reduced and let U be an open subset of X. We want to show that $\mathcal{O}_X(U)$ is a reduced ring. Let $f \in \mathcal{O}_X(U)$ be a section of U and suppose that $f^m = 0$, for some positive integer m. Plainly, the canonical image f_x of f in $\mathcal{O}_{X,x}$ is also nilpotent, so $f_x = 0$. Since $\mathcal{O}_X$ is a sheaf, then by definition 2.1.6 i) $f = 0$. The converse is clear.*

Recall a direct limit of reduced rings is also reduced.

Proposition 2.5.9 *Let $X = Spec(R)$ be an affine scheme, then X is reduced if and only if R is reduced.*

Proof. *If X is reduced by proposition 2.5.8 $\mathcal{O}_X(X)$ is reduced and by proposition 2.3.1 3) $\mathcal{O}_X(X) \simeq R$. So R is reduced. Conversely, suppose that R is reduced and let $P \in Spec(R)$. By proposition 2.3.1 3) we have $\mathcal{O}_{X,P} \simeq R_P$. Moreover, we know that any localisation of a reduced ring is reduced. So, $\mathcal{O}_{X,P}$ is reduced.*

Remark 2.5.4 *Let X be an affine scheme i.e., $X = Spec(R)$ for some ring R, then $X_{red} := Spec\big(R/N(R)\big)$ is a reduced scheme.*

Integral schemes

Definition 2.5.8 *Let X be a scheme.*

i) We say that X is an integral at $x \in X$ if $\mathcal{O}_{X,x}$ is integral domain.

ii) If X is integral at all points of X, and X is irreducible, then we say X is integral.

Proposition 2.5.10 *Let X be a scheme. Then X is an integral if and only if $\mathcal{O}_X(U)$ is an integral domain for every open subset U of X.*

Proof. *Assume that X is integral, U be an open subset of X, and let $f, g \in \mathcal{O}_X(U)$ such that $fg = 0$. For $x \in X$, let $f(x)$ be the image of f in $k(x)$. $X_f := \{x \in U \,|\, f(x) = 0\}$, and $X_g = \{x \in U \,|\, g(x) = 0\}$. X_f and X_g are two closed subsets of X. Indeed, it suffices to see that X_f is closed in any affine open subset $W = Spec(R)$ of U. We have $X_f \cap W = V(f)$, and $X_g \cap W = V(g)$. So X_f and X_g are closed in W. By lemma 1.3.1 X_f and X_g are closed in X. Moreover, we have $X_f \cup X_g = U$, since $fg = 0$. Because $\mathcal{U}$ is irreducible, then $X_f = U$ or $X_g = U$. We can assume $X_f = U$. We claim that $f = 0$. Indeed, we only need to show that $f_{|V} = 0$ for any affine open $V \subseteq U$. But $f_{|V} \in N(\mathcal{O}_X(V))$ which is reduced. So $f_{|V} = 0$. Hence $f = 0$. Conversely, assume that $\mathcal{O}_X(U)$ is integral for any nonempty open U of X. In particular, all local rings $\mathcal{O}_{X,x}$ are integral. It remains to check that X is irreducible. Write $X = X_1 \cup X_2$ with X_i two closed subsets of X such that $X_i \subsetneq X$. Let $V_i = X \setminus X_i$, $i = 1, 2$ which is open in X. Moreover, we have $V_1 \cap V_2 = \emptyset$. Hence $\mathcal{O}_X(V_1 \cup V_2) = \mathcal{O}_X(V_1) \times \mathcal{O}_X(V_2)$. In particular $\mathcal{O}_X(U)$, where $U = V_1 \cup V_2$, is not integral. A contradiction.*

Proposition 2.5.11 *Let $X = Spec(R)$ be an affine scheme, then X is integral if and only if R is integral domain.*

Proof. *If X is integral, then by proposition 2.5.10 we have for any open subset U of X, $\mathcal{O}_X(U)$ is an integral domain. In particular, for $U = X$ we get $R(= \mathcal{O}_X(X))$ is integral domain. Conversely, Assume that R is integral domain, then $N(R)$ is a prime ideal, so by theorem 2.2.4, $Spec(R)$ is irreducible. Now let $P \in Spec(R)$, then $\mathcal{O}_{X,P}$ being the localization of integral domain is also integral domain.*

Example 2.5.1 *Let $Z = Spec(k[T_1, \ldots, T_n])$ be an affine scheme, then X is integral.*

Proposition 2.5.12 *Let X be a scheme. Then X is integral if and only if it's reduced, and irreducible.*

Proof. *Assume X is integral. Clearly it is reduced. If X is reducible then there exist closed subsets X_1, X_2 of X such that $X = X_1 \cup X_2$, take $U_i = X \setminus X_i$ for $i = 1, 2$, which are disjoint open subsets of X. Then $\mathcal{O}_X(U_1 \cup U_2) = \mathcal{O}_X(U_1) \times \mathcal{O}_X(U_2)$, which is not an integral domain. A contradiction. Now, assume X is reduced and irreducible. Let $U \subseteq X$ be open and assume that $f, g \in \mathcal{O}_X(U)$ with $fg = 0$. Let*

$$X_f = \{x \in U \,|\, f_x \in \mathfrak{m}_x\}, \text{ and } X_g = \{x \in U \,|\, g_x \in \mathfrak{m}_x\}$$

For any affine open $W = Spec(R) \subseteq U$, we have

$$(f_{|W})_x \in \mathfrak{m}_x \text{ if and only if } x \in V(f|_W).$$

Thus, $X_f \cap W = V(f)$ and $X_g \cap W = V(g)$. So X_f and X_g are closed. Moreover, we $X_f \cup X_g = U$. But X is irreducible, so U is irreducible as well (see proposition 1.1.3). We can then assume that $X_f = U$. But then in R, f is in every prime ideal, so f is nilpotent. So $f = 0$. Hence X is integral.

Lemma 2.5.2 *Let X be an integral scheme with a generic point ϵ. Then :*

i) $k(X) := \mathcal{O}_{X,\epsilon}$ is a field (called the function field of X).

ii) For any open subset U of X, the natural maps $\mathcal{O}_X(U) \longrightarrow \mathcal{O}_{X,\epsilon}$, and $\mathcal{O}_{X,x} \longrightarrow \mathcal{O}_{X,\epsilon}$ are injective.

Proof. *i) To see that $\mathcal{O}_{X,\epsilon}$ is a field, we may take an arbitrary nonempty open affine subset $U = Spec(R)$ of X observe that $\mathcal{O}_{X,\epsilon} = R_{(0)}$ which is the fractions field of R.*

ii) We may reduceour proof to the case where $U = Spec(R)$ is affine. In this case $\mathcal{O}_X(U) = R \longrightarrow Frac(R) = \mathcal{O}_{X,\epsilon}$ is injective.

Corollary 2.5.3 *Let X be an integral scheme, $W \subseteq U$ be open subsets of X, then the restriction map $\mathcal{O}_X(U) \longrightarrow \mathcal{O}_X(W)$ is injective.*

We say that an element $f \in k(X)$ is defined (or regular) in the point x if $f \in \mathcal{O}_{X,x}$.

Proposition 2.5.13 *Let X be an integral scheme and let $f \in k(X)$. The set $U_f := \{x \in X \,|\, f \in \mathcal{O}_{X,x}\}$ where f is defined, is open.*

Proof. *Let $x \in U_f$ and let $V := Spec(R)$ be an affine neighbourhood of x. Consider the ideal $I_f := \{a \in R \,|\, af \in R\}$. If P is a prime ideal of R, then $f \in R_P$ if and only if $I_f \not\subseteq P$ that is, $V(I_f)$ is the complement of $U_f \cap Spec(R)$.*

Proposition 2.5.14 *Let X be an integral scheme with function field $k(X)$. Then*

$$\mathcal{O}_X(U) = \bigcap_{x \in U} \mathcal{O}_{X,x} = \{f \in k(X) \,|\, f \text{ can be represented as } \frac{g}{h}, \text{ where } h(x) \neq 0, \forall x \in U\} (\subseteq k(X)).$$

Proof. *Clearly, we have $\mathcal{O}_X(U) \subseteq \bigcap_{x \in U} \mathcal{O}_{X,x}$. Conversely, by the sheaf condition, and the injectivity proved in lemma 2.5.2 ii), we may assume that $U = Spec(R)$ is an affine open. Then we are reduced to prove that $R = \bigcap_{P \in Spec(R)} R_p$, seen as a subring of $Frac(R)$. Indeed, for $f \in Frac(R)$ such that $f \in \bigcap_{P \in Spec(R)} R_P$, then for $P \in Spec(R)$, there exists $(a_P, b_P) \in R \times (R \setminus P)$ such that $f = \frac{a_P}{b_P}$. As R is integral domain, we deduce then $fb_P \in R$. If we take $\{b_P, P \in Spec(R)\}$, which generates the unit ideal. So one can find $c_P \in R$, almost all zero, such that $1 = \sum_P c_P b_P$, so $f = \sum_P c_P f b_P = \sum_P c_p a_P$. This gives the result.*

Remark 2.5.5 *If $X = Spec(R)$, then*

1) $\mathcal{O}_X(D(f)) = \{\frac{a}{f^m} \,|\, a \in R, m \geq 0\} \subseteq Frac(R)$.

2) $\mathcal{O}_{X,x} = \{\frac{f}{g} \,|\, f, g \in R, g \notin P_x\}$.

Examples 2.5.4 *1) The function field of $\mathbb{A}_k^m = Spec(k[T_1, \ldots, T_m])$ is $k(T_1, \ldots, T_m)$.*

2) *The function field of $Spec(\mathbb{Z})$ is $\mathbb{Q}$.*

Let X be an integral scheme of finite type. We can study the dimension of X in terms of the function field:

Proposition 2.5.15 *Let X be be integral scheme of finite type over field K with function field $k(X)$. Then*

1) $dim(X) = tr.deg_K(k(X))$.

2) *For any open subset U of X, we have $dim(X) = dim(U)$.*

3) *If Z is a closed subset of X, then*

$$codim(Z, X) = inf\{dim(\mathcal{O}_{X,z}) \,|\, z \in Z\} \text{ and } dim(X) = dim(Z) + codim(Z, X).$$

In particular, for a closed point x of X, we have $dim(X) = dim(\mathcal{O}_{X,x})$.

Proof. 1) *We may assume that $X = Spec(R)$ is affine X. Since X is of finite type, then R is a finitely generated K-algebra, with the quotient field $K := k(X)$. By theorem 1.2.2, we have $dim(R) = tr.deg_K(Frac(R))$, and by proposition 2.4.5, we have $dim(R) = dim(Spec(R))$. So, $dim(X) = tr.deg_K(Frac(R))$.*

2) *Let U be an open subset of X. As X and U have the same function field, and by 1) $dim(U) = dim(X)$.*

3) *We may assume that $X = Spec(R)$, where R is a finitely generated K-algebra and then use the formula $dim(R/P) + ht(P) = dim(R)$ for any prime ideal of R.*

Example 2.5.2 $dim(\mathbb{P}^m_k) = dim(\mathbb{A}^m_k) = m$.

2.5.5 Normal schemes

A normal domain is a domain which is integrally closed in its field of fractions. Recall that a ring R is said to be normal if all its local rings are normal domains. Thus it makes sense to define a normal scheme as follows.

Definition 2.5.9 *Let X be a scheme.*

i) *We say that X is normal at $x \in X$ if the local ring $\mathcal{O}_{X,x}$ is a normal domain.*

ii) *We say that X is normal if its is irreducible and normal at all $x \in X$.*

Proposition 2.5.16 *Let X be a scheme. The following are equivalent.*

1) *X is normal.*

2) *For every open $U \subseteq X$ the ring $\mathcal{O}_X(U)$ is a normal domain.*

Proof. 1)$\Rightarrow$ 2) *Suppose that X is normal. Let U be an open of X. The scheme X integral, so $\mathcal{O}_X(U)$ is an integral domain. We may assume that U is affine, i.e., $U = Spec(R)$ for some ring R. As X is normal then U is normal, so for any prime ideal of R, the localization R_P is normal. So R is normal. Hence $\mathcal{O}_X(U)$ is a normal domain.*
2)$\Rightarrow$ 1) *Let $x \in X$, and let U be an open neighborhood of x. Then $\mathcal{O}_X(U)$ is a normal domain. So, $\mathcal{O}_{X,x}$ is normal domain. Hence X is normal at x.*

Corollary 2.5.4 *If X is normal. Then :*

i) *There exists an affine open covering* $X = \bigcup_{i\in I} U_i$ *such that each* $\mathcal{O}_X(U_i)$ *is normal.*

ii) *There exists an open covering* $X = \bigcup_{i\in I} X_i$ *such that each open subscheme* X_i *is normal.*

Example 2.5.3 $\mathbb{A}^m_k$ *and* $\mathbb{P}^m_k$ *are normal schemes.*

Proposition 2.5.17 *Let* X *be a normal scheme. Then* X *is reduced.*

Proof. *Let* $x \in X$. *Since* $\mathcal{O}_{X,x}$ *is a normal domain, then* $\mathcal{O}_{X,x}$ *is domain, so the only nilpotent element of* $\mathcal{O}_{X,x}$ *is* 0, *so* X *is reduced.*

Definition 2.5.10 *Let* $f : X \longrightarrow Y$ *be a morphism of schemes. We say that* f *is dominant if the image of* f *is dense in* Y.

If X *and* Y *are integral,* f *is dominant is equivalent to saying that the generic point of* X *maps to the generic point of* Y. *In this case,* $f^\sharp$ *induces a map from the stalk* $\mathcal{O}_{Y,\beta}$ *to* $\mathcal{O}_{X,\epsilon}$, *where* ϵ *and* β *are the generic points in* X *and* Y, *respectively. But by lemma 2.5.2 the stalks at the generic points are the function fields* $k(X)$ *and* $k(Y)$. *Hence we obtain a map* $\psi^\sharp : k(Y) \longrightarrow k(X)$, *which is injective.*

Proposition 2.5.18 *Let* $f : X \longrightarrow Y$ *be a morphism of integral schemes. Then the following are equivalent :*

1) f *is dominant.*

2) *For every affine open subsets* $U \subseteq X$, $V \subseteq Y$ *such that* $f(U) \subseteq V$, *the ring homomorphism* $f^\sharp : \mathcal{O}_Y(V) \longrightarrow \mathcal{O}_X(U)$ *is injective.*

3) *For all* $x \in X$, *the local homomorphism* $f^\sharp_x : \mathcal{O}_{Y,f(x)} \longrightarrow \mathcal{O}_{X,x}$ *is injective.*

Proof. 1)$\Leftrightarrow$ 2) *We may assume that* $U = X = Spec(R)$, *and* $V = Y = Spec(A)$ *and that* f *is induced by a homomorphism* $\psi : A \longrightarrow R$ *of integral domains. We see that* f *maps the generic point to the generic point if and only if* $\psi^{-1}(0) = (0)$ *which holds true if and only if* ψ *is injective.*
2)$\Rightarrow$ 3) *Let* $x \in X$ *Taking* U *be an affine open neighborhood of* x, *and* V *also an affine open neighborhood of* $f(x)$ *such that* $f(U) \subseteq V$. *By ii)* $f^\sharp : \mathcal{O}_Y(V) \longrightarrow \mathcal{O}_X(U)$ *is injective. Then by proposition 2.1.2 the induced morphism to stalks is also injective. Hence* $f^\sharp_x : \mathcal{O}_{Y,f(x)} \longrightarrow \mathcal{O}_{X,x}$ *is injective.*
3)$\Rightarrow$ 2) *Suppose that for any* $x \in X$, $f^\sharp_x : \mathcal{O}_{Y,f(x)} \longrightarrow \mathcal{O}_{X,x}$ *is injective. By proposition 2.1.2* $f^\sharp$ *is injective, so for any affine open* U *of* X, *and affine open subset* V *of* Y *such that* $f(U) \subseteq V$, $f^\sharp : \mathcal{O}_Y(V) \longrightarrow \mathcal{O}_X(U)$ *is injective.*

Theorem 2.5.2 *Let* X *be an integral scheme, then there is a normal scheme* $\tilde{X}$, *and a morphism* $\pi : \tilde{X} \longrightarrow X$ *satisfying the following universal property : For any dominant morphism* $g : Y \longrightarrow X$ *from a normal scheme* Y, *there is a unique morphism* $h : Y \longrightarrow \tilde{X}$ *such that* $g = \pi_X \circ h$.

Proof. *See [17, Proposition 1.22, p.**120**].*

Definition 2.5.11 *The scheme* $\tilde{X}$ *over* X *is called the normalization of* X.

Remark 2.5.6 X *and* $\tilde{X}$ *have the same dimension.*

Example 2.5.4 *Let* $X = Spec(R)$ *where* $R = k[X, Y]/(y^2 - X^3)$. *There is an isomorphism of* k-*algebras between* R *and* $k[t^2, t^3]$ *given by sending* $X \longmapsto t^2$ *and* $Y \longmapsto t^3$. *It is clear that* $k[t^2, t^3]$ *is a domain with fraction field* $K = k(t)$. *Moreover, the normalization of* R *equals* $\tilde{R} = k[t]$. *The inclusion* $R \longrightarrow \tilde{R}$ *induces the normalization morphism* $f : \mathbb{A}^1_k \longrightarrow X$.

2.5.6 Separated Schemes

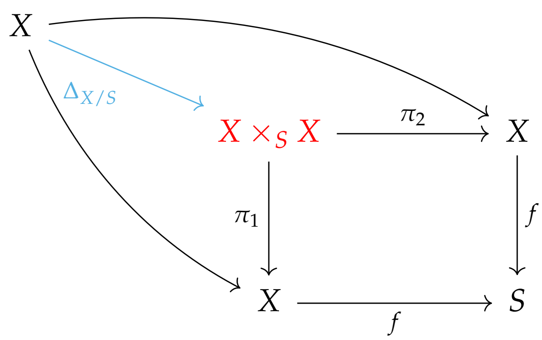
Recall that a topological space X is separated (or Hausdorff) if and only if the diagonal subset $\Delta(X)$ of $X \times X$ is a closed with respect to the product topology. The separation property fails on the underlying space of a scheme. So, one needs to refine the notion of separation to suite this context. For this, given a scheme X over a scheme S (with a morphism of schemes $f : X \longrightarrow S$), let's consider the diagonal morphism

$$\Delta_{X/S} : X \longrightarrow X \times_S X$$

defined to be the unique morphism of schemes such that

$$\pi_i \circ \Delta_{X/S} = id_X, i = 1, 2, \text{ where } \pi_i' s \text{ denote the two projections } X \times_S X \to X.$$

In terms of diagram we have the following diagram



Definition 2.5.12 *Let $f : X \longrightarrow S$ be a morphism of schemes. f is called an immersion if f factorizes as $X \longrightarrow U \longrightarrow S$, where $X \longrightarrow U$ is closed immersion and $U \longrightarrow S$ is open immersion.*

Lemma 2.5.3 *Let $f : X \longrightarrow Y$ be an immersion of schemes. Then f is closed immersion if and only if $f(X) \subseteq Y$ is a closed subset.*

Proof. *See [30, Lemma 26.10.4].*

Lemma 2.5.4 *If X and S are affine schemes. Then $\Delta_{X/S} : X \longrightarrow X \times_S X$ is a closed immersion.*

Proof. *Let $X = Spec(R)$, $S = Spec(A)$ and $f : X \longrightarrow Y$ be a morphism. f is separated. $\Delta_{X/S} : Spec(R) \longrightarrow Spec(R) \times_{Spec(A)} Spec(R) \cong Spec(R \otimes_A R)$ is induced by the canonical homomorphism of rings $\Delta : R \otimes_A R \longrightarrow R$. The latter is surjective, hence $\Delta_{X/S}$ is a closed immersion.*

Proposition 2.5.19 *Let X be a scheme over S. Then $\Delta_{X/S}$ is an immersion.*

Proof. *See [30, Lemma 26.21.2].*

Let R be a ring, then the natural ring homomorphism $\mathbb{Z} \to R$, $n \mapsto n \cdot 1_R$, induces a morphism of schemes $Spec(R) \to Spec(\mathbb{Z})$ and so any affine scheme can be considered as a $\mathbb{Z}$-scheme in a natural way. More generally, any scheme X can be considered as $\mathbb{Z}$ scheme in a canonical way.

Definition 2.5.13 *Let S be a scheme, and X an S-scheme with morphism $f : X \longrightarrow S$.*

i) *We say that f is separated if the diagonal morphism $\Delta_{X/S} : X \longrightarrow X \times_S X$ is closed immersion. In this case we say that X is separated S-scheme or X separated over S.*

ii) *A scheme is said to be separated if X separated over $Spec(\mathbb{Z})$.*

Example 2.5.5 *Any morphism of affine schemes is separated. In particular any affine scheme is separated.*

Proposition 2.5.20 *Let $f : X \longrightarrow S$ be a morphism of schemes. Then f is separated if and only if $\Delta_{X/S}(X)$ is a closed subset of $X \times_S X$.*

Proof. *If f is separated, then $\Delta_{X/S}$ is a closed immersion. So $\Delta_{X/S}(X)$ identifies with a closed of $X \times_S X$ (see definition 2.3.7). Hence $\Delta_{X/S}(X)$ is a closed. Conversely, as $\Delta : X \longrightarrow X \times_S X$ is an immersion (see proposition 2.5.19), and $\Delta_{X/S}(X)$ is closed. Then by lemma 2.5.3 $\Delta_{X/S}$ is a closed immersion.*

Proposition 2.5.21 *Let $f : X \longrightarrow S$ be a morphism of schemes with $S = Spec(R)$ is affine. The following are equivalent :*

1) *f is separated.*

2) *For every pair of affine opens $U, V \subseteq X$, $U \cap V$ is again affine. Moreover, the canonical homomorphism $\mathcal{O}_X(U) \otimes \mathcal{O}_X(V) \longrightarrow \mathcal{O}_X(U \cap V)$ is surjective.*

3) *There exists an open affine covering $X = \bigcup_{i \in I} U_i$ such that $U_i \cap U_j$ is affine and the canonical homomorphism $\mathcal{O}_X(U_i) \otimes \mathcal{O}_X(U_j) \longrightarrow \mathcal{O}_X(U_i \cap U_j)$ is surjective.*

Proof. *See [17, Proposition 3.6, p.**100**].*

Theorem 2.5.3 *i) Open and closed immersions are separated.*

ii) Let $f : X \longrightarrow Y$, and $g : Y \longrightarrow Z$ be two separated morphisms, then $g \circ f$ is separated. In particular, immersions are separated.

iii) Separated (resp. quasi-separated) morphisms are stable under base change.

iv) Let $f : X \longrightarrow Y$, and $g : Y \longrightarrow Z$ be morphisms such that $g \circ f$ is separated (resp. quasi-separated). Then f is separated (resp. quasi-separated).

v) A fibre product of separated (resp. quasi-separated) morphisms is separated (resp. quasi-separated).

Proof. *See [17, Proposition 3.9, p.**101**].*

2.5.7 Proper morphisms

In topology, a proper morphism is a morphism for which the inverse image of a compact Hausdorff† subspace set is compact Hausdorff. As above, the lack of good separation for the Zariski topology means one needs to use a some new notion on schemes.
Recall that a map of topological spaces $f : X \longrightarrow Y$ is said to be closed if for any closed subset Z of X, its image $f(Z) \subseteq Y$ is closed.

Definition 2.5.14 *Let $f : X \longrightarrow Y$ be a morphism of schemes*

i) f is said universally closed if every base change of f is a closed mapping.

ii) f is said to be proper if f is separated, of finite type, and universally closed. We say in this case that X is proper over Y.

iii) We say that X is proper if X is proper over $Spec(\mathbb{Z})$.

In i) f is said universally closed if for each morphism $Z \longrightarrow Y$, the projection $\pi_Z : Z \times_Y X \longrightarrow Z$ is closed.

†*A topological space X is compact Hausdorff if X is Hausdorff space and for every open cover of X has a finite subcover.*

Examples 2.5.5 *1) Closed morphisms are not stable under base change. For example,* $\mathbb{A}^1_k \longrightarrow Spec(k)$ *is closed but* $\mathbb{A}^2_k = \mathbb{A}^1_k \times \mathbb{A}^1_k \longrightarrow \mathbb{A}^1_k$*, which is not closed. Indeed, the image of* $V(xy-1)$ *is the open subset* $\mathbb{A}^1_k \setminus \{0\}$*, which is not closed.*

2) Let $f : R \longrightarrow A$ *be a homomorphism of rings such that* A *is a finite R-module, then the induced map* $Spec(A) \longrightarrow Spec(R)$ *is proper.*

Proposition 2.5.22 *Let* $f : X \longrightarrow S$ *be a morphism of schemes. The following are equivalent :*

1) f *is proper.*

2) There exists an open covering $S = \bigcup_{i \in I} U_i$ *such that* $f^{-1}(U_i) \longrightarrow U_i$ *is proper for all* $i \in I$*.*

Proof. *See [30, Lemma 29.41.2].*

Theorem 2.5.4 *We have the following properties :*

i) Closed immersions are proper.

ii) The composition of two proper morphisms is proper.

iii) The base change of a proper morphism is still proper.

iv) The product of two proper morphisms is proper : if $f : X \longrightarrow Y$ *and* $g : X^{'} \longrightarrow Y^{'}$ *are proper, where all morphisms are morphisms of* $S-$*schemes, then* $f \times g : X \times_S X^{'} \longrightarrow Y \times_S Y^{'}$ *is proper.*

Proof. *See [12, Corollary 4.8, p.**102**].*

2.5.8 Projective Schemes

We know that projective varieties are a special important class of varieties that are not affine, but still can be described globally without using glueing techniques. They arise from looking at homogeneous ideals, i.e., graded coordinate rings. A completely analogous construction exists in the category of schemes, starting with a graded ring and looking at homogeneous ideals in it.

