Noname manuscript No.
(will be inserted by the editor)

Classics Revisited: Éléments de Géométrie Algébrique

Ulrich Görtz

Received: date / Accepted: date

Abstract About 50 years ago, *Éléments de Géométrie Algébrique* (EGA) by A. Grothendieck and J. Dieudonné appeared, an encyclopedic work on the foundations of Grothendieck's algebraic geometry. We sketch some of the most important concepts developed there, comparing it to the classical language, and mention a few results in algebraic and arithmetic geometry which have since been proved using the new framework.

Keywords Éléments de Géométrie Algébrique · Algebraic Geometry · Schemes

Contents

U. Görtz
University of Duisburg-Essen, Fakultät für Mathematik, 45117 Essen, Germany
E-mail: ulrich.goertz@uni-due.de

1 Introduction

The work of A. Grothendieck has reshaped algebraic geometry. *Éléments de Géométrie Algébrique* (EGA) by A. Grothendieck and J. Dieudonné, which appeared about 50 years ago, is an opus which lays out the foundations of the new theory with all the technical details that are required, making it widely accessible. Its four chapters [EGA I], [EGA II], [EGA III], [EGA IV] have been published in 8 installments in Publications mathématiques de l'I.H.E.S., appearing between 1960 and 1967, comprising a total of around 1500 pages. Split up among the volumes, there is a Chapter 0 containing preliminary results from category theory, commutative algebra and homological algebra. Later, a new edition [EGA I_n] of the first chapter was published by Springer.

In this article, we will try to explain some of the context, and the content of EGA. More precisely, we start out with a few definitions and remarks about the classical theory, including some examples (Section 2). In Section 3, we define the notion of scheme which is the central notion of "geometric object" in EGA and in all of Grothendieck's algebraic geometry. We discuss the functorial point of view (Section 4), and in particular the notion of moduli spaces (Section 5). In the final sections, we briefly comment on volumes III and IV of EGA (Sections 6.1, 6.2), and discuss *very few* results building on the theory developed in EGA, before we conclude, in Section 8, with miscellaneous remarks. The choice of examples is definitively biased and reflects the personal taste of the author. We give references to EGA in many places; not so much because we would expect the reader to look them up, but rather to show "where we are" in our discussion, and also to illustrate what is covered in EGA, and what is not: While EGA is very easy to read in the sense that the proofs are spelled out in small steps and with detailed references to all previous results that are used, its style of writing at the same time makes it hard to look up a single result and its proof (because that might mean to follow up a long chain of backwards references), and to get a grasp of the big picture, since motivation and examples are scarce.

Although there are a few comments on historical developments in this note, I am aware that these are very much incomplete, and possibly also inaccurate. See Section 8 for pointers to the literature where this aspect is treated more competently.

Terminology. When we speak of a ring, in this note we always mean a commutative ring with 1.

The language of categories and functors is used below in several places. Recall that a category is given by a class of objects, together with "morphisms" between them. Each object has a distinguished identity morphism, and morphisms can be composed. A (covariant) functor $F\colon \mathscr{C} \to \mathscr{D}$ between categories attaches to each object X of $\mathscr{C}$ an object $F(X)$ of $\mathscr{D}$, and to each morphism $f\colon X' \to X$ a morphism $F(f)\colon F(X') \to F(X)$ between its images. This is required to be compatible with the identity morphisms and with composition.

Similarly, one has the notion of a contravariant functor, where the directions of arrows are reversed: For $f\colon X' \to X$ we obtain $F(f)\colon F(X) \to F(X')$. Basic examples are the category (Sets) of sets and the category (Rings) of rings. But the definition also allows for many other constructions, for example, given a topological space X, we obtain a category by taking as objects the open subsets of X, and as morphism set $\mathrm{Hom}(U,V)$ a one-point set if $U \subseteq V$, and the empty set otherwise (i.e., the morphisms are the inclusions between open subsets). Given functors $F,G\colon \mathscr{C} \to \mathscr{D}$ between the same categories, a *morphism $F \to G$ of functors* is given by morphisms $F(X) \to G(X)$ in $\mathscr{D}$, for all X in $\mathscr{C}$, such that for every morphism $X' \to X$ in $\mathscr{C}$, the obvious square is commutative. For more on categories see [34], [23] App. A. (We will neglect all set-theoretic issues in this article.)

Prerequisites. We assume that the reader is familiar with basic notions of (commutative) algebra: rings, ideals, prime ideals, maximal ideals, fields, finite fields. Some more commutative algebra (localization, tensor products, ...) is of course helpful, but hopefully not indispensable. Furthermore, some elementary topology is used. The notions of categories and functors are used in several places, but the definitions lined out in the previous paragraph should be enough to get by. Some knowledge of differentiable and/or complex manifolds is certainly useful, but the remarks pertaining to these subjects could otherwise be skipped without losing much.

For a shorter description of the notion of schemes and the use of categories and functors in algebraic geometry which requires less prerequisites and is much shorter, but less complete, see [42]. Se also the references given in Section 8.

2 Classical algebraic geometry

The topic of algebraic geometry is the geometric structure of solution sets of systems of polynomial equations.

In addition to being a fascinating topic in itself, it should be clear from this description that algebraic geometry has close connections to many other areas in mathematics, such as other variants of geometry (complex, differential, ...), number theory, etc.

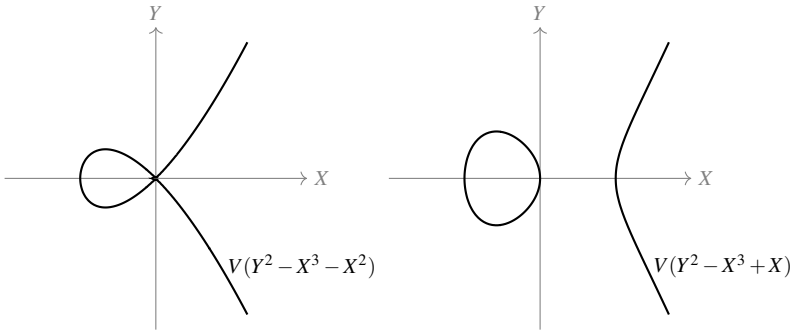
Also outside mathematics, polynomial equations appear in many places, and describing the structure of their zero sets has numerous applications — even if it is often not easy to apply the high-brow techniques of today's algebraic geometry machinery to specific questions arising from practical problems. As more or less random samples, we mention the papers by Penner [44] (molecule structure); Aholt, Sturmfels, Thomas [1], Lieblich, Van Meter [32] (computer vision); Carlini, Catalisano, Oneto [7] (algebraic statistics, ...).

Many textbooks on modern algebraic geometry choose to develop the classical theory first, before proceeding to Grothendieck's theory of schemes. See, e.g., [41] Ch. I, [25] Ch. 1, [23] Ch. 1.

2.1 Algebraic sets in affine space

Let k be an algebraically closed field, e.g., the field of complex numbers. Let $R = k[X_1,\dots,X_n]$ be a polynomial ring in n variables over k, and fix polynomials $f_1,\dots,f_m \in R$. We can then consider the common zero set

$$V(f_1,\dots,f_m) := \{(x_i)_i \in k^n;\ \forall j = 1,\dots,m : f_j(x_1,\dots,x_n) = 0\} \subseteq k^n$$



of the polynomials f_i. Subsets of k^n of the form $V(f_1,\dots,f_m)$ are called *algebraic subsets* of k^n, or *affine algebraic sets* or *affine algebraic varieties*.

Drawing examples is actually not so easy, since non-zero polynomials in one variable have only finitely many zeros, and starting with $\mathbb{C}^2$, it is difficult to draw a picture. To give some impression, we can draw the zero sets of polynomials in $\mathbb{R}^2$ as in the pictures. However, one has to be careful when drawing conclusions from these pictures. For example, both curves pictured here are connected for the Zariski topology which we will define later.

A *morphism* between $V(I)\subseteq k^n$ and $V(I')\subseteq k^{n'}$ is a map $V(I)\to V(I')$ which is given by polynomials, i.e., which is of the form $(x_1,\dots,x_n)\mapsto(g_1(x_\bullet),\dots,g_{n'}(x_\bullet))$ for polynomials $g_j\in k[X_1,\dots,X_n]$, $j=1,\dots,n'$. Note that every morphism extends to a morphism $k^n\to k^{n'}$, but there are in general many extensions, because changing the polynomials g_i by elements of I does not change the map $V(I)\to V(I')$. With the notion of morphism, we obtain a notion of isomorphism: a morphism which admits an inverse morphism.

2.2 Basic algebraic results

If in the above setting we denote by

$$I=\{\sum_{j=1}^{m} g_j f_j;\ g_j\in R\}\subset R$$

the ideal generated by the f_j, we have

$$V(f_1,\dots,f_m)=\{(x_i)_i\in k^n;\ \forall f\in I: f(x_1,\dots,x_n)=0\}=:V(I).$$

So passing to a different set of polynomials gives rise to the same common zero set, if the two families generate the same ideal. Furthermore, denoting by

$$\operatorname{rad} I:=\{f\in R;\exists n: f^n\in I\}$$

the radical of the ideal I, we obviously have $V(I)=V(\operatorname{rad} I)$. We call an ideal I a *radical ideal*, if $I=\operatorname{rad}(I)$.

Two results proved by D. Hilbert around 1890 further clarify the situation: By the Hilbert basis theorem, the ring R is noetherian, i.e., every ideal in R is finitely generated. This means that considering common zero sets of infinite families of polynomials does not give us a

more general notion. The more difficult result, Hilbert's Nullstellensatz, can be stated as saying that we obtain a bijection

$$\{\text{algebraic subsets of } V \subseteq k^n\} \longleftrightarrow \{\text{ideals } I \subseteq k[X_1,\dots,X_n] \text{ with } I = \operatorname{rad} I\}$$

by sending V to the ideal

$$I(V) := \{f \in R;\ \forall (x_i)_i \in V : f(x_1,\dots,x_n) = 0\}$$

of all polynomials vanishing on V and conversely, sending I to $V(I)$. Clearly, this bijection is inclusion-reversing.

As a consequence, the geometric objects $V(I)$ can actually be studied, by passing to the associated ideal, in purely algebraic terms. Hence geometric properties can be translated to algebraic properties. Moreover, expressing geometric properties for $k = \mathbb{C}$ in algebraic terms (e.g., using (formal) derivatives of polynomials), one can define "geometric properties" for general k by using the same algebraic description (and hoping for a reasonable outcome).

The Nullstellensatz implies that the maximal ideals of k^n are exactly the ideals which correspond to those non-empty algebraic sets which are minimal with respect to inclusion, i.e., to the points of k^n. Explicitly this says that every maximal ideal of R is of the form $(X_1 - x_1,\dots,X_n - x_n)$ for a point $(x_i)_i \in k^n$ (and clearly all those ideals are maximal). We see here that the assumption that k be algebraically closed is crucial at this point even if $n = 1$. This allows us to identify the set $V(I) \subseteq k^n$ with the set of those maximal ideals of R which contain I, or equivalently, with the set of maximal ideals of the ring R/I.

Every polynomial $f \in R$ gives rise to a map $k^n \to k$, $(x_i)_i \mapsto f(x_1,\dots,x_n)$, and restricting to an algebraic set $V(I)$, we can view f as a k-valued map on $V(I)$. We obtain a ring homomorphism $R \to \operatorname{Map}(k^n,k)$ which obviously factors through the canonical projection $R \to R/I$. If I is a radical ideal, then the resulting map $R/I \to \operatorname{Map}(k^n,k)$ is injective, and we then call R/I the *affine coordinate ring* of $V(I)$ — the ring of all polynomial functions on $V(I)$.

Using maps given by polynomials as morphisms between affine algebraic varieties, as above, we get an equivalence of categories

$$(\text{affine algebraic varieties}/k) \longleftrightarrow (\text{reduced fin. gen. } k\text{-algebras}), \tag{1}$$

where we call a k-algebra A *reduced*, if it has no nilpotent elements, and *finitely generated*, if there exists a surjective k-algebra homomorphism $k[X_1,\dots,X_n] \to A$ for some n. The equivalence is obtained by mapping $V(I) \subseteq k^n$ to $k[X_1,\dots,X_n]/I$, where I is assumed to be a radical ideal. To describe the inverse map, let A be a reduced finitely generated k-algebra. These properties imply (and are equivalent to) that there exists $n \geq 0$ and a surjective k-algebra homomorphism $k[X_1,\dots,X_n] \to A$ whose kernel, say I, is a radical ideal. We then map A to the affine algebraic variety $V(I) \subseteq k^n$.

We equip k^n with the *Zariski topology* which is defined by saying that the closed sets in k^n are the sets of the form $V(I)$. Similarly, we equip $V(J) \subseteq k^n$ with the induced topology. Even though this topology is very coarse, it has its uses. We denote k^n with the Zariski topology by $\mathbb{A}^n(k)$, "n-dimensional affine space over k".

We call a non-empty topological space X *irreducible*, if X cannot be written as the union of two proper closed subsets, or equivalently, if any two non-empty open subsets of X have non-empty intersection. This is a much stronger notion than X being connected, and is not interesting for Hausdorff topological spaces. But in algebraic geometry, irreducible spaces occur frequently. In fact, for I a radical ideal, the set $V(I)$ is irreducible if and only if I is a prime ideal. In particular, $\mathbb{A}^n(k) = V(0)$ is irreducible. The term *variety* is sometimes reserved for irreducible algebraic sets, but we chose to include all Zariski closed sets.

Example 2.1 Let us illustrate how the Zariski topology is useful (at least as a piece of terminology): The space $M_{n\times n}(k)$ of $(n\times n)$-matrices over k can be identified with $\mathbb{A}^{n^2}(k)$. The subset of diagonalisable matrices with n different eigenvalues is open (because its complement is the locus where the characteristic polynomial has multiple zeros, and this is equivalent to saying that the discriminant of the characteristic polynomial vanishes; since the discriminant of the characteristic polynomial is a polynomial in the entries of the matrix, this is in fact a Zariski-closed condition). Since it is clearly non-empty, and $M_{n\times n}(k)$ is irreducible, it is dense.

Therefore every property of matrices which is true for all (regular) diagonalisable matrices and such that the subset of matrices satisfying the property is a closed subset of $M_{n\times n}(k)$, is true for all $(n\times n)$-matrices. One example is the Theorem of Cayley-Hamilton saying that every matrix A is annihilated by its characteristic polynomial. This is trivial for diagonal matrices. Also, the subset of $M_{n\times n}(k)$ of all matrices which satisfy this property, is clearly Zariski-closed. Therefore the theorem holds for all square matrices.

Deeper evidence for the value of the Zariski topology is given by J.-P. Serre's results [49] about properties of cohomology of sheaves in this context. See also Section 6.1. As we will see, a slight variant of the Zariski topology is used in Grothendieck's language of schemes, as we will see in Section 3.

With the Zariski topology we also obtain a notion of dimension: We define the dimension of a topological space X as the supremum of the lengths ℓ of chains

$$\emptyset \neq Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_\ell \subseteq X$$

of irreducible closed subsets $Z_i \subseteq X$. With the correspondence between irreducible subsets and prime ideals, we see that the dimension of $V(I)$ is equal to the Krull dimension of the ring $k[X_1,\dots,X_n]/I$.

2.3 Projective space

In order to express (and study) certain properties of algebraic sets, it is sometimes more convenient to replace the affine space k^n by a different ambient space, namely the projective space

$$\mathbb{P}^n(k) := (k^{n+1}\setminus\{0\})/k^\times$$

where the group $k^\times$ of units of the field k acts by scalar multiplication on $k^{n+1}\setminus\{0\}$. In other words, we can view $\mathbb{P}^n(k)$ as the set of lines through the origin in k^{n+1}. To describe points of $\mathbb{P}^n(k)$ we use *homogeneous coordinates*, i.e., a point in $\mathbb{P}^n(k)$ is given as

$$[x_0 : \cdots : x_n], \quad (x_i)_i \in k^{n+1}\setminus\{0\},$$

where

$$[x_0 : \cdots : x_n] = [x_0' : \cdots : x_n'] \quad \Longleftrightarrow \quad \text{there exists } \lambda \in k^\times : \forall i : x_i' = \lambda x_i.$$

Since at least one of the homogeneous coordinates must not vanish, we see that $\mathbb{P}^n(k)$ is covered by the subsets

$$U_i := \{[x_0 : \cdots : x_n];\ x_i \neq 0\},$$

and we have bijections

$$U_i \to \mathbb{A}^n(k), \quad [x_0 : \cdots : x_n] \mapsto \left(\frac{x_0}{x_i}, \cdots, \frac{x_n}{x_i}\right),$$

where the term x_i/x_i is omitted.[1]

Using the covering $\mathbb{P}^n(k) = \bigcup U_i$, we can equip $\mathbb{P}^n(k)$ with the Zariski topology, i.e., the uniquely determined topology for which all U_i are open in $\mathbb{P}^n(k)$, and such that the subspace topology on each U_i is the Zariski topology on $\mathbb{A}^n(k)$ via the above bijection.

Because of the nature of homogeneous coordinates, if $f \in k[X_0, \ldots, X_n]$ is a polynomial and $[x_0 : \cdots : x_n]$ a point in projective space, there is no well-defined value $f(x_0, \ldots, x_n)$ (unless f is constant). But if f is homogeneous, i.e., all the monomials occurring inf f have the same degree, then it is independent of the choice of representative whether $f(x_0, \ldots, x_n)$ vanishes. Therefore we can define

$$V_+(f) := \{[x_0 : \cdots : x_n] \in \mathbb{P}^n(k);\ f(x_0, \ldots, x_n) = 0\}$$

for f a homogeneous polynomial. More generally, we have the *projective algebraic variety*

$$V_+(I) := \{[x_0 : \cdots : x_n] \in \mathbb{P}^n(k);\ f(x_0, \ldots, x_n) = 0 \text{ for all homogeneous } f \in I\}$$

for every ideal $I \subseteq k[X_0, \ldots, X_n]$ which is generated by homogeneous polynomials.

With the above notation for the standard charts $U_i \subset \mathbb{P}^n(k)$, and choosing $X_0, \ldots, X_{i-1}$, $X_{i+1}, \ldots, X_n$ as coordinates on U_i, we see that

$$V_+(f) \cap U_i = V(f(X_0, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n)).$$

Here is a simple, concrete example of a fact about algebraic sets which can be expressed in a cleaner fashion inside projective space than in affine space: Any two different lines in $\mathbb{P}^2(k)$, i.e., subsets of the form $V_+(f)$ with f a homogeneous polynomial of degree 1, intersect in a single point. This is easy to check: Viewing points of projective space as lines in k^3, a line is a 2-dimensional subspace, and any two different 2-dimensional subspaces in k^3 intersect in a line. Let us fix one of the standard charts, say U_0, and call $\mathbb{P}^2(k) \setminus U_0$, which we can naturally identify with $\mathbb{P}^1(k)$, the *line at infinity*. Then the concept of projective space gives a precise meaning to the statement that two different parallel lines in $\mathbb{A}^2(k) = U_0$ intersect in a point (of the line) at infinity.

A non-trivial generalization of this fact is Bézout's theorem which states that any two "curves", i.e., algebraic subsets $V_+(f), V_+(g) \subset \mathbb{P}^2(k)$ (assuming they intersect in only finitely many points) intersect in $\leq \deg(f)\deg(g)$ points, and if the intersection points are counted "with multiplicity", there are precisely $\deg(f)\deg(g)$ intersection points. The counting "with multiplicity" should be understood as the natural analog to the counting of zeros of a polynomial in one variable with multiplicity. Compare the statement that a polynomial in one variable of degree $n > 0$ has precisely n zeros, counting multiple zeros appropriately. Cf. Example 3.6.

Morphisms between projective algebraic varieties are by definition maps $V_+(I) \to V_+(I')$ which are Zariski-locally of the form $[x_0 : \cdots : x_n] \mapsto [f_0(x_\bullet) : \cdots : f_{n'}(x_\bullet)]$ for homogeneous polynomials $f_i \in k[X_0, \ldots, X_n]$, all of the same degree (and without a common zero on the open subset of $V_+(I)$ under consideration).

[1] Up to this point of this section, everything makes sense for an arbitrary field k, and we will occasionally use the notation $\mathbb{P}^n(k)$ in this more general setting below.

More generally, we can consider *quasi-projective* algebraic varieties, that is, open subsets of projective varieties (with an analogous notion of morphism). Then in particular every open subset of an affine variety is a quasi-projective variety (which is, however, not necessarily itself affine).

2.4 Smoothness

From this point, we can start the investigation of affine and projective algebraic varieties as geometric objects. Over the complex numbers (or over the real numbers, where it is easier to "draw pictures" as the ones above, but where we are leaving the setup with an algebraically closed base field), we certainly have some intuition about "geometric properties", namely those induced from the geometry of $\mathbb{C}^n$ and $\mathbb{R}^n$, or the complex/differentiable manifolds $\mathbb{P}^n(\mathbb{C})$, $\mathbb{P}^n(\mathbb{R})$.

Some of these properties can be readily translated into algebraic properties of the defining polynomials. We want to illustrate this with the property of smoothness, a key property of geometric objects which we will refer to several times below.

The intuition of a smooth point should be that the geometric set in question at this point "looks just like affine space" after "zooming in appropriately". In a similar fashion, we can express this by saying that the variety can be well approximated by an affine-linear space (which we would call the tangent space). In the examples drawn above, all points are smooth except for the origin inside $V(Y^2-X^3-X^2)$ where the two "branches" of that curve cross. This crossing point is called a *node* of the curve $V(Y^2-X^3-X^2)$.

Let us define when an algebraic variety V is smooth at a point $x \in V$. By analogy with the theorem of inverse functions in real/complex analysis, we say that V is smooth at x if and only if there exists an affine open neighborhood $U \subseteq V$ with $x \in U$ and an isomorphism between U and an open subvariety of $V(f_1,\dots,f_m)$ for polynomials $f_i \in k[X_1,\dots,X_n]$ mapping x to 0, say, such that the Jacobian matrix

$$\left(\frac{\partial f_i}{\partial X_j}\right)_{i=1,\dots m, j=1,\dots n}\Bigg|_{X_j=0} \in M_{m\times n}(k)$$

has rank m.

A projective algebraic variety $V_+(I)$ is called smooth at a point x if the intersection $V_+(I)\cap U_i$ is smooth at x for one (equivalently: every) chart U_i containing x. We call a (quasi-projective) algebraic variety *smooth*, if it is smooth at all of its points.

One can show that (for k algebraically closed and I a radical ideal), a point x in $V(I) \subseteq \mathbb{A}^n(k)$ is smooth if and only if the localization $(k[X_1,\dots,X_n]/I)_{\mathfrak{p}}$ of $k[X_1,\dots,X_n]/I$ at the prime ideal $\mathfrak{p}$ corresponding to x is a regular local ring.

Example 2.2 Let k be of characteristic 0, to avoid some small complications. Fix a non-zero homogeneous polynomial $f \in k[X_0,X_1,X_2,X_3]$ of degree 3. We call the variety $V_+(f) \subset \mathbb{P}^3(k)$ a cubic surface[2]. Assume moreover that $V_+(f)$ is smooth. It was observed classically, that $V_+(f)$ contains precisely 27 lines of $\mathbb{P}^3(k)$ (where a line in $\mathbb{P}^3(k)$ is a variety of the form $V_+(\ell_1,\ell_2)$ for linear homogeneous polynomials ℓ_1,ℓ_2 which are not multiples of each other). For a proof using the classical language, see van der Waerden's book [53]. Cf. Example 6.1 below.

[2] Strictly speaking, we should also ask that in the decomposition of f into irreducible polynomials, no factor occurs with power >1, because otherwise $V+(f)$ is equal to $V_+(g)$ for some g of smaller degree. The language of schemes will allow us to deal with this point more elegantly.

2.5 Elliptic curves

A very interesting class of examples is provided by cubic equations of the form[3]

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \qquad a,b \in k.$$

The polynomial $Y^2Z - X^3 + aXZ^2 + bZ^3$ then defines an algebraic variety E in $\mathbb{P}^2(k)$. If we pass to the chart $\{Z \neq 0\}$, we lose only the point with homogeneous coordinates $[0:1:0]$ which we will denote by O. Many properties of E can be studied in terms of the intersection $V_+(Y^2Z - X^3 + aXZ^2 + bZ^3) \cap \{Z \neq 0\}$, an affine curve in the affine plane, defined by the equation

$$Y^2 = X^3 + aX + b, \qquad a,b \in k.$$

We always make the assumption that E is smooth over k. It is not hard to check that this is equivalent to the condition that the polynomial $X^3 + aX + b$ has no multiple roots.

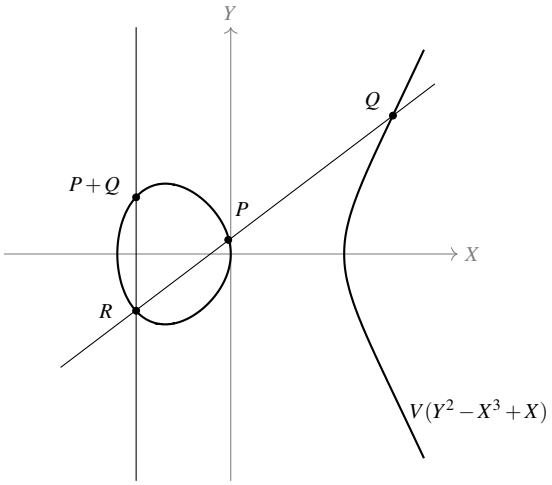
Quite surprisingly, at first, the set E can be equipped with the structure of an abelian group in a simple and very geometric way. This relies on a special case of the theorem of Bézout which we mentioned above: If f is a linear homogeneous polynomial, then E and $V_+(f)$ intersect in precisely 3 points (which have to be counted with multiplicity, cf. Example 3.6). More precisely, either the intersection consists of 3 points; or the intersection consists of 2 points, where the two "curves" intersect transversally in one of them, and touch in the other one; or the intersection consists of just one point, where the two curves touch "to the order 3".

Then the group law can be characterized by specifying that for any three points $P,Q,R \in E$, we have $P+Q+R = O$ if and only if there exists a line intersecting E in the three points P, Q, R (understood with multiplicities as described above). To describe the group law more explicitly, take points $P,Q \in E$. Let $V_+(f)$ be the line through P and Q (or the unique tangent line to E in P if $P = Q$). Let R denote the third point of intersection of E and $V_+(f)$. Now let $V_+(g)$ be the line connecting R and O, and let S be the third point of intersection of E with $V_+(g)$ (with analogous conventions in the case of multiple intersection points). The composition law on E is then defined by $P+Q := S$.

Most group axioms are visibly satisfied by this composition law (e.g., O is the neutral element, and the negative of a point is obtained by reflection with respect to the X-axis), with the exception of the associativity law. The associativity can be proved in several different ways, for instance using the Theorem of Cayley and Bacharach in projective geometry, or more advanced tools of algebraic geometry such as the Theorem of Riemann and Roch.

Over the complex numbers, there is also a different point of view, so assume that $k = \mathbb{C}$, and E is as above. Since polynomials are special cases of power series, and taking into account the smoothness condition which we imposed for elliptic curves, each of the open charts $E(\mathbb{C}) \cap U_i(\mathbb{C}) \subset U_i(\mathbb{C}) = \mathbb{C}^2$, and hence all of $E(\mathbb{C})$ carry the structure of a one-dimensional complex manifold, i.e., of a Riemann surface. Being closed in the projective plane, $E(\mathbb{C})$ equipped with the complex-analytic topology is compact. Using the group structure, it is not too hard to see that the universal covering of $E(\mathbb{C})$ is the complex plane $\mathbb{C}$, and arranging things so that $0 \in \mathbb{C}$ maps to the neutral element of $E(\mathbb{C})$, the covering map $\mathbb{C} \to E(\mathbb{C})$ is a group homomorphism. More precisely $E(\mathbb{C})$, as a Riemann surface, is isomorphic to a quotient $\mathbb{C}/\Lambda$, where $\Lambda \subset \mathbb{C}$ is a lattice, i.e., a subgroup of $\mathbb{C}$ generated by two $\mathbb{R}$-linearly independent complex numbers. Conversely, for every lattice $\Lambda \subset \mathbb{C}$, its

[3] If the characteristic of k is 2 or 3, then one must consider a slightly more general form of equation in order to obtain all elliptic curves over k. Cf. Def 5.3.



Weierstrass $\wp$-function gives rise to an embedding $\mathbb{C}/\Lambda \to \mathbb{P}^2(\mathbb{C})$ whose image is the zero set of a homogeneous cubic polynomial of the above form, defining an elliptic curve.

2.6 The search for new foundations of algebraic geometry

Algebraic geometry had been an important subject in mathematics for a long time and had been thriving with the results of the Italian School around 1900, with a highly developed geometric intuition, in particular concerning the theory of algebraic surfaces. In the first half of the 20th century, however, it became clear that a new foundation of the whole subject was desirable: For one thing, some proofs lacked sufficient rigor to make them understandable by the mathematical community. There also was the impact of the new methods developed in algebraic topology which were adopted for tackling algebro-geometric questions.

Furthermore, in particular with the Weil conjectures (see below), there came the search for a theory which encompassed non-algebraically closed base fields of arbitrary characteristic.

With B. L. van der Waerden, A. Weil and O. Zariski, to name only the most prominent ones, several mathematicians worked on new foundations for algebraic geometry. See e.g., the books [53] by van der Waerden and [56] by Weil and Zariski's report [59] at the ICM 1950.

A landmark were the Weil conjectures, stated by André Weil at the end of the 1950s. Generalizing a conjecture by E. Artin on algebraic curves (proved by Weil [56]) to algebraic varieties over finite fields of arbitrary dimension, these conjectures were one of the main driving forces for the further development of algebraic geometry, until their proof by P. Deligne in the 1970s. Scheme theory was absolutely indispensable for Deligne's proof, and in fact a significant part of the conjectures had already been proved before by Grothendieck's theory of étale cohomology.

According to the Weil conjectures, algebraic varieties over finite fields behave in some sense like topological varieties. In fact, Weil himself built the conjectures on the observation that they could be proved by constructing a suitable cohomology theory in this setting.

Unfortunately, the published part of EGA never reaches this point, which was an important motivation for building this theory. In the beginning, there was the plan to get there in Chapter XII or XIII of EGA. The chapters after Chapter IV never appeared though. Instead, the theory of étale cohomology was treated in Grothendieck's *Séminaire de Géométrie Algébrique* and the written notes of the seminar authored by Grothendieck and his students (again, several thousand pages).

2.7 The Weil Conjectures

Because of their significance in motivating the further development of algebraic geometry, we give a statement of the Weil conjectures. Let $\mathbb{F}_q$ be the finite field with q elements, and fix an algebraic closure $\mathbb{F}/\mathbb{F}_q$. Denote by $\mathbb{F}_{q^m}$ the unique extension field of $\mathbb{F}_q$ inside $\mathbb{F}$ of degree m. Let X be a smooth projective variety over $\mathbb{F}$ which is defined by polynomials with coefficients in $\mathbb{F}_q$. We denote by N_m the number of "points of X with values in $\mathbb{F}_{q^m}$". Say $X \subseteq \mathbb{P}^n(\mathbb{F})$, then the points in question are those points of X which lie in $\mathbb{P}^n(\mathbb{F}_{q^m})$, i.e., which can be written as $[x_0 : \cdots : x_n]$ with all $x_i \in \mathbb{F}_{q^m}$. Equivalently, they are the fix points in X of the q^m-Frobenius map $[x_0 : \cdots : x_n] \mapsto [x_0^{q^m} : \cdots : x_n^{q^m}]$ (which fixes X since X is defined by equations with coefficients in $\mathbb{F}_q$).

With this definition, we define the *zeta function* of X as

$$\zeta(X,s) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} q^{-ms}\right),$$

for $s \in \mathbb{C}$ with $\mathrm{Re}(s)$ sufficiently large so that the sum converges.

Example 2.3 For $X = \mathbb{P}^n_{\mathbb{F}_q}$, we get $N_m = q^{mn} + q^{m(n-1)} + \cdots + q^m + 1$. From this, it is easy to compute the zeta function of projective space:

$$\zeta(\mathbb{P}^n,s) = \frac{1}{(1-q^{-s})(1-q^{1-s})\cdots(1-q^{n-s})}.$$

It is useful to introduce a new variable T and to slightly rewrite the zeta function as follows:

$$Z(X,T) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} T^m\right), \tag{2}$$

an expression which we consider as a formal power series with coefficients in $\mathbb{Q}$. We then have $\zeta(X,s) = Z(X,q^{-s})$. With these definitions, we can state:

Theorem 2.4 *(Weil conjectures) Let X be a smooth, projective variety over $\mathbb{F}$ defined by equations over $\mathbb{F}_q$.*

1. ***Rationality:*** *The power series $Z(X,T)$ is a rational function of T. More precisely, there exist polynomials $P_0,\ldots,P_{2n} \in \mathbb{Z}[T]$, $n = \dim X$, such that*

$$Z(X,T) = \frac{P_1(T)\cdots P_{2n-1}(T)}{P_0(T)\cdots P_{2n}(T)}$$

and such that
   - *$P_0(T) = 1-T$, $P_{2n}(T) = 1-q^nT$,*
   - *for $0 < i < 2n$, $P_i(T) = \prod_j (1-\alpha_{ij}T)$ for certain $\alpha_{ij} \in \mathbb{C}$.*

2. ***Functional equation:*** *$Z(X,q^{-n}T^{-1}) = \pm q^{\frac{nE}{2}} T^E Z(X,T)$ where $E \in \mathbb{Z}$ is an integer depending on X, the so-called* Euler characteristic *of X (it is not hard to show that the expression nE is always even).*
3. ***Riemann hypothesis:*** *We have $|\alpha_{ij}| = q^{\frac{i}{2}}$ for all i, j.*

Weil suggested to prove the conjecture by constructing a cohomology theory satisfying certain natural conditions, and in particular allowing to apply a formula analogous to the Lefschetz fixed point formula to the Frobenius map.

The third part of the Weil conjectures is usually named the "Riemann hypothesis" because of the similarity to the statement of the usual Riemann hypothesis saying that the non-trivial zeros of the Riemann zeta function all have real part $\frac{1}{2}$. Note that the above statement about the absolute values of the α_{ij} is equivalent to saying that the values of s where $\zeta(X,s)$ has a zero or pole, have real part $\frac{i}{2}$ (where i is determined by which P_i the zero/pole comes from). We postpone the discussion in which sense the definition of the zeta function for X actually is analogous to the definition of the classical Riemann zeta function to Section 7.1, because it is slightly more convenient to do it in the modern language which we are going to get to know in the next sections.