The Proj construction

The functor Spec is the basic operation going from rings to schemes. We describe a related operation Proj from graded rings to schemes.

Definition 2.5.15 *Let* R *be graded ring of the form* $R = \oplus_{d\geq 0} R_d$ *and let* $R_+ := \oplus_{d>0} R_d$*.*

i) We denote by $Proj(R)$ *the set of homogeneous prime ideals* $P \subseteq R$ *such that* P *does not contain* R_+*. It is called the projective spectrum of* R*.*

ii) For a homogeneous ideal J*, we let*

$$V_h(J) = \{P \in Proj(R) \mid J \subseteq P\}.$$

Remark 2.5.7 *The operation* V_h *has properties analogous to the properties for* V *listed in proposition 2.2.1. So we can define a topology on* $Proj(R)$ *for which the closed subsets are exactly those of the form* $V_h(J)$*, for* J *a homogeneous ideal of* R_r*. This topology is called the Zariski topology on* $Proj(R)$*. Note by definition we have* $V_h(R_+) = \emptyset$*.*

Principals opens of Proj(R)

Recall, in the affine case a principal open of $Spec(R)$ is defined as $D(f) := \{P \in Spec(R) \mid f \notin P\}$ for some $f \in R$ (see definition 2.2.2). We define the principal $D_+(f)$ of $Proj(R)$ by

$$D_+(f) = \{P \in Proj(R) \mid f \notin P\}$$

with f is homogeneous of positive degree i.e $f \in R_d$, and $d > 0$.

Proposition 2.5.23 *Let $f, g \in R$ be homogeneous of positive degree. Then*

1) *$D_+(f) \cap D_+(g) = D_+(fg)$.*

2) *The sets $D_+(f)$ form a basis for the Zariski topology on $Proj(R)$ when f runs through the homogeneous element of R of positive degree.*

Proof. *See [9, Proposition 10.6, p.**144**].*

Notation. *If P is a homogeneous prime ideal of a graded ring R, then $R_{(P)}$ will denote the elements of degree zero in the localisation of R at the set of homogeneous elements which do not belong to P.*

Definition 2.5.16 *Let R be graded ring, and $X = Proj(R)$. We define a sheaf of ring $\mathcal{O}_X$ by considering for any open subset $U \subseteq X$, all functions*

$$s : U \longrightarrow \coprod_{P \in X} R_{(P)}$$

such that $s(P) \in R_{(P)}$, which are locally represented by quotients. That is given any $P \in U$ there is $a, f \in R$ homogeneous elements of the same degree and an open $V \subseteq U$ such that $V \subseteq D_+(f)$, and $s(Q) = \frac{a}{f}$ for all $Q \in V$.

Proposition 2.5.24 *Let R be graded ring and set $X = Proj(R)$.*

1) *For every $P \in X$, the stalk $\mathcal{O}_{X,P}$ is isomorphic to $R_{(P)}$.*

2) *For any homogeneous element $f \in R_+$, we have*

$$\left(D_+(f), \mathcal{O}_{X|D_+(f)}\right) \simeq Spec(R_{(f)}).$$

where $R_{(f)}$ consists of all element of degree zero in the localization R_f. In particular, $Proj(R)$ is a scheme.

Proof. *See [12, Proposition 2.5, p.**76**].*

Definition 2.5.17 *Let R be a ring. The Projective n-space over R denote $\mathbb{P}^n_R$ is the proj of the polynomial ring $R[T_0, \ldots, T_n]$. When $R = \mathbb{Z}$ we write simply $\mathbb{P}^n$ for $Proj(\mathbb{Z}[T_0, \ldots, T_n])$.*

Remarks 2.5.3 1) *Note that $\mathbb{P}^n_R$ is a scheme over $S = Spec(R)$.*

2) *We define the n-space $\mathbb{P}^n_S$ over an arbitrary scheme S as $\mathbb{P}^n_S = \mathbb{P}^n \times_{Spec(\mathbb{Z})} S$.*

Some basic properties of Proj(R)

Theorem 2.5.5 *Let R be a graded ring.*

i) $Proj(R)$ is separated.

ii) If R is Noetherian, then $Proj(R)$ is Noetherian. In particular $Proj(R)$ is compact.

iii) If R is of finitely generated over R_0, then $Proj(R)$ is a finite type over $Spec(R_0)$ is the 0-component of R.

iv) If R is an integral domain, then $Proj(R)$ is integral.

Proof. *See [9, Proposition 10.16, p.**150**].*

Definition 2.5.18 *(Projective morphisms) Let $f : X \longrightarrow Y$ be a morphism of schemes. We say that f is projective if there exists an open covering $Y = \bigcup_i Y_i$ such that $f_{|f^{-1}(Y_i)} : f^{-1}(Y_i) \longrightarrow Y_i$ can be factored as*

$$f^{-1}(Y_i) \overset{j}{\hookrightarrow} \mathbb{P}^{n_i}_{Y_i} = \mathbb{P}^{n_i} \times_{Spec(\mathbb{Z})} Y_i \longrightarrow Y_i$$

with j a closed immersion.

Example 2.5.6 *$X = \mathbb{P}^n_R \longrightarrow Spec(R)$ is a projective morphism.*

Proposition 2.5.25 *The projective space $\mathbb{P}^n_{\mathbb{Z}}$ is separated and of finite type.*

Proof. *See [30, Section 27.13, Projective space].*

Theorem 2.5.6 *Let S be a scheme. Then any projective morphism to S is proper.*

Proof. *See [17, Theorem 3.30, p.**108**].*

Corollary 2.5.5 *We have the following properties :*

i) Closed immersions are projective morphisms.

ii) The composition of two projective morphisms is a projective morphism.

iii) Projective morphisms are stable under base change.

iv) Let $f : X \longrightarrow S$ and $g : Y \longrightarrow S$ be projective morphisms, then $X \times_S Y \longrightarrow S$ is a projective morphism.

Definition 2.5.19 *(projective schemes) Let X be a scheme over S. We say that X is projective over S if the structure morphism $f : X \longrightarrow S$ is projective.*

2.6 Tangent spaces

Let X be a scheme and $x \in X$, $\mathfrak{m}_x$ be the maximal ideal of $\mathcal{O}_{X.x}$, and $k(x) = \mathcal{O}_{X,x}/\mathfrak{m}_x$ be the residue field . It is clear that m_x/m_x^2 is a vector space over $k(x)$.

Definition 2.6.1 *Let X be a scheme, and let $x \in X$. Zariski tangent space of X at x is the dual*

$$T_xX = \left(\mathfrak{m}_x/\mathfrak{m}_x^2\right)^\vee.$$

Remarks 2.6.1 *1) For any point $x \in X$, if the local ring $\mathcal{O}_{X,s}$ is Noetherian, Nakayama's lemma shows that $dim_{k(x)}(\mathfrak{m}_x/\mathfrak{m}_x^2)$ is the minimal number of generators of $\mathfrak{m}_x$ (see remark 1.5.2). In particular, if X is locally Noetherian, $dim_{k(x)}(T_xX)$ is finite.*

2) For any open neighborhood U of x, we have $T_xX = T_xU$.

3) Let $f : X \longrightarrow Y$ be a morphism of schemes, $x \in X$ and $y = f(x)$. Then $f_x^\sharp : \mathcal{O}_{Y,y} \longrightarrow \mathcal{O}_{X,x}$ canonically induces a $k(x)$-homomorphism of vector spaces

$$T_xf : T_xX \longrightarrow T_yY \otimes_{k(y)} k(x)$$

called the tangent map of f at x.

Proposition 2.6.1 *Let X be a scheme. Then :*

1) If X is locally Noetherian, then for any $x \in X$, we have $dim_{k(x)}(T_xX) \geq dim(\mathcal{O}_{X,x})$.

2) Let $f : X \longrightarrow Y$ and $g : Y \longrightarrow Z$ be morphisms of schemes. Then $T_x(g \circ f) = \left(T_{f(y)} \otimes id_{k(x)}\right) \circ T_xf$

Proof. *See [17, Proposition 2.2, p.**126**]*

Definition 2.6.2 *Let X be a locally Noetherian scheme and $x \in X$ be a point. We say that x is a regular point of X if $dim(\mathcal{O}_{X,x}) = dim_{k(x)}(T_xX)$. If x is not regular, we say that it is a singular point.*

Proposition 2.6.2 *Let X be a locally Noetherian scheme. Then X is regular if and only if for any $x \in X$, $dim(\mathcal{O}_{X,x}) = dim_{k(x)}(T_xX)$.*

Proof. *X is regular if and only if for all $x \in X$, $\mathcal{O}_{X,x}$ is regular if and only if for all $x \in X$, $dim_{k(x)}(T_xX) = dim(\mathcal{O}_{X,x})$.*

2.7 Modules over schemes

So far we discussed general properties of sheaves, in particular, of rings (see section 2.2.2). Similarly as in the module theory in abstract algebra, the notion of sheaves of modules allows us to increase our understanding of a given ringed space, and to provide further techniques. There are particularly important notions, namely, quasi-coherent and coherent sheaves. They are analogous notions of the usual modules (respectively, finitely generated modules) over a given ring. They also generalize the notion of vector bundles.

2.7.1 Sheaves of modules

Definition 2.7.1 *Let $(X, \mathcal{O}_X)$ be a ringed space. A sheaf of $\mathcal{O}_X$-modules, or simply an $\mathcal{O}_X$-modules, is a sheaf $\mathcal{F}$ on X such that*

i) The group $\mathcal{F}(U)$ is an $\mathcal{O}_X(U)$-module for each open set $U \subseteq X$.

ii) For any $V \subseteq U$ opens subsets of X he restriction map $res_{U,V} : \mathcal{F}(U) \longrightarrow \mathcal{F}(V)$ is compatible with the module structure via the rings homomorphism $\mathcal{O}_X(U) \longrightarrow \mathcal{O}_X(V)$. In other words the natural diagram below is required to commute

$$\begin{array}{ccc} \mathcal{F}(U) \times \mathcal{O}_X(U) & \longrightarrow & \mathcal{F}(U) \\ \downarrow & & \downarrow {\scriptstyle res_{U,V}} \\ \mathcal{F}(V) \times \mathcal{O}_X(V) & \longrightarrow & \mathcal{F}(V) \end{array}$$

where vertical arrows represent restrictions maps and horizontal ones multiplication maps.

Definition 2.7.2 *A morphism $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ of $\mathcal{O}_X$-modules is a morphism of sheaves such that the map $\psi(U) : \mathcal{F}(U) \longrightarrow \mathcal{G}(U)$ is an $\mathcal{O}_X(U)$-module homomorphism for every open $U \subseteq X$.*

Remarks 2.7.1 *i) We obtain a category of $\mathcal{O}_X$-modules, which we denote by $\mathcal{M}od_X$.*

ii) Let $\mathcal{F}$ be an $\mathcal{O}_X$-module and $x \in X$, then the stalk $\mathcal{F}_x$ carries a natural $\mathcal{O}_{X,x}$-module structure. The $k(x)$-vector space $\mathcal{F}(x) := \mathcal{F}_x \otimes_{\mathcal{O}_{X,x}} k(x)$ is called the fiber of $\mathcal{F}$ over x.

Example 2.7.1 *Let $(X, \mathcal{O}_X)$ be a ringed space, $\mathcal{F}$, $\mathcal{G}$ be $\mathcal{O}_X$-modules, and let $\psi : \mathcal{F} \longrightarrow \mathcal{G}$ be a morphism. Then :*

1) "$ker(\psi)$", "$Im(\psi)$" are again $\mathcal{O}_X$-modules.

2) If $\mathcal{F} \subseteq \mathcal{G}$ is an $\mathcal{O}_X$-submodule, then the quotient sheaf $\mathcal{G}/\mathcal{F}$ (see definition 2.1.13) is an $\mathcal{O}_X$-module.

Definition 2.7.3 *Let $\mathcal{F}, \mathcal{G}$ be two $\mathcal{O}_X$-modules*

i) We denoted the group morphisms from $\mathcal{F}$ to $\mathcal{G}$ by $Hom_X(\mathcal{F}, \mathcal{G})$ (or $Hom_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})$).

ii) For $U \subseteq X$. The presheaf

$$U \longmapsto Hom_{\mathcal{O}_X}(\mathcal{F}_{|U}, \mathcal{G}_{|U})$$

is a sheaf and we will call it the sheaf Hom.

iii) We may define the direct sum as

$$\mathcal{F} \oplus \mathcal{G} := \mathcal{F} \times \mathcal{G}.$$

More generally, Given a any set I and for each $i \in I$ a $\mathcal{O}_X$-module $\mathcal{F}_i$. We can form the direct sum

$$\oplus_{i \in I} \mathcal{F}_i$$

which is the sheafification of the presheaf that associates to each open U the direct sum of the modules $\mathcal{F}_i(U)$.

Tensor product

Let $\mathcal{F}, \mathcal{G}$ be sheaves of abelien groups on X. For any $U \subseteq X$ open subset. We consider the correspondence

$$U \longmapsto \mathcal{F}(U) \otimes_{\mathcal{O}_X(U)} \mathcal{G}(U).$$

This defines a presheaf on X.

Definition 2.7.4 *The sheaf associated to the presheaf $U \longmapsto \mathcal{F}(U) \otimes_{\mathcal{O}_X(U)} \mathcal{G}(U)$ is called the tensor product. We denote it by $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$. When there is no confusion, we write simply $\mathcal{F} \otimes \mathcal{G}$.*

Properties 2.7.1 *Let $\mathcal{F}, \mathcal{G}$ be two $\mathcal{O}_X$-modules.*

i) Stalk $(\mathcal{F} \otimes \mathcal{G})_x$ at the point x is naturally isomorphic to tensor product $\mathcal{F}_x \otimes_{\mathcal{O}_{X,x}} \mathcal{G}_x$.

ii) Tensor product is right exact in the category of $\mathcal{O}_X$-modules i.e if $\mathcal{F}$ is an $\mathcal{O}_X$-module and if

$$\mathcal{F}_1 \longrightarrow \mathcal{F}_2 \longrightarrow \mathcal{F}_3 \longrightarrow 0$$

is an exact sequence of $\mathcal{O}_X$-modules, then the induced sequence

$$\mathcal{F}_1 \otimes_{\mathcal{O}_X} \mathcal{F} \longrightarrow \mathcal{F}_2 \otimes_{\mathcal{O}_X} \mathcal{F} \longrightarrow \mathcal{F}_3 \otimes_{\mathcal{O}_X} \mathcal{F} \longrightarrow 0.$$

is exact.

iii) (Adjunction between Hom and $\otimes$) For any $\mathcal{O}_X$-modules $\mathcal{F}, \mathcal{G}$ there is natural isomorphism

$$Hom_{\mathcal{O}_X}(\mathcal{F}, Hom_{\mathcal{O}_X}(\mathcal{G}, \mathcal{H})) \simeq Hom_{\mathcal{O}_X}(\mathcal{F} \otimes \mathcal{G}, H).$$

*(See [9, 10.10, p.**187**]).*

Pushforward and Pullback

Let $f : X \to Y$ be a continuous map between topological spaces. In section 2.1.2, we introduced two functors between the categories $\mathcal{S}h_X$ and $\mathcal{S}h_Y$.

* *The **first functor** :*

$$\begin{array}{rccc} f_* : & \mathcal{S}h_X & \longrightarrow & \mathcal{S}h_Y \\ & \mathcal{F} & \longmapsto & f_*\mathcal{F} \end{array}$$

defined by $f_*\mathcal{F}(U) = \mathcal{F}(f^{-1}(U))$ for any U open of Y. This functor is called the pushforward (see definition 2.1.14).

* *The **second functor** :*

$$\begin{array}{rccc} f^{-1} : & \mathcal{S}h_Y & \longrightarrow & \mathcal{S}h_X \\ & \mathcal{G} & \longmapsto & f^{-1}\mathcal{G} \end{array}$$

and $f^{-1}\mathcal{G}(U) = (f_P\mathcal{G})^\dagger(U)$ for any open U of X (see definition 2.1.17)

In this paragraph, we parallel these two constructions when f is a morphism of schemes to obtain functors f_* and f^* between $\mathcal{M}od_X$ and $\mathcal{M}od_Y$.

Pushforward

Let $f : (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ be a morphism of schemes. Let $\mathcal{F}$ be an $\mathcal{O}_X$-module, then for each open $U \subseteq Y$, $f_*\mathcal{F}(U)$ is a module over $f_*\mathcal{O}_X$. $f^\sharp : \mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X$ equips $f_*\mathcal{F}$ with a natural structure of $\mathcal{O}_Y$-module.

Definition 2.7.5 *The above $\mathcal{O}_Y$-module $f_*\mathcal{F}$ is called the direct image (or the pushforward) of $\mathcal{F}$ under f.*

Remarks 2.7.2 *i) This construction is clearly functorial in the sheaf $\mathcal{F}$, and gives a functor $f_* : \mathcal{M}od_X \longrightarrow \mathcal{M}od_Y$.*

ii) The pushforward is functorial in the morphism f in the sens that $(f \circ g)_* = f_* \circ g_*$.

Proposition 2.7.1 *Let $f : (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ be a morphism of schemes. The functor*

$$f_* : \mathcal{M}od_{\mathcal{O}_X} \longrightarrow \mathcal{M}od_{\mathcal{O}_Y}$$

is left exact.

Proof. *See [30, Section 18.14, Lemma 18.14.3].*

Pullback

Let $f : (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ be a morphism of schemes.
Recall that if $\mathcal{G}$ is a sheaf on Y, the inverse image $f^{-1}\mathcal{G}$ is by the sheaf canonically associated to the presheaf

$$f_p\mathcal{G}(U) = \varinjlim_{f(U) \subseteq V} \mathcal{G}(V)$$

(see definition 2.1.16, definition 2.1.17). When $\mathcal{G}$ is an $\mathcal{O}_Y$-module, this sheaf is naturally an $\mathcal{O}_X$ an $f^{-1}\mathcal{O}_Y$-module and we can make $f^{-1}\mathcal{G}$ into an $\mathcal{O}_X$-module using the map $f^{-1}\mathcal{O}_Y \longrightarrow \mathcal{O}_X$.
We define :

$$f^*\mathcal{G} := f^{-1}\mathcal{G} \otimes_{f^{-1}\mathcal{O}_Y} \mathcal{O}_X.$$

Definition 2.7.6 *The $\mathcal{O}_X$-module $f^*\mathcal{G}$ is called the pullback of $\mathcal{G}$ under f.*

Remarks 2.7.3 *i) In particular, $f^*\mathcal{O}_Y = f^{-1}\mathcal{O}_Y \otimes_{f^{-1}\mathcal{O}_Y} \mathcal{O}_X = \mathcal{O}_X$.*

iii) As in the case of the pushforward, we also get here a functor $f^* : \mathcal{M}od_{\mathcal{O}_Y} \longrightarrow \mathcal{M}od_{\mathcal{O}_X}$.

Proposition 2.7.2 *Let X be a scheme, for any $x \in X$ we have*

$$(f^*\mathcal{G})_x = \mathcal{G}_{f(x)} \otimes_{\mathcal{O}Y, f(x)} \mathcal{O}_{X,x}$$

Proof. *The stalks commutes with sheafification and tensor product (see properties 2.7.1 i)), and $(f^{-1}\mathcal{G})_x = \mathcal{G}_{f(x)}$ (see lemma 2.1.4). So*

$$\begin{aligned} (f^*\mathcal{G})_x &= (f^{-1}\mathcal{G} \otimes_{f^{-1}\mathcal{O}_Y} \mathcal{O}_X)_x \\ &= (f^{-1}\mathcal{G})_x \otimes_{f^{-1}\mathcal{O}_{Y,x}} \mathcal{O}_{X,x} \\ &= \mathcal{G}_{f(x)} \otimes_{\mathcal{O}_{Y,f(x)}} \mathcal{O}_{X,x}. \end{aligned}$$

Proposition 2.7.3 *Let $f : (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ be a morphism of schemes. The functor*

$$f^* : \mathcal{M}od_{\mathcal{O}_Y} \longrightarrow \mathcal{M}od_{\mathcal{O}_X}$$

is right exact.

Proof. *See [30, Section 18.14, Lemma 18.14.3].*

Global generation

Let $(X, \mathcal{O}_X)$ be a ringed space, $\mathcal{F}$ be an $\mathcal{O}_X$-module, U be an open of X. It is clear that $\mathcal{F}_x$ is an $\mathcal{O}_{X,x}$-module (see remarks 2.7.1).

Definition 2.7.7 *i) $\mathcal{F}$ is globally generated at $x \in X$ if the image of $\mathcal{F}(X) \longrightarrow \mathcal{F}_x$ generates $\mathcal{F}_x$ as an $\mathcal{O}_{X,x}$-module. In other words, $\mathcal{F}(X) \otimes_{\mathcal{O}_X(X)} \mathcal{O}_{X,x} \longrightarrow \mathcal{F}_x$ is surjective.*

ii) We say that $\mathcal{F}$ is globally generated if $\mathcal{F}$ is globally generated at every point $x \in X$.

Remark 2.7.1 *If $\mathcal{O}_X$ is globally generated, then any direct sum $\bigoplus_{i\in I} \mathcal{O}_X$ is also globally generated.*

Proposition 2.7.4 *Let $\mathcal{F}$ be an $\mathcal{O}_X$-module. Then $\mathcal{F}$ is generally generated if and only if there is some set I such that there is an epimorphism $\bigoplus_{i\in I} \mathcal{O}_X \longrightarrow \mathcal{F}$.*

Proof. *See [17, Lemma 1.3, p.**158**].*

2.7.2 Quasi-coherent modules

In this section, we introduce the notion of quasi-coherent $\mathcal{O}_X$-module. This notion is very useful in algebraic geometry, since quasi-coherent modules on a scheme have a good description on any affine open.

Quasi-coherent sheaves

Definition 2.7.8 *Let $(X, \mathcal{O}_X)$ be a ringed space and let $\mathcal{F}$ be a sheaf of $\mathcal{O}_X$-modules. We say that $\mathcal{F}$ is a quasi-coherent sheaf of $\mathcal{O}_X$-modules if for every point $x \in X$ there exists an open neighbourhood $x \in U \subseteq X$ such that $\mathcal{F}_{|U}$ is isomorphic to the cokernel of a map*

$$\bigoplus_{j\in J} \mathcal{O}_U \longrightarrow \bigoplus_{i\in I} \mathcal{O}_U.$$

Note that the direct sum of two quasi-coherent $\mathcal{O}_X$-modules is quasi-coherent $\mathcal{O}_X$-modules.
It is not true in general that an infinite direct sum of quasi-coherent $\mathcal{O}_X$-modules is quasi-coherent (see [30, chap. 17.10.9, Example 10.9]).

Notation. *We will denote The category of quasi-coherent $\mathcal{O}_X$-modules by $\mathcal{Q}Coh_{\mathcal{O}_X}$.*

Example 2.7.2 *The structure sheaf $\mathcal{O}_X$ is quasi-coherent.*

Proposition 2.7.5 *Let $f : (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ be a morphism of ringed spaces. The pullback $f^*\mathcal{G}$ of a quasi-coherent $\mathcal{O}_Y$-module is quasi-coherent.*

Proof. *See [9, Proposition 14.14, p.**207**].*

2.7.3 Sheaves associated to modules

Since thinking about affine schemes is supposed to be equivalent to thinking about rings (the two categories are equivalent, see theorem 2.3.2), we would like our thinking about sheaves of modules on affine schemes to be equivalent to thinking about modules over rings. In this section, we will define the sheaf to modules.

Definition 2.7.9 *Let R be a ring and let M be an R-module. We define the sheaf associated to M on $X = Spec(R)$, denoted by $\tilde{M}$, as follows. For any open subset U of X we define*

$\tilde{M}(U) := \{s : U \longrightarrow \coprod_{P \in X} M_P \mid$ *for all* $P \in U$, *we have* $s(P) \in M_P$, *and for all* $P \in U$ *there is* $a \in M, r \in R$, *and an open neighbourhood* $V \subseteq U$ *such that* $V \subseteq D(r)$ *and* $s(Q) = \frac{a}{r}$ *for all* $Q \in V\}$.

Remark 2.7.2 *The sheaf* $\tilde{M}$ *carries an obvious* $\mathcal{O}_X$*-module structure (see [12, Proposition 5.2, p.**110**]). The* $\sim$ *is functorial in* M*. For any* R*-module homomorphism* $f : M \longrightarrow N$ *there is an obvious way of obtaining an* $\mathcal{O}_X$*-module homomorphism* $\tilde{f} : \tilde{M} \longrightarrow \tilde{N}$*. Indeed, The maps* $f_r : M_r \longrightarrow N_r$ *are* $\mathcal{O}_X(D(r))$*-modules homomorphisms compatible with localization maps i.e., the following diagram*

$$\begin{array}{ccc} M_r & \xrightarrow{f_r} & N_r \\ \downarrow & & \downarrow \\ M_d & \xrightarrow{f_d} & N_d \end{array}$$

is commutative, and thus induce a map between $\tilde{M}$ *and* $\tilde{N}$*. Moreover, one has* $\widetilde{f \circ g} = \tilde{f} \circ \tilde{g}$*. So We have thus defined a functor from the category of* R*-modules to the category of* $\mathcal{O}_X$*-modules.*

Proposition 2.7.6 *Let* R *be a ring and* M *be an* R*-modules. The sheaf* $\tilde{M}$ *on* $Spec(R)$ *has the following three properties :*

1) *For all* $r \in R$, *we have a canonical isomorphism*

$$\tilde{M}(D(r)) \simeq M_r.$$

2) *If* $d \in R$ *and* $d \in (r)$*, then there is a commutative diagram*

$$\begin{array}{ccc} \tilde{M}(D(r)) & \longrightarrow & \tilde{M}(D(d)) \\ \simeq \downarrow & & \downarrow \simeq \\ \tilde{M}_r & \longrightarrow & \tilde{M}_d \end{array}$$

where the vertical isomorphisms one from 1).