For general algebraic curves, the statement had been conjectured by E. Artin, and has been proved by Weil. The rationality and the functional equation follow relatively easily from the Riemann-Roch theorem. The Riemann hypothesis is more subtle, even for curves (see e.g. Lorenzini's book [33] for a detailed account of an approach by S. A. Stepanov and E. Bombieri which is different from Weil's).

Example 2.5 For elliptic curves the conjectures were proved by H. Hasse in the 1930s; the Riemann hypothesis is equivalent to the famous *Hasse-Weil bound* on the number of points of an elliptic curve E over the finite field $\mathbb{F}_q$ (i.e., with coefficients a, b as above lying in $\mathbb{F}_q$):

$$|q+1-N_1| \leq 2\sqrt{q},$$

i.e., the difference between the number of "points on E with coefficients in $\mathbb{F}_q$", and the number of points on the projective line over $\mathbb{F}_q$, $q+1$, is bounded by $2\sqrt{q}$.

If we define $a_q := q+1-N_1$, then the zeta function for E is

$$Z(E,T) = \frac{1-a_qT+qT^2}{(1-T)(1-qT)}.$$

(But in contrast to the corresponding statement for $\mathbb{P}^1(k)$ or even $\mathbb{P}^n(k)$, this is not a trivial fact.)

In the general case, the Weil conjectures were later proved by Dwork, Grothendieck and Deligne; see Section 7.1 for a brief discussion.

3 The Language of Schemes

The theory of varieties outlined above has a number of shortcomings, for instance:

- Since $V(I) = V(\operatorname{rad} I)$, some information is lost when passing from an ideal to its algebraic set. This means, for instance, that we cannot distinguish different kinds of intersections (of curves in a plane, say, which could intersect transversally, or could be tangent to each other to some order) geometrically.

- The classical language is much worse adapted to the case that the base field k is not algebraically closed. Similarly, there is no natural way of describing the passage from a base field k to an extension field k'. (In Weil's theory, there are some methods to deal with this kind of problem, but Grothendieck's approach is much more elegant.)
- It is impossible to consider families in mixed characteristic, i.e., to take polynomial equations with integer coefficients and to relate the resulting algebraic sets over fields such as $\mathbb{C}$ and $\mathbb{F}_p$, in the classical framework.

How to go about a generalization? Recall that an affine algebraic variety V is determined by its affine coordinate ring, the ring of polynomial functions $V \to \mathbb{A}^1(k)$. This is a reduced algebra of finite type over the (algebraically closed) base field. Rather than starting with geometric objects, let us start out by contemplating which kinds of rings we would like to allow in the general theory. In other words: Which rings could conceivable arise as the "rings of functions" on some algebro-geometric object?

Grothendieck's solution is very simple and extremely powerful at the same time: Just allow any ring! While at first sight it may sound overly ambitious to attach a geometric object to an arbitrary ring, generalizing the construction for finite type algebras over an algebraically closed field outlined above, it turns out that this allows for solutions of the defects stated above and also makes much of the theory simpler and more powerful, at the same time.

3.1 Affine schemes

For R a reduced finitely generated algebra over an algebraically closed field we saw above how to attach to R a "geometric object" X such that R is the affine coordinate ring of X. Furthermore, R and X determine each other, and morphisms of finitely generated k-algebras correspond bijectively to morphisms of affine k-varieties.

Now let R be an arbitrary ring. How can we generalize the above procedure?

In the above situation, as a set the space attached to R could be found as the set of maximal ideals of R. It is however easy to see that this is not a good definition in general: For one thing, there are many rings of quite different nature with just one maximal ideal, and attaching a one-point space to all of them would not be ideal. A more substantial problem is that for a ring homomorphism $R \to R'$, the inverse image of a maximal ideal in R' is not in general a maximal ideal in R (even for very simple ring homomorphisms such as the inclusion $\mathbb{Z} \to \mathbb{Q}$). This means that there would be no obvious way to define a functor as we had done before.

For these reasons, it is better to work with the set of prime ideals in R, rather than with the set of maximal ideals, and we define

$$\operatorname{Spec} R := \{\mathfrak{p} \subset R;\ \mathfrak{p} \text{ is a prime ideal}\}.$$

the *(prime) spectrum of* R, [EGA I], (1.1.1). With this definition — even if a geometric interpretation is still lacking — we at least get something that still resembles the previous notion, and also is functorial in R: If $\varphi\colon R \to R'$ is a ring homomorphism, and $\mathfrak{p}' \subset R'$ is a prime ideal, then $\varphi^{-1}(\mathfrak{p}')$ is a prime ideal in R, so that we obtain from φ a map $\varphi^*\colon \operatorname{Spec} R' \to \operatorname{Spec} R$.

With this definition it is less obvious, how we could consider R as the ring of functions on $\operatorname{Spec} R$. It turns out, however, that the following approximation is good enough for our

purposes: For $f \in R$ and $\mathfrak{p} \in \operatorname{Spec} R$, we define the value $f(\mathfrak{p})$ of f at the point $\mathfrak{p}$ as the image of f under the natural map

$$R \to R/\mathfrak{p} \subseteq \operatorname{Frac}(R/\mathfrak{p}) =: \kappa(\mathfrak{p}).$$

The target $\kappa(\mathfrak{p})$, the field of fractions of $R/\mathfrak{p}$, of this map is called the *residue class field* of R at the prime ideal $\mathfrak{p}$, [EGA I] (1.1.1). So we get a "function" f on $\operatorname{Spec} R$ in the sense that we can evaluate f at every point. But the values lie in different fields! (If R is a finitely generated algebra over an algebraically closed field, and $\mathfrak{p} \subset R$ is a *maximal* ideal, then $f(\mathfrak{p}) \in \kappa(\mathfrak{p}) = k$ is the value of f in the sense of the language of varieties.)

The next step towards our goal of defining a *geometric* object is to define a topology on $\operatorname{Spec} R$. Clearly, the zero set of any function $f \in R$ should be closed, and correspondingly one calls sets of the form

$$V(I) := \{\mathfrak{p};\ I \subseteq \mathfrak{p}\}, \quad I \subseteq R \text{ an ideal},$$

closed. It is easy to check that this does define a topology, i.e., the empty set as well as $\operatorname{Spec} R$ are of this form, and this family is stable under arbitrary intersections and under finite unions. Note that the inclusion $I \subseteq \mathfrak{p}$ can be rewritten as

$$f(\mathfrak{p}) = 0 \text{ for all } f \in I,$$

so viewing elements of R as function, the set $V(I)$ really is the set of common zeroes of the functions in I. This topology is again called the Zariski topology, [EGA I] (1.1)[4]. It is easy to see that the above defined map $\varphi^*\colon \operatorname{Spec} R' \to \operatorname{Spec} R$ attached to a ring homomorphism φ is continuous, [EGA I] Cor. 1.2.3.

A basis of the topology is given by the *principal open subsets*

$$D(f) := \operatorname{Spec} R \setminus V(f) = \{\mathfrak{p} \in \operatorname{Spec} R;\ f \notin \mathfrak{p}\},$$

the non-vanishing loci of $f \in R$. From a geometric point of view, we would expect that the restriction of the function f to $D(f)$ becomes an *invertible* function; after all, f does not vanish anywhere on $D(f)$. On the algebraic side, there is a well-known method of "making elements invertible", namely we have the localization $R \to R_f$, a ring homomorphism which is universal for homomorphisms from R to rings where f becomes a unit. (If R is a domain and $f \neq 0$, then R_f is the subring of the field of fractions of R generated by R and f^{-1}. If R is arbitrary and f is nilpotent, then $R_f = 0$.) It follows from basic results of commutative algebra that the continuous map $\operatorname{Spec} R_f \to \operatorname{Spec} R$ attached to the localization homomorphism induces a homeomorphism between $\operatorname{Spec} R_f$ and $D(f)$, so the above intuition fits well with the algebraic picture.

Example 3.1 1. Spectrum of a field. If K is a field, then $\operatorname{Spec} K$ consists of a single point.
2. Let K be a field, $n \geq 2$. Then $\operatorname{Spec} K[X]/(X^n)$ again consists of a single point. See Section 3.2.1 for a discussion of spectra of non-reduced rings.
3. The spectrum $\operatorname{Spec} \mathbb{Z}$ of the ring of integers $\mathbb{Z}$ has one point for each prime number p (or rather the corresponding prime ideal (p)), and another point given by the zero ideal (0). The points (p) are closed, and the closure of (0) is all of $\operatorname{Spec} \mathbb{Z}$. See also Section 3.4.

[4] In [EGA I], the topology thus defined is called the *spectral topology* or *Zariski topology*. It appears that Zariski has only considered this topology on the sets of maximal ideals of (certain) rings. On the other hand, Jacobson [29] had defined this topology on the set of prime ideals several years earlier.

4. Let R be a discrete valuation ring (equivalently: a principal ideal domain which is not a field and has a unique maximal ideal $\mathfrak{m}$). Then (0) and $\mathfrak{m}$ are the only prime ideals of R, so $\operatorname{Spec} R$ has two points: the closed point $\mathfrak{m}$, and the "generic" point (0) whose closure is all of $\operatorname{Spec} R$.
5. For a ring R, we define $\mathbb{A}^n_R := \operatorname{Spec} R[X_1,\dots,X_n]$, "$n$-dimensional affine space over R". (Note however: While true for noetherian rings R, in general it is not true that $\dim \mathbb{A}^n_R = \dim R + n$. There exist many pretty strange rings ...)

Example 3.2 Let k be an algebraically closed field, and let A be a finitely generated k-algebra. The *closed* points in $\operatorname{Spec} A$ correspond to the maximal ideals of A. Therefore, if we choose an isomorphism $A \cong k[X_1,\dots,X_n]/I$, then we can identify the set of closed points with the set $V = V(I) \subseteq \mathbb{A}^n(k)$ in the sense of Section 2. If we equip the set of closed points in $\operatorname{Spec} A$ with the subset topology, then this identification is a homeomorphism. The non-maximal prime ideals in A correspond to additional points in $\operatorname{Spec} A$ which are not present in the "variety" V. We obtain a bijection

$$\operatorname{Spec} A \longleftrightarrow \{Z \subseteq V(I) \text{ closed irreducible}\}$$

given by $z \mapsto \overline{\{z\}} \cap V(I)$, where $\overline{\{z\}}$ denotes the closure of $\{z\}$ in $\operatorname{Spec} A$. In particular, for k-algebras of finite type, we can recover the topological space $\operatorname{Spec} A$ entirely from the classical picture. This remains true, if k is not assumed to be algebraically closed. Compare Section 3.2.2. Cf. [EGA IV] §10, [EGA $\mathrm{I_n}$] 6.4.

From now on we consider $\operatorname{Spec} R$ as a topological space, with the Zariski topology. However, this topology is quite coarse so although one could argue that a topological space is already a geometric object — certainly more so than just a set, we cannot yet really be satisfied. For example, at this point there is no way to characterize which continuous maps $\operatorname{Spec} R' \to \operatorname{Spec} R$ come from ring homomorphisms $R \to R'$.

It is not hard to show that for every ring R, the topological space $\operatorname{Spec} R$ is quasi-compact, i.e., every open cover admits a finite subcover: Without loss of generality, we can consider a cover of the form $\operatorname{Spec} R = \bigcup_{i\in I} D(f_i)$ for elements $f_i \in R$. But this is equivalent to the elements f_i, $i \in I$, generating the unit ideal in R. If that holds, then it obviously holds already for some finite subset of I. See [EGA I] Prop. 1.1.10.

The key point to nail down the geometric structure is to keep track in a useful way of the "functions" defined on $\operatorname{Spec} R$ *and its open subsets*. The collection of all this information is best encoded as a "sheaf" on $\operatorname{Spec} R$, so we will discuss the notion of sheaf before we come back to affine schemes.

3.2 Sheaves

It is a useful slogan that "A geometric theory is determined by the type of functions we use." In complex geometry, we use holomorphic functions, in differential geometry we use differentiable/smooth functions. The functions "determine" the theory, for instance: Two complex (or differentiable) manifolds are isomorphic if and only if they are homeomorphic and the sets of holomorphic (or differentiable) functions to $\mathbb{C}$, or $\mathbb{R}$, respectively, on each open subset are the same.

We want to generalize this approach to the setting of affine schemes. This generalization relies on the notion of sheaf which was first defined in the context of algebraic topology by J. Leray, and the notion of ringed space, defined by H. Cartan.

In the end, this will also provide us with an elegant definition of morphism between affine schemes, and with a way of "gluing" affine schemes (Example 3.10) in order to construct non-affine "schemes" such as projective space and the elliptic curves mentioned in the beginning. In fact, we should think of affine schemes as the local building blocks of the theory from which we construct more complicated objects, very much like gluing open subsets of $\mathbb{R}^n$ in order to construct arbitrary differentiable manifolds.

Thinking of a differentiable manifold X, say, the functions on an open $U \subseteq X$ we consider are differentiable maps $U \to \mathbb{R}$. In algebraic geometry, the situation is less clear: Although we think of elements of a ring R as functions on $\operatorname{Spec} R$, as we have discussed above, the target of the "map" f varies with the point in $\operatorname{Spec} R$: $f(\mathfrak{p}) \in \kappa(\mathfrak{p})$. Also, if R has non-zero nilpotent elements, then f is not determined by its values $f(\mathfrak{p})$. On the other hand, elements of the ring R share certain properties with functions: We can "restrict" f from $\operatorname{Spec} R$ to a principal open subset $D(s)$ by applying the localization map $R \to R_s$ (as far as evaluation at prime ideals is concerned, this really is the restriction). Furthermore it is not hard to show that we can "glue" elements of R, similarly as we can glue functions which are defined on subsets which cover the ambient space and which agree on all intersections. More precisely, one shows that whenever $\operatorname{Spec} R = \bigcup_{i\in I} D(s_i)$ (this condition is equivalent to asking that the s_i generate the unit ideal), and $f_i \in R_{s_i}$, $i \in I$, are such that the images of f_i and f_j in $R_{s_i s_j}$ coincide, there exists a unique element $f \in R$ which, for all i, maps to f_i under the localization map $R \to R_{s_i}$. As it turns out, these properties are enough to continue in the theory, and are subsumed in the following definition:

Definition 3.3 ([EGA I] Ch. 0, §3) Let X be a topological space.

1. A *presheaf* $\mathscr{F}$ on X is given by sets $\mathscr{F}(U)$ for each open $U \subseteq X$ together with maps ("restriction maps") $\operatorname{res}^U_V : \mathscr{F}(U) \to \mathscr{F}(V)$ whenever $V \subseteq U$ are open in X.
2. A presheaf $\mathscr{F}$ on X is called a *sheaf*, if for every open subset U of X and every cover $U = \bigcup_{i\in I} U_i$ of U by open subsets U_i, we have: For every family $f_i \in \mathscr{F}(U_i)$, $i \in I$, such that
$$\operatorname{res}^{U_i}_{U_i\cap U_j}(f_i) = \operatorname{res}^{U_j}_{U_i\cap U_j}(f_j) \quad \text{for all } i, j \in I,$$
there exists a unique element $f \in \mathscr{F}(U)$ such that $\operatorname{res}^U_{U_i}(f) = f_i$ for all i.
3. A *morphism* $\mathscr{F} \to \mathscr{G}$ of presheaves is given by maps $\mathscr{F}(U) \to \mathscr{G}(U)$ for each open $U \subseteq X$ which are compatible in the obvious way with the restriction maps for $V \subseteq U$ open in X. A morphism of sheaves is by definition a morphism of the underlying presheaves.

The elements of $\mathscr{F}(U)$ are called the *sections* of the (pre-)sheaf $\mathscr{F}$ on U.

Similarly to this definition of (pre-)sheaves of sets, one defines (pre-)sheaves of groups, abelian, groups, rings, etc., by requiring that all $\mathscr{F}(U)$ are groups, etc., that all restriction maps are homomorphisms of groups, etc., and for morphisms of (pre-)sheaves, that all maps $\mathscr{F}(U) \to \mathscr{G}(U)$ are homomorphisms of groups, etc. Using the language of categories, we can rephrase this by observing that a presheaf is a contravariant functor from the category with objects the open subsets of X, and morphisms the inclusions between them, to the category of sets. A morphism between presheaves is a morphism of functors. With this formulation, we can just replace the category of sets by the category of groups, abelian groups, rings, etc., in order to obtain presheaves of the desired type. For the categories mentioned here, the sheaf property can be checked on the underlying sets.

Note that the sheaf conditions never refer to an "evaluation" of an element of $\mathscr{F}(U)$, so even if our motivation was to encode the notion of "function on U", it can be used in abstract situations where no actual functions are around.

In addition to the "functions" defined on an open subset of the space X, it is often useful to be able to talk about the "germs of functions" at a point $x \in X$, i.e., all sections of $\mathscr{F}$ which are defined on some arbitrarily small open neighborhood, where we identify two such germs if they give the same function on some open neighborhood of x (possibly smaller than their domain of definition). This is formally expressed by taking the inductive limit

$$\mathscr{F}_x := \varinjlim_{x \in U} \mathscr{F}(U),$$

where the limit runs over all open neighborhoods of x, ordered by inclusion, with transition maps the restriction maps of the sheaf $\mathscr{F}$. The set (group, ...) $\mathscr{F}_x$ is called the *stalk* of $\mathscr{F}$ at the point x, [EGA I] Ch. 0, (3.1.6).

If $\mathscr{B}$ is a basis of open subsets of the topological space X, then the sheaf axiom formalizing the "gluing of functions" implies that a sheaf $\mathscr{F}$ on X is determined by its values $\mathscr{F}(U)$ for $U \in \mathscr{B}$ together with all restriction maps res_V^U for $V \subseteq U$, $U, V \in \mathscr{B}$. This also means that specifying this data for all $U, V \in \mathscr{B}$, there is at most one way to extend $\mathscr{F}$ to a sheaf on X. In view of this, we can formulate

Proposition 3.4 ([EGA I] 1.3) *Let R be a ring. There is a unique sheaf $\mathscr{O}_X$ of commutative rings on $X = \operatorname{Spec} R$ (with the Zariski topology) with*

$$\mathscr{O}_X(D(f)) = R_f, \quad f \in R,$$

and such that for $f, g \in R$ with $D(g) \subseteq D(f)$ the restriction map $\operatorname{res}_{D(g)}^{D(f)}$ is the natural map $R_f \to R_g$ between the localizations. It is called the structure sheaf of $\operatorname{Spec} R$.

Recall that $D(f)$ is homeomorphic to $\operatorname{Spec} R_f$, so the above is certainly a natural definition. (Although we can clearly have $D(f_1) = D(f_2)$ without f_1 being equal to f_2, it is easy to see that in this case there is a canonical isomorphism $R_{f_1} \cong R_{f_2}$ which we use to identify these two rings.) A key observation in checking the sheaf property is the following: We have $\operatorname{Spec} R = \bigcup D(f_i)$ if and only if the f_i generate the unit ideal in R. In this case, there exists a "partition of unity" $\sum_i g_i f_i = 1$ (with $g_i \in R$, only finitely many of them $\neq 0$).

The stalk of $\mathscr{O}_X$ at a point $\mathfrak{p}$ is the localization $R_\mathfrak{p}$ of the ring R with respect to the prime ideal $\mathfrak{p}$, i.e., where all elements of the multiplicative subset $R \setminus \mathfrak{p}$ are allowed as denominators. If R is a domain with field of fractions K, then $\mathscr{O}_{X,\mathfrak{p}} = R_\mathfrak{p}$ is the subring of K consisting of all elements which can be written as $\frac{f}{g}$ with $f, g \in R$, $g \notin \mathfrak{p}$ — these are exactly those elements which can be meaningfully "evaluated" at $\mathfrak{p}$, yielding a value in $\kappa(\mathfrak{p})$. The rings $R_\mathfrak{p}$ are local rings, i.e., they have a unique maximal ideal — the ideal generated by $\mathfrak{p}$.

With the notion of sheaf available, we can turn the slogan of "space with functions" into a precise definition. A ringed space is a pair consisting of a topological space X and a sheaf of rings on X. While this is already close to what we need, we add a slight twist to this definition, in the following sense. (It is necessary to consider only *locally* ringed spaces in order to ensure that Prop. 3.7 is true.)

For a continuous map $f\colon X \to Y$ between topological spaces and a sheaf $\mathscr{F}$ on X, we denote by $f_*\mathscr{F}$ the sheaf on Y given by

$$(f_*\mathscr{F})(V) := \mathscr{F}(f^{-1}(V)).$$

We call $f_*\mathscr{F}$ the *direct image sheaf* of $\mathscr{F}$ under f, [EGA I] Ch. 0, 3.4.

Definition 3.5 ([EGA I] Ch. 0, (5.5.1), [EGA I_n] Ch. 0, (4.1.9)), (4.1.12)) A *locally ringed space* is a pair $(X, \mathscr{O}_X)$ consisting of a topological space X and a sheaf of rings $\mathscr{O}_X$ on X such that for every $x \in X$, the stalk $\mathscr{O}_{X,x}$ is a local ring.

A morphism of locally ringed spaces is a pair consisting of a continuous map $f\colon X \to Y$ and a morphism of sheaves $f^\flat\colon \mathscr{O}_Y \to f_*\mathscr{O}_X$ such that for every $x \in X$ the homomorphism $\mathscr{O}_{Y,f(x)} \to \mathscr{O}_{X,x}$ of local rings induced by $f^\flat$ is a *local homomorphism*, i.e., maps the maximal ideal of the source ring into the maximal ideal of the target ring.

The maps between sheaves figuring in the definition of morphism of locally ringed spaces should be seen as "pull-back of functions" along f. In cases where the sections of the structure sheaves are actually given as functions on open subsets of X, and Y, it is typically just given by composition with f. Since by definition of a morphism the homomorphism $\mathscr{O}_{Y,f(x)} \to \mathscr{O}_{X,x}$ is local, it induces a homomorphism $\kappa(f(x)) \to \kappa(x)$ between the residue class fields of these local rings.

If $(X, \mathscr{O}_X)$ is a (locally) ringed space and $U \subseteq X$ is open, we define the sheaf $\mathscr{O}_{X|U}$ on U by $V \mapsto \mathscr{O}_X(V)$, the restriction or pull-back of $\mathscr{O}_X$ to U. We then obtain a (locally) ringed space $(U, \mathscr{O}_{X|U})$.

A ring R gives rise to a locally ringed space $\operatorname{Spec} R$ by the construction of the topological space $\operatorname{Spec} R$ and the structure sheaf on it. For a ring homomorphism $\varphi\colon R \to R'$, we have a continuous map $\operatorname{Spec} R' \to \operatorname{Spec} R$, $\mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q})$. The maps induced by φ on the localizations, $R_s \to R'_{\varphi(s)}$, define a homomorphism of sheaves, so that we obtain a morphism $\operatorname{Spec} R' \to \operatorname{Spec} R$ of locally ringed spaces. We thus obtain a contravariant functor from the category of rings to the category of locally ringed spaces.

The notion of (locally) ringed space is due to H. Cartan, see [16] VIIIb. The sheaf $\mathscr{O}_X$ is usually called the *structure sheaf* of the (locally) ringed space $(X, \mathscr{O}_X)$. Its stalks are called the *local rings* of $\mathscr{O}_X$ or of X. We usually denote a locally ringed space $(X, \mathscr{O}_X)$ just by X.

3.2.1 Non-reduced Rings

We have already seen the equivalence (1) between the categories of affine algebraic varieties over k — the prototypical examples of geometric objects that we want to understand — and reduced, finite type k-algebras, where k is an algebraically closed field. More generally, for any ring R, closed subsets in $\operatorname{Spec} R$ correspond to radical ideals in R.

Given any ideal $I \subset R$, we have ring homomorphisms $R \to R/I \to R/\operatorname{rad} I$ and correspondingly,

$$\operatorname{Spec}(R/\operatorname{rad} I) \to \operatorname{Spec}(R/I) \to \operatorname{Spec} R.$$

It is easy to see what happens on topological spaces here: The first of these maps is a homeomorphism, and the second one is a homeomorphism onto its image, the closed subset $V(I) \subset \operatorname{Spec} R$.

But whenever $I \neq \operatorname{rad} I$, the structure sheaves of $\operatorname{Spec}(R/\operatorname{rad}(I))$ and $\operatorname{Spec}(R/I)$ are different. Let us discuss what this difference "means" heuristically.

Taylor series. Let $R = k[X]$ be a polynomial ring in one variable over a field k. For every $n \geq 1$ the projection $\pi\colon k[X] \to k[X]/(X^n)$ gives rise to a morphism $\operatorname{Spec} k[X]/(X^n) \to \operatorname{Spec} k[X] = \mathbb{A}^1_k$ whose topological image is just the origin, i.e., the point corresponding to the prime ideal $(X) \subset R$ (which is the radical of the kernel (X^n) of π). For a polynomial $f \in k[X]$ its image $\pi(f) \in k[X]/(X^n)$ "is" the restriction of f to $\operatorname{Spec} k[X]/(X^n)$. This means that an element of $k[X]/(X^n)$, i.e., a function on $\operatorname{Spec} k[X]/(X^n)$, encodes not only the value of the function at the one point of this space, but all the first n coefficients of the Taylor expansion

of f. Heuristically, to recover these coefficients, the underlying space must be large enough to compute the $(n-1)$-th derivative of f, i.e., it should be viewed as containing a "small infinitesimal neighborhood in the X-direction". This infinitesimal neighborhood is invisible in the topological space and is only "encoded" in the structure sheaf.

Example 3.6 (Intersections) Another motivation for considering non-reduced rings is that they describe intersections of closed subsets more appropriately. This should be seen in analogy with the distinction between simple and multiple zeros of a polynomial. In fact, consider closed subsets $V(f)$ and $V(g)$ inside the affine plane $\mathbb{A}^2_k = \operatorname{Spec} k[X,Y]$. The intersection of two zero loci of polynomials naturally should be given as the locus where all those polynomials vanish simultaneously, i.e., in our example, by $V(f,g)$.

We illustrate this by a trivial example: Taking $f = Y$, $g = X - Y$, we get $V(Y, X-Y) = V(X,Y) = \{0\}$, the origin. Taking $f = Y$, $g = Y - X^2$ instead, we get $V(Y, Y-X^2) = V(X^2, Y)$. As a subset of k^2, the common vanishing locus of the polynomials Y and X^2 is again just the origin. The scheme-theoretic point of view, however, means that we should regard $V(Y,X^2)$ as the affine scheme $\operatorname{Spec} k[X,Y]/(X^2,Y) \cong \operatorname{Spec} k[X]/(X^2)$, the spectrum of the non-reduced ring $k[X]/(X^2)$. This reflects that the curves $V(Y)$ and $V(Y-X^2)$ do not intersect transversally at the origin, but that they are tangent to each other.

Consider a field k and non-constant polynomials $f, g \in k[X,Y]$. We view $V(f)$, $V(g) \subset \mathbb{A}^2_k = \operatorname{Spec} k[X,Y]$. The intersection $V(f) \cap V(g)$ as a scheme should be the common zero locus of f and g, i.e., $V(f,g) =: Z$ (cf. Example 4.5). For $z \in Z$ we define the intersection multiplicity of $V(f)$ and $V(g)$ at z as

$$i_z(f,g) := \dim_k \mathscr{O}_{Z,z}.$$

This is a non-negative integer, unless f and g have a common factor h with $z \in V(h)$, in which case it is infinity. This is the "correct" multiplicity to use in Bézout's Theorem (cf. Section 2) and similar statements. By passing to an affine chart, we can use the above to define the intersection multiplicity of curves $V_+(f), V_+(g) \subset \mathbb{P}^2_k$.

3.2.2 Generic Points

Another difference between the classical language of varieties and the language of (affine) schemes is that not only maximal ideals but all prime ideals of the coordinate ring give rise to points in the topological space, see Example 3.2 above. In a sense this is really an unavoidable consequence of the decision to admit arbitrary rings as coordinate rings, since in general the inverse image of a maximal ideal under a ring homomorphism is not a maximal ideal in the target.

While the additional points allow for the generalization to arbitrary rings, in the case of finitely generated algebras over a field (or, more generally, in rings where every prime ideal is equal to an intersection of maximal ideals, so-called *Jacobson rings*), one can show that the inclusion of the space of maximal ideals into the space of all prime ideals, both equipped with the Zariski topology, induces bijections (by taking the intersection with the set of maximal ideals) between the sets of open subsets on each side, and similarly between the sets of closed subsets on each side. On can then construct the larger space in a purely formal way by adding, to the smaller space, one point z for each closed irreducible subset Z, with the property that the closure of z in the new space is Z. So for Jacobson rings, the difference between the two approaches is not essential.

But as it turns out, often the additional points are actually helpful. In fact, many geometric properties will typically not be satisfied at all points, but (maybe) only "for a general

point", or "generically", i.e., for all points in a dense (open) subset. With our new points at hand, we can rephrase this as follows: Every irreducible closed subset Z of an (affine) scheme contains a unique point η_Z with closure $\overline{\{\eta_Z\}} = Z$. We call η_Z the *generic point* of Z. For many properties of points in an irreducible scheme (satisfying suitable finiteness conditions) one can show that they hold on a dense open subset as soon as they hold at the generic point. See also the discussion at the end of Section 4.3.

3.3 The notion of scheme

Above we have constructed, given a ring R with spectrum $X = \operatorname{Spec} R$, a locally ringed space $(X, \mathscr{O}_X)$. The following proposition shows that we can recover R from this locally ringed space (this is clear: $R = \mathscr{O}_X(X)$), and the morphisms $\operatorname{Spec} R' \to \operatorname{Spec} R$ between locally ringed spaces correspond one-to-one to ring homomorphisms $R \to R'$. This shows that passing from a ring to the corresponding locally ringed space does not lose any information, and also justifies why we should work with *locally* ringed spaces rather than all ringed spaces.

Proposition 3.7 ([EGA I] Thm. 1.7.3) *The functor from the category of rings to the category of locally ringed spaces which attaches to a ring R the locally ringed space $(\operatorname{Spec} R, \mathscr{O}_{\operatorname{Spec} R})$ (where we consider $\operatorname{Spec} R$ as a topological space with the Zariski topology, and define the structure sheaf $\mathscr{O}_{\operatorname{Spec} R}$ as above) is fully faithful, i.e., for any two rings R, R', the natural map*

$$\operatorname{Hom}_{\mathrm{Ring}}(R, R') \to \operatorname{Hom}_{\text{loc. rgd sp.}}((\operatorname{Spec} R', \mathscr{O}_{\operatorname{Spec} R'}), (\operatorname{Spec} R, \mathscr{O}_{\operatorname{Spec} R}))$$

is bijective.

With this proposition, we define

Definition 3.8 ([EGA I] Déf. 1.7.1) An *affine scheme* is a locally ringed space $(X, \mathscr{O}_X)$ which is isomorphic to a locally ringed space of the form $(\operatorname{Spec} R, \mathscr{O}_{\operatorname{Spec} R})$ for some ring R. A morphism of affine schemes is a morphism of locally ringed spaces.

Finally we can now define the notion of *scheme*:

Definition 3.9 ([EGA I] Déf. 2.1.2, Déf. 2.2.1) A *scheme*[5,6] is a locally ringed space $(X, \mathscr{O}_X)$ such that there exists an open covering $X = \bigcup_i U_i$ with the property that for every i, the locally ringed space $(U_i, \mathscr{O}_{X|U_i})$ is an affine scheme.

A morphism of schemes is a morphism of locally ringed spaces.

By definition, locally, every scheme is isomorphic to an affine scheme. If $U \subseteq X$ and U (more precisely: $(U, \mathscr{O}_{X|U})$) is an affine scheme, then we must have $U \cong \operatorname{Spec} \mathscr{O}_X(U)$. Since an affine scheme "is" just a ring (i.e., determined by the corresponding ring), properties of rings give rise to "local properties" of schemes. For example, we call a scheme X reduced ([EGA I] Ch. 0, Déf. 4.1.4), if for every affine open subscheme $U \subseteq X$, the ring $\mathscr{O}_X(U)$ is

[5] The term *scheme* was used earlier by Chevalley [9] in a more restrictive sense. See also [EGA I] 8.3.

[6] What we call a *scheme* here was called a *prescheme* in EGA I–IV. A *scheme* was by definition a *separated prescheme*. In the new edition [EGA I_n] of EGA I, the terminology was changed, and the definition given here is the one which is universally used nowadays.

reduced, i.e., has no non-trivial nilpotent elements. It is equivalent to require that all local rings $\mathscr{O}_{X,x}$ are reduced rings.

Other properties are determined by the underlying topological space of a scheme X alone. For instance, we call a scheme X *irreducible*, or *connected*, if the underlying topological space is irreducible, or connected, respectively ([EGA I] (2.1.8)). Often, these topological properties can also be expressed in terms of the structure sheaf or the affine coordinate ring. For example, an affine scheme X is reduced and irreducible if and only if the ring A is a domain.

Subschemes. ([EGA I] 4.1, 4.2) If X is a scheme, and $U \subseteq X$ is an open subset, we can restrict the structure sheaf of X to the open subset U and obtain a locally ringed space $(U, \mathscr{O}_{X|U})$, which is again a scheme. Schemes of this form are called *open subschemes* of X. A morphism $U \to X$ which identifies U with an open subscheme of X (i.e., on topological spaces, the map is a homeomorphism onto an open subset, and the structure sheaf of U is identified with the restriction of the structure sheaf of X) is called an *open immersion*. If $X = \operatorname{Spec} R$ is an affine scheme, and $I \subseteq A$ is an ideal, then the canonical projection $R \to R/I$ yields a morphism $\operatorname{Spec} R/I \to \operatorname{Spec} R$ which identifies $\operatorname{Spec} R/I$ with the closed subset $V(I)$ of $\operatorname{Spec} R$. We call the set $V(I)$ with the sheaf given by $\operatorname{Spec} R/I$ a closed subscheme of $\operatorname{Spec} R$ and denote it by $V(I)$ again. As a consequence, with this new definition of the notation $V(-)$, ideals $I, J \subseteq R$ define the same closed subscheme $V(I) = V(J)$ if and only if $I = J$; it is not enough that their radicals coincide. Globalizing this construction, one defines the notion of closed subscheme $Z \subseteq X$ in a general scheme Z. Correspondingly, one obtains the notion of *closed immersion* for scheme morphisms. Combining the two notions, we say that a subscheme of X is a closed subscheme of some open subscheme of X. Note that, unlike in the situation for open subschemes, a closed subscheme is not determined by the underlying closed subset alone, as can already be seen in the affine case: Different ideals with the same radical ideal give rise to different closed subschemes with the same underlying topological space. On the other hand, for every closed subset of a scheme X, there exists a unique *reduced* closed subscheme whose underlying topological space is the given subset.