3) *There is natural isomorphism* $\tilde{M}_P \simeq M_P$ *for all* $P \in Spec(R)$*. This a natural isomorphism fits in a commutative diagram*

$$\begin{array}{ccc} \tilde{M}_P & \xrightarrow{\simeq} & M_P \\ \uparrow & & \uparrow \\ \tilde{M}(Spec(R)) & \xrightarrow{\simeq} & M \end{array}$$

Here the vertical morphisms are the natural ones and the lower horizontal ones come from 1).

Proof. *The proof of this Proposition is similar to the proof of proposition 2.3.1. For more details, see [17, Proposition 5.10].*

Theorem 2.7.1 *The functor* $M \longrightarrow \tilde{M}$ *from the category of* R*-modules to the category of* $\mathcal{O}_X$*-modules where* $X = Spec(R)$ *is exact and fully faithful.*

Proof. *See [9, Theorem 14.4, p.**195**].*

Tensor products, Pushforward and Pullback

Proposition 2.7.7 *Let R be a ring and let $X = Spec(R)$. Also let $\psi : R \longrightarrow A$ be a ring homomorphism, and $f : Spec(A) \longrightarrow Spec(R)$ be the corresponding morphism of spectra. Then :*

1) *If M and N are two R-modules. Then $\widetilde{M \otimes_R N} \simeq \tilde{M} \otimes_{\mathcal{O}_X} \tilde{N}$.*

2) *The A-module M can be considered as an $R-$module via the map $\psi : R \longrightarrow A$, and we denote this A-module by M_R. We have*
$$f_* \tilde{M} = \tilde{M}_R.$$

3) *Let M be an R-module. Then*
$$f^* \tilde{M} = \widetilde{M \otimes_R A}.$$

4) *If $\{M_i\}$ is any family of R-modules, then $\widetilde{\bigoplus_i M_i} = \bigoplus_i \tilde{M}_i$.*

Proof. *See [12, Proposition 5.2, p.**110**].*

Theorem 2.7.2 *$\tilde{M}$ is quasi-coherent sheaf.*

Proof. *See [9, Proposition 13.8, p.**192**].*

2.7.4 Coherent sheaves

Definition 2.7.10 *Let X be a ringed space, and let $\mathcal{F}$ be a sheaf of $\mathcal{O}_X$-module.*

i) *We say that $\mathcal{F}$ is finitely generated if for every $x \in X$, there exist an open neighborhood U of x, an integer $n \geq 1$ and a surjective homomorphism on $\mathcal{O}^n_{X_{|U}} \longrightarrow \mathcal{F}_{|U}$.*

ii) *We say that $\mathcal{F}$ is coherent if it is finitely generated, and if for every every open subset U of X, and for every homomorphism $\beta : \mathcal{O}^n_{X_{|U}} \longrightarrow \mathcal{F}_{|U}$,Let $(X, \mathcal{O}_X)$ the kernel $Ker(\beta)$ is finitely generated.*

Theorem 2.7.3 *Let X be a scheme. Let $\mathcal{F}$ be a quasi-coherent $\mathcal{O}_X$-module. Let us consider the following properties:*

i) *$\mathcal{F}$ is coherent.*

ii) *$\mathcal{F}$ is finitely generated.*

iii) *For every affine open subset U of X, $\mathcal{F}(U)$ is finitely generated over $\mathcal{O}_X(U)$.*

Then $i) \Rightarrow ii) \Rightarrow iii)$. Moreover, if X is locally Noetherian then these properties are equivalent.

Proof. *See [17, Proposition 1.11, p.**161**].*

Coherence of pushforwards

Proposition 2.7.8 *Let $f : X \longrightarrow Y$ be a finite morphism of schemes.*

1) *If $\mathcal{F}$ be a quasi-coherent sheaf on X, then $f_*\mathcal{F}$ is quasi-coherent on Y.*

2) *If X and Y are Noetherian, $f_*\mathcal{F}$ is even coherent if $\mathcal{F}$ is.*

Proof. *See [9, Theorem 14.15, p.**208**].*

Notation. *The category of coherent $\mathcal{O}_X$-modules is denoted $Coh(\mathcal{O}_X)$.*

2.8 Some cohomology interpretations

In this section, we consider the theory of cohomology in algebraic geometry. It is an extremely rich and varied theory. In this section we are interested in one of the most elementary cohomology theories, the Čech cohomology of quasi-coherent sheaves.

2.8.1 Some homological algebra

Complexes of abelian groups

- *Recall that a complex of abelian groups $A^\bullet$ is a sequence of groups A^i together with maps between them*

$$\cdots \longrightarrow A^{i-1} \xrightarrow{d_i} A^i \xrightarrow{d_{i+1}} A^{i+1} \longrightarrow \cdots$$

such that $d^{i+1} \circ d^i = 0$ for each i.

- *A morphism of complexes $A^\bullet \xrightarrow{f^\bullet} B^\bullet$ is a collection $f_i^\bullet : A^i \longrightarrow B^i$ of maps making the following diagram commutative :*

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & A^{i-1} & \xrightarrow{d^i} & A^i & \xrightarrow{d^{i+1}} & A^{i+1} & \longrightarrow & \cdots \\ & & \downarrow f_{i-1}^\bullet & & \downarrow f_i^\bullet & & \downarrow f_{i+1}^\bullet & & \\ \cdots & \longrightarrow & B^{i-1} & \xrightarrow{\eta^i} & B^i & \xrightarrow{\eta^i} & B^{i+1} & \longrightarrow & \cdots \end{array}$$

- *We say that an element $\sigma \in A^i$ is a cocycle if it lies in the kernel of the map d^i, i.e $d^i(\sigma) = 0$.*
- *A coboundary is an element in the image of d^{i-1}, i.e $\sigma = d^{i-1}(\tau)$. For some $\tau \in A^{i-1}$. These form subgroups of A^n, denoted by $Z^i(A^\bullet)$, and $B^i(A^i)$, respectively. Since $d^i(d^{i-1})(x) = 0$ for all x, all coboundaries are cocycles, so that $B^i(A^\bullet) \subseteq Z^i(A^\bullet)$.*
- *The cohomology groups of the complex $A^\bullet$, are set up to measure the difference between these two notions. We define the i-The cohomology group as the quotient group*

$$H^i(A^\bullet) := Z^i(A^\bullet)/B^i(A^\bullet).$$

- *An exact sequence of complexes noted : $0 \longrightarrow A^\bullet \xrightarrow{f^\bullet} B^\bullet \xrightarrow{g^\bullet} C^\bullet \longrightarrow 0$ is the given for all i of an exact sequence of abelian groups $0 \longrightarrow A^i \xrightarrow{f_i^\bullet} B^i \xrightarrow{g_i^\bullet} C^i \longrightarrow 0$.*
- *Given the previous definition, we deduce morphisms $\tilde{f}_i^\bullet : H^i(A^\bullet) \longrightarrow H^i(B^\bullet)$*

Theorem 2.8.1 *We consider the exact sequence of complexes $0 \longrightarrow A^\bullet \xrightarrow{f^\bullet} B^\bullet \xrightarrow{g^\bullet} C^\bullet \longrightarrow 0$. Then there is a long exact sequence of cohomology groups*

$$\longrightarrow H^i(A^\bullet) \longrightarrow H^i(B^\bullet) \longrightarrow H^i(C^\bullet) \longrightarrow H^{i+1}(A^\bullet) \longrightarrow H^{i+1}(B^\bullet) \longrightarrow H^{i+1}(C^\bullet) \longrightarrow$$

Proof. *See [26, Proposition D.1.10, p.**503**].*

Complexes of sheaves

Remark 2.8.1 *The definitions and arguments of the previous subsection apply much more generally (to any abelian category). In particular, we make the following sheaf analogue.*

Definition 2.8.1 *A complex of sheaves $\mathcal{F}^\bullet$, is a sequence of sheaves with maps between then*

$$\cdots \xrightarrow{d^{i-2}} \mathcal{F}_{i-1} \xrightarrow{d^{i-1}} \mathcal{F}_i \xrightarrow{d^i} \mathcal{F}_{i+1} \xrightarrow{d^{i+1}} \cdots$$

such that $d^{i+1} \circ d^i = 0$ for each i.

Definition 2.8.2 *Given a complex, we define the cohomology sheaves $H^p(\mathcal{F}^\bullet)$, as $Ker(d^p)/Im(d^{p-1})$.*

As in theorem 2.8.1, a short exact sequence of complexes of sheaves gives rise to a long exact sequence of cohomology sheaves.

2.8.2 The Čech cohomology

Notation. *Let X be a topological space, and let $\mathcal{F}$ be a sheaf of abelien group on X. Let $\mathcal{U} := \{U_i\}_{i\in I}$ be an open cover of X. We denote by $U_{ij} = U_i \cap U_j$ and more generally $U_{i_0\cdots i_p} = U_{i_0} \cap \cdots \cap U_{i_p}$.*

Definition 2.8.3 *i) For all $p \geq 1$, we denoted by*

$$C^p(\mathcal{U}, \mathcal{F}) := \prod_{i_0<\cdots<i_p} \mathcal{F}(U_{i_0\cdots i_p}) = \prod_{i_0<\cdots<i_p} \mathcal{F}(U_{i_0} \cap \cdots \cap U_{i_p}).$$

We have thus constructed a complex of abelian groups $C^\bullet(\mathcal{U}, \mathcal{F})$.

ii) The elements of $C^p(\mathcal{U}, \mathcal{F})$ are called cochains. $C^p(\mathcal{U}, \mathcal{F})$ is called also group of p-cochains with values in $\mathcal{F}$.

iii) We also define the differential :

$$\begin{array}{cccc} \delta^p : & C^p(\mathcal{U}, \mathcal{F}) & \longrightarrow & C^{p+1}(\mathcal{U}, \mathcal{F}) \\ & s & \longmapsto & \delta s \end{array}$$

by

$$(\delta^p s)_{i_0\cdots i_{p+1}} = \sum_{k=0}^{p+1} (-1)^k s_{i_0\cdots \hat{i}_k \cdots i_p | U_{i_0\cdots \hat{i}_k \cdots i_p}}.$$

Note that for $p \geq 0$, we have $\delta^{p+1} \circ \delta^p = 0$.

Notation. $\ast$ $Z^P(\mathcal{U}, \mathcal{F}) = \{\sigma \in C^p(\mathcal{U}, \mathcal{F}) | \delta^p(s) = 0\}$

$\ast$ $B^p(\mathcal{U}, \mathcal{F}) = \begin{cases} \delta(C^{p-1}(\mathcal{U}, \mathcal{F})) & \text{if} \quad p > 0 \\ 0 & \text{otherwise} \end{cases}$

Definition 2.8.4 *The p-th Čech cohomology of $\mathcal{F}$ with respect to $\mathcal{U}$ is defined as*

$$H^p(\mathcal{U}, \mathcal{F}) = Z^P(\mathcal{U}, \mathcal{F}) / B^p(\mathcal{U}, \mathcal{F}) = ker(\delta^p) / Im(\delta^{p-1})$$

Remark 2.8.2 *Note that a sheaf homomorphism $\psi : \mathcal{F} \longrightarrow G$ induces a mapping of Čech cohomology groups, so we obtain functors $\mathcal{F} \longrightarrow H^p(\mathcal{U}, \mathcal{F})$ from abelian sheaves to abelian groups.*

Proposition 2.8.1 *For any open cover $\mathcal{U}$ of X we have :*

$$H^0(\mathcal{U},\mathcal{F}) = \Gamma(X,\mathcal{F}).$$

Proof. *See [9, Theorem 17.13, p.***258***].*

Examples 2.8.1 *1) Let $X = \mathbb{S}^1$ be the unit circle and equip it with a standard covering $\mathcal{U} = \{U_1, U_2\}$, consisting of two intervals (intersecting in two intervals S and N) and let $\mathcal{F} = \mathbb{Z}_X$ be the constant sheaf. Here we have*

- $C^0(\mathcal{U},\mathcal{F}) = \mathbb{Z}_X(U_1)\times\mathbb{Z}_X(U_2) \simeq \mathbb{Z}\times\mathbb{Z}$
- $C^1(\mathcal{U},\mathcal{F}) = \mathbb{Z}_X(U_1\cap U_2) \simeq \mathbb{Z}\times\mathbb{Z}$.
- *The map $\delta^0 : C^0(\mathcal{U},\mathcal{F}) \longrightarrow C^1(\mathcal{U},\mathcal{F})$ is the map $\phi : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$ given by $\delta^0(x,y) = (y-x, y-x)$.*
  Hence $H^0(\mathcal{U},\mathcal{F}) = ker(\delta^0) = \mathbb{Z}(1,1) \simeq \mathbb{Z}$ and $H^1(\mathcal{U},\mathcal{F}) = Coker(\delta^0) = (\mathbb{Z}\times\mathbb{Z})/\mathbb{Z}(1,1) \simeq \mathbb{Z}$.

2) *Let X be an irreducible topological space. Then for any finite covering $\mathcal{U}$ of X we have for a constant sheaf A_X*

$$H^p(\mathcal{U}, A_X) = 0$$

*for $p > 0$. (See [9, Proposition 13.11, p.***251***]).*

The inductive system of $H^p(\mathcal{U},\mathcal{F})$

We will describe in this paragraph the inductive system which will allow us to define the $H^p(\mathcal{U},\mathcal{F})$.

Definition 2.8.5 *(Refinement function) If $\mathcal{U} \subseteq \Omega$, with $\mathcal{U} = (V_j)_{j\in J}$ and $\Omega = (U_i)_{i\in I}$ then there exists a function τ called refinement function $\tau : J \longrightarrow I$ such that $V_j \subseteq U_{\tau(j)}$ used to define maps :*

$$\begin{array}{cccc} \tau^p : & C^p(\Omega,\mathcal{F}) & \longrightarrow & C^p(\mathcal{U},\mathcal{F}) \\ & (s_{j_0\cdots j_p}) & \longmapsto & \left(s_{\tau(j_0)\cdots\tau(j_p)}\right)_{|V_{j_0\cdots j_p}} \end{array}$$

Theorem 2.8.2 *Let $\tau, \tilde{\tau} : J \longrightarrow I$ be two refinement functions such that $V_j \subseteq U_{\tau(j)} \cap U_{\tilde{\tau}(j)}$. Then τ and $\tilde{\tau}$ induces the same function $\phi^{\Omega}_{\mathcal{U}} : H^p(\Omega,\mathcal{F}) \longrightarrow H^p(\mathcal{U},\mathcal{F})$.*

Proof. *See [30, Section 20.15 Refinements and Čech cohomology].*

Long exact sequence in cohomology

Theorem 2.8.3 *Let $\mathcal{F}, \mathcal{G}$ and $\mathcal{H}$ be sheaves on X and $\mathcal{F} \xrightarrow{\alpha} \mathcal{G}$ and $\mathcal{G} \xrightarrow{\beta} \mathcal{H}$ be two morphisms of sheaves.*
If for any covering Ω of X there exists a covering $\Omega' \subseteq \Omega$ such that for any finite intersection W of open sets of Ω' the following sequence

$$0 \longrightarrow \mathcal{F}(W) \xrightarrow{\alpha} \mathcal{G}(W) \xrightarrow{\beta} \mathcal{H}(W) \longrightarrow 0$$

is exact. Then the following infinite sequence

$$0 \longrightarrow H^0(X,\mathcal{F}) \xrightarrow{\tilde{\alpha}} H^0(X,\mathcal{G}) \xrightarrow{\tilde{\beta}} H^0(X,\mathcal{H}) \xrightarrow{\Delta} H^1(X,\mathcal{F}) \longrightarrow \cdots$$

$$\cdots \longrightarrow H^p(X,\mathcal{F}) \xrightarrow{\tilde{\alpha}} H^p(X,\mathcal{G}) \xrightarrow{\tilde{\beta}} H^p(X,\mathcal{H}) \xrightarrow{\Delta} H^{p+1}(X,\mathcal{F}) \longrightarrow \cdots$$

is exact.

Proof. *See [9, Proposition 17.2, p.**251**].*

Theorem 2.8.4 *Let X be a topological space and let $\mathcal{F}$ be a sheaf on X.*

i) The Čech cohomology groups are functors $H^i(X,.) : \mathcal{A}b\mathcal{S}h_X \longrightarrow \mathcal{A}b\mathcal{G}$.

ii) (Leray's theorem) If $\mathcal{F}$ is a sheaf and $\mathcal{U}$ is a covering such that $H^i(U_{i_1} \cap \cdots U_{i_p}, \mathcal{F}) = 0$ for all $i > 0$ and multi-indices $i_1 < \cdots < i_p$, then

$$H^i(X, \mathcal{F}) = H^i(\mathcal{U}, \mathcal{F}).$$

Proof. *See [9, Theorem 13.13, p.**254**].*

Theorem 2.8.5 *(Serre) Let R be a Noetherian ring, let $X = Spec(R)$ and let $\mathcal{F}$ be a quasi-coherent sheaf on X. Then*

$$H^p(X, \mathcal{F}) = 0.$$

for all $p > 0$.

Proof. *See [9, Theorem 14.1, p.**256**].*

Corollary 2.8.1 *Let X be a Noetherian affine scheme and*

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow 0$$

be an exact sequence of $\mathcal{O}_X$-modules with $\mathcal{F}$ is quasi-coherent. Then the following sequence

$$0 \longrightarrow \mathcal{F}(X) \longrightarrow \mathcal{G}(X) \longrightarrow \mathcal{H}(X) \longrightarrow 0$$

is exact.

Proof. *See [9, Corollary 14.5, p.**202**].*

Theorem 2.8.6 *(Grothendieck) Let X be a Noetherian topological space of dimension m, and let $\mathcal{F}$ be an abelian sheaf on X. Then*

$$H^p(X, \mathcal{F}) = 0$$

for all $p > m$.

Proof. *See [30, Proposition 20.20.7 Grothendieck].*

2.9 Divisors defined by means of schemes

We previously described in the first chapter divisors on curves. We give here the interpretation (and generalization) of these divisors in the language of schemes. We present then in this section Weil and Cartier Divisors and some relations between them.

2.9.1 Cartier Divisors

Definition 2.9.1 *(Sheaf of meromorphic functions)*
Let R be a commutative ring. We denote by $\mathcal{R}(R)$ for the set of nonzero divisors of R. Let X be a scheme, the sheaf $\mathcal{R}_X$ is defined as follows : For any open subset $U \subseteq X$

$$\mathcal{R}_X(U) := \{f \in \mathcal{O}_X(U) \,|\, \forall x \in U, f_x \in \mathcal{R}(\mathcal{O}_{X,x})\}.$$

Let $\mathcal{K}'_X$ to be the presheaf on X defined by $\mathcal{K}'_X(U) := \mathcal{R}_X(U)^{-1}\mathcal{O}_X(U)$ and $\mathcal{K}_X$ to be the sheafification of $\mathcal{K}'_X$. We call $\mathcal{K}_X$ the sheaf of meromorphic functions on X.

Remarks 2.9.1 *i) $\mathcal{K}_X$ is called also the sheaf of total quotient rings of $\mathcal{O}_X$.*

ii) Note that if U is an affine open subset of X, then $\mathcal{R}_X(U) = \mathcal{R}(\mathcal{O}_X(U))$

iii) Note that there is a natural morphism of sheaves $\mathcal{O}_X \longrightarrow \mathcal{K}_X$, which is a monomorphism because of the nonzerodivisor condition.

Example 2.9.1 *Let k is a field and $Y = Spec(k[x])$. Then $\mathcal{O}_Y(U)$ is the ring of rational functions on an open set U in Y. The image of any nonzero $f \in \mathcal{O}_Y(U)$ in $\mathcal{O}_{Y,x} = k[x]_{\mathfrak{p}}$ (x corresponds to a prime $\mathfrak{p} \subseteq k[x]$) is a nonzerodivisor for any x, since the localization of an integral domain is again an integral domain, so $\mathcal{K}_Y(U)$ is the fraction field of $\mathcal{O}_Y(U)$, which is clearly $k(x)$. As such, $\mathcal{K}'_Y = \mathcal{K}_Y$ is just the constant sheaf $k(x)$, which is also isomorphic to $\mathcal{O}_{Y,\epsilon} = k[x]_{(0)}$, where ϵ is the generic point (0).*

Remark 2.9.1 *In fact, for any integral scheme X, $\mathcal{K}_X$ is the constant sheaf associated to $\mathcal{O}_{X,\epsilon}$, by the same argument in the example 2.9.1.*

Definition 2.9.2 *Let $\mathcal{K}_X^\times$ be the subsheaf of invertible elements of $\mathcal{K}_X$ and $\mathcal{O}_X^\times$ be the subsheaf of invertible elements of $\mathcal{O}_X$. We denote $\mathcal{K}_X^\times/\mathcal{O}_X^\times$ to be the sheafification of the presheaf $U \longrightarrow \mathcal{K}_X^\times(U)/\mathcal{O}_X^\times(U)$. Then there is a natural morphism $\mathcal{K}_X^\times \longrightarrow \mathcal{K}_X^\times/\mathcal{O}_X^\times$.*

i) The group of Cartier divisors on X is defined to be $CaDiv(X) := H^0(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times)$.

ii) The natural morphism above yields a homomorphism

$$div : H^0(X, \mathcal{K}_X^\times) \longrightarrow H^0(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times).$$

A Cartier divisor D is said to be a principal Cartier divisor if $D \in Im(div)$. Note that a principal divisor can be described with the singleton collection $\{(X, f)\}$ for $f \in \mathcal{K}_X^*(X)$.

iii) We denote the group law on $CaDiv(X)$ as addition. For any $D, D' \in CaDiv(X)$, we say D and D' are linearly equivalent, $D \sim D'$, if $D - D' \in Im(div)$.

iv) Let $D \in CaDiv(X)$, D is said to be effective if and only if $D \in Im\big(H^0(X, \mathcal{O}_X \cap \mathcal{K}_X^\times) \longrightarrow H^0(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times)$. We then write $D \geq 0$, and the set of effective Cartier divisors is denoted by $CaDiv_+(X)$.

v) The group of Cartier divisors mod principal divisors is denoted $CalCl(X) := CaDiv(X)/\sim$. Also $Cacl(X)$ is called Cartier divisor class group.

Remarks 2.9.2 *i) For a sheaf of rings $\mathcal{F}$ on X, we can construct the sheaf $\mathcal{F}^\times$ of invertible elements, which is a sheaf of abelian groups, by defining*

$$\mathcal{F}^\times(U) := \{s \in \mathcal{F}(U) \,|\, st = 1_U \text{ for some } t \in \mathcal{F}(U)\}$$

Note that if $st = 1_U$ in $\mathcal{F}(U)$ and $W \subseteq U$, then $s_{|W}t_{|W} = 1_W$.

ii) Definition 2.9.2 allows us to represent a Cartier divisors by a system $\{(U_i, f_i)\}$ where $\{U_i\}$ is an open cover of X and $f_i \in H^0(U_i, \mathcal{K}_X^\times)$ such that $f_i f_{j|U_{ij}}^{-1} \mathcal{O}_X^\times(U_{ij})$, where $U_{ij} = U_i \cap U_j = U_{ji}$. In other words, there are units $h_{ij} \in \mathcal{O}_X(U_{ij})$ such that $f_i = h_{ij} f_j$ over U_{ij}.

Definition 2.9.3 *The pairs (U_i, f_i) are called the local defining data or the local equations for the divisor D (with respect to the covering U_i).*

Not that the local defining data are not unique : Suppose now we have two systems $\{(U_i, f_i)\}$ and $\{(W_j, f_j)\}$ which represent a same Cartier divisor D. Then on $U_i \cap W_j$, $f_i = h_{ij} g_j$ for some $h_{ij} \in \mathcal{O}_X^\times(U_i \cap W_j)$. Therefore, for convenience, we denote $D = [\{(U_i, f_i)\}]$.
Now, the set of Cartier divisors naturally form an abelian group with the group law defined by : If $D = [\{(U_i, f_i)\}]$ and $D' = [\{(V_j, g_j)\}] \in CaDiv(X)$, then

$$D + D' := [\{(U_i \cap V_j, f_i g_j)\}].$$

The inverse $-D$ is $[\{(U_i, f_i^{-1})\}]$.
Additionally, let $D = [\{(U_i, f_i)\}] \in CaDiv(X)$. Then $D \in CaDiv_+(X)$ if and only if $f_i \in \mathcal{O}_X(U_i)$ for all i. Moreover, D is principal if $[\{(U_i, f_i)\}] = [\{(X, f)\}]$ for some convenient f.

Example 2.9.2 *On $\mathbb{P}^1$ we can take the standard covering $U_0 = Spec(k[s])$ and $U_1 = Spec(k[s^{-1}])$. Then there is a Cartier divisor D given by (U_0, s) and $(U_1, 1)$.*

Correspondence Between Sheaves and Cartier Divisors

We would like to reinterpret Cartier divisors in the language of sheaves.

For any $D \in CaDiv(X)$, we would like to associate a sheaf to D. Namely, let $D = [\{(U_i, f_i)\}] \in \mathcal{O}_X(D)$, the associated sheaf on X is defined by

$$\mathcal{O}_X(D)_{|U_i} := f_i^{-1} \mathcal{O}_{X|U_i} = f_i^{-1} \mathcal{O}_{U_i}$$

i.e., the sheaves $f_i^{-1} \mathcal{O}_{U_i}$ glue to a sheaf $\mathcal{O}_X(D)$ defined on all of X. It is by construction invertible, since it is invertible on each U_i.
This construction is independent of the choice of the representatives. Indeed, Two different representatives (U_i, f_i) and (W_j, g_j) for the same divisor D give rise to the same invertible sheaf. This is because over $U_i \cap W_j$, we have $f_i = h_{ij} g_j$ for some sections $h_{ij} \in \mathcal{O}_X^\times(U_i \cap W_j)$. This means that $f_i^{-1} \mathcal{O}_{U_i \cap W_j} = g_i^{-1} \mathcal{O}_{U_i \cap W_j}$, and so the sheaf is uniquely determined as a subsheaf of $\mathcal{K}_X$.