Example 3.10 (Gluing) ([EGA I] 2.3) Given a family of schemes, we can "glue" them by specifying how they should intersect (if you are unfamiliar with the concept, you should read the remainder of this example with "scheme" replaced by "set" or "topological space" first; the result is easy to prove, and the proof for schemes is basically the same as for topological spaces). Let $(U_i)_{i \in I}$ be a family of schemes; for each i, let $U_{ij} \subseteq U_i$ be open subschemes, $j \in I$; and for each pair i, j let $\varphi_{ji} \colon U_{ij} \to U_{ji}$ be an isomorphism of schemes, such that

$$U_{ii} = U_i \text{ for all } i \in I,$$

and the following "cocycle condition" is satisfied: $\varphi_{ji}(U_{ij} \cap U_{ik}) \subseteq U_{jk}$ and

$$\varphi_{kj} \circ \varphi_{ji} = \varphi_{ki} \text{ on } U_{ij} \cap U_{ik}$$

for all $i, j, k \in I$.

Then there exists a scheme X together with open immersions $\iota_i \colon U_i \to X$ such that $\iota_i(U_{ij}) \cong \iota_i(U_i) \cap \iota_j(U_j)$ for all i, j, $X = \bigcup_i \iota_i(U_i)$ and $\iota_j \circ \varphi_{ji} = \iota_i$ on U_{ij}. Furthermore, X together with the maps ι_i is unique up to unique isomorphism.

Example 3.11 1. As noted above, every ring gives rise, by passing to the spectrum, to an (affine) scheme, so we can consider all the examples in Example 3.1 as schemes.

2. Let R be a ring and $n \geq 0$. By gluing $n+1$ copies of $\mathbb{A}^n_R$, we can construct *projective space* $\mathbb{P}^n_R$ over R. Similarly as before, for homogeneous polynomials $f_i \in R[X_0, \ldots, X_n]$, we obtain closed subschemes $V_+((f_i)_i) \subseteq \mathbb{P}^n_R$. See [EGA II] 4.1.1, [EGA $\mathrm{I_n}$] 9.7.
3. An approach allowing for gluing as above can also be carried out in classical algebraic geometry (cf. [41] Ch. I or [23] Ch. 1). Hironaka was the first to give an example which showed that by gluing one can produce varieties (even over $\mathbb{C}$) which are not quasi-projective. With the language introduced above: By gluing affine schemes of the form $\operatorname{Spec} A$, where A is a reduced finitely generated $\mathbb{C}$-algebra, one can construct schemes which are not isomorphic to a subscheme in any $\mathbb{P}^n_{\mathbb{C}}$.
4. In Sections 3.4 and 7.3, we will very briefly touch on schemes with significance in number theory.

Example 3.12 (Morphisms of schemes)

1. *Morphisms from the spectrum of a field:* Let K be a field, and let X be a scheme. Every morphism $\operatorname{Spec} K \to X$ has a unique point $x \in X$ as its topological image, and induced an embedding $\kappa(x) \to K$ between the two residue class fields. Conversely, an embedding from $\kappa(x)$ into a field K induces a morphism $\operatorname{Spec} K \to X$, and these two constructions are inverse to each other.
2. *Morphisms to affine schemes:* For every scheme X and affine scheme $\operatorname{Spec} R$, the natural map
$$\operatorname{Hom}(X, \operatorname{Spec} R) \to \operatorname{Hom}(R, \mathscr{O}_X(X))$$
sending $(f, f^\flat)$ to $f^\flat(\operatorname{Spec} R)\colon R = \mathscr{O}_{\operatorname{Spec} R}(\operatorname{Spec} R) \to f_* \mathscr{O}_X(\operatorname{Spec} R) = \mathscr{O}_X(X)$, is a bijection.

Remark 3.13 One can use the concept of locally ringed space not only in algebraic geometry, but for other variants of geometry as well: A differentiable manifold X gives rise to a locally ringed space if we define $\mathscr{O}_X(U)$ as the ring of differentiable functions $U \to \mathbb{R}$, for $U \subseteq X$ open. In fact, $\mathscr{O}_X(U)$ is even an $\mathbb{R}$-algebra, and the restriction maps are $\mathbb{R}$-algebra homomorphisms, i.e., we obtain an $\mathbb{R}$-locally ringed space. Similarly, a complex manifold gives rise to a $\mathbb{C}$-locally ringed space if we define $\mathscr{O}_X(U)$ as the ring of holomorphic functions $U \to \mathbb{C}$, for $U \subseteq X$ open. In this way, we obtain fully faithful functors from the category of differentiable manifolds, and complex manifolds, respectively, to the category of $\mathbb{R}$-locally ringed spaces, and $\mathbb{C}$-locally ringed spaces, respectively. See Wedhorn's book [55] for an approach to differential geometry based on this method. (One reason why the advantage of using locally ringed spaces is much bigger in algebraic geometry, than in differential geometry, is that in the latter case, the condition that the homomorphisms on local rings induced by a morphism of manifolds are local, is automatic; see loc. cit. Example 4.5 for details. Also, the questions that are asked in algebraic vs. differential geometry are often of a different nature. While sheaves are well-adapted to questions of passage from local to global, in differential geometry often the local problems, described by (partial) differential equations, are hard and are the main focus.)

3.4 The arithmetic situation

One compelling feature of the notion of scheme which has no analog in the world of varieties over a field is the possibility to consider schemes whose points have residue class fields of different characteristic. For this very reason, much of today's research in algebraic number

theory heavily uses methods of algebraic geometry. Bringing geometric intuition to number theoretic questions (even if there are some caveats!) has proved to be immensely fruitful.

The prototype of this situation is, of course, the spectrum of the ring $\mathbb{Z}$ of integers. The prime ideals in $\mathbb{Z}$ are the zero ideal (0), and the ideals (p) where p is a prime number. The latter ones are the maximal ideals of $\mathbb{Z}$ and hence correspond to the closed points of $\operatorname{Spec}\mathbb{Z}$. The zero ideal, on the other hand, is not maximal, and is contained in all the prime ideals. Its closure, therefore, is all of $\operatorname{Spec}\mathbb{Z}$, whence we call it the generic point of $\operatorname{Spec}\mathbb{Z}$. The residue class field of a prime ideal (p) is the finite field $\mathbb{F}_p = \mathbb{Z}/(p)$ with p elements. The residue class field of (0) is the field $\mathbb{Q} = \operatorname{Frac}(\mathbb{Z})$ of rational numbers. From the inclusion relations, we see that the Krull dimension of $\mathbb{Z}$, and hence the scheme dimension of $\operatorname{Spec}\mathbb{Z}$, is equal to 1. This means that geometrically we should think of $\operatorname{Spec}\mathbb{Z}$ as a curve.

Now let $K/\mathbb{Q}$ be a finite field extension (K is called a number field). Generally speaking, the study of such extensions is one of the most important topics of algebraic number theory. Denote by $\mathscr{O}_K$ the ring of integers of K, i.e., the subring of all elements $x \in K$ whose minimal polynomial over $\mathbb{Q}$ has integral coefficients. Then $\mathscr{O}_K$ again has Krull dimension 1, and all localizations $\mathscr{O}_{K,\mathfrak{p}}$ at maximal ideals $\mathfrak{p}$ are discrete valuation rings.

Thus $\operatorname{Spec}\mathscr{O}_K$ should again be viewed as a curve, and the ring homomorphism $\mathbb{Z} \to \mathscr{O}_K$ gives rise to a "covering map of curves" $\operatorname{Spec}\mathscr{O}_K \to \operatorname{Spec}\mathbb{Z}$. This gives a very natural interpretation to the notions of ramified, unramified, split, inert prime ideal, etc.

Of course, the terminology used in number theory (ramified, unramified, ...) was introduced long before EGA, by L. Kronecker and D. Hilbert who wanted to emphasize the similarity between number fields and function fields of Riemann surfaces where these notions have a direct interpretation in geometric terms. But with Grothendieck's algebraic geometry, the analogy received a more solid and extendable foundation.

We will come back to the usefulness of considering families over $\operatorname{Spec}\mathbb{Z}$ or, more generally, over schemes with residue classes of different characteristics in Sections 7.2 and 7.3 below.

4 The categorical point of view

4.1 Morphisms

At this point, let us introduce the terminology of "relative scheme": Let S be a scheme. An S-scheme is a morphism $f\colon X \to S$ of schemes. Usually we drop f from the notation, and just say that X is an S-scheme, understanding the "structure morphism" from X to S as given. A morphism between S-schemes X, Y is a scheme morphism $X \to Y$ such that the triangle given by this morphism and the structure morphisms $X \to S$, $Y \to S$ commutes. In this way we obtain the category of S-schemes. If $S = \operatorname{Spec}R$ is affine, we also speak of R-schemes. A particularly important case is of course the case $S = \operatorname{Spec}k$, where k is a field. If $S = \operatorname{Spec}R$ is an affine scheme, then we usually talk about R-schemes rather than S-schemes. This construction should be compared with the notion of (commutative) algebra A over a ring R, which is the same thing as a ring homomorphism $R \to A$.

The emphasis on relative schemes, or equivalently on morphisms of schemes, is a crucial paradigm in EGA and in Grothendieck's view on algebraic geometry. By Example 3.12, every scheme is equipped with a unique morphism to $\operatorname{Spec}\mathbb{Z}$. Similarly, the spectrum of an algebra A over a field k admits a morphism $\operatorname{Spec}A \to \operatorname{Spec}k$, and if X is constructed by gluing pieces of this form along identifications compatible with the k-algebra structure, we

obtain a morphism $X \to \operatorname{Spec} k$, again. So in these situations, it is easy to replace schemes by relative schemes over a suitable "base scheme".

While nothing is lost by replacing schemes by relative schemes, there is a gain: Given an S-scheme X, i.e., a morphism $f\colon X \to S$, for every point $s \in S$ we can consider the fiber $f^{-1}(s)$ which we will equip with a natural scheme structure below (Example 4.4). In this way, we can view the morphism f as a *family of objects indexed by the points of S*. Of course, this is not a one-one translation: only very special families indexed by the points of S come from morphisms. And that is a good thing, because families which do not, are in a sense too chaotic and not interesting. From this point of view, every result about morphisms of schemes can be viewed as a result about families of schemes over fields.

Example 4.1 Let K be a field, and let X be a K-scheme. By Example 3.12 1., the morphisms $\operatorname{Spec} K \to X$ of K-schemes correspond to the points $x \in X$ with residue class field $\kappa(x) = K$ (since we only consider morphisms *of K-schemes*, the morphism $\kappa(x) \to K$ in the previous example is necessarily the identity morphism). One can show that all these points are closed. We call these morphisms, or equivalently their image points, the *K-valued points of X* (or $\operatorname{Spec} K$*-valued points of X*).

Now let L be an extension field of K. We can then consider the morphisms $\operatorname{Spec} L \to X$ of K-schemes. By Example 3.12 1., these morphisms correspond to pairs of a point $x \in X$ together with a K-homomorphism $\kappa(x) \to L$. Analogously, we call these morphisms the *L-valued points of X* (or $\operatorname{Spec} L$*-valued points of X*). Note however that for a proper extension L/K there may be several L-valued points attached to the same topological point $x \in X$. Cf. Section 4.5.

We denote the set of K-valued and L-valued points by $X(K)$ and $X(L)$, respectively.

Assume specifically that $X \subseteq \mathbb{A}^n_K$ is a closed subscheme of affine space over K, i.e., $X = V(f_1,\dots,f_m) = \operatorname{Spec} K[X_1,\dots,X_n]/(f_1,\dots,f_m)$ for polynomials f_i. Then X is a K-scheme in a natural way, and the L-valued points of X correspond one-to-one to the K-algebra homomorphisms $K[X_1,\dots,X_n]/(f_1,\dots,f_m) \to L$, i.e., to the common solutions of the f_j in L^n. If L/K is a Galois extension, then the Galois group naturally acts on this solution set. The Galois orbits then correspond to the topological points of X.

4.2 Fiber products

Since a scheme is a somewhat complicated object, being a pair of a topological space and a sheaf, it is not always clear how to translate notions from topology (or even set-theoretic notions) to the world of schemes.

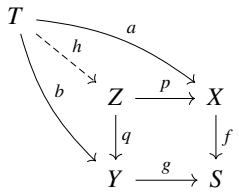
For example, it is easy to find examples of morphisms between affine schemes which are bijective, but whose corresponding ring homomorphisms are not isomorphisms, so that the scheme morphism is not an isomorphism, either. Instead, the correct notion of isomorphism is the categorical one: a morphism is called an isomorphism if it admits an inverse morphism. Since composition of maps and identity morphisms are present in an arbitrary category, this definition always works.

Of course, this phenomenon does not come as a surprise, since the situation for topological spaces, say, is similar. Nevertheless, it points in the right direction: One should try to find categorical definitions as much as possible.

As it turns out, a key notion in this regard is the notion of fiber product, because it encompasses as special cases many important constructions. Some of those we will discuss below, but we start with the general definition:

Definition 4.2 ([EGA I_{n}] 1.2[7]) Let $\mathscr{C}$ be a category, and let $f\colon X \to S$, $g\colon Y \to S$ be morphisms in $\mathscr{C}$. An object Z together with morphisms $p\colon Z \to X$, $q\colon Z \to Y$ with $f \circ p = g \circ q$ is called a *fiber product of X and Y over S* (or, more precisely, a fiber product of f and g), if for all objects T and morphisms $a\colon T \to X$, $b\colon T \to Y$ with $f \circ a = g \circ b$, there exists a unique morphism $h\colon T \to Z$ with $a = p \circ h$, $b = q \circ h$.

We visualize this definition by the following diagram:



In view of the universal property in the definition, it is clear that a fiber product Z is determined uniquely up to unique isomorphism (if it exists), and therefore we usually speak of "the" fiber product, and denote it by $X \times_S Y$. In a more fancy language, the fiber product just is a special case of (projective) limit. In an arbitrary category, fiber products need not exist in general. But in the category of sets, all fiber products exist. In fact, with notation as above,

$$X \times_S Y = \{(x,y) \in X \times Y;\ f(x) = g(y)\}. \tag{3}$$

Fiber products of sets. Using the notion of fiber product in the theory of sets, we can express the universal property of fiber product in a general category $\mathscr{C}$ as follows:

$$\mathrm{Hom}(T, X \times_S Y) = \mathrm{Hom}(T,X) \times_{\mathrm{Hom}(T,S)} \mathrm{Hom}(T,Y),$$

where the fiber product on the right hand side is taken in the category of sets. This means that we can view the fiber product as the object representing a certain functor (see Def. 4.14).

Contemplating the situation in the theory of sets, we see easily that certain important operations can be expressed as fiber products:

Products. If $S = \{s\}$ is a single point, then the cartesian product $X \times Y$ together with the projections to X and Y satisfies the universal property of the fiber product and hence "is" the fiber product (recall that the fiber product is only determined up to unique isomorphism anyway).

Fibers of morphisms. Let $f\colon X \to S$ be any map of sets, and let $s \in S$. Write $g\colon \{s\} \to S$ for the inclusion of the one-point set $\{s\}$ into S. Then the fiber $f^{-1}(s)$ together with the inclusion into X and the (unique) map to $\{s\}$ satisfies the universal property of the fiber product. (Of course, it is also easy to see directly that the fiber product as constructed in (3) admits a unique bijection with $f^{-1}(s)$ which is compatible with the maps to X and $\{s\}$.

Intersection. Second, consider injective maps $f\colon X \to S$ and $g\colon Y \to S$. We view X and Y as subsets of S via these maps. Then the intersection $X \cap Y$ (together with the inclusions into X and Y) is the fiber product of X and Y over S.

A crucial insight at this point is that the universal property of the fiber product allows for a reasonable approach to these notions (products, fibers of morphisms, intersections) in other categories, notably in the category of schemes.

To get started, let us consider for a moment the category of affine schemes. It is very easy to see that in this category fiber products exist. Namely, we can identify the category

[7] The original [EGA I] Déf 3.2.1 only has the definition specialized to the category of schemes.

of affine schemes with the opposite of the category of rings, and thus the fiber product of morphisms $\operatorname{Spec} B \to \operatorname{Spec} A$, $\operatorname{Spec} C \to \operatorname{Spec} A$ exists, if and only if in the category of rings, there exists the push-out, or amalgamated sum, of the ring homomorphisms $A \to B$, $A \to C$, i.e., a ring satisfying the dual universal property to the universal property of the fiber product. (Here, as usual, dual means that we reverse the directions of all arrows.) Writing down what this means, one sees immediately that in fact such an object exists, namely the tensor product $B \otimes_A C$ (together with the natural maps $B \to B \otimes_A C$, $C \to B \otimes_A C$). Going back to affine schemes we obtain that the fiber product of $\operatorname{Spec} B \to \operatorname{Spec} A$ and $\operatorname{Spec} C \to \operatorname{Spec} A$ is $\operatorname{Spec}(B \otimes_A C)$ (together with the natural maps $\operatorname{Spec}(B \otimes_A C) \to \operatorname{Spec} B$, $\operatorname{Spec}(B \otimes_A C) \to \operatorname{Spec} C$).

By Example 3.12 2., $\operatorname{Spec}(B \otimes_A C)$ even satisfies the universal property of the fiber product if T is an arbitrary (i.e., not necessarily affine) scheme. Furthermore one checks that for general schemes one can construct a fiber product by using suitable affine open coverings, and gluing.

This allows us to speak of fiber products of schemes over a common base, and, as we will spell out below, of fibers of scheme morphisms, and of intersections of subschemes, by using analogs of the above definitions.

Example 4.3 (Products) Even from the simplest examples it is clear that one has to be careful with the notion of product in algebraic geometry. For instance, if k is an algebraically closed field, as sets we have $\mathbb{A}^2(k) = k^2 = k \times k = \mathbb{A}^1(k) \times \mathbb{A}^1(k)$, and certainly it is only reasonable to expect that the affine plane $\mathbb{A}^2_k$ is the product of two copies of the affine line $\mathbb{A}^1_k$. However, the Zariski topology on $\mathbb{A}^2(k)$ is not equal to the product topology on $\mathbb{A}^1(k) \times \mathbb{A}^1(k)$ induced by the Zariski topology on $\mathbb{A}^1(k)$. (This is easy to see since the only closed subsets of $\mathbb{A}^1(k)$ are the whole space and finite sets.)

Thinking of schemes, i.e., adding the points corresponding to non-maximal prime ideals, it is not even true anymore that the set underlying $\mathbb{A}^2$ would equal the cartesian product of two copies of the set $\mathbb{A}^1$. But the notion of fiber product works well here. Namely, the scheme theoretic product is

$$\mathbb{A}^1_k \times_{\operatorname{Spec} k} \mathbb{A}^1_k = \operatorname{Spec}(k[T] \otimes_k k[T]),$$

and the tensors product $k[T] \otimes_k k[T]$ is naturally identified with the polynomial ring in 2 variables over k, so its spectrum is $\mathbb{A}^2_k$.

More generally, let X, Y be S-schemes. Then the fiber product $X \times_S Y$ is again an S-scheme, and is the product of X and Y in the category of S-schemes.

As another example, consider the inclusion $\mathbb{R} \to \mathbb{C}$ of the field of real numbers into the complex numbers. Correspondingly we can consider $\operatorname{Spec} \mathbb{C}$ as a $\mathbb{R}$-scheme. Of course, topologically both these spectra have only one point each. We compute the product

$$\operatorname{Spec} \mathbb{C} \times_{\operatorname{Spec} \mathbb{R}} \operatorname{Spec} \mathbb{C} = \operatorname{Spec}(\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}).$$

Using the isomorphism $\mathbb{C} \cong \mathbb{R}[T]/(T^2+1)$, one sees that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$, the product of two copies of $\mathbb{C}$ which has two prime ideals $\{0\} \times \mathbb{C}$ and $\mathbb{C} \times \{0\}$. Both of these are actually maximal ideals, so the product $\operatorname{Spec} \mathbb{C} \times_{\operatorname{Spec} \mathbb{R}} \operatorname{Spec} \mathbb{C}$ is the disjoint union of two closed points.

Example 4.4 (Fibers) In analogy with the situation for sets, we use fiber products to define the fibers of a morphism $f\colon X \to Y$. To equip a point y in the topological space Y with the structure of a scheme, we pass to the spectrum $\operatorname{Spec} \kappa(y)$ of its residue class field. We

obtain a canonical scheme morphism $\operatorname{Spec}\kappa(y) \to Y$ (cf. Example 3.12 1.) and can define the scheme-theoretic fiber

$$f^{-1}(y) := X \times_Y \operatorname{Spec}\kappa(y).$$

One can show that the underlying topological space of this scheme is just the fiber $f^{-1}(y)$ of the continuous map f with the subspace topology.

Example 4.5 (Intersections) For subschemes $Z_1, Z_2 \subseteq X$, we can define the scheme-theoretic intersection as

$$Z_1 \times_X Z_2.$$

Note that there are no good naive notions of products, fibers and intersections for schemes, e.g., given a scheme morphism $f\colon X \to Y$, and $y \in Y$, it is clear what the topological space $f^{-1}(y)$ should be, but there is no obvious way to define a scheme structure on this space.

Given an S-scheme X and a morphism $S' \to S$, we sometimes call the fiber product $X \times_S S'$, considered as an S'-scheme via the second projection, the *base change* of X along $S' \to S$. In fact, say $S' \to S$ is a morphism of affine schemes, corresponding to a ring homomorphism $R \to R'$, and X is a closed subscheme of $\mathbb{A}^n_R$, given by polynomials $f_i \in R[T_1, \ldots, T_n]$. Then the base change $X \times_S S'$ is the closed subscheme of $\mathbb{A}^n_{R'} (= \mathbb{A}^n_R \times_S S')$ given by the same polynomials f_i, now viewed as elements of $R'[T_1, \ldots, T_n]$ via the ring homomorphism $R \to R'$, i.e., we simply consider the equations describing X over the ring R'.

The notion of fiber product also shows the correct way to translate properties of topological spaces into algebraic geometry, as in the following examples.

Example 4.6 (Hausdorff Spaces and Separated Schemes) Because the Zariski topology is so coarse, topological spaces obtained as the prime spectrum of a ring are almost never Hausdorff. On the other hand, spaces like affine or projective space over a field should reflect, to some extent, nice properties of Hausdorff spaces. For example, two morphisms $\mathbb{A}^n_k \to \mathbb{A}^m_k$ coincide, if they coincide on a non-empty open subset (note that every non-empty open subset is dense). We would like to extend this to more general scheme morphisms $X \to Y$. For topological spaces, we could say that continuous maps $S \to T$ which coincide on an open dense subset of S must coincide on all of S, *if T is Hausdorff*. The Hausdorff property for T can be expressed by saying that the diagonal embedding $T \to T \times T$ has closed image. (Since here we are talking about usual topological spaces, the topology on $T \times T$ is just the product topology; at the same time $T \times T$ is the fiber product of T with itself over the one-point topological space, in the category of topological spaces).

Therefore, for an S-scheme Y, the analogous property would be to ask that the diagonal morphism $Y \to Y \times_S Y$ is a closed embedding (i.e., identifies Y with a closed subscheme) of schemes. If this is the case, then Y is called *separated over S* ([EGA I] Déf. 5.4.1). Every affine scheme and every scheme which is quasi-projective (see Section 4.3) over a separated scheme is separated ([EGA I] Prop. 5.5.1, Cor. 5.5.7, [EGA II] (5.3.1)), and it is not hard to prove

Proposition 4.7 *Let X, Y be S-schemes, and suppose that X is reduced and that Y is separated over S. If morphisms $f, g\colon X \to Y$ coincide on a dense open subset of X, then they are equal.*

Example 4.8 (A non-separated scheme, [EGA I] Exemple 5.5.11) Let k be a field. Gluing two copies of $\mathbb{A}^1_k$ by identifying their open subschemes $\mathbb{A}^1_k \setminus \{0\}$, we obtain a scheme X which looks like the affine line over k with the origin doubled. This scheme is not separated.

Example 4.9 (Compact Spaces and Proper Scheme Morphisms) Another property which can be expressed using fiber products is the property of compactness. Note that all affine schemes are quasi-compact as topological spaces, i.e., every open cover has a finite subcover. However, we want to view affine space, for instance, as a "non-compact object" (lying as an open subset in the "compact" projective space of the same dimension. This kind of "compactness" is called *properness* in algebraic geometry.

Before we define it, note the following result from topology: Let $f\colon X \to Y$ be a continuous map between topological spaces where X is Hausdorff and Y is locally compact. Then $f^{-1}(Z)$ is compact for every compact $Z \subseteq Y$ if and only if for all topological spaces Y' the product map $X \times Y' \to Y \times Y'$ is closed (i.e., images of closed subsets are closed). In particular, if Y is the one-point topological space, then we obtain a characterization of X being compact.

We now define that a morphism $f\colon X \to Y$ of schemes is *proper*, if it is separated, of finite type, and if for all scheme morphisms $Y' \to Y$ the morphism $X \times_Y Y' \to Y \times_Y Y' \cong Y'$ is closed. (As before, the property of a morphism of being closed is by definition purely topological: images of closed subsets are closed.)

For every scheme S, projective space $\mathbb{P}^n_S$ is proper over S, as we expect, [EGA II] Thm. 5.5.3. This is a version of the so-called fundamental theorem of elimination theory. On the other hand, $\mathbb{A}^n_S$ is not proper over S whenever $n > 0$. To illustrate this, consider the affine line $\mathbb{A}^1_k$ over a field k. The map $\mathbb{A}^1_k \times_{\operatorname{Spec} k} \mathbb{A}^1_k \to \mathbb{A}^1_k$ is not closed, because the image of $V(XY-1)$ is $\mathbb{A}^1_k \setminus \{0\}$.

4.3 Properties of morphisms

Let us discuss some important properties of morphisms of schemes, or equivalently, of relative schemes. Recall that we heuristically view an S-scheme X, i.e., a morphism $f\colon X \to S$, as the family of its fibers $f^{-1}(s)$, $s \in S$, where we define $f^{-1}(s) := X \times_S \operatorname{Spec} \kappa(s)$ so that we have a structure of $\kappa(s)$-scheme on the fiber $f^{-1}(s)$.

Flat morphisms. ([EGA I] Ch. 0, (6.7.1)) While the mere existence of a morphism $X \to S$ already contains a kind of compatibility condition on the family $(f^{-1}(s))_s$ of fibers, in many cases a stronger condition on compatibility, or "continuity" of the fibers is desirable. The corresponding algebraic notion which turns out to be very useful here is the notion of flatness. Recall that an A-algebra B (or more generally, an A-module B) is called *flat over* A, if tensoring over A by B turns injections $N \to N'$ of A-modules into *injections* $N \otimes_A B \to N' \otimes_A B$. We say that a morphism $f\colon X \to S$ of schemes is flat, if for every $x \in X$, the homomorphism of local rings, $\mathcal{O}_{S,f(x)} \to \mathcal{O}_{X,x}$ is flat. A large part of [EGA IV] is devoted to the study of flat morphisms.

Smooth morphisms. ([EGA IV] Déf. 17.3.1; the definition there is different from the one given here: cf. loc. cit. Thm. 17.5.1 and its proof) Above we have seen the key ingredients of the definition when a morphism $f\colon X \to S$ is called *smooth*: Locally at points $x \in X$, the morphism can be described by an open subscheme of a closed subscheme given by m equations in n-dimensional space such that the Jacobi matrix at the point corresponding to x has full rank m. This is a strong condition on f with many nice consequences. For example, every smooth morphism is flat. Conversely, if $f\colon X \to S$ is a flat morphism such that every fiber $f^{-1}(s)$ is smooth over $\kappa(s)$, then f is smooth ([EGA IV] Thm. 17.5.1). Since in the examples below, we almost always restrict to the simpler smooth cases, we will not need to refer to the notion of flatness directly.

Finiteness properties. We say that a morphism $f\colon X \to S$ is *quasi-compact*, if for every quasi-compact open $V \subseteq S$, the inverse image $f^{-1}(V)$ is quasi-compact ([EGA I] Déf. 6.6.1). We say that a morphism $f\colon X \to S$ is *of finite type* (or that X is of finite type over S, or that the S-scheme X is of finite type), if f is quasi-compact and if there exists coverings $S = \bigcup_j V_j$, $f^{-1}(V_j) = \bigcup_i U_{j,i}$ by affine open subschemes, such that for all i, j, the $\mathscr{O}_S(V_j)$-algebra $\mathscr{O}_X(U_{j,i})$ is of finite type, i.e., finitely generated as an $\mathscr{O}_S(V_j)$-algebra ([EGA I] Déf. 6.3.1).

Projective morphisms. Let S be an affine scheme. We call an S-scheme X projective (or we say that the morphism $X \to S$ is projective), if X is isomorphic as an S-scheme to a closed subscheme of some projective space $\mathbb{P}^n_S$ ([EGA II] Déf. 5.5.2, Remarque 5.5.4 (ii)).[8] We say that X is quasi-projective over S if X is isomorphic to an open subscheme of a projective S-scheme ([EGA II] Déf. 5.3.1, Prop. 5.3.2).

Example 4.10 We now have all the ingredients in order to reinterpret the classical definition of variety from Section 2 in terms of schemes. Let us start with an algebraically closed field k. In the affine case, we have equivalences of categories between

(i) the category of affine algebraic varieties over k,
(ii) the category of reduced finitely generated k-algebras,
(iii) the category of reduced affine schemes of finite type over k.

The equivalences (i) $\leftrightarrow$ (ii) and (ii) $\leftrightarrow$ (iii) are contravariant. For the first one of these, cf. (1). The second one follows immediately from the definitions.

The equivalence (i) $\leftrightarrow$ (iii) extends naturally to the quasi-projective case: We have equivalences between

(i′) the category of quasi-projective algebraic varieties over k,
(iii′) the category of reduced quasi-projective schemes of finite type over k.

Moreover, for a scheme X as in (iii′), the topological space of the corresponding variety is given by the subset of closed points of X with the subspace topology, as can be seen by passing to the affine situation.

Let X be a k-scheme of finite type. For $x \in X$, the composition $\operatorname{Spec}\kappa(x) \to X \to \operatorname{Spec} k$ of the morphism in Example 3.12, 1., and the structure morphism gives us a homomorphism $k \to \kappa(x)$. As a consequence of Hilbert's Nullstellensatz, one can show that this homomorphism is an isomorphism if and only if the point x is closed. We thus obtain a bijection between the set of $\operatorname{Spec} k$-morphisms $\operatorname{Spec} k \to X$ (i.e., the set of k-valued points of X, Example 4.1) and the set of closed points of X. See [EGA I_n] Cor. 6.5.3.

Let k be a field, and let X, Y be k-schemes of finite type. Even to study schemes like X and Y which are close to the classical picture, it is often useful to consider schemes which are not of finite type, such as $\operatorname{Spec}\mathscr{O}_{X,x}$ for a point $x \in X$. For example, if $f\colon X \to Y$ is a morphism of k-schemes, then f induces a ring homomorphism $\mathscr{O}_{Y,f(x)} \to \mathscr{O}_{X,x}$. If this is an isomorphism, then one can show that there exist open neighborhoods of x and $f(x)$ such that f restricts to an isomorphism between them, [EGA I] Prop. 6.5.1.

In another direction, the non-closed points (cf. Section 3.2.2) are often useful, in particular in connection with scheme morphisms. For example, let $S = \operatorname{Spec} A$, where A is a noetherian ring which has a unique minimal prime ideal, so that S is irreducible. We denote

[8] If S is not necessarily affine, we can still define projective space over S as the fiber product $\mathbb{P}^n_S := \mathbb{P}^n_{\operatorname{Spec}\mathbb{Z}} \times_{\operatorname{Spec}\mathbb{Z}} S$. Then there is a similar notion of projective S-scheme, but the situation is a little more subtle and one finds slightly differing variants of this notion in the literature.

the point of S corresponding to the minimal prime ideal by η. Let $f\colon X \to S$ be a morphism of schemes of finite type. For $s \in S$, denote by $f^{-1}(s)$ the scheme-theoretic fiber of f. This is a scheme of finite type over the residue class field $\kappa(s)$. Then there exists a dense open subset $U \subseteq S$ such that for all $s \in S$, $\dim f^{-1}(s) = \dim f^{-1}(\eta)$, [EGA IV] Prop. 9.2.6.1. This is typical behavior: Many properties which are present at the generic point (or in this case: which hold for the fiber of some morphism over the generic point) hold on a dense open subscheme. These so-called "constructibility properties" are studied in detail in [EGA IV], see also [23], App. E for a survey.

4.4 Parameter Spaces and Representable Functors

In many areas of mathematics, classification problems are of great importance. Classification can mean many different things: For certain kinds of objects one can show that there are only finitely many, and enumerate them (e.g., the sporadic simple finite groups). In other cases, there could be infinite families (e.g., complex Lie algebras). Sometimes one might be able to prove that achieving a complete classification is basically hopeless (e.g., certain "wild" problems in representation theory).

In algebraic geometry, the following interesting phenomenon occurs, and plays a key role in much of the current research: Given a kind of object that we would like to classify, or parameterize, is is often possible to equip the set of (isomorphism classes) of all of these objects with the structure of an algebraic variety (or scheme). In other words, for many interesting kinds of algebro-geometric objects, the entirety of these objects "is" again an algebro-geometric object. Schemes arising like this are called parameter spaces or moduli spaces. This is a very enriching situation, because we can then relate local and global properties of the parameter space to properties of the objects which are classified. This relationship can be used fruitfully in both directions: Good knowledge about the original objects gives results about the parameter space, but we can also use information about the parameter space to find out something about the parameterized objects (cf. Example 6.1). Furthermore, it turns out that this is a key method to construct algebraic varieties which are amenable to further study. (While one can write down examples of algebraic varieties by "randomly" writing out polynomial equations, it is not at all easy to produce "meaningful" varieties, i.e., varieties which can be shown to have interesting properties.)

The simplest example of this situation we have already seen: The set of all lines through the origin in k^{n+1} "is" projective space $\mathbb{P}^n(k)$. Similarly, one can construct the *Grassmann variety* (or *Grassmannian*, [EGA $\mathrm{I_n}$] 9.7) $\mathrm{Grass}_{r,n}$ of all r-dimensional subvector spaces of k^n. Another situation where a parameter space is easy to obtain is when we are interested in all closed subschemes (inside $\mathbb{A}^n_k$ or $\mathbb{P}^n_k$, say) defined by equations of a specific form: For instance, consider the set of all quadrics in the affine plane $\mathbb{A}^2_k$ over an algebraically closed field k, in other words, the set of all closed subschemes $C \subset \mathbb{A}^2_k$ of the form $C = V(f)$, where $f \in k[X,Y]$ is a polynomial of total degree 2. A polynomial like that is given by its 6 coefficients. At least one of the coefficients of X^2, XY, and Y^2 must be $\neq 0$. Two polynomials define the same curve if and only if the differ by a unit in k, i.e., we should consider the 6 values as homogeneous coordinates in $\mathbb{P}^5(k)$. Hence as the parameter space we obtain an open subset of $\mathbb{P}^5(k)$. For closed subschemes of projective space described by homogeneous equations of a fixed degree, the situation is even a little simpler; see Example 6.1 where we use a space like this in the context of cubic surfaces.