Theorem 2.9.1 *The map $D \longmapsto \eta(D) = \mathcal{O}_X(D)$ gives a one-to-one correspondence between Cartier divisors on X and invertible subsheaves on $\mathcal{K}_X$.*

Proof. *See [12, Proposition 6.13, p.**144**].*

2.9.2 Weil Divisors

In this subsection, we will introduce Weil divisors. We consider the schemes satisfying the following condition : $(*)$ X is a Noetherian integral separated scheme which is regular in codimension one (We say a scheme X is regular in codimension one (or sometimes nonsingular in codimension one) if every local ring $\mathcal{O}_{X,x}$ of X of dimension one is regular.)
Recall that this means that each local ring $\mathcal{O}_{X,x}$ is an integral domain, which is integrally closed in its function field $K = k(X)$. Recall that if Z is an irreducible closed subset of a scheme X, then the codimension of Z in X is equal to the dimension of the local ring $\mathcal{O}_{X,\epsilon}$, where $\epsilon \in Z$ is the generic point (see proposition 2.5.15).

Definition 2.9.4 *Let X satisfy $(*)$*

i) A prime divisor on X is a closed integral subscheme Z of codimension one.
We denote by $X^{(1)}$ the set of closed integral subschemes of codimension 1, or equivalently, their generic points.

ii) A Weil divisor on X is a finite formal sum

$$D = \sum_i n_i Y_i \tag{2.8}$$

where $n_i \in \mathbb{Z}$ and Y_i are prime divisors. Then the set of Weil divisors $Div(X)$ is the free abelian group on $X^{(1)}$.

iii) We say D is effective if all the n_i are non-negative in (2.8).

iv) The support of a Weil divisor D, denoted $Supp(D)$, is the subset $\cup_{n_i \neq 0} Y_i$.

Remark 2.9.2 *If Z is a prime divisor on X and $V \subseteq X$ is an open set, then $Z \cap V$ is naturally a prime divisor on V. It follows that we obtain a presheaf $V \longmapsto Div(V)$.*

Our next task is to define the Weil divisor associated to a rational function.

The assumption $(*)$ "regular in codimension one" implies that $Z \subseteq X$ is a prime divisor with generic point $\epsilon \in X$, the local ring $\mathcal{O}_{X,\epsilon}$ is a discrete valuation ring, with a corresponding valuation $\mathcal{V} : K^{\times} \longrightarrow \mathbb{Z}$. The concept of a valuation is a generalization of the "order" of a zero or a pole of a meromorphic function in complex analysis.
In same logical, an element $f \in K^{\times}$ has positive valuation m if it vanishes to order m along Z, and negative valuation $-m$ if it has a pole of order m there.
To define this properly, let $Z \subseteq X$ be a prime divisor, and let $\epsilon \in X$ be its generic point. Then we define for a nonzero element $f \in \mathcal{O}_{X,\epsilon}$,

$$\mathcal{V}_Z(f) = d \tag{2.9}$$

where d is the unique non-negative integer so that $f \in \mathfrak{m}^d \setminus \mathfrak{m}^{d+1}$
In the function field $K = k(X)$, an element f is represented by a fraction h/g and we define $\mathcal{V}_Z(f) = \mathcal{V}_Z(h) - \mathcal{V}_Z(g)$. With this definition, we have $\mathcal{O}_{X,\epsilon} = \mathcal{V}_Z^{-1}(\mathbb{Z}_{\geq 0})$, $\mathcal{O}_{X,\epsilon}^{\times} = \mathcal{V}_Z^{-1}(0)$ and the maximal ideal is given by $\mathfrak{m} = \mathcal{V}_Z^{-1}(\mathbb{Z}_{\geq 1})$.

Definition 2.9.5 *Let $f \in K^{\times}$, we define its corresponding Weil divisor as*

$$div(f) = \sum_Z \mathcal{V}_Z(f) Z.$$

Divisors of the form $div(f)$ are called principal divisors, and they generate a subgroup $Div^0(X) \subseteq Div(X)$.

In the definition 2.9.5 the sum is taken over all prime divisors on X. To see that this is well defined, see the following lemma.

Lemma 2.9.1 *Let X be an integral noetherian scheme which is regular in codimension one, with fraction field K and let $f \in K$. Then $\mathcal{V}_Z(f) = 0$ for all but finitely many prime divisors Z.*

Proof. *See [9, Lemma 15.3, p.**275**].*

Lemma 2.9.2 *Let $f, g \in K^{\times}$. Then*

$$div(fg) = div(f) + div(g)$$

as Weil divisors on X.

Proof. *See [30, Section 31.26.6, Weil divisors].*

Example 2.9.3 *Let $X = Spec(k[x]) = \mathbb{A}^1_k$ and $K = k(x)$. Here prime divisors in X correspond to closed points $Z = [b] \in \mathbb{A}^1_k$ associated to maximal ideals $(x - b)$. Let $f = \frac{x^3(x-1)}{x+1} \in K$. Then $\mathcal{V}_Z(f) = 0$ for all b except when $b = 0, +1, -1$,where we have $\mathcal{V}_{[0]}(f) = 2$, $\mathcal{V}_{[1]}(f) = 1$ and $\mathcal{V}_{[-1]}(f) = -1$. Hence the divisor of f is $2[0] + [1] - [-1]$.*

The sheaf associated to a Weil divisor

As in the subsection 2.9.1, we have been successful to associate any Cartier divisors with a sheaf. The same way we would like to form a sheaf, denoted $\mathcal{O}_X(D)$ where $D = \sum n_Z Z$ is Weil divisors, which should consist of rational functions with poles at worst along D.
If $f = \frac{h}{g}$ is such a rational function where h, g are coprime, we have $div(f) = div(h) - div(g)$.
So if D is a prime divisor, we want the pole $div(g)$ to be 'cancelled out' by D, i.e., $D - div(g)$ is effective. In other words, we want $div(f) + D$ to be an effective Weil divisor. Thus, concretely, we define the sheaf $\mathcal{O}_X(D)$ as follows :

$$\begin{aligned} \mathcal{O}_X(D)(U) &= \{f \in K \,|\, (div(f) + D)_{|U} \geq 0\} \cup \{0\} \\ &= \{f \in K \,|\, \mathcal{V}_Z(f) \geq -n_Z, \text{for all } n_Z \in \mathbb{Z}\} \cup \{0\} \end{aligned}$$

Here Z ranges over all prime divisors in X and ϵ_Z denotes thegeneric point of Z. Moreover, The sheaf $\mathcal{O}_X(D)$ is a quasi-coherent sheaf on X and it is invertible if and only if D is a Cartier divisor.

Connection between Weil Divisors and Cartier Divisors

For each open subset $U \subseteq X$ the following exact sequence :

$$0 \longrightarrow \mathcal{O}_X^{\times}(U) \longrightarrow K^{\times} \xrightarrow{div} Div(U)$$

This gives an exact sequence of sheaves

$$0 \longrightarrow \mathcal{O}_X^{\times} \longrightarrow \mathcal{K}_X^{\times} \xrightarrow{div} Div \tag{2.10}$$

and we obtain the following injective map of sheaves

$$\Psi : \mathcal{K}_X^{\times}/\mathcal{O}_X^{\times} \longrightarrow Div.$$

If we take global sections, we get an injective map

$$\beta : CaDiv(X) \longrightarrow Div(X).$$

Let D be a Cartier divisor given by the data (U_i, g_i). If Z is a prime divisor on X, with generic point ϵ, then since U_i is a cover, $\epsilon \in U_i$ for some i. We can then define

$$\mathcal{V}_Z(D) = \mathcal{V}_Z(g_i)$$

This is independent of the choice of U_i. Indeed, If $\epsilon \in U_i \cap U_j$, then $g_i g_j^{-1} \in \mathcal{O}_X^{\times}(U_i \cap U_j)$, and so $\mathcal{V}_Z(g_i g_j^{-1}) = 0$, hence $\mathcal{V}_Z(g_i) = \mathcal{V}_Z(g_j)$. Then β is defined by

$$\beta(D) = \sum_Z \mathcal{V}_Z(D) Z$$

Remark 2.9.3 *So by explicit description above, we may view Cartier divisors as a subgroup of the group of Weil divisors.*

Theorem 2.9.2 *Let X be an integral normal scheme. Then the following statement are equivalent :*

i) $\beta : CaDiv(X) \longrightarrow Div(X)$ *is an isomorphism.*

ii) The exact sequence

$$0 \longrightarrow \mathcal{O}_X^\times \longrightarrow \mathcal{K}_X^\times \xrightarrow{div} Div$$

is exact on the right.

iii) X *is locally factorial (all the local rings* $\mathcal{O}_{X,x}$ *are UFDs).*

Proof. *See [9, Proposition 15.27, p.**287**].*

Corollary 2.9.1 *Let k be an algebraically closed field. Then* $Pic(\mathbb{A}_k^n) = Cl(\mathbb{A}_k^n) = CaCl(\mathbb{A}_k^n) = 0.$

Proof. *See [9, Theorem 20.43. p.**311**].*

Chapter 3

Introduction to Central Simple Algebra, Severi-Brauer Varieties

The aim of this chapter is to present some basic properties of central simple algebras and to introduce Severi-Brauer varieties with a special focus on relationships between these varieties and splitting field of central simple algebras. We give at first a brief introduction to simple and semisimple modules, then we prove fundamental theorems on central simple algebras. In particular, this includes Wedderburn's theorem, the double centralizer theorem and Skolem-Noether theorem. We show how to construct Brauer group of a field and show how crossed products relate this group to a second Galois cohomology group. We define then Severi-Brauer varieties and present some of their properties. In particular, we are interested here in canonical connections between these varieties, central simple algebras and some cohomological interpretations.

3.1 Simple and semisimple modules

Let R be a commutative ring. An associative algebra over R, is a pair (A, ψ) consisting of an associative ring A and a ring homomorphism

$$\psi : R \longrightarrow Z(A)$$

called the structure map of A over R, where

$$Z(A) = \{a \in A \,|\, xa = ax \text{ for all } x \in A\}$$

is called the center of A, which is a subring of A.
An algebra homomorphism $\phi : A \longrightarrow B$ between two R-algebras is a ring homomorphism such that the diagram

$$\begin{array}{ccc} A & \xrightarrow{\ \phi\ } & B \\ {\scriptstyle \psi_1}\nwarrow & & \nearrow{\scriptstyle \psi_2} \\ & R & \end{array}$$

commutes. This defines the category $\mathcal{A}lg_R$ of R-algebras.

3.1.1 Simple Modules

Recall that a ring R is simple if it has no two-sided ideals but 0 and R.

Definition 3.1.1 *Let A be an algebra, M be a left (resp., right) A-module. We say that M is simple (or irreducible) if $M \neq 0$ and it has no proper nonzero submodules.*

Convention. *In what follows, the word module will mean a* left *module.*

Examples 3.1.1 *1) Any field k is simple as k-module.*

2) *Take $A = \mathbb{Z}$ and $M = \mathbb{Z}/5\mathbb{Z}$. Then M is a simple A-module.*

3) *Let J be maximal left ideal of A. Then A/J is a simple A-module. Indeed, let P be a submodule of A/J, and set $\tilde{P} := \{a \in A \,|\, a + J \in P\}$, then $\tilde{P}$ is a left ideal of A containing J and we have $\tilde{P}/J = P$. Since J is a maximal ideal of A, then $\tilde{P} = J$ or $\tilde{P} = A$. So $P = 0$ or $P = A/J$. Conversely, let I be a left ideal of A such that A/J is a simple A-module, then J is a maximal left ideal. Indeed, Let L be a left ideal of A such that $I \subseteq L$, then L/I is a submodule of A/I. Since A/I is a simple, then we have $L/I = \{0\}$ or $L/I = A/I$. Hence $L = I$ or $L = A$.*

In what follows, A will denote an algebra (over some commutative ring).

Proposition 3.1.1 *Let M be a nonzero A-module, then the followings statements are equivalent :*

1) *M is simple.*

2) *For all $m \in M \setminus \{0\}$, $Am = M$.*

3) *$M = A/J$ for some maximal left ideal J of A.*

Proof. *1)$\Rightarrow$ 2) Since Am is a nonzero submodule of M and M is simple, so $Am = M$.*
2)$\Rightarrow$ 1) Let P be a nonzero submodule of M and let m be a nonzero element of P, then we have $M = Am \subseteq P$, which shows that $P = M$. This proves that M is a simple A-module.
3) $\Rightarrow$ 1) This is a direct consequence of examples 3.1.1 3).

Lemma 3.1.1 *(Schur's lemma) Let M and N be simple A-modules. If $\phi : M \longrightarrow N$ is a homomorphism of modules, then either $\phi = 0$ or ϕ is an ismorphism.*

Proof. *Suppose that $\phi \neq 0$, then $ker(\phi) \neq M$. It follows that $ker(\phi) = 0$. Also, $im(\phi) \neq 0$, so $im(\phi) = N$. Thus, ϕ is an isomorphism.*

Corollary 3.1.1 *Let M, N be simple modules. Then $M \simeq N$ (as A-modules) or $Hom_A(M, N) = 0$.*

Proof. *Let $\phi \in Hom_A(M, N)$. If $\phi \neq 0$, then by lemma 3.1.1 ϕ is an isomorphism. Hence M and N are isomorphic.*

Definition 3.1.2 *A division algebra is an algebra in which every nonzero element has a multiplicative inverse, but multiplication is not necessarily commutative. A ring (which is obviously a $\mathbb{Z}$-algebra) that is a division ($\mathbb{Z}$-)algebra is also called a division ring or a skew field.*

Corollary 3.1.2 *Let M be a simple A-module and $D := End_A(M)$, i.e., the algebra of endomorphisms of M (endowed with its canonical laws). Then D is a division algebra.*

Proof. *Let $d \in D \setminus \{0\}$, then by lemma 3.1.1 d is an ismorphism. So d is invertible in D.*

3.1.2 Semisimple modules

Definition 3.1.3 *A left (resp. right) A-module M is semisimple if there exist simple A-modules M_i $(i \in I)$ such that*

$$M \simeq \bigoplus_{i \in I} M_i$$

(isomorphism of A-modules).

Example 3.1.1 *A simple module is semisimple.*

Definition 3.1.4 *Let M be an A-module. We say that M is indecomposable if writing $M = P \bigoplus Q$ for some submodules P, Q of M, then necessarily $P = 0$ or $Q = 0$.*

Proposition 3.1.2 *Let M be a semisimple A-module. Then followings statements are equivalent :*

1) *M is a simple A-module.*

2) *$End_A(M)$ is a division algebra.*

3) *M is indecomposable.*

Proof. *1) ⇒2) This follows from corollary 3.1.2.*
2⇒3) Let P and Q be two submodules of M. If we suppose that $M = P \oplus Q$ with $P \neq 0$ and $Q \neq 0$. Consider the followings homomorphism of A-modules :

$$\begin{array}{rccc} \alpha := (id_M, 0): & M = P \bigoplus Q & \longrightarrow & M \\ & p + q & \longmapsto & p \end{array}$$

By the hypothesis here α must be an isomorphism, which is not the case. Therefore M is indecomposable.
3)⇒1) Immediate.

Proposition 3.1.3 *Let M be a nonzero A-module and let Q be proper submodule of M. Assume that $M = \sum_{i \in I} M_i$, where each M_i are a simple submodules. Then there exists $J \subseteq I$ such that $M = (\bigoplus_{j \in J} M_j) \bigoplus Q$*

Proof. *Since $Q \neq M$, then there exists $i \in I$ such that $M_i \nsubseteq Q$. In this case, we have $M_i \cap Q = \{0\}$, because if $x \neq 0 (\in M_i \cap Q)$ we obtain $M_i = Ax \subseteq Q$ (see proposition 3.1.1). So $M_i + Q = M_i \bigoplus Q$. Consider J be a maximal for the property $P_1 := \sum_{j \in J} M_j + Q = \sum_{j \in J} M_j \bigoplus Q$. Now, let $i \in I \setminus J$ if we may assume that $P_1 + M_i = P_1 \bigoplus M_i = \sum_{k \in J \cup \{i\}} M_k \bigoplus Q$. But that contradicts the maximality of J. Thus $M_i \cap P_1 \neq 0$. Let $z \in M_i \cap P_1$, we have $M_i = Az \subseteq P_1$. So for all $i \in I$ $M_i \subseteq P_1$, then $M \subseteq P_1$, so $M = P_1$. Hence $M = \sum_{j \in J} M_j \bigoplus Q$.*

Remark 3.1.1 *In proposition 3.1.3, if we take $Q = 0$ we obtain $M = \bigoplus_{j \in J} M_j$. Then M is semisimple.*

Definition 3.1.5 *Let M be an A-module $(\neq 0)$. Let P and Q be submodules of M.*

i) *Q is called a complement of P if $P \bigoplus Q = M$.*

ii) *If any submodule of M has a complement in M. We say that M supplemented.*

Lemma 3.1.2 *Let M be an A-module. Then the followings are equivalent :*

i) *M is a supplemented.*

ii) *Any submodule of M is supplemented.*

Proof. *i) ⇒ ii) Let N be a submodule of M, and let P be a submodule of P. Then P is also be a submodule of M, since M is supplemented, then there exists Q be a submodule of M such that $M = P \bigoplus Q$, so we have $N = N \cap M = (P \bigoplus Q) \cap N = P \bigoplus (Q \cap N)$. Hence P has a complement in N.*
ii) ⇒ i) Immediate.

Proposition 3.1.4 *Let M be a nonzero A-module. Then the followings are equivalent :*

1) *M is semisimple.*

2) *M is the sum of its simple submodules.*

3) *M is supplemented.*

Proof. *1)⇒2) Immediate.*
2)⇒3) proposition 3.1.3.
2)⇒1 remark 3.1.1.
3)⇒1) Let S be a maximal (proper) submodule of M. Since M is supplemented, then there exists a submodule $Q \neq 0$ such that $S \bigoplus Q = M$. Also, since S is maximal in M then necessarily Q is a simple submodule of M. This prove that M has a simple submodule. Let N be sum of all simple submodules of M and let N' be a submodule of M such that $M = N \bigoplus N'$. Assume that $N' \neq 0$, then N' is supplemented (see lemma 3.1.2). So for the same reason as in above, N' has a simple submodule P. Plainly, P is also a simple submodule of M, but this contradicts the fact that N is the sum of all simple submodules of M. This shows that M is the sum of its simple submodules.

Corollary 3.1.3 *Let M be a semisimple A-module and let P be a nonzero submodule of M, then*

i) *P is semisimple.*

ii) *M/P is semisimple.*

Proof. i) *Since M is supplemented, then by lemma 3.1.2 P is also supplemented. So by proposition 3.1.4 P is semisimple.*

ii) *Since M is supplemented, then there exists a submodule Q of M such that $P \bigoplus Q = M$. So $M/P \simeq Q$. Hence by i) M/P is semisimple.*

Corollary 3.1.4 *The direct sum of a family of the semisimple A-modules is a semisimple A-module.*

Proof. *This corollary is a direct consequence of the definition 3.1.3.*

Proposition 3.1.5 *Let $M = \bigoplus_{i \in I} M_i$ where M_i are simple A-modules. Suppose that N is a simple A-module and suppose that there exists a nonzero homomorphism of A-modules $\psi : N \longrightarrow M$. Then there exists $j_0 \in I$ such that $M = \psi(N) \bigoplus (\bigoplus_{i \neq j_o} M_i)$, and $N \simeq M_{j_0}$ (isomorphism of A-modules).*

Proof. *By proposition 3.1.3, there exists a subset J of I such that $M = \psi(N) \bigoplus (\bigoplus_{i \in J} M_i)$. Since N is simple, then so is $\psi(N)$; moreover we have the following canonical isomorphisms of A-modules :*

$$\psi(N) \simeq M/\bigoplus_{j \in J} M_j \simeq \bigoplus_{j \in I \setminus J} M_j.$$

so necessarily $|I \setminus J| = 1$. So there exists $j_0 \in I$ such that $J = I \setminus \{j_0\}$. The rest of the proof is obvious.

Notation. *Let M be an A-module. We denoted by $S(M)$ the set for all submodules of M.*

Definition 3.1.6 *Let M be an A-module. The radical of M is $rad(M) := \bigcap \{N \in S(M) \mid M/N \text{ is simple}\}$.*

Remark 3.1.2 *$rad(M)$ is a submodule of M.*

Proposition 3.1.6 *Let M be an A-module and N be a submodule of M. Then the following statements hold :*

1) *If $rad(M/N) = 0$, then $rad(M) \subset N$.*

2) *$rad(M/rad(M)) = 0$.*

Proof. *See [21].*

Lemma 3.1.3 *Let M be a semisimple an A-module. The followings are equivalent :*

i) M is *finitely generated*.

ii) M is *Noetherian*.

iii) M is *Artinian*.

Proof. *See [21, Proposition, p.**36**].*

Theorem 3.1.1 *Let M be an A-module. The following statements hold : (what you wrote here and the implications you have in the proof have no sense) are equivalent :*

i) M is semisimple and finitely generated.

ii) $rad(M) = 0$ and M is Artinian.

Proof. *$i) \Rightarrow ii)$ Suppose that M is semisimple and finitely generated, so by lemma 3.1.3 M is Artinian. Write $M = \bigoplus_{j\in I} M_j$ with M_i simple. For $i \in I$, put $P_i = \bigoplus_{j\neq i} M_j$, then*

$$M/P_i \simeq M_i (\text{is simple})$$

So $rad(M) \subseteq \bigcap_{J\in I} P_j = 0$.
$ii) \Rightarrow i)$ Assume that $rad(M) = 0$ and M is Artinian and consider the family of all finite intersections $M_{i_1} \cap \cdots \cap M_{i_k}$, where M_i is a submodule of M such that M/M_i is simple. Since M is Artinian, then this family has a minimal element that we may take to be by $M_1 \cap \cdots \cap M_r$ for some positive integer r. Necessarily, $M_1 \cap \cdots \cap M_r = 0$. Indeed, for any submodule N of M such that M/N is simple, we have

$$(M_1 \cap \cdots \cap M_r) \cap N = M_1 \cap \cdots \cap M_r$$

because $M_1 \cap \cdots \cap M_r$ is minimal. So $M_1 \cap \cdots \cap M_r \subseteq N$, which yields that $rad(M) = M_1 \cap \cdots \cap M_r$. Now, consider the canonical map :

$$\begin{array}{rccc} \psi : & M & \longrightarrow & \bigoplus_{i=1}^{r} M/M_i \\ & m & \longmapsto & (m + M_i)_{1\leq i\leq r} \end{array}$$

Since M/M_i are simple, then $\bigoplus_{i=1}^{r} M/M_i$ is semisimple. Hence $\psi(M)$ is semisimple (because $\psi(M)$ is submodule of $\bigoplus_{i=1}^{r} M/M_i$). We have $ker(\psi) = M_1 \cap \cdots \cap M_r$, $M \simeq \psi(M)$. Therefore, M is semisimple. Moreover, by lemma 3.1.3, M is also Noetherian, so M is a finitely generated.

3.2 Semisimple and simple algebras

Throughout this section, F is a field. Recall that all algebras are associative and have an identity, denoted 1 (sometimes denoted 1_A). Most results will be written in terms of left modules (which we hence often will simply call modules). If we need to work with right modules then this will be specifically stated. The endomorphism ring of an A-module M is denoted $End_A(M)$. Similarly, we will use $Hom_A(M, N)$ to denote the set of module homomorphism from M to N.

3.2.1 Semisimple algebras

Definition 3.2.1 *Let A be an algebra. We say that A is semisimple if A is semisimple when it is considered (in the natural way) as a left A-module.*

Remark 3.2.1 *Note that if A is semisimple i.e., $A = \bigoplus_{i \in I} A_i$, where each A_i is a simple left A-module (or equivalently, where each A_i is a left ideal of A).*

Definition 3.2.2 *Let A be an algebra, we say that A is left Artinian (resp. Noetherian) if A is an Artinian left A-module (resp., a Noetherian left A-module).*

Proposition 3.2.1 *An algebra A is semisimple if and only if it is left Artinian and $rad(A) = 0$.*

Proof. *This follows from theorem 3.1.1 and remark 3.2.1.*

Proposition 3.2.2 *Let A be a semisimple algebra. Then every A-module is semisimple and every image of A by a homomorphism of algebras is a semisimple algebra. Moreover, every simple A-module is isomorphic to a minimal left ideal of A.*

Proof. *Since A is a semisimple A-module, then the direct sum of β copies of A is also a semisimple A-module, for all the cardinal β. Therefore, every free left A-module is semisimple. Clearly, for any left A-module M, there exists a free A-module N and submodule P of N such that*

$$M \simeq N/P$$

As seen above, N is semisimple, so by corollary 3.1.3 N/P is also a semisimple A-module. Write the argument here which show that simple A-modules are isomorphic to minimal left ideal of A, after showing that the image of a semisimple algebra by a homomorphism of algebras is a semisimple algebra (see below), then by proposition 3.1.1, there exists a maximal left ideal J of A such that $M \simeq A/J$ (as A-module). Since A is semisimple (as A-module), then A is supplemented (see proposition 3.1.4). Therefore, there exists a left ideal I of A such that $I \bigoplus J = A$, so we have

$$A/J \simeq I \text{ (as } A\text{-module)}$$

Also since J is a maximal left ideal of A, then necessarily, I is a minimal left ideal of A, so

$$M \simeq A/J \simeq I$$

and I is a minimal left ideal of A.
Assume that A is R-algebra where R is a commutative ring. Let B be a R-algebra and assume that there exists a homomorphism of R-algebras

$$\psi : A \longrightarrow B$$

Let's show that $C := \psi(A)$ is a semisimple algebra. Without losing the generality we can assume that ψ is surjective i.e $B = C$. Note that ψ induces an action of A on B given by

$$a \cdot x := \psi(a)x \text{ for all } a \in A \text{ and } x \in B$$

Therefore B is a (left) A-module (left). and so by the above, B is a semisimple A-module. We can write $B = \bigoplus_{i \in I} B_i$ with B_i simple A-submodule of B. Since ψ is surjective, then each also a simple B-submodule of B, so B is a semisimple algebra.

3.2.2 Simple algebras

Definition 3.2.3 *Let A be an algebra. We say that A is simple algebra if $A \neq 0$, i.e., $A \neq 0$*[*]*and the only two-sided ideals of A are $\{0\}$ and A.*

Examples 3.2.1 *1) Let D be a division algebra (see definition 3.1.2). Then clearly D is a simple algebra.*

2) For any field F and any positive integer n, the algebra $A := M_n(F)$ is simple. Indeed, let $(e_{ij})_{1\leq i,j\leq n}$ be the canonical base of A, i.e., e_{ij} is the matrix of A for which all entries are 0 except the ij-entry which equals 1. Let I be a two-sided ideal of A and suppose that I contains some nonzero element $a = (a_{ij})_{1\leq i,j\leq n}$. Let $1 \leq r, s \leq n$ be such that $a_{rs} \neq 0$, then for any $1 \leq i \leq n$, we have $a_{rs}^{-1}e_{ir}ae_{si} = e_{ii}$. It follows that I contains the unit element of A and so $I = A$.

3) Another important example of a finite dimensional noncommutative algebra over a field that was discovered by William Rowan Hamilton[†] *on 16 October 1843, is the algebra of quaternions (over the field $\mathbb{R}$ of real numbers), a 4-dimensional algebra with basis $1, i, j, k$ over $\mathbb{R}$, the multiplication being determined by the rules*

$$i^2 = -1, j^2 = -1, ij = -ji = k.$$

This algebra algebra which is often called the Hamilton algebra, is usually denoted by $\mathbb{H} = (-1,-1)_{\mathbb{R}}$. One can see that $\mathbb{H}$ is a division algebra. Indeed, for any nonzero element $x = \alpha + \beta i + \gamma j + \eta k$ of $\mathbb{H}$, where α, β and γ are real numbers, denoting $\overline{x} := \alpha - \beta i - \gamma j - \eta k$ and $N(x) := x\overline{x}$ (i.e., $N(x) = \alpha^2 + \beta^2 + \gamma^2 + \eta^2$, called the norm of x), one can easily check that $\frac{\overline{x}}{N(x)}$ is the inverse for x in $\mathbb{H}$.

4) Let F be a field of characteristic not 2. For any two elements $a, b \in F^*$, in a similar way as for the quaternion algebra $\mathbb{H}$, the (generalized) quaternion algebra $(a, b)_F$ is defined to be the 4-dimensional F-algebra with basis $1, i, j, k$ and with multiplication being determined by

$$i^2 = a, j^2 = b, ij = -ji = k.$$

The set $\{1, i, j, k\}$ is called a quaternion basis of $(a, b)_F$. The algebra $(a, b)_F$ is a simple algebra with $Z\big((a, b)_F\big) = F$. Indeed, let's define on $(a, b)_F$ a new operation, the Lie bracket, by $[x, y] = xy - yx$ for $x, y \in (a, b)_F$. It is clear that $F \subseteq Z\big((a, b)_F\big)$. Let $x = \alpha + \beta i + \gamma j + \eta k \in (a, b)_F$, where $\alpha, \beta, \gamma, \eta \in F$. If $x \in Z\big((a, b)_F\big)$, then in particular, $[i, x] = [j, x] = [k, x] = 0$. We have :

- $[i, x] = 2a\eta j + 2\gamma k.$
- $[j, x] = -2b\eta - 2\beta k.$
- $[k, x] = 2b\gamma i - 2a\beta j.$

So, if $x \in Z\big((a, b)_F\big)$, then $\beta = \gamma = \eta = 0$, hence $x = \alpha \in F$. Thus, $Z((a, b)_F) = F$.
Let's now consider a nonzero two-sided ideal J of $(a, b)_F$, and let x be a nonzero element of J. Since J is an ideal of A, then $[i, x] = ix - xi \in J$, also $[j, x], [k, x] \in J$. So $[j, [i, x]], [k, [j, x]], [i, [k, x]] \in J$. One can easily see that we have :

- $[j, [i, x]] = -4b\gamma i.$

---

[*] *For some authors an algebra is always assumed to be different from $\{0\}$.*

[†] *William Rowan Hamilton (4 August 1805-2 September 1865) was an Irish mathematician, Andrews Professor of Astronomy at Trinity College Dublin, and Royal Astronomer of Ireland at Dunsink Observatory. He made major contributions to optics, classical mechanics and abstract algebra. His work was of importance to theoretical physics, particularly his reformulation of Newtonian mechanics, now called Hamiltonian mechanics. It is now central both to electromagnetism and to quantum mechanics. In pure mathematics, he is best known as the inventor of quaternions.*

- $\ast$ $[k,[j,x]] = 4ab\eta j$.
- $\ast$ $[i,[k,x]] = -4a\beta k$.

So, J contains necessarily an invertible element of $(a,b)_F$*, which yields. So* $J = (a,b)_F$*. Therefore,* $(a,b)_F$ *is simple.*

Let A be an algebra and M be an A-module. We denote $ann_A(M) := \{a \in A \mid ax = 0 \text{ for all } x \in M\}$ *that we call the annulator of M. We say that M is a faithful A-module if* $ann_A(M) = 0$*. In other words, considering the (canonical) associated representation* $\psi : A \longrightarrow End_A(M)$*, defined by* $a \longmapsto l_a$*, where* $l_a : M \longrightarrow M$*, is given by* $l_a(x) = ax$*, for all* $x \in M$*, M is a faithful A-module if and only if* ψ *is injective. To each module M over A, one can associate a faithful module over some algebra B by proceeding in this way : The ring homomorphism* $\psi : A \longrightarrow End_A(M)$ *induces naturally an injective ring homomorphism* $\tilde{\psi} : A/\ker(\psi) \longrightarrow End_A(M)$ *where* $\ker(\psi)$ *is none but* $ann(M)$*. This gives rise to a faithful structure on M as an* $A/ann(M)$*-module.*

Lemma 3.2.1 *Let R be a ring and let e be a nonzero idempotent of R. Then we have a ring isomorphism*

$$eRe \simeq End_R(eR).$$

where eR is considered as a right R-module.

Proof. *Let* $r \in R$*, we define the following map*

$$\begin{array}{rccc} \psi_r : & R & \longrightarrow & R \\ & x & \longmapsto & rx \end{array}$$

It's clear that ψ_r *is a group homomorphism, and also for all* $x, y \in R$*, we have* $\psi_r(xy) = (rx)y) = \psi_r(x)y$*. Therefore* $\psi_r \in End_R(R)$*. Moreover, if* $r \in eRe$*, then clearly* ψ_r *restricts to an endomorphism of eR. So we get a map*

$$\begin{array}{rccc} \Phi : & eRe & \longrightarrow & End_R(eR) \\ & r & \longmapsto & \psi_r \end{array}$$

One can easily see that Φ *is a ring isomorphism.*

Lemma 3.2.2 *Let R be a ring and let M be a right R-module. For all* $r \geq 1$*, we have a ring isomorphism*

$$End_R(M^r) \simeq M_r(End_R(M)).$$

Proof. *See [4, Lemma III.2.6, p.8].*

Wedderburn‡'s theorem

Our aim here is to prove (a restricted version of) Wedderburn's theorem, a fundamental theorem in central simple algebra theory showing that a finite-dimensional central simple algebra over a field is a matrix algebra over this field. We assume throughout the rest, except other mention or other appearance from the context, that all algebras are finite-dimensional nonzero algebras over some fixed field (often denoted by F). We continue to assume that an algebra is always associative with a unit element and a homomorphism of algebras from an algebra A into an algebra B always map to the unit element of A on that of B.

Let A be a (finite-dimensional) F-algebra, then clearly A has a minimal left (resp. right) ideal Let A be a F-algebra and M be finitely generated free left (resp., right) nonzero A-module, then $M \simeq A^r$ *for a (uniquely determined) positive integer r. The integer r is called the rank of M and will be denoted by* $rank_A(M)$*.*

‡*Joseph Henry Maclagan Wedderburn (2 February 1882, Forfar, Angus, Scotland-9 October 1948, Princeton, New Jersey) was a Scottish mathematician, who taught at Princeton University for most of his career. A significant algebraist, he proved that a finite division algebra is a field, and part of the Artin–Wedderburn theorem on simple algebras. He also worked on group theory and matrix algebra.*

Lemma 3.2.3 *Let A be a simple F-algebra and let J be a minimal right ideal. Then :*

1) *Every finitely generated right A-module M is isomorphic to J^n for some positive integer n.*

2) *All finitely generated simple right A-module is isomorphic to J.*

3) *A non zero finitely generated right A-module M is free (as a right A-module) if and only if $dim_F(A)|dim_F(M)$. Moreover, we have*

$$rank_F(M) = \frac{dim_F(M)}{dim_F(A)}.$$

4) *Two nonzero finitely generated right A-modules are isomorphic if and only if they have the same dimension over F.*

Proof. *1) Let M be a nonzero finitely generated A-module. The left ideal generated by the elements of J is a nonzero two-sided ideal of A, hence equals A. In particular one many write*

$$1 = \sum_{i=1}^{m} b_i\alpha_i, b_i \in A, \alpha_i \in J.$$

Thus for all $x \in A$, we have

$$x = (\sum_{i=1}^{m} b_i\alpha_i)x = \sum_{i=1}^{m} b_i(\alpha_i x).$$

Since J is a right ideal, we have $\alpha_i x \in J$ for all $1 \leq i \leq m$, and therfore we have

$$A = \sum_{i=1}^{m} b_i \cdot J$$

Since M is finitely generated right A-module there exists $m_1, \cdots, m_r \in M$ such that

$$M = \sum_{i=1}^{r} m_i A$$

Therefore,

$$M = \sum_{i=1}^{r} m_i \sum_{j=1}^{m} b_i \cdot I = \sum_{i,j} m_i \cdot (b_j \cdot J) = \sum_{i,j} (m_i \cdot b_j) \cdot J.$$

Hence we may then write $M = \sum_{i=1}^{s} m_i \cdot J$ with s minimal for this properties. Now we want to prove that

$$M = \oplus_{i=1}^{s} m_i \cdot J$$

Assume that $\sum_{i=1}^{s} m_i\gamma_i = 0$ for some $\gamma_i \in J$. If one of the γ_i's is nonzero say γ_s, then $\gamma_s A$ is a nonzero right ideal of A contained in J and hence $J = \gamma_s A$ (for J is a minimal right A-ideal of A). We obtain :

$$m_s \cdot J = (m_s \cdot \gamma_s)A = -\sum_{i=1}^{s-1} m_i \cdot J.$$

This yields

$$M = \sum_{i=1}^{s-1} m_i \cdot J$$

Contradicting the minimality of s. So $\gamma_i = 0$ for all i. It follows that the $A-$ linear map

$$\begin{array}{cccc} \Phi : & J^s & \longrightarrow & M \\ & (\gamma_1, \cdots, \gamma_s) & \longmapsto & \sum_{i=1}^{s} m_i\gamma_i \end{array}$$

is an isomorphism of right A-modules.

2) *Let M be a finitely generated simple right A−module. In particular, M is nonzero and by i) there exists an integer* $s \geq 1$ *such that* $M \simeq J^s$*(as A-module). Since M is simple we have necessarily* $s = 1$*. Otherwise* J^s*, and thus M, would have a nontrivial submodule. Hence* $M \simeq J$*.*

3) *Let M be a nonzero finitely generated A-module. If M is free, then* $M \simeq A^r$ *(as A-modules) where* $r = rank_A(M)$*. Since M and* A^r *are isomorphic as F-vector spaces, we have*

$$dim_F(M) = rank_A(M) \cdot dim_F(A).$$

In particular,

$$dim_F(A) | dim_F(M)$$

and

$$rank_A(M) = \frac{dim_F(M)}{dim_F(A)}$$

Conversely, suppose that $dim_F(A)|dim_F(M)$*. Since M and A are both nonzero finitely generated A-modules, then by 1) we have* $M \simeq J^{r_1}$*, and* $A \simeq J^{r_2}$ *(as A-modules) for some integers* $r_1, r_2 \geq 1$*. The assumption implies that* $r_2|r_1$ *by comparing dimensions over F, write* $r_1 = nr_2$*, then we get* $M \simeq J^{r_2 n} \simeq (J^{r_2})^n \simeq A^{r_1}$*. Hence M is a free (right) A-module.*

4) *Let M and N be two nonzero finitely generated right A-modules. Then by 1)* $M \simeq J^{r_1}$ *and* $N \simeq I^{r_2}$ *for some integers* $r_1, r_2 \geq 1$*. In particular, if M and N have the same dimension as F-vector spaces, then* $r_1 dim_F(J) = r_2 dim_F(J)$ *and therfore* $r_1 = r_2$*. So in this case*

$$M \simeq J^{r_1} \simeq N.$$

Conversely, if $M \simeq N$ *(as A-modules), then plainly they are isomorphic as F-vector spaces. Thus M and N have the same dimension over F.*

Note that this lemma is also true if we consider left A-modules rather than right A-modules.

Proposition 3.2.3 *Let D be a division F-algebra. Then every nonzero finitely generated right D-module is isomorphic to* D^r *for some* $r \geq 1$*.*

Proof. *Since D is a division algebra, then D itself is a minimal right ideal. So by lemma 3.2.3, any nonzero finitely generated D-module M is isomorphic to* D^r *for some positive integer r.*

As an application, we can prove the following result :

Proposition 3.2.4 *Let* m, n *be two positive integers and* D_1, D_2 *be two division F-algebras, then*

$$M_n(D_1) \simeq M_m(D_2) \text{ if and only if } D_1 \simeq D_2 \text{ and } n = m.$$

Proof. *Let* $A_1 = M_m(D_1)$*,* $A_2 = M_n(D_2)$ *and* $e = e_{11}$*, where* $(e_{ij})_{1 \leq i,j \leq m}$ *is the canonical basis of* A_1*, i.e.,* e_{ij} *is the matrix of* $M_m(D_1)$ *with all entries equal to 0 but the ij-entry equal to 1. We have* $e^2 = e$*,* $eA_1e = D_1e = eD_1$ *and that the map*

$$\begin{array}{cccc} \Phi : & D_1 & \longrightarrow & eA_1e \\ & d & \longmapsto & de \end{array}$$

is a ring isomorphism, thus $D_1 \cong eA_1e$*. Also, we have the following ring isomorphism :*

$$eA_1e \simeq End_{A_1}(eA_1)$$

see lemma 3.2.1. Let $I_1 = eA_1$ *which is easily seen to be the set of matrices whose only possibly nonzero row is the first one. This is a minimal right ideal of* A_1 *and by the above, we have* $D_1 \cong End_{A_1}(I_1)$*.*

Similarly, $D_2 \simeq End_{A_2}(I_2)$, where I_2 is a similar right ideal of A_2. Now, if $\psi : A_1 \longrightarrow A_2$ is an isomorphism of F-algebras, then $\psi(I_1)$ is a minimal right ideal of A_2. Since all the minimal right ideals of A_2 are isomorphic by lemma 3.2.3, we have $I_2 \simeq \psi(I_1)$. Therefore, we have a ring isomorphism

$$D_1 \simeq End_{A_1}(I_1) \simeq End_{A_2}(I_2) \simeq D_2.$$

All these isomorphisms are F-linear, so D_1 and D_2 are isomorphic as F-algebras. It follows easily that $m = n$.

Theorem 3.2.1 *(Wedderburn's theorem) Let A be a simple F-algebra. Then A is isomorphic to $M_n(D)$ for some integer m and some division F-algebra D with $Z(D) = Z(A)$.*

Proof. *Let J be a minimal left ideal of A. Since J is a simple left A-module, then by corollary 3.1.2 $D := End_A(J)$ is a division algebra. Moreover, since A is a left A-module, then by lemma 3.2.3 there exists an integer $r \geq 1$ such that $A \simeq J^r$ (as A-module). So taking $e = 1$ in lemmas 3.2.1, 3.2.2 we obtain*

$$A \simeq End_A(A) \simeq End_A(J^r) \simeq M_r(End_A(J)) \simeq M_r(D).$$

The uniqueness of the positive integer r and the division algebra D (up to an algebra isomorphism) comes directly from proposition 3.2.4 and the formula

$$dim_F(A) = r^2 dim_F(D).$$

For the second statement, one can easily see that we have the following canonical algebra isomorphisms :

$$Z(D) \simeq_F Z(M_r(D)) \simeq_F Z(A).$$

The division algebra D, which is unique up to an algebra isomorphism, is called the underlying division algebra of A (or the division algebra Brauer-equivalent to A).

Central simple algebras

Definition 3.2.4 *(Central simple algebra) An F-algebra A is called a central simple algebra over F if A is simple and $Z(A) = F$.*

Notation. *The class of all central simple algebras over F we will denoted by CSA/F.*

Examples 3.2.2 *1) $M_n(F)$ is central simple algebra over F.*

2) Any division F-algebra D is simple and if also D satisfying $Z(D) = F$ is a central simple algebra over F.

3) By examples 3.2.1, for any field F of characteristic different from 2 and any elements $a, b \in F^*$, the quaternion algebra $(a, b)_F$ is simple algebra and $Z((a, b)_F) = F$. Then $(a, b)_F$ is a central simple algebra over F.

4) Any field F is a central simple algebra over itself.

Corollary 3.2.1 *Let A be a simple F-algebra. Then there exists a field extension E/F of finite degree such that A is a central simple E-algebra.*

Proof. *By theorem 3.2.1, $A \simeq M_n(D)$ for some D. It suffices to take $E = Z(D)$, when identifying D with its canonical image in A.*

Proposition 3.2.5 *Let A and B two central simple F-algebras. For every integer $r \geq 1$, we have*

$$M_r(A) \simeq M_r(B) \text{ if and only if } A \simeq_F B.$$

Proof. *By theorem 3.2.1 we may write*

$$A \simeq M_{r_1}(D_1) \text{ and } B \simeq M_{r_2}(D_2).$$

where D_1, D_2 are central division F-algebras and r_1, r_2 are positive integers. Therefore, if $M_r(A) \sim M_r(B)$, then we have $M_{rr_1}(D_1) \simeq M_{rr_2}(D_2)$. It follows then by proposition 3.2.3 that $r_1 = r_2$ and $D_1 \simeq D_2$ (as F-algebras) which implies $A \simeq_F B$.

Lemma 3.2.4 *Let D be a finite dimensional division algebra over an algebraically closed field F. Then, D is isomorphic to F.*

Proof. *Let $d \in D$, d be a nonzero element of D. As D is finite dimensional, the powers $1, d, \ldots, d^i, \ldots.$ are linearly dependent over F. Therefore, we can write :*

$$\sum_{k=0}^{m-1} \alpha_k d^k + d^m = 0.$$

for some m that can be chosen to be the smallest possible with all $\alpha_k \in F$. Now, consider the polynomial $\pi(x) = \alpha_0 + \alpha_1 x + \ldots + x^m$. Since F is algebraically closed, π has a root r in F i.e $\pi(x) = (x - r)q(x)$ with $deg(q) = deg(\pi) - 1$. Evaluating at d we obtain $\pi(d) = (d - r)q(d) = 0$. As π was chosen to be of smallest degree, $q(d) \neq 0$. Hence $d = r \in F$, thus $D = F$.

Corollary 3.2.2 *If F is algebraically closed, then every central simple F-algebra is isomorphic to a (square) matrix algebra with entries in F.*

Proof. *Let A be an F-algebra. By theorem 3.2.1, $A \simeq M_n(D)$ for some integer positive n and some central division algebra D over F. By lemma 3.2.4 D is isomorphic to F, so A is isomorphic to the matrix algebra $M_n(F)$.*

Throughout the rest, we assume familiarity with the properties of tensor products of modules and (associative) algebras. For more details, we refer the reader to Chapter 9 in Pierce book [21]. We now recall the main properties of the tensor product of F-algebras.
We summarize here some properties of tensor products of algebras that we will need in what follows : Let A, B and C be F-algebras.

* *Note that If $(e_i)_{i\in I}$ and $(e'_j)_{j\in J}$ are F-bases of A and B, respectively, then $(e_i \otimes e'_j)_{(i,j)\in I\times J}$ is a F-basis of $A \otimes_F B$.*

* *In particular, the above yields that $A \otimes_F B$ is finite-dimensional F if and only A and B are so, and in this case we have*
$$dim_F(A \otimes_F B) = dim_F(A) dim_F(B). \tag{3.1}$$

* *Let $f : A \longrightarrow C$, $g : B \longrightarrow C$ be homomorphisms of F-algebras such that $f(a)g(b) = g(b)f(a)$ for all $(a, b) \in A \times B$. Then there exists a unique homomorphism of F-algebras $h : A \otimes_F B \longrightarrow C$ such that*
$$h(a \otimes 1) = f(a) \text{ and } h(1 \otimes b) = g(b) \text{ for all } a \in A, b \in B. \tag{3.2}$$

* *If $f : A \longrightarrow B$ and $g : A' \longrightarrow B'$ are homomorphisms of F-algebras. Then $f \otimes g : A \otimes A' \longrightarrow B \otimes B'$ is a homomorphism of F-algebras satisfying*
$$(f \otimes g)(a \otimes b) = f(a) \otimes g(b) \text{ for all } a \in A, b \in B. \tag{3.3}$$
Moreover, if f and g are isomorphisms, then so is $f \otimes g$.

* *Let E/F be a field extension. If B is also an E-algebra, then $A \otimes_F B$ has a natural structure of an E-algebra, where the structure of E-vector space is defined by (linearly) extension of the equalities:*

$$\alpha(a \otimes b) = a \otimes \alpha b \text{ for all } \alpha \in E, a \in A, b \in B. \tag{3.4}$$

In particular $A \otimes_F E$ has a natural structure of an E-algebra. Moreover, $A \otimes_F E$ is finite dimensional over E if and only if A is finite dimensional over F. Furthermore, in this case we have

$$dim_E(A \otimes_F E) = dim_F(A). \tag{3.5}$$

We have also a natural isomorphism of E-algebras

$$(A \otimes_F B) \otimes_E B \simeq_E A \otimes_E B. \tag{3.6}$$

* *We have a natural E-algebra isomorphism*

$$(A \otimes_F B) \otimes_F E \simeq_E (A \otimes_F E) \otimes_E (B \otimes_F E) \tag{3.7}$$

Hence, if $L \subseteq F \subseteq E$ is a tower of field extensions, then we have

$$(A \otimes_L F) \otimes_F E \simeq_E A \otimes_F E.$$

* *We have (the associativity property of tensor products) :*

$$(A \otimes_F B) \otimes_F C \simeq A \otimes_F (B \otimes_F C). \tag{3.8}$$

* *We have also (the commutativity property of tensor products) :*

$$A \otimes_F B \simeq B \otimes_F A. \tag{3.9}$$

* *If A is an algebra over F, and E/F be a field extension. We call the E-algebra*

$$A_E := A \otimes_F E \tag{3.10}$$

the scalar extension of A by E. We have $dim_F(A) = dim_E(A_E)$.

* *For any positive integers m, n, we have a natural isomorphism of algebras :*

$$M_m(A) \otimes_F M_n(B) \simeq M_{mn}(A \otimes_F B). \tag{3.11}$$

* *We have also a natural isomorphism of F-algebras :*

$$M_m(M_n(A)) \simeq M_{mn}(A). \tag{3.12}$$

* *For a field extension E/F, we have a natural F-algebra isomorphism $M_n(F) \otimes_F A \simeq_F M_n(A)$. Also we have a natural E-algebra isomorphism $M_n(F) \otimes E \simeq_E M_n(E)$.*

Proposition 3.2.6 *Let F be a field and let A, B be F-algebras. The following statements hold :*

1) *If A and B are central, then so is $A \otimes_F B$.*
2) *If A is central simple and B is simple, then $A \otimes_F B$ is simple.*
3) *If A and B are central simple, then $A \otimes_F B$ is central simple.*
4) *If $A \otimes_F B$ is a simple then A and B are simple algebras.*

Proof. 1) Let $x = \sum_i a_i \otimes b_i \in Z(A \otimes_F B)$. We may assume b_i belong to a basis of B, so that the a_i are then uniquely determined. For every $a \in A$, we have

$$\sum_i aa_i \otimes b_i = (a \otimes 1)x = x(a \otimes 1) = \sum_i a_i a \otimes b_i$$

So, for all i, we have $aa_i = a_i a$, which implies $a_i \in F$. We can then write $x = \sum_i 1 \otimes a_i b_i = 1 \otimes c$ where $c = \sum_i a_i b_i$. Using the fact that x commutes with $1 \otimes B$, we get $c \in F$. Thus, $Z(A \otimes_F B) = F$.