This phenomenon was studied already by B. Riemann who coined the term of "moduli" (whence these parameter spaces are nowadays usually called *moduli spaces*). Riemann stud-

ied compact complex-analytic curves (which we now call Riemann surfaces). First, there is a discrete invariant, namely the genus (see Lemma 4.12 below). If we fix $g \geq 2$, then Riemann showed that the space of Riemann surfaces of genus g depends on $3g-3$ parameters (i.e., has dimension $3g-3$), which he called *moduli*.

The case of genus 1 is a famous classical classification problem, as well. It is solved by the "modular curve" of elliptic curves over the complex numbers. As we have discussed in Section 2.5, over the complex numbers the notion of elliptic curve is equivalent to the notion of compact Riemann surface E of genus 1 together with a distinguished point $O \in E$ (the neutral element of the group law on the elliptic curve), and all those are isomorphic to quotients $\mathbb{C}/\Lambda$, where $\Lambda \subseteq \mathbb{C}$ is a lattice, i.e., a subgroup of $\mathbb{C}$ generated by two $\mathbb{R}$-linearly independent elements. Elliptic curves $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are isomorphic if and only if there exists $\alpha \in \mathbb{C}^\times$ with $\Lambda' = \alpha\Lambda$; in this case we call the lattices Λ and Λ' homothetic. We thus obtain a bijection between the set of isomorphism classes of elliptic curves over $\mathbb{C}$ and the set of homothety classes of lattices in $\mathbb{C}$.

Every lattice is homothetic to a lattice of the form $\mathbb{Z} \oplus \mathbb{Z}\tau$ with $\tau \in \mathbb{H} := \{z \in \mathbb{C};\ \mathrm{Im}(\tau) > 0\}$, the upper half plane.

It is easy to convince oneself that for $\tau, \tau' \in \mathbb{H}$,

$$\mathbb{Z} \oplus \mathbb{Z}\tau \text{ and } \mathbb{Z} \oplus \mathbb{Z}\tau' \text{ are homothetic} \iff \text{there exists } A \in SL_2(\mathbb{Z}) \text{ with } \tau' = A\tau.$$

Here, a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ acts on $\mathbb{H}$ by $A\tau := \frac{a\tau+b}{c\tau+d}$.

We denote by $Y := SL_2(\mathbb{Z})\backslash\mathbb{H}$ the set of orbits of this action of $SL_2(\mathbb{Z})$ on the complex upper half-plane $\mathbb{H}$ and obtain a bijection

$$Y \to \mathrm{Ell}(\mathbb{C}),$$

where $\mathrm{Ell}(\mathbb{C})$ denotes the set of isomorphism classes of elliptic curves over $\mathbb{C}$.

This is a nice description, and in fact it is an instance of the above-mentioned phenomenon: Indeed, since the action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$ is sufficiently well-behaved, Y carries a natural structure of Riemann surface (at "almost all" points, the projection $\mathbb{H} \to Y$ is a local isomorphism).

While so far it may sound as if this was an example in complex geometry rather than algebraic geometry, Y is actually an *algebraic variety* over $\mathbb{C}$! (Or, more precisely, Y is the Riemann surface attached to an algebraic curve over $\mathbb{C}$.) To see this, one can use ad hoc arguments, or use the following general method: one shows that Y can be compactified by adding finitely many points (in fact, in the case at hand one point is enough, and the compactification in this case is the Riemann sphere). But every compact Riemann surface is algebraic; for the Riemann sphere, the corresponding algebraic curve is the projective line $\mathbb{P}^1_{\mathbb{C}}$. Removing finitely many points from an algebraic curve gives us another (now affine) algebraic curve, and for Y specifically we see that $Y \cong \mathbb{A}^1(\mathbb{C}) = \mathbb{C}$ is the affine line over $\mathbb{C}$.

Let us now explain how Grothendieck's point of view provides an essential piece of input to the construction and study of these moduli spaces. One question we left open in the sketchy presentation of the general phenomenon above, and maybe the most important one, is the following: How do we get the geometric structure which we would like to impose on the parameter set *in a natural way*? Clearly, we have to use information beyond the set of isomorphism classes of objects — after all, this *set alone* is determined, up to bijection, by its cardinality, and hence does not carry a substantial amount of information.

To find the right procedure of defining moduli spaces, let us first think about an optimal situation. In order to make this discussion more readable, let us think specifically of the

moduli space of curves. Let us start by a few definitions. Below we will always understand the notion of curve in the strict sense of the following definition:

Definition 4.11 (cf. [EGA II] 7.4) Let k be a field. A (smooth, geometrically connected, projective) *curve* over k is a k-scheme C of dimension 1, such that C is smooth over k, and projective over k (i.e., isomorphic to a closed subscheme of some projective space $\mathbb{P}^n_k$), and such that for every field extension k'/k, the base change $C \times_{\operatorname{Spec} k} \operatorname{Spec} k'$ is connected.

There exists a relatively simple discrete invariant of curves over a field, namely the genus. Recall that for a compact Riemann surface X, the genus of X is a non-negative integer determined by the underlying topological space of X: It is equal to the number of "handles" one needs to attach to a sphere in order to obtain the topological space X. The Riemann sphere has genus 0 (and is the unique compact Riemann surface of genus 0), a torus has genus 1, etc. An analogous notion exists for smooth, projective algebraic curves (and over the complex numbers, it coincides with the topological one). We will not give the precise definition here, but only state the following result which gives the genus for curves which can be embedded into the projective plane.

Lemma 4.12 *Let k be a field. Let $C \cong V_+(f) \subset \mathbb{P}^2_k$ be a curve (in the above sense) which is isomorphic to the closed subscheme defined by a homogeneous polynomial f of degree d. Then the genus of C is equal to*

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

For example, elliptic curves, being defined by cubic polynomials in $\mathbb{P}^2_k$, have genus 1. The curve $\mathbb{P}^1_k$ is isomorphic to the closed subscheme in $\mathbb{P}^2_k$ defined by a linear polynomial, and hence has genus 0 (and if k is algebraically closed, then every curve of genus 0 is isomorphic to $\mathbb{P}^1_k$).

The notion of (always: smooth, geometrically connected, projective) curve of genus g is then the exact analogue of the notion of compact Riemann surface of genus g, so we are in the situation of Riemann's moduli mentioned above. In fact, the complex-geometry version of the Theorem of Riemann-Roch shows that every compact Riemann surface is projective, i.e., can be embedded into projective space $\mathbb{P}^n(\mathbb{C})$, and can thus be "identified" with an algebraic curve. So over the complex numbers, the above is not just an analogue, but a precise reformulation.

We will give other examples below, and emphasize that the theory described below applies to every moduli problem; it just makes for nicer reading (the author hopes) to speak of curves than of "the objects we want to classify".

Let us fix, for simplicity, an algebraically closed field k. Assume we had constructed a moduli space $\mathscr{M}_g$ of curves of genus g. By this we mean that it parameterizes all curves of genus g, up to isomorphism, or in other words: Each of its points corresponds to a curve, and curves corresponding to different points are not isomorphic.

(We have to be a little careful with what we mean by "all" curves. More precisely, the above requirement should be understood as saying that $\mathscr{M}_G(k)$, the set of closed points of $\mathscr{M}_g$, is in bijection with the set of isomorphism classes of smooth curves of genus g over k. Since we are just developing an idea at the moment, we allow ourselves to ignore the non-closed points. In the final wrap-up this problem will disappear in a natural way.)

This means that we have a family of curves over $\mathscr{M}_g$, and by the discussion in Section 4.5 we should expect, or at least hope, that a family like that is given by a morphism $\pi\colon \mathscr{C} \to \mathscr{M}_g$. The key property of π would be that for every (closed) point $x \in \mathscr{M}_g$, the fiber $\pi^{-1}(x)$

is a curve over k, that no two fibers over different points are isomorphic, and that every curve over k is isomorphic to one of the fibers.

Now what happens if we consider another morphism $f\colon C \to S$ which is a "family of curves", i.e., S is a k-scheme (of finite type) and for every $s \in S$, the fiber $f^{-1}(s)$ is a curve over the residue class field $\kappa(s)$. Then we can define a map $S \to \mathscr{M}_g$ which is given on closed points by mapping $s \in S(k)$ to the point $x \in \mathscr{M}_g(k)$ such that the curves $f^{-1}(s)$ and $\pi^{-1}(x)$ are isomorphic. The key point here is of course that there exists a unique such x by the defining property of $\mathscr{M}_g$.

Conversely, every morphism $g\colon S \to \mathscr{M}_g$ gives rise to a family of curves on S: Namely, for $s \in S$, we just take the curve given by the point $g(s)$. In fact, we can express the resulting family of curves as a morphism to S more directly: It is just given by the projection $\mathscr{C} \times_{\mathscr{M}_g} S \to S$. To simplify matters, we will only consider smooth, projective families of curves here, i.e., smooth projective morphisms $g\colon C \to S$ such that every fiber of g is a curve in the above sense. We call such a morphism a *family of curves* below.

We can summarize this discussion by saying that for all k-schemes S we expect to have

$$\mathrm{Hom}(S, \mathscr{M}_g) = \{\text{families of curves over } S\}/\cong . \tag{4}$$

Since the family referred to on the right hand side should be given by taking the fibers over points of S, for a morphism $S' \to S$ we get a commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}(S, \mathscr{M}_g) & \longrightarrow & \{\text{families of curves over } S\}/\cong \\ \downarrow & & \downarrow \\ \mathrm{Hom}(S', \mathscr{M}_g) & \longrightarrow & \{\text{families of curves over } S'\}/\cong \end{array}$$

where the horizontal arrows are the identifications above, the left vertical map is composition with $S' \to S$, and the right vertical map is the base change $C \mapsto C \times_S S'$.

The surprising fact is that this reformulation solves the problem of nailing down a geometric structure (if one exists)! The reason is that for every scheme X the collection of sets $\mathrm{Hom}(S,X)$ together with the composition maps $\mathrm{Hom}(S,X) \to \mathrm{Hom}(S',X)$ for every morphism $S' \to S$ *determine the scheme* X (see Section 4.5). So if we can define what a family of curves over a scheme S should be (such that for a morphism $S' \to S$ and a family of curves over S we obtain a family of curves over S' by base change), then there is at most one scheme with the property (4).

4.5 The Yoneda Lemma

We still need to explain why the collection of sets $\mathrm{Hom}(S,X)$ together with the composition maps $\mathrm{Hom}(S,X) \to \mathrm{Hom}(S',X)$ for every morphism $S' \to S$ determines a scheme X. This is a purely formal result which has nothing to do with schemes, called the Yoneda Lemma (after N. Yoneda). The language of categories and representable functors is the topic of the very first sections of the new edition [EGA I_n] (Ch. 0, 1.1) and is not yet present explicitly in the first edition — in contrast to the emphasis on relative schemes and morphisms.

To formulate it, let $\mathscr{C}$ be a category. For an object $X \in \mathscr{C}$ we denote by h_X the contravariant functor $\mathscr{C} \to (\mathrm{Sets})$, $T \mapsto \mathrm{Hom}_{\mathscr{C}}(T,X)$. For a morphism $X \to Y$ in $\mathscr{C}$, and any $T \in \mathscr{C}$, we obtain, by composition, a map $\mathrm{Hom}_{\mathscr{C}}(T,X) \to \mathrm{Hom}_{\mathscr{C}}(T,Y)$ and thus a morphism $h_X \to h_Y$ of functors. In other words, we obtain a functor $\mathscr{C} \to \mathrm{Fun}^{\mathrm{contra}}(\mathscr{C}, (\mathrm{Sets}))$ from $\mathscr{C}$ to the category of contravariant functors $\mathscr{C} \to (\mathrm{Sets})$.

Theorem 4.13 (Yoneda Lemma, [EGA I_n] Ch. 0, 1.1.7) *The functor*

$$\mathscr{C} \to \mathrm{Fun}^{\mathrm{contra}}(\mathscr{C}, (\mathrm{Sets})), \qquad X \mapsto h_X,$$

is fully faithful, i.e., for any two objects $X, Y \in \mathscr{C}$ the natural map

$$\mathrm{Hom}_{\mathscr{C}}(X,Y) \to \mathrm{Hom}_{\mathrm{Fun}}(h_X, h_Y),$$

where the right hand side denotes the set of morphisms of functors, is bijective.

The first immediate consequence is that two objects X and Y of $\mathscr{C}$ are isomorphic if and only the attached functors h_X and h_Y are isomorphic functors. Using this for $\mathscr{C}$ the category of (S-)schemes, we obtain precisely the statement that we were aiming for.

Besides this special case of the Yoneda Lemma, the general statement is also quite interesting, in particular in the context of parameter spaces. It tells us that defining a morphism of schemes is equivalent to defining a morphism between the attached functors. In the case of a moduli space, we usually start out by defining this functor and hence typically have good control over it.

Even though, because of its great merits in algebraic geometry, the Yoneda Lemma is called a theorem above, its proof is not difficult. In fact, we can construct an inverse map by sending a morphism $\alpha\colon h_X \to h_Y$ to $\alpha(X)(\mathrm{id}_X)$.

In the context of schemes, we also call $\mathrm{Hom}(T,X)$ the *set of T-valued points of X* and denote it by $X(T)$, or, for $T = \mathrm{Spec}\, R$ affine, by $X(R)$. Similarly, we can fix a scheme S and apply the above to the category of S-schemes. In this case, we consider S-schemes T, and morphisms of S-schemes $T \to X$, but use the same notation $X(T)$, $X(R)$; cf. Example 4.1.

Definition 4.14 ([EGA I_n], (1.1.8)) A contravariant functor $\mathscr{C} \to (\mathrm{Sets})$ is called *representable*, if it is (isomorphic to a functor) of the form h_X for some $X \in \mathscr{C}$.

This gives us a method to find moduli spaces: Define a contravariant *moduli functor* $(\mathrm{Sch}) \to (\mathrm{Sets})$ from the category of schemes to the category of sets, and then prove that it is representable. Similarly, we could restrict to the category (Sch/S) of S-schemes for some fixed base scheme S, for example $S = \mathrm{Spec}\, k$ for some field. Proving representability is often a hard problem.

In this situation, i.e., if (4) holds for some moduli space $\mathscr{M}$ and all S, we can in particular apply it to $S = \mathscr{M}$ and $\mathrm{id} \in \mathrm{Hom}(\mathscr{M}, \mathscr{M})$, and obtain a family over $\mathscr{U} \to \mathscr{M}$ of the objects that are parameterized by $\mathscr{M}$ (a family of curves in the above example). This family is called the *universal object*, or *universal family*. For all morphisms $f\colon S \to \mathscr{M}$, the family corresponding to this morphism via (4) is equal to the family $\mathscr{U} \times_{\mathscr{M},f} S \to S$ obtained by base change along f from the universal family.

4.6 Group schemes

The functorial viewpoint also allows us to say easily what we mean by a *scheme with a group structure*, or as we will call it, a *group scheme* (and similarly, we could define *group objects* in an arbitrary category in which finite products exist, [EGA I_n] Ch. 0, (1.6.3)).

We fix a base scheme S.

Definition 4.15 An S-group scheme is an S-scheme G together with a contravariant functor $\tilde{h}_G\colon (\mathrm{Sch}/S) \to (\mathrm{Groups})$ such that h_G equals the composition of $\tilde{h}_G$ with the forgetful functor $(\mathrm{Groups}) \to (\mathrm{Sets})$.

Note that this can be spelled out quite explicitly: For every S-scheme T, $\tilde{h}_G(T)$ is a group with underlying set $h_G(T)$, and the group structure is functorial in T, i.e., for $T' \to T$, the map $\tilde{h}_G(T) \to \tilde{h}_G(T')$ is a group homomorphism. Then we obtain morphisms of functors $h_G \times h_G \to h_G$ (multiplication), $h_G \to h_G$ (inverse), and $h_S \to h_G$ (neutral element). By the Yoneda Lemma, they correspond to scheme morphisms, so the above definition is equivalent to

Definition 4.16 An S-group scheme is an S-scheme G together with morphisms $m\colon G \times_S G \to G$, $i\colon G \to G$ and $e\colon S \to G$ such that "the group axioms are satisfied for these morphisms".

When we write that the group axioms should be satisfied, we mean that the "obvious" diagrams expressing these axioms should be commutative. For instance, the diagrams expressing associativity and the defining property of (right) inverse elements are

$$\begin{array}{ccc} G \times_S G \times_S G & \xrightarrow{(m,\mathrm{id})} & G \times_S G \\ \downarrow{\scriptstyle (\mathrm{id},m)} & & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow{m} & G \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{(\mathrm{id},i)} & G \times_S G \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle m} \\ S & \xrightarrow{e} & G \end{array}$$

where $f\colon G \to S$ denotes the structure morphism making G an S-scheme.
Both definitions allow for an obvious variant defining *commutative* group schemes.