2) Let J be a nonzero two-sided ideal of $A \otimes_F B$. Fix a basis $(b_i)_i$ of B and let $x = \sum_{i=1}^r a_i \otimes b_i \in J$ with r is minimal. In particular, $a_1 \neq 0$, so by the simplicity of A we have $Aa_1A = A$, we may modify x on both sides by elements of $A \otimes 1$ to arrange that x is of the form $x = 1 \otimes b_1 + \sum_{i \geq 2} a_i \otimes b_i$. Now, for $a \in A$, we have

$$(a \otimes 1)x - x(a \otimes 1) = \sum_{i=2}^{n} (aa_i - a_i a) \otimes b_i \in J$$

This must be zero (by minimality of r), hence $aa_i = a_i a$ for all $a \in A$ and for all $i \geq 2$. So, $a_i \in Z(A) = F$. Therefore, we can write the element $x = 1 \otimes b$ for some nonzero element of B. Thus, J contains an element of the form $1 \otimes b$ with $b \neq 0$. Note that B being a simple algebra, then so is $1 \otimes B$. Note also that $J \cap (1 \otimes B)$ is a two-sided ideal of $1 \otimes B$, it is nonzero because it contains $1 \otimes b$, so it must be equal to $1 \otimes B$. Therefore, J contains $1 \otimes B$. But then it contains $(A \otimes 1)(1 \otimes B) = A \otimes B$.

3) Follows from 1) and 2).

4) Since $A \otimes_F B$ is simple algebra, then $A \otimes_F B \neq 0$, hence $A \neq 0$ and $B \neq 0$. Assume that A is not a simple algebra. Then, there exists be an F-algebra C and a nonzero homomorphism of F-algebras $\psi : A \longrightarrow C$ such that $ker(\psi) \neq 0$. Let $\Phi := \psi \otimes id_B : A \otimes_F B \longrightarrow C \otimes_F B$, then Φ is a nonzero homomorphism and we have

$$ker(\psi) \otimes B \subseteq ker(\Phi)$$

So, $ker(\Phi) \neq 0$. But this yields that $A \otimes_F B$ is not a simple algebra, a contradiction.

Definition and Notation 3.2.1 *Let A be an F-algebra and B be a subalgebra of A. The centralizer (or the commutator) of B in A is*

$$C_A^B = \{a \in A \,|\, ab = ba, \text{ for all } b \in B\}. \tag{3.13}$$

It is easy to check that C_A^B is also a subalgebra of A which contains $Z(A)$. Furthermore, we have $B \subseteq C_A^B$ if and only if B is commutative. Note that $C_A^{Z(A)} = A$ and $C_A^A = Z(A)$.

Lemma 3.2.5 *Let A be a (finite-dimensional) central simple F-algebra, B be a simple subalgebra of A with E and C a subalgebra of C_A^B, then the following statements are equivalent :*

1) $A = BC$

2) $dim_F(A) = dim_F(B)dim_F(C)$.

3) The canonical injections $\imath_B : B \longrightarrow A$ and $\imath_C : C \longrightarrow A$ induce canonically an isomorphisms of algebras $\Phi : B \otimes C \longrightarrow A$.

Proof. 1) $\Rightarrow$ 2) *Let $(e_i)_{i\in I}$ be a basis of B, $(e_j^{'})_{j\in J}$ be a basis of Cand assume that there exist $\gamma_{ij} \in F$ such that $\sum_{i,j}\gamma_{ij}e_ie_j^{'} = 0$. We have $\sum_i e_i(\sum_j \gamma_{ij}e_j^{'}) = 0$, so putting $d_i = \sum_j \gamma_{ij}e_j^{'}$, we get $\sum_i e_id_i = 0$ with all $d_i \in C$, so for all $d_i = 0$, i.e. $\sum_j \gamma_{ij}e_i^{'} = 0$ but since $(e^{'})_{j\in J}$ is a basis of C, so for all i, j, we have $\forall j \in J$ $\gamma_{ij} = 0$. This shows that $(e^ie_j^{'})_{(i,j)\in I\times J}$ is a free family of elements of A (over F). By assumption, we have $A = BC$, so $(e_ie_j^{'})_{(i,j)\in I\times J}$ is a basis of A. Hence $dim_F(A) = dim_E(B)dim_F(C)$.*
2) $\Rightarrow$ 3) *Since $\imath_B : B \longrightarrow A$ and $\imath_C : C \longrightarrow A$ are be homomorphisms of algebras and $C \subseteq C_A^B$, then the bilinear map $b : B\otimes_F C \longrightarrow A$, $(b, c) \longmapsto bc$, induces an algebra homomorphism Φ : $B \otimes_F C \longrightarrow A$. Since all F-linearly independent family of elements of B is still linearly independent over C, then necessarily Φ is injective. Moreover, since $dim_F(A) = dim_F(B)dim_F(C)$, then Φ is an algebra isomorphism.*
3) $\Rightarrow$ 1) *Clear.*

Lemma 3.2.6 *Let A, B be two F-algebras and $C := A\otimes_F B$. Then :*

1) $C_C^{A\otimes_F F} = Z(A) \otimes_F B$.
2) $Z(C) = Z(A) \otimes_F Z(B)$

Proof. 1) *Let $(e_i)_{i\in I}$ be a basis of B. Then every element $d \in A \otimes_F B$ can be written in the form $d = \sum a_i \otimes e_i$ for some $a_i \in A$. In particular, if $d = 0$, then $a_i = 0$, for all i. Now if $d = \sum a_i \otimes e_i \in C_C^{A\otimes_F F}$, then for any $a \in A$, we have $(a \otimes 1)d = d(a \otimes 1)$, so $\sum(aa_i - a_ia) \otimes e_i = 0$, which implies that $aa_i = a_ia$, for all i, i.e., $a_i \in Z(A)$. Hence $C_C^{A\otimes_F F} \subseteq Z(A) \otimes_F B$. The inverse sense is trivial. Thus $C_C^{A\otimes_F F} = Z(A) \otimes_F B$.*

2) *We have $C = A \otimes_F B = (A \otimes_F F)(F \otimes_F B)$, so $Z(C) = C_C^{A\otimes_F F} \bigcap C_C^{F\otimes_F B} = (Z(A) \otimes B) \bigcap (A \otimes_F Z(B)) = Z(A) \otimes_F Z(B)$.*

Proposition 3.2.7 *Let E/F be a field extension and A be a central simple F-algebra. Then $A \otimes_F E$ is a central simple algebra over E (when we identify $F \otimes_F E$ with E).*

Proof. *By proposition 3.2.6 $A \otimes_F E$ is simple E-algebra and by lemma 3.2.6 $Z(A \otimes_F E) = Z(A) \otimes E = F \otimes_F E \simeq E$.*

Definition 3.2.5 *(Opposite algebra) Given an F-algebra A, we denote by A^{op} the F-algebra that we get from A just by reversing the order of multiplication in A (i.e., the algebra over F having the same underlying set of element as A and for which the addition and scalar multiplication are those of A). We call this algebra the opposite algebra of A.*

Proposition 3.2.8 *Let A be a central simple algebra over F. Then, A^{op} is a central simple algebra over F.*

Proof. *Clear.*

Proposition 3.2.9 *Let A be a central simple algebra over F. Then the dimension of A over F is a square.*

Proof. *Let $\overline{F}$ be an algebraic closure of F, then by corollary 3.2.2, there is a positive integer r such that $A_{\overline{F}} \simeq M_r(\overline{F})$ (as $\overline{F}$-algebras). Thus,*

$$dim_F(A) = dim_{\overline{F}}(A_{\overline{F}}) = dim_{\overline{F}}(M_r(\overline{F})) = r^2 \tag{3.14}$$

Definition 3.2.6 *Let A be a central simple F-algebra. The integer $\sqrt{dim_F(A)}$ is called the degree of A. The Schur index of A is the degree of the underlying division algebra of A. We denote it by $ind(A)$, i.e., $ind(A) = deg(D)$, where D is the underlying division algebra of A.*

Lemma 3.2.7 *Let A be a central simple algebra over F with degree r. Then $A \otimes_F A^{op} \simeq M_r(F)$ (as a F-algebras).*

Proof. *Let's consider the mapping*

$$\begin{array}{rccc} \Psi : & A & \longrightarrow & End_F(A) \\ & a & \longmapsto & \Psi(a) := l_a \end{array}$$

where $l_a(x) = ax$, for all $x \in A$. It is clear that Ψ is F-algebra homomorphism. In the same way, we define the F-algebra homomorphism

$$\begin{array}{rccc} \Phi : & A^{op} & \longrightarrow & End_F(A) \\ & a & \longrightarrow & \Phi(a) := l_a^{op} \end{array}$$

where $l_a^{op}(x) = xa$, for all $x \in A$. One can check that the images of Ψ and Φ commute in $End_F(A)$. So, there is a unique F-algebra homomorphism $\Theta : A \otimes_F A^{op} \longrightarrow End_F(A)$ satisfying $\Theta(a \otimes b) = \Psi(a)\Phi(b)$. Since $A \otimes_F A^{op}$ is simple, Θ is injective. Moreover, we have the equalities $dim_F(A \otimes_F A^{op}) = dim_F(End_F(A)) = r^2$. So hence, Θ is also surjective. It suffices now to see that $End_F(A)$ is isomorphic to $M_r(F)$ (as F-algebras).

Theorem 3.2.2 *(Double centralizer theorem (**DCT**)) Let A be a central simple algebra over F and let B be a simple subalgebra of A. Then, the following properties hold :*

1) *The centralizer C_A^B of B in A is a simple subalgebra of A having the same center as B. Moreover, we have*
$$dim_F(A) = dim_F(B) dim_F(C_A^B). \tag{3.15}$$

2) *We have $C_A^{C_A^B} = B$.*

Proof. 1) *To show that C_A^B is simple, we will show that $C_A^B \simeq End_C(A)$, where $C := B \otimes_F A^{op}$ and where A is considered as a left C-module for the operation defined by linearly extending the following equalites :*

$$(\alpha \otimes \gamma)x = \alpha x \gamma \text{ for all } \gamma \in A^{op}, \alpha \in B \text{ and } x \in A \tag{3.16}$$

Consider the map

$$\begin{array}{rccc} \Phi : & C_A^B & \longrightarrow & End_C(A) \\ & c & \longmapsto & \Phi(c) \end{array}$$

where $\Phi(c) : x \longmapsto cx$, for any $x \in A$. It is clear that Φ is a F-algebra homomorphism. In particular, we have $c = \Phi(c)(1) = 0$, hence Φ is injective. One can easily see that Φ is also surjective. Indeed, let $g \in End_C(A)$ and let $c = g(1)$, then for every $b \in B$, we have :

$$cb = (1 \otimes b)c = (1 \otimes b)g(1) = g((1 \otimes b)1) = g(b).$$

We have also $bc = (b \otimes 1)c = (b \otimes 1)g(1) = g((b \otimes 1)1) = g(b)$, Consequently, $cb = bc$, that is $c \in C_A^B$. Moreover, for any $x \in A$, we have

$$\Phi(c)(x) = cx = (1 \otimes x)c = (1 \otimes x)g(1) = g((1 \otimes x)) = g(x)$$

Thus $g = \Phi(c)$. Now, we aim to prove the two F-algebras C_A^B and $End_C(A)$ have some dimension (over F). Note that by proposition 3.2.6 C is a simple algebra. Moreover, since C is finite-dimensional over F, then C is also semisimple, so there is a C-module N, up to an isomorphism, such that every C-module is a finite direct sum of copies of N. In particular, $A \simeq N^r$, for *some positive integer r. Let* $D := End_C(N)$*. As N is a simple C-module, it follows by lemma 3.1.1 that D is a division algebra. We proved above that* $C_A^B \simeq End_C(A)$*, so*

$$C_A^B \simeq End_C(A) \simeq End_C(N^r) \simeq M_r(End_C(N)) = M_r(D).$$

Therefore, we have

$$dim_F(C_A^B) = dim_F(M_r(D)) = r^2 dim_F(D) \tag{3.17}$$

It is clear that N is also a D-module, so we have $N \simeq D^m$*, for some positive integer m, so*

$$C = End_D(N) \simeq End_D(D^m) \simeq M_m(D).$$

Thus $A \simeq D^{rm}$*, hence*

$$dim_F(A) = rm dim_F(D) \tag{3.18}$$

On the other hand, we have

$$dim_F(A)^2 = dim_F(C)dim_F(End_C(A)) = dim_F(B \otimes_F A^{op})dim_F(C_A^B) = dim_F(B)dim_F(A^{op})dim_F(C_A^B)$$

Hence

$$dim_F(A) = dim_F(B)dim_F(C_A^B).$$

2) *Since* C_A^B *is simple, applying 1) gives*

$$dim_F(C_A^B)dim_F(C_A^{C_A^B}) = dim_F(A)$$

Since

$$dim_F(B)dim_F(C_A^B) = dim_F(A)$$

We deduce that

$$dim_F(B) = dim_F(C_A^{C_A^B})$$

Now, the definition easily imply that $B \subseteq C_A^{C_A^B}$*. The equality between dimensions then implies that* $B = C_A^{C_A^B}$*.*

The Skolem[§]-Noether theorem

For a ring R and unit $r \in R^\times$*,* $Int(r)(x) := r^{-1}xr$ *is an automorphism of R. Such automorphisms are called an inner automorphisms of R.*

Lemma 3.2.8 *Let A be a (finite-dimensional) simple F-algebra and suppose that B is an F-space. Let* ϕ *and* ψ *be two F-algebras homomorphisms of A to* $End_F(B)$*, then there exists* $\theta \in End_F(B)^\times$ *such that* $\phi(a) = \theta^{-1}\psi(x)\theta$ *for all* $x \in A$*.*

Proof. *See [21, Lemma, p.* **230***].*

Theorem 3.2.3 *Let A be a central simple algebra over F and let B be simple F-subalgebra of A. For any F-algebra homomorphism* $\varphi : B \longrightarrow A$ *there exists* $a \in A^\times$ *such that* $\varphi(x) = a^{-1}xa$ *for all* $x \in B$*.*

[§]*Thoralf Albert Skolem* (Norwegian 23 May 1887-23 March 1963) *was a Norwegian mathematician who worked on mathematical logic and set theory.*

Proof. *By lemma 3.2.7, there is an algebra isomorphism* $\Lambda : A \otimes A^{op} \longrightarrow End_F(A)$. *Define* $\phi := \Lambda(id \otimes \varphi) : A^{op} \otimes B \longrightarrow End_F(A)$ *and* $\psi := \Lambda(id \otimes \jmath) : A^{op} \otimes B \longrightarrow End_F(A)$, *where* $\jmath : B \longrightarrow A$ *is the inclusion homomorphism. Since* $A^{op} \otimes B$ *is simple (see proposition 3.2.6), it follows from lemma 3.2.8 that there exists* $\theta \in End_F(A)^{\times}$ *such that* $\phi(x \otimes y) = \theta^{-1}\psi(x \otimes y)\theta$ *for all* $x \in A^{op}$, $y \in B$. *Let* $z = \Lambda^{-1}(\theta) \in A^{op} \otimes A$. *Since* θ *is unit, so is* z *and* $\theta^{-1} = \Lambda(z^{-1})$. *Moreover,*

$$\begin{array}{rcl} \Lambda(z(x \otimes \varphi(y))) & = & \Lambda(z)\Lambda(x \otimes \varphi(y)) \\ & = & \theta\phi(x \otimes y) \\ & = & \psi(x \otimes y)\theta \\ & = & \Lambda((x \otimes y)\Lambda(z)) \\ & = & \Lambda(x \otimes y)z) \end{array}$$

Since Λ *is injective, then*

$$x \otimes \varphi(y) = z^{-1}(x \otimes y)z \text{ for all } x \in A^{op}, y \in B \tag{3.19}$$

By taking $y = 1$ *in (3.19), we get* $z(x \otimes 1) = (x \otimes 1)z$ *that is* $z \in C_{A \otimes A^{op}}^{A^{op} \otimes F} = F \otimes A$ *(see lemma 3.2.6). Similarly,* $z^{-1} \in F \otimes A$, *therfore* $z = 1 \otimes v$ *and* $z^{-1} = 1 \otimes v$, *with* $u, v \in A$. *Hence* $uv = 1$, $u \in A^{op}$ *and* $v = u^{-1}$. *Finally, if* $x = 1$ *in (3.19) then* $1 \otimes \varphi(y) = 1 \otimes u^{-1}yu$ *for all* $y \in B$, *therfore* $\varphi(y) = u^{-1}yu$.

3.3 Cyclic algebras

We will usually denote a cyclic Galois group by $\langle\sigma\rangle$, *where* σ *is a generator of the group* G.

Definition 3.3.1 *Let* M/F *be a cyclic Galois field extension of dimension* n *with Galois group* $G = Gal(M/F)$ *generated by* σ. *Choose an element* β *a nonzero element of* E. *We construct a non-commutative algebra* A, *denoted by* $(M/F, \sigma, \beta)$, *as follows :*

$$A = M \bigoplus Me \bigoplus \cdots \bigoplus Me^{n-1}$$

where e *is an indeterminate satisfying the multiplicative conditions :*

$$e^n = \beta \text{ and } \lambda e = e\sigma(\lambda) \text{ for all } \lambda \in M \tag{3.20}$$

(the addition and scalar multiplication being defined componentwise). Such an algebra is called a cyclic algebra.

Notation. *When there is no risk of confusion, we omit* F *and the algebra* A *we will denoted by* (M, σ, β).

Remark 3.3.1 *Assume that* $char(F) \neq 2$, $M = F(\sqrt{d})$ *be a quadratic extension, defined by an element* $d \in F^*$, *and let* σ *be the unique nontrivial* F*-automorphism of* M. *Then we have* $(M/F, \sigma, \beta) \simeq_F (a, b)_F$. *Hence cyclic algebras may be viewed as a generalization of quaternion algebras. (See [4, Remark VII.1.4, p.**130**]).*

Let A *be a central simple algebra over* F *and let* K *be a subfield of* A *(i.e., a field extension of* F *in* A*), then* $dim_F(K) \leq deg(A)$ *(see [21, Corollary a, p.**236**]). Let* A *be a central simple algebra over* F *and let* K *be a subfield of* A. *If* $dim_F K = deg(A)$, *then we say that* K *is a strictly maximal subfield of* A. *Such subfield does not always exist, but when* A *is a division algebra, then any maximal subfield of* A *is strictly maximal (see [21, corollary b, p.**236**]). We say that a field extension* L *of* F *is a splitting field of* A *if* $A \otimes_F L$ *is isomorphic to a matrix algebra over* F, *i.e., if and only if the underlying division algebra of* $A \otimes_F L$ *is* L.
If K *is a strictly maximal subfield of* A, *then* K *is a splitting field of* A *(see [21, Corollary, p.**241**]). In particular, if* $A = (M/E, \sigma, \beta)$ *is a cyclic algebra, then* M *is a strictly maximal subfield of* A, *so* M *is a splitting field of* A.

Example 3.3.1 *Consider the real matrix algebra* $A = M_r(\mathbb{H})$ *for some positive integer* r*. We have* $dim_{\mathbb{R}}(A) = 4r^2$*. Note that* $\mathbb{R}$ *and* $\mathbb{C}$ *are the only finite field extensions of* $\mathbb{R}$*. Therefore* A *has no strictly maximal subfields for any* $r \in \mathbb{N}^*$*.*

Theorem 3.3.1 *The cyclic algebra* $A = (M/F, \sigma, \beta)$ *is a central simple algebra over* F*.*

Proof. *The arguments of this proof were used before several times. Let*

$$x = x_0 + x_1 e + \ldots + x_{n-1} e^{n-1}$$

be an element of the center of A*. The equation* $xe = ex$ *gives rise to the following equalities*

$$x_{n-1}\beta + x_0 e + \ldots + x_{n-2} e^{n-1} = \sigma(x_{n-1})\beta 1 + \sigma(x_0) e + \ldots + \sigma(x_{n-2}) e^{n-1}.$$

Now the equation $x(\alpha 1) = \alpha x$ *for all* $\alpha \in M$ *gives*

$$x_0 \alpha 1 + x_1 \sigma(\alpha) e + \ldots + x_{n-1} \sigma^{n-1}(\alpha) e^{n-1} = \alpha x_0 1 + \alpha x_1 e + \ldots + \alpha x_{n-1} e^{n-1}.$$

Hence $x_1 = \cdots = x_{n-1} = 0$*. So,* $Z(A) = F$*.*
Let J *be a two-sided nonzero ideal of* A *and let* $x = x_0 + x_1 e + \ldots + x_m e^m$ *be a nonzero element of* J *with* m *minimal. If* $m = 0$*, then* $x = x_0 \in E$*, so* $J = A$*.*
Suppose that $m > 0$*, and suppose that* $J \neq A$*, then consider an element* $\alpha \in M$ *such that* $\sigma^i(\alpha) \neq \alpha$ *for all* $\sigma^i \neq id$*. Then, the following contradicts the minimality of* m *:*

$$(\alpha x - x\alpha)e^{-1} \in J.$$

Theorem 3.3.2 *A central simple algebra* A *of dimension* n^2 *is isomorphic to a cyclic algebra if* A *contains a subfield* M *of dimension* n *over* F *such that* M/F *is a cyclic Galois field extension.*

Proof. *Let* σ *be a generator of the Galois group of* M/F*. By Skolem-Noether theorem, there is an invertible element* e *of* A *such that*

$$\sigma(\alpha) = e\alpha e^{-1}.$$

for all $\alpha \in M$*. Since conjugation by* e^n *is the identity on* M*, we see* $e^n \in C_A^M = M$*. Since* $ee^n e^{-1} = e^n$*, in fact* e^n *is a central element of* A*, so* $e^n \in F$*. It remains to prove that* $1, e, \ldots, e^{n-1}$ *are linearly independent over* M*. Otherwise, we consider a relation*

$$x = x_0 + x_1 e + \ldots + x_m e^m = 0$$

with $x_m \neq 0$ *and* m *minimal. This leads to a contradiction in the same way as above : Choose a primitive element* $\alpha \in E$ *and consider the equality* $0 = (\alpha x - x\alpha)e^{-1}$*. This leads to a contradiction with the minimality of* m*.*

Definition 3.3.2 *(Norm and Trace) Let* M/F *be a Galois field extension of dimension* n*, with* $\sigma_1, \ldots, \sigma_n$ *denoting all elements of* $Gal(M/F)$*. For an element* x *of* M*, the elements* $\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x)$ *are called the conjugates of* x *and*

$$N(x) = \prod_{i=1}^{n} \sigma_i(x), Tr(x) = \sum_{i=1}^{n} \sigma_i(x).$$

are called, respectively, the norm and the trace of x*.*

Remark 3.3.2 *Whenever the context is not clear, we write* $N_{M/F}$*, resp.,* $Tr_{M/F}$ *to avoid ambiguity.*

Definition 3.3.3 *A cyclic algebra which is also a division algebra is called a cyclic division algebra.*

Theorem 3.3.3 *Let* M/F *be a cyclic field extension of dimension* n *with Galois group* $Gal(M/F) = \langle\sigma\rangle$*. If* $0 \neq \beta, \beta^2, \ldots, \beta^{n-1}$ *are not a norm of elements of* M*, then* $(M/F, \sigma, \beta)$ *is a cyclic division algebra.*

Proof. *See [21, 45, p.279].*

3.4 Brauer group and Crossed products

3.4.1 The Brauer group

*Let F be a field and let **CSA**(F) be the class of all central simple algebras over F. We say that two central simple F-algebras A and B are similar, denoted by $A \sim$ ¶ B, if there are positive integers r_1 and r_2 such that $M_{r_1}(A)$ is isomorphic to $M_{r_2}(B)$ as a F-algebra. In the next lemma we prove that this defines an equivalence relation on **CSA**(F), which reduces to F-algebra isomorphism when the two central simple algebras have the same dimension over F.*

Lemma 3.4.1 *Let F be a field. Then $\sim$ is an equivalence relation on **CSA**(F), which reduces to F-algebra isomorphism when two central simple algebras have the same dimension over F.*

Proof. *It is clearly that $\sim$ is reflexive and symmetric on **CSA**(F). Let A, B and C be elements of **CSA**(F) such that $A \sim B$ and $B \sim C$. Then there are $r_1, r_2, r_3, r_4 \in \mathbb{N}^*$ such that*

$$M_{r_1}(A) \simeq M_{r_2}(B) \text{ and } M_{r_3}(B) \simeq M_{r_4}(C)$$

So we have

$$M_{r_1 r_3}(A) \simeq M_{r_3}(M_{r_1}(A)) \simeq M_{r_3}(M_{r_2}(B)) \simeq M_{r_2}(M_{r_3}(C)) \simeq M_{r_2}(M_{r_4}(C)) \simeq M_{r_2 r_4}(C).$$

Hence $A \simeq C$. Consequently, $\sim$ is also transitive. The rest follows by applying Wedderburn's theorem.

The next proposition shows that the tensor product is a class invariant under similarity.

Proposition 3.4.1 *Let A, B, A' and B' be central simple F-algebras such that $A \sim A'$ and $B \sim B'$. Then $A \otimes_F B \sim A' \otimes_F B'$.*

Proof. *There exists $r_1, r_2, r_3, r_4 \in \mathbb{N}^*$ such that*

$$M_{r_1}(A) \simeq M_{r_2}(A') \text{ and } M_{r_3}(B) \simeq M_{r_4}(B')$$

Observe that

$$M_{r_1}(A) \otimes_F M_{r_2}(B) \simeq M_{r_3}(A') \otimes_F M_{r_4}(B').$$

and that (3.11) implies that we have the F-algebra isomorphism

$$M_{r_1 r_2}(A \otimes_F B) \simeq M_{r_3 r_4}(A' \otimes_F B').$$

Hence $A \otimes_F B \sim A' \otimes_F B'$.

Remark 3.4.1 *Observe that for a field F the class **CSA**(F) is not empty, since for every positive integer n, the matrix algebra $M_n(F)$ is an element of **CSA**(F).*

Theorem 3.4.1 *Let F be a field. Then there exists a pair (G, s) consisting of a group G and a surjective map $s : \textbf{CSA}(F) \longrightarrow G$ that satisfy for every two central simple F-algebras A and B the following conditions :*

i) $s(A \otimes_F B) = s(A)s(B)$.

ii) *The equality $s(A) = s(B)$ holds if and only if A and B are Brauer equivalent.*

¶ *When $A \sim B$ we say also A and B are Brauer equivalent.*

Moreover, the pair (G, s) is uniquely determined up to a unique isomorphism, that is, if (G', s') is another pair satisfying the above, then there is a unique group isomorphism $\beta : G \longrightarrow G'$ such that we have the equality $s' = \beta \circ s$.

Proof. *Let K be a subclass of **CSA**(F) that is a set such that every element of **CSA**(F) is isomorphic as a F-algebra to at least one element of K, and let G be the quotient set of K by $\sim$, i.e., $G := K/\sim$. For an element A of **CSA**(F) we let $[A]$ denote the element of G that contains the elements of K that are Brauer equivalent to A, which gives a surjective map*

$$\begin{array}{rccc} \pi : & \mathbf{CSA}(F) & \longrightarrow & G \\ & C & \longmapsto & [C] \end{array}$$

Now, We will show that G is an abelian group under the tensor product over F. To this end, observe that the map

$$\begin{array}{rccc} \mathfrak{u} : & G \times G & \longrightarrow & G \\ & ([B], [C]) & \longmapsto & [B \otimes_F C] \end{array}$$

is well-defined by proposition 3.4.1, so it remains to prove that G satisfies the group axioms and commutativity with respect to the tensor product.

- *Observe that for any central simple algebra A over F, it clearly holds that $A \otimes_F F$ is isomorphic to A as a F-algebra. Hence, $[F]$ functions as the identity element of G under the tensor product over F.*
- *Associativity follows from (3.8), and commutativity follows from (3.9).*
- *The existence of inverse elements in G is proven by lemma 3.2.7, which states that the inverse of an element $[A]$ of G is given $[A^{op}]$, where A^{op} is the opposite algebra of A.*

Consequently, we have showed that G is an abelian group under the tensor product over F.
*It is clear that for every A, B $\in$ **CSA**(F) the map π satisfies the equality $\pi(A \otimes_F B) = \pi(A)\pi(B)$, hence, we have a pair (G, π) with $s = \pi$ that satisfies the theorem.*
Now, if (G', s') is another pair that satisfies the theorem, and define

$$\begin{array}{rccc} \beta : & G & \longrightarrow & G' \\ & [A] & \longmapsto & s'(A) \end{array}$$

It is clear that β is a unique group isomorphism satisfying the equality $s = \beta \circ s'$. It follows that (G, s) is uniquely determined up to isomorphism.

Definition 3.4.1 *The group of the uniquely determined pair (G, s) is called the Brauer group of F, denoted by $Br(F)$, and is written multiplicatively. For a central simple algebra A over F, we denote $s(A)$ by $[A]$.*
*Moreover, an element b of $Br(F)$ is often denoted by $[A]$, where A is an element of **CSA**(F) that is similar to an element of b.*

Definition 3.4.2 *The exponent of A (or period of A) is the order of $[A]$ in $Br(F)$.*

Proposition 3.4.2 *Every element of $Br(F)$ contains a unique central division F-algebra up to isomorphism.*

Proof. *This follows by applying Wedderburn's theorem.*

Some examples of Brauer groups

1) *We have already seen in corollary 3.2.2 that there are no nontrivial central division algebras over an algebraically closed field. So the Brauer group of an algebraically closed field is trivial.*

2) *Let F be a finite field, then by [Joseph Wedderburn] F is the unique central division algebra over F, so the Brauer group of F is trivial.*

3) *By [15, 6.6 Die Brauergruppe von $\mathbb{R}$, p.**54**], $\mathbb{R}$ and $\mathbb{H}$ are the only central division algebras over $\mathbb{R}$. Consequently, the Brauer group of $\mathbb{R}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.*

The Brauer group as a functor

For any nonzero homomorphism $\psi : F \longrightarrow M$ between fields, one can consider M as a field extension of F and then form the tensor product $A \otimes_F M$ that we denote by A_ψ. In what follows a homomorphism between fields will always mean a nonzero homomorphism.

Lemma 3.4.2 *Let $\psi : F \longrightarrow M$ be a field homomorphism. Then the mapping $Br(\psi) : Br(F) \longrightarrow Br(M)$ defined by $[A] \longmapsto [A_\psi]$, is a group homomorphism.*

Proof. *Let $\psi : F \longrightarrow M$ be a field homomorphism and let A be a central simple algebra over F. A_ψ is central simple over E. Define the map*

$$\begin{array}{rccc} Br(\psi): & Br(F) & \longrightarrow & Br(M) \\ & [A] & \longmapsto & [A_\psi] \end{array}$$

and observe that this is a well-defined function by proposition 3.4.1. Moreover, by associativity and commutativity of the tensor product (see (3.8) and (3.9)), we have

$$\begin{array}{rcl} Br(\psi)([A])Br([B]) & = & [A \otimes_F M][B \otimes_F M] \\ & = & [(A \otimes_F M) \otimes_M (B \otimes_F M)] \\ & = & [A \otimes_F (M \otimes_F B)] \\ & = & [(A \otimes_F B) \otimes_F M] \\ & = & Br(\psi)([A \otimes_F B]) \end{array}$$

This shows that $Br(\psi)$ is a group homomorphism.

Notation. *Let $\mathcal{F}ield$ denote the category of fields with morphisms given by field homomorphisms, and let $\mathcal{A}b$ denote the category of abelian groups with morphisms given by group homomorphisms.*

Theorem 3.4.2 *The Brauer group defines a covariant functor $Br : \mathcal{F}ield \longrightarrow \mathcal{A}b$ that maps a field F to $Br(F)$ and maps a field homomorphism ψ to $Br(\psi)$.*

Proof. *Clear.*

Let K be a field extension of F and consider the canonical group homomorphism $\phi_{K/F} : Br(F) \longrightarrow Br(K)$, $[A] \longmapsto [A \otimes_F K]$. Plainly, $\ker(\phi_{K/F})$ is a subgroup of $Br(F)$. We call it the relative Brauer group of K/F.

Relative Brauer groups

In this subsection, we show that for every central simple algebra A over a field F there exists a finite Galois extension of F (i.e., a finite-dimensional Galois field extension of F) that splits A. This enables us to write the Brauer group of F as a union of relative Brauer groups of finite Galois extensions of F, i.e

$$Br(F) = \bigcup_{K \supseteq F \text{ finite Galois}} Br(K/F).$$

Remark 3.4.2 *Let A be a central simple algebra over F and let K be a field extension of F. Then, by definition K is a splitting field of A if and only if* $[A] \in Br(K/F)$.

Theorem 3.4.3 *Let x be an element of* $Br(F)$. *Then there is a separable field extension* $K \supseteq F$ *such that x is an element of* $Br(K/F)$.

Proof. *See [15, Existenz eines separablen Zerfällungskörpers, p.**47**].*

Corollary 3.4.1 *Let x be an element of* $Br(F)$. *Then there is a finite Galois field extension* $E \supseteq F$ *such that x is an element of* $Br(E/F)$.

Proof. *Indeed, by the previous theorem, we can consider a separable field extension M of F such that* $x \in Br(M/F)$. *It suffices to take a Galois field extension K of F that contains M.*

Corollary 3.4.2 *For any field F. We have the following equality*

$$Br(F) = \bigcup_{K \supseteq F \text{ finite Galois}} Br(K/F).$$

Proof. *Clear.*

3.4.2 Crossed products

In this section, we will construct a very important type of central simple algebra via a finite Galois field extension of F. This algebra is called crossed product. As will be seen later, this algebra will connect the Brauer group of a field F to a second Galois cohomology group obtained by considering all finite-dimensional Galois field extensions of F.
Throughout this subsection, when not mentioned, we assume that K/F is a finite Galois field extension. We assume throughout the rest familiarity with basic (Galois) cohomological notions. In particular, recall that when considering a finite Galois field extension with Galois group G, then a 2-cycle of G with values in K^* *is a map* $a : G \times G \longrightarrow K^*$ *satisfying* $a(\sigma,\tau)a(\sigma\tau,\gamma) = a(\sigma,\tau\gamma)\sigma(a(\sigma,\gamma))$ *for all* $\sigma,\tau,\gamma \in G$.

Proposition 3.4.3 *Let K/F be a finite Galois extension with Galois group* $Gal(K/F)$. *Let a be a 2-cocycle of G with values in* K^* *and let A be a left vector space over E with basis* $\{e_\sigma\}_{\sigma\in G}$ *the multiplication defined by*

$$\Big(\sum_{\sigma\in G} x_\sigma e_\sigma\Big)\cdot\Big(\sum_{\tau\in G} y_\tau e_\tau\Big) = \sum_{\sigma\in G}\sum_{\tau\in G} x_\sigma \sigma(y_\tau) a(\sigma,\tau) e_{\sigma\tau} \tag{3.21}$$

where $x_\sigma, y_\tau \in K$ *for* $\sigma,\tau \in G$. *Then, A is a central simple algebra over F that contains K as a strictly maximal subfield.*

Proof. *Let* $\sigma,\tau,\rho \in G$, *Then*

$$a(\sigma,\tau)a(\sigma\tau,\rho) = \sigma(a(\tau,\rho))a(\sigma,\tau) \tag{3.22}$$

Using (3.22), one can see that A is indeed an associative algebra with unit (equal to $a(id,id)^{-1}e_{id}$. *It is clear that* $dim_F A = (dim_F K)^2$, *so K is a strictly maximal subfield of A. Also, since for all* $x, y \in K^*$

and $\sigma, \tau \in G$, wehavexe$_\sigma$ye$_\tau$ $= x\sigma(y)a(\sigma,\tau)e_{\sigma\tau}$, then one can easily see that $Z(A) = K^*$ (for K/F is a Galois field extension).
A is a simple algebra . Indeed, let I be a nonzero two-sided of A and let $x = \sum_{i=1}^{r} x_{\sigma_i} e_{\sigma_i}$ be a nonzero element of I, where all $x_{\sigma_i} \in K$ (with r is minimal integer). Suppose that $r > 1$ and choose $z \in K$ such that $\sigma_1(z) \neq \sigma_2(z)$

$$\sigma_1(z)^{-1}xz = \sigma_1^{-1}x_{\sigma_1}\sigma_1(z)e_{\sigma_1} + \sigma_1^{-1}(z)x_{\sigma_2}\sigma_2(z)e_{\sigma_2} + \ldots.$$

We get $0 \neq x - \sigma_1(z)^{-1}xz \in I$, which contradicts the minimality of r, so $x = ye_\sigma$ for some $y \in E^*$, $\sigma \in G$. But in this case, x will be an invertible element of A, so $I = A$.

Definition 3.4.3 *The central simple algebra A over F defined in proposition 3.4.3 is called the crossed product algebra over F of K and G with respect to a, denoted by (K, G, a).*

Proposition 3.4.4 *Let K/F be Galois field extension with Galois group G, and let $a, b : G \times G \longrightarrow K^*$ be two 2-cocycle. Then*

$$(K, G, a) \otimes_F (K, G, b) \sim (K, G, ab).$$

Proof. *See [15, Multiplikativitätssatz, p.**68**].*

Remark 3.4.3 *A cyclic algebra is an example of a crossed product. Indeed, let (K, G, β) be a cyclic algebra as defined in section 3.3. We can define a 2-cocycle as follows :*

$$\begin{array}{rccc} a: & G \times G & \longrightarrow & E^* \\ & (\sigma^i, \sigma^j) & \longmapsto & \begin{cases} 1 & \text{if } i+j < n \\ \beta & \text{if } i+j \geq n \end{cases} \end{array}$$

*One can check that the F-algebra (K, G, a) is isomorphic to (K, σ, β). For more details we refer to [15, section 10.3 Existenzsatz, p.**83**].*

3.5 Cohomological interpretation of the Brauer group

As claimed in the previous subsection, we will see here that the relative Brauer group $Br(K/F)$ of a (finite) Galois field extension K/F is isomorphic to the second cohomology group $H^2(Gal(K/F), K^*)$.

Proposition 3.5.1 *Let $K \supseteq F$ be a finite Galois extension with Galois group G. Then two 2-cocycles a and b of G with values in K^* are cohomologous if and only if (K, G, a) and (K, G, b) are isomorphic as F-algebras.*

Proof. *See [15, 7.7 Isomorphiekriterium für verschränkte Produkte, p.**63**].*

Theorem 3.5.1 *Let x be an element of $Br(F)$. Then for each finite Galois extension $K \supseteq F$ that splits x, there exists a 2-cocycle a of $Gal(K/F)$ with values in K^* that is unique up to cohomology such that the crossed product algebra $(K, Gal(K/F), a)$ is Brauer-equivalent to x.*

Proof. *See [15, 8, Die Isomorphie $H^2(G, L^*) \simeq Br(L/K)$, p.**68**].*

Theorem 3.5.2 *Let K/F be a finite Galois field extension. Then the map*

$$\begin{array}{rccc} \Psi: & H^2(Gal(E/F), E^*) & \longrightarrow & Br(E/F) \\ & [a] & \longmapsto & [(E, Gal(E/F), a)] \end{array}$$

is a group isomorphism.

Proof. *Using theorem 3.5.1, one sees that the map Ψ is well-defined and injective.*
By theorem 3.5.1, for any element x of $Br(K/F)$ there exists a 2-cocycle a of G with values in K^* such that $x = [(K, G, a)]$. So Ψ is surjective. Hence ψ bijection. Also by proposition 3.5.1, one sees that Ψ is a group homomorphism, hence a group isomorphism.

3.6 Some non-abelian cohomology

In this section we recall elementary facts about non-abelian group cohomology. Fore more details we refer the reader to [24, Cohomologie Galoisienne].

Definition 3.6.1 *Let G be a finite group.*

i) *A G-set E is a set equipped with a G-operation from the left. We will use the notation ${}^gx := g \cdot x$ for $x \in E$ and $g \in G$.*

ii) *A morphism of G-sets, a G-morphism for short, is a map $\gamma : E \longrightarrow F$ between G-sets such that the diagram*

$$\begin{array}{ccc} G \times E & \longrightarrow & F \\ {\scriptstyle id_G \times \gamma}\downarrow & & \downarrow{\scriptstyle \gamma} \\ G \times F & \longrightarrow & F \end{array}$$

commutes.

iii) *A G-group M is a G-set carrying a group structure such that ${}^g(xy) =^g x^gy$ for every $g \in G$ and $x, y \in M$.*

Note that, for all $g \in G$ this forces ${}^g1_M = 1_M$ and for all $x \in M$ ${}^g(x^{-1}) = ({}^gx)^{-1}$. If M is abelian then it is called a G-module.

Example 3.6.1 *Let G be an abelien group and H a subgroup of G. Then we can viewed G as a H-set.*

For a G-set M, we let $M^G := \{x \in E \,|\, {}^gx = x \text{ for all } g \in G\}$

Definition 3.6.2 *Let G be a finite group.*

i) *For any G-module M, we set $H^0(G, M) := M^G$, the zeroth cohomology set of G with coefficients in M is just the subset of G-invariants in M. If M is a G-group, then one can see that $H^0(G, M)$ is a group.*

ii) *If M is a G-group. A map $\rho : G \longrightarrow M$ is called a 1-cocycle if for any $g, h \in G$, we have*

$$\rho(gh) = \rho(g)\,{}^g\rho(h). \tag{3.23}$$

iii) *Let M be a G-group. We say that 1-cocycles $\rho, \rho' : G \longrightarrow M$ are cohomologous if there is $x \in M$*

$$\rho(g) = x^{-1}\rho'(g)\,{}^gx, \text{ for all } g \in G.$$

Remarks 3.6.1

* *The map $G \longrightarrow M$ sending every element of G to 1_M is a 1-cocycle. We call this the trivial cocycle.*
* *For any G-group M and any $x \in M$, the map $G \longrightarrow M$ given by $g \longmapsto x^{-1}\,{}^gx$ is a 1-cocycle.*
* *For any 1-cocycle $\rho : G \longrightarrow M$ we necessarily have $\rho(1_G) = 1_M$ (this follows by (3.23)).*
* *For any G-group M, one can easily see that 'to be cohomologous' is an equivalence relation on the set of 1-cocycles of G in M.*
  The quotient set of this equivalence relation, called the first cohomology set of G with coefficients in M, is denoted by $H^1(G, M)$, i.e., $H^1(G, M) = \{$ equivalence classes of 1-cocycles $\rho : G \longrightarrow M\}$.

* $H^0(G,M)$ and $H^1(G,M)$ are covariant functors in M. If $\imath : M \longrightarrow M^{'}$ is a morphism of G-sets then the induced map will be denoted by $\imath_* : H^0(G,M) \longrightarrow H^0(G,M^{'})$, resp., $\imath_* : H^1(G,M) \longrightarrow H^1(G,M')$.

* If M is abelian then the definitions above coincide with the usual group cohomology as one of the possible descriptions for $H(G,M)$ is just the cohomology of the complex

$$0 \longrightarrow \mathcal{C}^0(G,M) \xrightarrow{\theta_0} \mathcal{C}^1(G,M) \xrightarrow{\theta_1} .... \longrightarrow \mathcal{C}^n(G,M) \xrightarrow{\theta_n} \mathcal{C}^{n+1}(G,M) \longrightarrow$$

where $\mathcal{C}^n(G,M) := \{f : G^n \longrightarrow M\}, \mathcal{C}^0(G,M) = M$, with the differential map θ_n defined by $\theta_n(f)(g_1,\dots,g_{n+1}) :=^{g_1} f(g_2,\dots,g_{n+1}) + \sum_{j=1}^{n}(-1)^j f(g_1,\dots,g_j g_{j+1},\dots,g_{n+1}) + (-1)^{n+1} f(g_1,\dots,g_n)$.

Theorem 3.6.1 *Let G be a finite group.*

i) If $N \subseteq M$ is G-group extension (i.e., M and N are G-groups and the action of $g \in G$ on an element $x \in N$ coincides with the action of g on x when x is considered as an element of M) and M/N is the set of left cosets, then there is a natural exact sequence of pointed sets

$$1 \longrightarrow H^0(G,N) \longrightarrow H^0(G,M) \longrightarrow H^0(G,M/N) \xrightarrow{d} H^1(G,N) \longrightarrow H^1(G,M)$$

ii) If in addition N is a normal subgroup of M, then there is a natural exact sequence of pointed sets

$$1 \longrightarrow H^0(G,N) \longrightarrow H^0(G,M) \longrightarrow H^0(G,M/N) \xrightarrow{d} H^1(G,N) \longrightarrow$$

$$H^1(G,M) \longrightarrow H^1(G,M/N)$$

iii)) If in particular N is a subgroup of the center of M, then there is a natural exact sequence of pointed set

$$1 \longrightarrow H^0(G,N) \longrightarrow H^0(G,M) \longrightarrow H^0(G,M/N) \xrightarrow{d} H^1(G,N) \longrightarrow \cdots$$

$$\cdots \longrightarrow H^1(G,M) \longrightarrow H^1(G,M/N) \xrightarrow{d^{'}} H^2(G,M)$$

Here the abelian group $H^2(G,M)$ is considered as a pointed set with the unit element.

We note that a sequence

$$(M,a) \xrightarrow{i} (N,b) \xrightarrow{j} (P,c)$$

of pointed sets is said to be exact in (N,b) if $i(M) = j^{-1}(P)$.

Proof. *See [14, Proposition 1.4, p.6].*

Definition 3.6.3 *Let $\psi : G \longrightarrow G^{'}$ be a homomorphism of finite groups. Then for an arbitrary G-set E one has a natural pull-back map $\psi^* : H^0(G^{'},E) \longrightarrow H^0(G,E)$.*
If E is a G-group then the pullback map is a group homomorphism.
For an arbitrary G-group M there is the natural pullback map $\psi^* : H^1(G^{'},M) \longrightarrow H^1(G,M)$ which is a morphism of pointed sets.

- ∗ *If ψ is the inclusion of a subgroup then the pullback* $res^G_{G'} := \psi^*$ *is usually called the restriction map.*
- ∗ *If ψ is the canonical projection on a quotient group then* $inf^G_{G'} := \psi^*$ *is said to be the inflation map.*
- ∗ *The composition of* $res^{G'}_G$ *or* $inf^{G'}_G$ *with some extension of the G-set E (the G-group M) is usually called the restriction, respectively inflation, as well.*

Remark 3.6.1 *Note that Non-abelian group cohomology can easily be extended to the case where G is a profinite group and M is a discrete G-set (respectively G-group) on which G operates continuously. Indeed, set for* $i = 0, 1$

$$H^i(G, M) := \varinjlim_{G'} H^i(G/G', M^{G'}).$$

where the direct limit is taken over the inflation maps and G' *runs through the normal open subgroups* G' *of G such that the quotient* G/G' *is finite.*

3.7 Some geometric interpetations of Galois descent

Let E/F be a finite Galois extension of fields with Galois group $G = Gal(E/F)$.
The descent problem deals with the following question : When can a scheme X over E be descended to F, that is, is there a scheme Y over F such that $X \simeq Y \times_{Spec(F)} Spec(E)$*? Grothendieck explored the analogy with the classical case, where a topological space or a differentiable manifold can be constructed by glueing together open subsets via transition functions which satisfy a compatibility condition on triple intersections. A "descent datum" is an analogue of this for schemes.*
Throughout F is a field, and E/F is usually a Galois field extension. We may assume E/F to be finite.

Definition 3.7.1 *Let E be a field and* $F \subseteq E$ *be a subfield such that E/F is a finite Galois extension. Let* $p_1 : X_1 \longrightarrow Spec(E)$ *and* $p_2 : X_2 \longrightarrow Spec(F)$ *be two E-schemes. Then, by a morphism from p_1 to p_2 that is twisted by* $\sigma \in Gal(E/F)$ *we will mean a morphism* $\phi : X_1 \longrightarrow X_2$ *of schemes such that the diagram*

$$\begin{array}{ccc} X_1 & \xrightarrow{\quad\phi\quad} & X_2 \\ \downarrow & & \downarrow \\ Spec(E) & \xrightarrow{\quad\sigma^\sharp\quad} & Spec(E) \end{array}$$

commutes. Here $\sigma^\sharp : Spec(E) \longrightarrow Spec(E)$ *denotes the morphism of affine schemes induced by*

$$\sigma^{-1} : E \longrightarrow E.$$

The next theorem gives some equivalences of categories.

Theorem 3.7.1 *Let E/F be a finite Galois extension of fields and* $G := Gal(E/F)$ *be its Galois group. Then :*

i) There are the following equivalences of categories

$$\begin{array}{ccc}
\{\text{ F-vector spaces }\} & \longrightarrow & \left\{\begin{array}{l} E-\text{ vector spaces with a} \\ G-\text{ operation from the left where each} \\ \sigma\in G \text{ operates } \sigma-\text{ linearly}\end{array}\right\} \\
\{\text{F-algebras }\} & \longrightarrow & \left\{\begin{array}{l} E-\text{ algebras} \\ \text{with a } G\text{-operation from the left} \\ \text{where each } \sigma\in G \text{ operates } \sigma-\text{ linearly}\end{array}\right\} \\
\{\text{ central simple algebras over F }\} & \longrightarrow & \left\{\begin{array}{l} E-\text{ algebras} \\ \text{with a } G\text{-operation from the left} \\ \text{where each } \sigma\in G \text{ operates } \sigma-\text{ linearly}\end{array}\right\} \\
\{\text{ commutative F-algebras }\} & \longrightarrow & \left\{\begin{array}{l} \text{commutative } E\text{-algebras} \\ \text{with a } G\text{-operation from the left} \\ \text{where each } \sigma\in G \text{ operates } \sigma-\text{ linearly}\end{array}\right\} \\
\{\text{ commutative F-algebras with unit }\} & \longrightarrow & \left\{\begin{array}{l} \text{commutative } E\text{-algebras with unit} \\ \text{with a } G\text{-operation from the left} \\ \text{where each } \sigma\in G \text{ operates } \sigma-\text{ linearly}\end{array}\right\} \\
A & \longmapsto & A\otimes_F E
\end{array}$$

ii) here is the following equivalence of categories,

$$\begin{array}{ccc}
\{\text{ quasi-projective F-schemes }\} & \longrightarrow & \left\{\begin{array}{l} \text{quasi-projective } E\text{-schemes} \\ \text{with a } G\text{-operation from the left} \\ \text{by morphisms of } F\text{-schemes} \\ \text{where each } \sigma\in G \text{ operates} \\ \text{by a morphism twisted by } \sigma \end{array}\right\} \\
X & \longmapsto & X\times_{Spec(F)} Spec(E)
\end{array}$$

iii) Let X be a F-scheme and r be a natural number. Then there are the following equivalences of categories

$$\begin{array}{ccc}
\{\text{ quasi-coherent sheaves on } X\ \} & \longrightarrow & \left\{\begin{array}{l} \text{quasi-coherent sheaves } \mathcal{M} \\ \text{on } X\times_{Spec(F)} Spec(E) \\ \text{together with a system } (\iota_\sigma)_{\sigma\in G} \\ \text{of isomorphisms } \iota_\sigma : x_\sigma^*\mathcal{M}\longrightarrow\mathcal{M} \text{ satisfying} \\ \iota_\tau\circ x_\tau^*(\iota_\sigma)=\iota_{\sigma\tau} \\ \text{for every } \sigma,\tau\in G \end{array}\right\} \\
\{\text{ locally free sheaves of rank } r \text{ on } X\ \} & \longrightarrow & \left\{\begin{array}{l} \text{locally free sheaves of rank } r \text{ on } X \\ \text{on } X\times_{Spec(F)} Spec(E) \\ \text{together with a system} (\iota_\sigma)_{\sigma\in G} \\ \text{of isomorphisms } \iota_\sigma : x_\sigma^*\mathcal{M}\longrightarrow\mathcal{M} \text{ satisfying} \\ \iota_\tau\circ x_\tau^*(\iota_\sigma)=\iota_{\sigma\tau} \\ \text{for every } \sigma,\tau\in G \end{array}\right\} \\
\mathcal{F} & \longmapsto & \mathcal{M}:=\pi^*\mathcal{F}
\end{array}$$

Here the morphisms in the categories are the obvious ones, i.e. those respecting all the extra structures $\pi : X\times_{Spec(F)} Spec(E)\longrightarrow X$ is the canonical morphism and $x_\sigma : X\times_{Spec(F)} Spec(E)\longrightarrow X\times_{Spec(F)} Spec(E)$ denotes the morphism that is induced by $\sigma^\sharp : Spec(E)\longrightarrow Spec(E)$.

Proof. *See [14, Theorem 2.2, p.7].*

Proposition 3.7.1 *(Galois descent-geometric version) Let E/F be a finite Galois extension of fields and $G := Gal(E/F)$ its Galois group Further, let Y be a quasi-projective E-scheme together with an operation of G from the left by twisted morphisms, i.e., such that the diagrams*

$$\begin{array}{ccc} Y & \xrightarrow{\phi_\sigma} & Y \\ \downarrow & & \downarrow \\ Spec(E) & \xrightarrow{\sigma^\sharp} & Spec(E) \end{array}$$

commute, where $\sigma^\sharp : Spec(E) \longrightarrow Spec(E)$. Then there exists a quasi-projective E-scheme X such that there is an isomorphism of E-schemes

$$X \times_{Spec(F)} Spec(E) \overset{f\sim}{\dashrightarrow} Y$$

where $X \times_{Spec(F)} Spec(E)$ is equipped with the G-operation induced by the one on Spec L and f is compatible with the operation of G.

Proof. *See [14, Proposition 2.5, p.**9**].*

Proposition 3.7.2 *(Galois descent for quasi-coherent sheaves) Let E/F be a finite Galois extension of fields and $G := Gal(E/F)$ be its Galois group. Further, let X be a F-scheme, $\pi : X \times_{Spec(F)} Spec(E) \longrightarrow X$ the canonical morphism and $x_\sigma : X \times_{Spec(F)} Spec(E) \longrightarrow X \times_{Spec(F)} Spec(E)$ be the morphism induced by $\sigma^\sharp : Spec(E) \longrightarrow Spec(E)$.*
Let $\mathcal{M}$ be a quasi-coherent sheaf over $X \times_{Spec(F)} Spec(E)$ together with a system $(\imath_\sigma)_{\sigma\in G}$ of isomorphism $\imath_\sigma : x_\sigma^*\mathcal{M} \longrightarrow \mathcal{M}$ that are compatible in the sense that for each $\sigma, \tau \in G$ there is the relation $\imath_\tau \circ x_\tau^*(\imath_\sigma) = \imath_{\sigma\tau}$.
Then there exists a quasi-coherent sheaf $\mathcal{F}$ over X such that there is an isomorphism

$$\pi^*\mathcal{F} \xrightarrow{b} \mathcal{M}$$

under which the canonical isomorphism $i_\sigma : x^*\pi^*\mathcal{F} = (\pi x_\sigma)^*\mathcal{F} : \pi^*\mathcal{F} = \pi^*\mathcal{F} \longrightarrow \pi^*\pi^*\mathcal{F}$ is identified with $\imath_\sigma$ fr each σ, i.e. the diagrams

$$\begin{array}{ccc} x_\sigma^*\pi^*\mathcal{F} & \xrightarrow{x_\sigma^*(b)} & x_\sigma^*\mathcal{M} \\ {\scriptstyle i_\sigma}\downarrow & & \downarrow{\scriptstyle \imath} \\ \pi^*\mathcal{F} & \xrightarrow{b} & \mathcal{M} \end{array}$$

commute.

Proof. *See [14, Proposition 2.6, p.**10**].*

Remark 3.7.1 *Note there is a Galois descent-algebraic version. We refer the reader to [14, Proposition 2.3, p.8].*

The next proposition gives the import result of Galois descent for homomorphisms.

Proposition 3.7.3 *Let E/F be a finite Galois extension of fields and $G := Gal(E/F)$ be its Galois group. Then it is equivalent.*

1) *to give a homomorphism $f : V \longrightarrow V'$ of F-vector spaces (of algebras over F, of central simple algebras over F, of commutative F-algebras, of commutative F-algebras with unit, $\cdots$).*

2) *to give a homomorphism* $f_E : V \times_F E \longrightarrow V^{'} \otimes_F E$ *of* E*-vector spaces (of algebras over* E*, of central simple algebras over* E*, of commutative* E*-algebras, of commutative* E*-algebras with unit,* $\cdots$*) which is compatible with the* G*-operations, i.e., such that for each* $\sigma \in G$ *the diagram*

$$\begin{array}{ccc} V \otimes_F E & \xrightarrow{f_E} & V^{'} \otimes_F E \\ \sigma \downarrow & & \downarrow \sigma \\ V \otimes_F E & \xrightarrow{f_E} & V^{'} \otimes_F E \end{array}$$

commutes.

Proof. *See [14, Proposition 2.7, p.**11**].*

Proposition 3.7.4 *(Galois descent for morphisms of schemes) Let* E/F *be a finite Galois extension of fields and* $G := Gal(E/F)$ *be its Galois group. Then it is equivalent.*

i) *to give a morphism of* F*-schemes* $\psi : X \longrightarrow X^{'}$.

ii) *to give a morphism of* E*-schemes* $\psi_E : X \times_{Spec(F)} Spec(E) \longrightarrow X^{'} \times_{Spec(F)} Spec(E)$ *which is compatible with the* G*-operations, i.e., such that for each* $\sigma \in G$ *the diagram*

$$\begin{array}{ccc} X \times_{Spec(F)} Spec(E) & \xrightarrow{\psi_E} & X^{'} \times_{Spec(F)} Spec(E) \\ \sigma \downarrow & & \downarrow \sigma \\ X \times_{Spec(F)} Spec(E) & \xrightarrow{\psi_E} & X^{'} \times_{Spec(F)} Spec(E) \end{array}$$

commutes.

Proof. *See [14, Proposition 2.8, p.**12**].*

Remark 3.7.2 *Note that there is a Galois descent for morphisms of quasi-coherent sheaves, we refer the reader to [14, Proposition 2.9, p.**12**].*

We conclude this section, by giving the following theorem.

Theorem 3.7.2 *(A.Grothendieck and J. Dieudonné) Let* E/F *be a finite field extension and* X *be a* F*-scheme such that* $X \times_{Spec(F)} Spec(E)$ *is*

i) *reduced.*

ii) *irreducible.*

iii) *compact.*

iv) *locally of finite type.*

v) *of finite type.*

vi) *locally Noetherian.*

vii) *Noetherian.*

viii) *proper.*

ix) *quasi-projective.*

x) *projective.*
or

xi) *regular.*

Then X admits the same property.

Proof. *See [14, Lemma 2.12, p.**14**].*

3.8 Central simple algebras and non-abelian cohomology

In this section, we will give the relation between Central simple algebras and non-abelian cohomology.

Lemma 3.8.1 *(Theorem of Skolem-Noether) Let R be a commutative ring with unit. Then $GL_n(R)$ operates on $M_n(R)$ by conjugation,*

$$(g, m) \longmapsto gmg^{-1}.$$

If $R = F$ is a field then this defines an isomorphism

$$PGL_n(F) := GL_n(F)/F^* \longrightarrow Aut_F\big(M_n(F)\big).$$

Proof. *See [14, Lemma 3.4, p.**34**].*

Definition 3.8.1 *Let n be a natural number.*

i) *If F is a field then we will denote by Az_n^F the set of all isomorphy classes of central simple algebras A of dimension n^2 over F.*

ii) *Let E/F be a field extension. Then $Az_n^{E/F}$ will denote the set of all isomorphy classes of central simple algebras A which are of dimension n^2 over F and split over E. Obviously, $Az_n^F := \bigcup_{E/F} Az_n^{E/F}$.*

Theorem 3.8.1 *Let E/F be a finite Galois extension of fields, $G := Gal(E/F)$ its Galois group and n be a natural number. Then there is a natural bijection of pointed sets.*

$$\begin{array}{rccc} a = a_n^{E/F} : & Az_n^{E/F} & \longrightarrow & H^1(G, PGL_n(E)) \\ & A & \longmapsto & a_A \end{array}$$

Proof. *See [14, Theorem 3.6, p.**20**].*

Proposition 3.8.1 *Let E/F be a finite Galois extension of fields and n be a natural number*

1) *Let K be a field extension of E such that K/F is Galois again. Then the following diagram of morphisms of pointed sets commutes,*

$$\begin{array}{ccc} Az_n^{E/F} & \xrightarrow{\quad a_n^{E/F} \quad} & H^1(Gal(E/F), PGL_n(E)) \\ \big\downarrow & & \big\downarrow {\scriptstyle inf_{Gal(E/F)}^{Gal(K/F)}} \\ Az_n^{K/F} & \xrightarrow{\quad a_n^{K/F} \quad} & H^1(Gal(K/F), PGL_n(K)) \end{array}$$

2) *Let K be an intermediate field of the extension E/F. Then the following diagram of morphisms of pointed sets commutes,*

$$\begin{array}{ccc} Az_n^{E/F} & \xrightarrow{a_n^{E/F}} & H^1(Gal(E/F), PGL_n(E)) \\ \downarrow & & \downarrow {\scriptstyle inf_{Gal(E/F)}^{Gal(E/K)}} \\ Az_n^{E/K} & \xrightarrow{a_n^{E/K}} & H^1(Gal(E/K), PGL_n(E)) \end{array}$$

Proof. *See [14, Lemma 3.7, p.21].*

Corollary 3.8.1 *Let F be a field and n be a natural number. Then there is a unique natural bijection*

$$a = a_n^F : Az_n^F \longrightarrow H^1\big(Gal(F^{sep}/F), PGL_n(F^{sep})\big).$$

such that $a^F_{n|Az_n^{E/F}} = a_n^{E/F}$

Proposition 3.8.2 *Let F be a field and m and n be natural numbers. Then the diagram*

$$\begin{array}{ccc} Az_n^F & \xrightarrow{a_n^F} & H^1(Gal(F^{sep}/F), PGL_n(F^{sep})) \\ {\scriptstyle A \mapsto M_m(A)} \downarrow & & \downarrow {\scriptstyle (i^n_{nm})_*} \\ Az_{nm}^F & \xrightarrow{a_{nm}^F} & H^1(Gal(F^{sep}/F), PGL_n(F^{sep})) \end{array}$$

commutes where $(i^n_{nm})_*$ *is the map induced by the block-diagonal embedding*

$$\begin{array}{cccc} i^n_{nm}: & PGL_n(F^{sep}) & \longrightarrow & PGL_{mn}(F^{sep}) \\ & \overline{E} & \longmapsto & \overline{\begin{pmatrix} E & 0 & \cdots & 0 \\ 0 & E & \cdots & 0 \\ \cdots & \cdots & \ddots & \cdots \\ 0 & 0 & \cdots & E \end{pmatrix}} \end{array}$$

Proof. *See [14, Proposition 3.9, p.22].*

Remark 3.8.1 *The proposition above shows*

$$Br(F) \simeq \varinjlim_n H^1(Gal(F^{sep}/F), PGL_n(F^{sep})).$$

3.9 Severi-Brauer varieties

In the final section of this chapter, we arrive at the objects we are most interested in studying; Severi-Brauer varieties. We focus here especially in the relation between these varieties and central simple algebras.

Definition 3.9.1 *Let F be a field. A scheme X over F is called a Brauer-Severi variety if there exists a finite, separable field extension E/F such that* X_E *is isomorphic to a projective space* $\mathbb{P}^n_E$.
A field extension E of F admitting the property that $X \times_F E \simeq \mathbb{P}^n_E$ *for some* $n \in \mathbb{N}$ *is said to be a splitting field for X. In this case one says X splits over E.*

Notation. $X_E := X \times_F E := X \times_{Spec(F)} Spec(E)$.

Remark 3.9.1 *Severi-Brauer varieties are twisted forms of projective space.*

We now come to the fundamental result about Severi–Brauer varieties.

Proposition 3.9.1 *Let X be a Brauer-Severi variety over a field F. Then*

1) *X is a variety, i.e. a reduced and irreducible scheme.*
2) *X is projective and regular.*
3) *X is geometrically integral.*
4) *One has $\Gamma(X, \mathcal{O}_X) = F$.*
5) *F is algebraically closed in the function field $F(X)$.*

Remark 3.9.2 *For 3) Recall that for X be a scheme over the field F. We say X is geometrically integral over F if the scheme X_E is integral for every field extension E of F.*

Proof. *See [14, Proposition 4.2, p.23].*

Theorem 3.9.1 *(Châtelet) Let X be a Severi–Brauer variety of dimension $n-1$ over the field F. The following are equivalent :*

i) *X is isomorphic to projective space $\mathbb{P}_F^{n-1}$ over F.*
ii) *X is birationally isomorphic to projective space $\mathbb{P}_F^{n-1}$ over F.*
iii) *X has a F-rational point.*
iv) *X contains a twisted-linear subvariety[||] Y of codimension 1.*

Proof. *See [10, Theorem 5.1.3, p.**115**].*

Passing to the next paragraph, we will gives the relation between Severi-Brauer varieties and non-abelian H^1.

Severi-Brauer varieties and non-abelian H^1

Proposition 3.9.2 *Let R be a commutative ring with unit.*

1) *Then $GL_n(R)$ operates on $\mathbb{P}_R^{n-1}$ by morphisms of R-schemes as follows : $A \in GL_n(R)$ gives rise to the morphism given by the graded automorphism*

$$\begin{array}{rccc} \Phi: & R[T_0, \cdots, T_{n-1}] & \longrightarrow & R[T_0, \ldots, T_{n-1}] \\ & f(T_0, \ldots, T_{n-1}) & \longmapsto & f((T_0, \ldots, T_{n-1}) \cdot A^t) \end{array}$$

of the coordinate ring.

2) *If $R = E$ is a field then this induces an isomorphism*

$$PGL_n(E) \xrightarrow{\simeq} Aut_{E-\text{ schemes}}(\mathbb{P}_E^{n-1})$$

[||] *We say that a closed subvariety $Y \longrightarrow X$ defined over F is a twisted-linear subvariety of X if Y is a Severi-Brauer variety and moreover over $\overline{F}$ the inclusion $Y_{\overline{F}} \subseteq X_{\overline{F}}$ becomes isomorphic to the inclusion of a linear subvariety $\mathbb{P}_{\overline{F}}^{n-1}$.*

Proof. *See [14, Lemma 4.3, p.24].*

Definition 3.9.2 *Let m be natural number.*

i) If F is a field then we will denote by BS_m^F the set of all isomorphy classes of Brauer-Severi varieties X of dimension m over F.

ii) Let E/F be a field extension. Then $BS_m^{E/F}$ will denote the set of all isomorphy classes of Severi-Brauer varieties X over F which are of dimension m and split over E. Obviously, $BS_m^F := \bigcup_{E/F} BS_m^{E/F}$.

Theorem 3.9.2 *Let E/F be a finite Galois extension, $G := Gal(E/F)$ its Galois group and m be a natural number. Then there exists a natural bijection of pointed sets*

$$\beta = \beta_{m-1}^{E/F} : \begin{array}{ccc} BS_{m-1}^{E/F} & \longrightarrow & H^1(G, PGL_m(E)) \\ X & \longmapsto & \beta_X \end{array}$$

Proof. *See [14, Theorem 4.5, p.25].*

Lemma 3.9.1 *Let E/F be a finite Galois extension of fields and m be a natural number.*

i) Let E' be a field extension of E such that E'/F is Galois again. Then the following diagram of morphisms of pointed sets commutes

$$\begin{array}{ccc} BS_{m-1}^{E/F} & \xrightarrow{\beta_{m-1}^{E/F}} & H^1(Gal(E/F), PGL_m(E)) \\ \downarrow & & \downarrow {\scriptstyle inf_{Gal(E/F)}^{Gal(E'/F)}} \\ BS_{m-1}^{E'/F} & \xrightarrow{\beta_{m-1}^{E'/F}} & H^1(Gal(E'/F), PGL_m(E')) \end{array}$$

ii) Let K be an intermediate field of the extension E/F. Then the following diagram of morphisms of pointed sets commutes

$$\begin{array}{ccc} BS_{m-1}^{E/F} & \xrightarrow{\beta_{m-1}^{E/F}} & H^1(Gal(E/F), PGL_m(E)) \\ {\scriptstyle \times_{Spec(F)} Spec(K)} \downarrow & & \downarrow {\scriptstyle inf_{Gal(E/F)}^{Gal(E'/F)}} \\ BS_{m-1}^{E/K} & \xrightarrow{\beta_{m-1}^{E/K}} & H^1(Gal(E/K), PGL_m(E)) \end{array}$$

Proof. *See [14, Lemma 4.6, p.26].*

Corollary 3.9.1 *Let F be a field and m be a natural number. Then there is a natural bijection*

$$\beta = \beta_{m-1}^{E/F} : \begin{array}{ccc} BS_{m-1}^{E/F} & \longrightarrow & H^1(Gal(F^{sep}/F), PGL_m(F^{sep})) \\ X & \longmapsto & \beta_X \end{array}$$

Proposition 3.9.3 *Let m be a natural number. If X is a Severi-Brauer variety of dimension m over a field F and $X(F) \neq \emptyset$ then, necessarily, $X \simeq \mathbb{P}_F^m$.*

Proof. *See [25, Exercises 1 (Châtelet), p. **168**].*

Proposition 3.9.4 *Let E/F be a finite Galois extension of fields, $G := Gal(E/F)$ its Galois group and $m \in \mathbb{N}$. Then $H^1(G, GL_m(E)) = 0$.*

Proof. *See [14, Lemma 4.10, p.**27**].*

Definition 3.9.3 *Let F be a field, m a natural number and X be a Brauer-Severi variety of dimension m. Then a linear subspace of X is a closed subvariety $Y \subseteq X$ such that $Y \times_{Spec(F)} Spec(F^{sep}) \subseteq X \times_{Spec(F)} Spec(F^{sep}) \simeq \mathbb{P}^m_{F^{sep}}$ is a linear subspace of the projective space. This property is independent of the isomorphism chosen.*

Theorem 3.9.3 *(F. Châtelet, M. Artin) Let F be a field, m and d be natural numbers, X be a Severi-Brauer variety of dimension m and Y a linear subspace of dimension d. Then the natural boundary maps send the cohomology classes $\beta^F_m(X) \in H^1(Gal(F^{sep}/F), PGL_{m+1}(F^{sep}))$ and $\beta^F_d(Y) \in H^1\big(Gal(F^{sep}/F), PGL_{d+1}(F^{sep})\big)$ to one the same class in the cohomological Brauer group $H^2\big(Gal(F^{sep}/F), (F^{sep}$*

Proof. *See [14, Proposition 4.13, p.**28**].*

The next paragraph gives the connection between Central simple algebras and Severi-Brauer varieties.

Central simple algebras and Severi-Brauer varieties

Theorem 3.9.4 *Let A a central simple algebra over F of dimension n^2*

i) Then there exists a Severi-Brauer variety X_A of dimension $n-1$ over F satisfying

(+) If E/F is a finite Galois extension being a splitting field for A then is a splitting field for X_A, too, and there is one and the same cohomology class

$$a_A = \beta_{X_A} \in H^1\big(Gal(E/F), PGl_n(E)\big).$$

associated with A and X_A.

(+) determines X_A uniquely up to isomorphism of F-schemes.

ii) The assignment $A \longrightarrow X_A$ admits the following properties.

a) It is compatible with extensions E/F of the base field, i.e

$$X_{A \otimes_F E} \simeq X_A \times_{Spec(F)} Spec(E).$$

b) E/F is a splitting field for A if and only if E/F is a splitting field for X_A.

Proposition 3.9.5 *1) Let F be a field and n a natural number. Then X induces a bijection*

$$X^F_n : Az^F_n \longrightarrow BS^F_{n-1}$$

2) Let E/F be a field extension. Then X induces a bijection

$$X^{E/F}_n : Az^{E/F}_n \longrightarrow BS^{E/F}_{n-1}$$

3) These mappings are compatible with extensions of the base field, i.e., the diagram

$$\begin{array}{ccc} Az_n^F & \xrightarrow{X_n^F} & BS_{n-1}^F \\ \downarrow{\scriptstyle \otimes_F E} & & \downarrow{\scriptstyle \times_{Spec(F)} Spec(E)} \\ Az_n^E & \xrightarrow{X_n^E} & BS_{n-1}^E \end{array}$$

commutes for every field extension E/F.

Proof. *See [14, Corollary 5.3, p.**30**].*

Proposition 3.9.6 *Let F be a field, n be a natural number and A a central simple algebra of dimension n^2 over F. Then there is an isomorphism*

$$x_A : Aut_F(A) \longrightarrow Aut_{F-schemes}(X_A).$$

Proof. *See [14, Proposition 5.5, p.**30**].*

Theorem 3.9.5 *Let F be a field, n and d be natural numbers, and A be a central simple algebra of dimension n^2 over F. Then the Severi-Brauer variety X_A associated with A admits a linear subspace of dimension d if and only if $d \leq n-1$ and $d \equiv -1[ind(A)]$.*

Proof. *See [14, Proposition 5.6, p.**31**].*

Bibliography

[1] *S.A. Amitsur, **Generic splitting fields of central simple algebras**, Ann. Math. 62, 43, 1955.*

[2] *M. Artin, **Brauer Severi varieties, in "Brauer Groups in Ring Theory and Algebraic Geometry"** F. van Oystaeyen and A. Verschoren, Eds, Lecture Notes in Math, Vol. 1917, pp. 194-210, Springer-Verlag, 1981.*

[3] *M. F. Atiyah, I. G.Macdonald, **Introduction to commutative algebra**, Addison-Wesley Series in Mathematics, 1969.*

[4] *G. Berhuy and F. Oggier, **An Introduction to Central Simple Algebras and Their Applications to Wireless Communication**, Mathematical Surveys and Monographs Volume 191, American Mathematical Society, 2010.*

[5] *N. Bourbaki, **Elements of mathematics- Algebra**, Springer-Verlag, 1973.*

[6] *A. Chambert-Loir, **Commutative Algebra**, https://webusers.imj-prg.fr/antoine.chambert-loir.*

[7] *F. Châtelet, **Variations sur un thème de H. Poincaré**, Ann. Sci. Ecole Norm. Sup. 61 . 1944 , 249 300.*

[8] *C. W. Curtis and I. Reiner, **Representation theory of finite groups and associative algebra**, A.M.S Chelsea Publishing, 1962.*

[9] *G. Ellingsrud and J. Christian Ottem, **Introduction to Schemes**, University of Oslo. October, 15, 2018.*

[10] *P. Gille and T. Szamuely, **Central Simple Algebras and Galois Cohomology**, Cambridge Studies In Advanced Mathematics 101, 2006.*

[11] *A. Grothendieck, J. Dieudonné, **Eléments de Géométrie Algébrique (EGA)**, Publ. Math. IHES, 4, 8, 11, 17, 20, 24, 28, 32, 1960–1967.*

[12] *R. Hartshorne. **Algebraic Geometry**. Springer-Verlag, G.T.M, 52, 1977.*

[13] *T. W. Hungerford, **Algebra**, G.T.M, Springer, 1974.*

[14] *J. Jahnel, **The Brauer-Severi Variety Associated with a Central Simple Algebra**, Version of September 25th, 2000.*

[15] *I. Kersten, **Brauergruppen, Universitätsverlag Göttingen**, 2007.*

[16] *A. W. Knapp, **Advanced Algebra Along with a companion volume Basic Algebra**, Birkhäuser Boston•Basel• Berlin, 2008.*

[17] *Q. Liu, **Algebraic Geometry and Arithmetic Curves** , Oxford Graduate Texts in Mathematics, 2002.*

[18] *J. Milne,* ***Class field theory, Course notes****,* *https://www.jmilne.org/math/.*

[19] *H. Niederreited and C. Xing* ***Algebraic Geometry in Coding Theory and Cryptography****, Princeton University Press, 2009.*

[20] *Z. Oscar and S. Pierre.* ***Commutative Algebra****, Vol, I, II, Springer, 1958-60.*

[21] *R. S. Pierce,* ***Associative Algebras****, Springer-Verlag, 1998.*

[22] *P. Ribenboim,* ***On the Riemann-Roch theorem****, Rendiconti del Circolo Mathematico di Palermo 10, 59-68 (1961), https://doi.org/10.1007/BF02844809.*

[23] *D. Sante and G. Silvio.* ***Normal varieties****, 1978.*

[24] *J.-P. Serre,* ***Cohomologie Galoisienne****, Springer, Lecture Notes in Mathematics 5, Quatrième Edition, Berlin 1973.*

[25] *J.-P. Serre,* ***Corps locaux****, Hermann, Paris, 1962.*

[26] *J. R. Smith,* ***Introduction to Algebraic Geometry****, Five Edition Press.*

[27] *I. Sophie Kriz,* ***Introduction to algebraic geometry****, Kindle Edition, 2021.*

[28] *M. Spivak,* ***A comprehensive Introduction to Differential Geometry****, Publish or Perish, Incorporated, 1975.*

[29] *H. Strichtenoth,* ***Algebraic Functions Fields and Codes****, Springer Berlin, Heidelberg, 2009.*

[30] *The Stacks Project Authors.* ***Stacks Project*** *http://stacks.math.columbia.edu.*