Example 4.17 1. Let S be a scheme, and let G be an abstract group. The group structure on G naturally induces a group scheme structure on the disjoint union

$$\underline{G}_S := \bigsqcup_{g \in G} S$$

of copies of S indexed by G. (Think first about the case $S = \operatorname{Spec} k$, the spectrum of a field. Then the underlying topological space of $\underline{G}_{\operatorname{Spec} k}$ is just G with the discrete topology, and it is easy to convince oneself that the group structure of G gives morphisms as in the second definition of group scheme. Group schemes of this form are called *constant group schemes*.

2. A large class of examples is given by matrix groups such as the general linear group of invertible $n \times n$-matrices. In fact, for any ring R, $GL_n(R)$ is a group, and the natural map $GL_n(R) \to GL_n(R')$ is a group homomorphism for any ring homomorphism $R \to R'$. We hence obtain a group scheme GL_n over $\operatorname{Spec} \mathbb{Z}$, invoking the first definition above. Of course, in order to show that $GL_n(R)$ is in fact a group, one probably has to write down the matrix product and inverse matrix as polynomials in the entries of the matrix (assuming that the determinant is invertible, and hence allowing to use it in the denominator, so that Cramer's rule can be applied). As a scheme, GL_n is simply the principal open subset $D(\det) \subset \mathbb{A}^{n^2}_{\operatorname{Spec} \mathbb{Z}}$, where we use $X_{11}, \ldots, X_{nn}$ as the n^2 variables, and det denotes the determinant of the matrix $(X_{ij})_{i,j}$.
Assuming we knew that $GL_n(R)$ is a group, functorially in R, for some other reason, we can see in this case why the Yoneda Lemma works. In fact, the interesting question is why the inverse of a matrix with coefficients in some ring R and invertible determinant can be expressed in terms of polynomials in the matrix entries and the inverse of the

determinant. Moreover, since the inverse should be a morphism $GL_n \to GL_n$ of schemes, this expression should be "independent of R". To get this expression, consider the ring

$$A := \mathbb{Z}[X_{11}, \dots, X_{nn}][\frac{1}{\det}],$$

the subring of the field of fractions of $\mathbb{Z}[X_{11}, \dots, X_{nn}]$ generated by $\mathbb{Z}[X_{11}, \dots, X_{nn}]$ and $1/\det$. Since $GL_n(A)$ is a group by assumption, and the matrix $(X_{ij})_{i,j}$ has invertible determinant in A by construction, the inverse matrix $(X_{ij})_{i,j}^{-1}$ has entries in A, and this is exactly what we were looking for.

Similarly, we can consider other classical groups as group schemes.

3. The group structure on elliptic curves (Section 2.5) is given by rational functions, so invoking the second definition, we see that every elliptic curve is a group scheme. Cf. also Sections 5.3, 7.3.

5 Moduli spaces

5.1 Coming back to moduli spaces of curves

Let us contemplate which properties a moduli functor must have in order to possibly be representable.

One immediate obstruction is the existence of "locally constant, but non-constant" objects: For instance let C_0 be a curve over the fixed algebraically closed field k, and assume that there exists a k-scheme S (of finite type, reduced) together with a family of curves $f\colon C \to S$ such that every fiber $f^{-1}(s)$ is isomorphic to C_0 (for closed points $s \in S$). If a moduli space $\mathscr{M}_g$ as above exists, then under the corresponding morphism $S \to \mathscr{M}_g$, each of these points s is mapped to the point corresponding to C_0, i.e., the morphism $S \to \mathscr{M}_g$ is constant. Since we can recover the family of curves $f\colon C \to S$ from this morphism by taking a fiber product, we see that the family $C \to S$ necessarily is constant, i.e., of the form $C \times_{\operatorname{Spec} k} S \to S$.

Looking at this in the other direction, we see that if there exists S and a family $C \to S$ of curves such that all fibers over closed points are isomorphic to C_0, but which is not of the form $C_0 \times_{\operatorname{Spec} k} S \to S$, then a moduli space $\mathscr{M}_g$ in the sense above cannot exist. As it turns out, for the moduli functor of smooth curves of genus g, such locally constant, but non-constant families do in fact exist, which means that the functor $\mathscr{M}_g$ is *not* representable. Indeed, given a curve C_0 which admits non-trivial automorphisms, one can produce such examples by gluing pieces of the form $C_0 \times_{\operatorname{Spec} k} U_i$ along "twisted" identification maps, for a suitable open cover $X = \bigcup U_i$.

However, not all is lost and there are several approaches to deal with this situation. The three methods which we mention are closely related.

The most powerful and technically most demanding way is to replace schemes by the more general concept of algebraic stacks (originally due to Grothendieck, once again). From the functorial point of view, the key idea is to replace functors from the category of schemes to the category of sets by "functors" which attach to each scheme a groupoid rather than a set, and to each scheme morphism a functor between groupoids. A groupoid is a category in which every morphism is an isomorphism. Replacing set-valued functors by groupoid-valued "functors" allows to deal with objects with automorphisms when considering moduli functors. Of course, similarly as only very few functors from schemes to sets are well-behaved (representable), suitable conditions have to be imposed on a functor

from sets to groupoids before one would call it an algebraic stack. In geometric terms, an essential feature of stacks is that it is easier to construct quotients by group actions (or more general equivalence relations) in the world of stacks. See the papers by Edidin [19], and Fantechi [21] for short surveys, and the Stacks Project [52] initiated by A. J. de Jong for a comprehensive — currently at more than 6,000 pages, and counting — treatment, starting from zero.

The second approach to attach a scheme to a moduli functor $\mathscr{M}$ is to look for a scheme M with a morphism $\mathscr{M} \to h_M$ of functors such that $\mathscr{M}(\operatorname{Spec} K) \to h_M(\operatorname{Spec} K)$ is a bijection for all algebraically closed fields K (extending the base field), and which satisfies a weaker property for S-valued points, which we do not spell out, but which characterizes it uniquely; see Mumford's book [40], Def. 5.6. This is called a *coarse moduli space* (whereas by a *fine moduli space* one means a scheme representing a given moduli functor in the sense that (4) holds for all S, functorially in S). An example is the modular curve $Y(1)$ mentioned above. Also for the moduli functor $\mathscr{M}_g$ of curves of genus g, a coarse moduli space exists.

For this article, let us consider yet another method to avoid the problem mentioned above: We can *rigidify* the moduli problem. By this we mean that we modify the moduli problem slightly so that the objects parameterized by the modified moduli functor do not have automorphisms. In the case of curves this can be achieved as follows:

Definition 5.1 Fix integers $g \geq 0$, $n \geq 0$. Let S be a scheme. An n-pointed curve of genus g over S is a smooth projective morphism $f\colon C \to S$ of schemes together with n sections $p_i\colon S \to C$ (i.e., morphisms p_i satisfying $f \circ p_i = \mathrm{id}_S$ for all i) such that for every $s \in S$, the fiber $C_s := f^{-1}(s) := C \times_S \operatorname{Spec} \kappa(s)$ is a curve of genus g over $\kappa(s)$, and such that the images of the p_i are pairwise disjoint.

We then define, for fixed g and n, the functor

$$\mathscr{M}_{g,n}\colon (\text{Schemes}) \to (\text{Sets})$$

by setting

$$S \mapsto \mathscr{M}_{g,n}(S) := \{(C, p_1, \ldots, p_n) \text{ an } n\text{-pointed curve}/S\}/\cong .$$

Here, families (C, p_i) and (C', p_i') over S are isomorphic if there exists an isomorphism $f\colon C \to C'$ of S-schemes, such that $f \circ p_i = p_i'$ for all i.

Theorem 5.2 (See [2], Ch. XII[9]) *For n sufficiently large (depending on g), the functor $\mathscr{M}_{g,n}$ is representable.*

The schemes $\mathscr{M}_{g,n}$ (and their compactifications) are interesting geometric objects and have been studied intensely.

5.2 Deformation theory

We briefly mention another aspect of the theory of moduli spaces where the functorial point of view is combined nicely with the use of non-reduced rings: Deformation theory. The setup here is that we fix an object (a pointed curve C_0, say) over an algebraically closed field k, and want to understand how it "varies in families", i.e., we want to study morphisms

[9] Although all the ingredients are in the quoted book, at least over $\mathbb{C}$, it seems that the result in the form given here is not explicitly stated. See the discussion [36] for a sketch of how to conclude.

$f\colon C \to S$ together with a point $s_0 \in S$ such that $\kappa(s_0) \cong k$ and $f^{-1}(s_0) \cong C_0$. More precisely, we are interested in the behavior of the fibers of f at points *close to* s_0.

Thinking in terms of equations, we would start with a k-scheme, say a closed subscheme of some $\mathbb{A}^n_k$, given by polynomial equations. To let this vary in a family (inside $\mathbb{A}^n_S$), we could add a further parameter t (or several ones ...) which perturbs the equation, and gives back the original equation when setting $t = 0$. For example,consider the equation

$$Y^2 - X^3 - X^2 + tX^2 + tX = 0.$$

It defines a closed subscheme $Z \subset \mathbb{A}^3_k = \operatorname{Spec} k[X,Y,t]$. Setting $t = 0$ (equivalently: passing to the fiber over the origin of the projection $Z \to \operatorname{Spec} k[t] = \mathbb{A}^1_k$), we obtain $Z_0 = V(Y^2 - X^3 - X^2)$, the first two of the curves pictured (over $\mathbb{R}$) in Section 2. Setting $t = 1$, we obtain the curve $V(Y^2 - X^3 + X)$, the affine part of an elliptic curve, also pictured above. Since smoothness of the fibers is an open condition on the target $\mathbb{A}^1_k$ of our map, only finitely many fibers are non-smooth, and in particular, all fibers in a suitable open neighborhood of the origin are smooth. While this is a concrete interpretation, it has obvious restrictions: Perturbing the equations involves a choice of describing equations of the original object, and a choice of where to put the parameter, so that we might obtain only special types of deformations. On the other hand, if we want to deform something inside a fixed class of objects (curves; elliptic curves; etc.) we must check whether the equations, when specialized at $t \neq 0$, still define an object that belongs to the given class.

Let us interpret deformations in terms of moduli spaces. To start with, we will take the above remark, that we are interested in the fibers over points close to s_0, more seriously, and implement it in the spirit of EGA. Viewing it "only" topologically is not optimal: Once again, it turns out that the Zariski topology is too coarse. On the other hand, it is very fruitful to study the behavior for points "infinitesimally close" to s_0. This allows us to restrict to the case that $S = \operatorname{Spec} A$, where A is a "local Artin ring", i.e., A is a noetherian ring with a unique prime ideal — the prime ideal corresponding to the point s_0. A simple example is $k[t]/(t^n)$: In terms of the previous paragraph it would mean that the new parameter t is nilpotent. Topologically, then the fiber over s_0 — the one we started with —is the only fiber of the morphism f. Nevertheless additional information is contained in families over local Arting rings, and EGA provides the machinery to extract this information. Let us elaborate a little more on this; for details see [26].

Let us assume that we had already proved the existence of a moduli space $\mathscr{M}$ of the objects we are interested in. Fixing C_0 over k is then the same as fixing a k-valued point $f_0\colon \operatorname{Spec} k \to \mathscr{M}$ of the moduli space. For $S = \operatorname{Spec} A$, A a local Artin ring, a family of objects deforming C_0 is the same as a morphism $f\colon S \to \mathscr{M}$ whose topological image is equal to the one point c_0 which is the (topological) image of f_0. Let $\mathscr{O} = \mathscr{O}_{\mathscr{M},c_0}$ be the local ring of $\mathscr{M}$ at c_0. We obtain a morphism $\operatorname{Spec} \mathscr{O} \to \mathscr{M}$ (cf. Example 3.12 1.), and since A is a local ring, every morphism $\operatorname{Spec} A \to \mathscr{M}$ with image $\{c_0\}$ factors through $\operatorname{Spec} A \to \operatorname{Spec} \mathscr{O}$. This means that the local ring $\mathscr{O}$ (together with the restriction of the universal object over $\mathscr{M}$ to $\operatorname{Spec} \mathscr{O}$) contains all the information about the infinitesimal deformations of C_0. (In fact, we can even pass to the "completion" of $\mathscr{O}$.)

Conversely, and this is the direction which is typically more useful, good knowledge about the deformations of C_0 gives us information about the completion of the local ring of $\mathscr{M}$ at c_0. For example, from a good understanding of the deformations of C_0 we can conclude whether $\mathscr{M}$ is smooth at c_0.

Even if we do not yet know about the existence of a moduli space (i.e., have not proved the representability of the moduli functor), we could study deformations of individual objects in order to find out something about the local rings that would have to occur in the

moduli space. On the one hand, this is sometimes a path to proving the existence of moduli spaces (cf. the work of M. Artin, see, e.g., [3]). This point of view is closely related to the notion of *formal scheme* developed in [EGA I] §10, and their algebraizability, [EGA III] 5.4. On the other hand, this method often gives interesting information in those cases where a moduli space is known not to exist.

5.3 Modular curves

We now come back to the parameter spaces of elliptic curves, or *modular curves*, of which we have seen an avatar as Riemann surfaces.

To define the moduli functor, we need to define the notion of *elliptic curve over a scheme* S (to be viewed as a family of elliptic curves indexed by the points of S). We start by translating the definition we gave in the classical setting (over an algebraically closed field) into the language of schemes, at the same time dropping the hypothesis that the field be algebraically closed.

Definition 5.3 Let k be a field. A proper k-scheme E together with a point $O \in E(k)$ is called an *elliptic curve*, if it satisfies the following equivalent conditions:

1. E is smooth, of dimension 1 and of genus 1,
2. E can be equipped with a structure of commutative group scheme over k (Def. 4.15),
3. E is isomorphic to a smooth curve $V_+(f) \subset \mathbb{P}^2_k$, where f is a cubic homogeneous polynomial,
4. (if $\mathrm{char}(k) \neq 2,3$) E is isomorphic to a curve $V_+(f) \subset \mathbb{P}^2_k$, where f is a cubic homogeneous polynomial of the form

$$f = Y^2Z - X^3 - aXZ^2 - bZ^3$$

such that the polynomial $X^3 + aX + b$ is separable, i.e., $4a^3 + 27b^2 \neq 0$.

We have listed the fourth point above to make the connection with the definition we gave in the beginning. For fields of characteristic 2 or 3, a similar, slightly more complicated, "normal form" can be given. Cubic equations of this special form are called *in Weierstrass form*. But note that in either case different such Weierstrass equations can give rise to isomorphic elliptic curves. In the second characterization above, the commutativity of the group law is in fact automatic. Furthermore, the group law can be chosen so that the point O is its neutral element, and then is unique.

Now we can define families of elliptic curves, or in other words: elliptic curves over a general base scheme S. A reference for this and the theory of moduli spaces of elliptic curves are the books [50], [51] by Silverman and the book [30] by Katz and Mazur.

Definition 5.4 Let S be a scheme. An *elliptic curve over* S is a proper smooth morphism $f\colon E \to S$, together with a section $O\colon S \to E$ such that for every $s \in S$, the fiber E_s is an elliptic curve over the field $\kappa(s)$.

Proposition 5.5 *Let S be a scheme, and let E/S be an elliptic curve with section $O\colon S \to E$. Then E can be equipped, in a unique way, with a structure of commutative group scheme over S such that O is the neutral element of the group structure.*

Elliptic curves admit non-trivial automorphisms (at least there is always the automorphism $x \mapsto -x$ induced by the group structure), so in this case we also will add "level structure" to our moduli problem:

For $N \in \mathbb{Z}$, we have the "multiplication by N" morphism $[N]\colon E \to E$, and we denote by $E[N]$ its kernel (in the scheme theoretic sense, i.e., it is the fiber product $E \times_{[N],E,O} S$). By formal reasons, this is again a group scheme over S.

Definition 5.6 Let S be a scheme, and let E/S be an elliptic curve. Let $N \geq 3$ be a natural number. A *level N structure on E* is an isomorphism

$$\alpha : \mathbb{Z}/N\mathbb{Z}^2 \to E[N]$$

of group schemes over S.

Note that it is not clear whether given an elliptic curve E/S and an integer N, a level N structure exists. On the other hand, if $S = \operatorname{Spec}\mathbb{C}$, then we can identify $E(\mathbb{C}) = \mathbb{C}/\Lambda$ as abelian groups, for some lattice $\Lambda \subset \mathbb{C}$, and in this case it is immediate that $E[N] = \frac{1}{N}\Lambda/\Lambda \cong \mathbb{Z}/N\mathbb{Z}^2$. More generally, let $S = \operatorname{Spec} k$ for k an algebraically closed field of characteristic 0 or positive but not dividing N. Then one can show that $E[N] \cong \mathbb{Z}/N\mathbb{Z}^2$, so a level N structure exists. Starting from this, one can show that for a scheme S such that N is a unit in the ring $\Gamma(S, \mathcal{O}_S)$ and an elliptic curve E/S, there exists an étale morphism $S' \to S$, i.e., the morphism is smooth and has 0-dimensional fibers, such that on the elliptic curve $E \times_S S'$ over S' a level N structure exists. In contrast, if $S = \operatorname{Spec} k$ for a field of positive characteristic dividing N, one can show that a level N structure never exists.

We now fix an integer $N \geq 3$ and define a functor $Y(N) : (\text{Schemes}) \to (\text{Sets})$ by

$$S \mapsto Y(N)(S) := \{(E, \alpha); E/S \text{ an elliptic curve}, \alpha \text{ a level-}N\text{-structure on } E\}/\cong$$

(The notion of morphism between pairs (E, α), (E', α') is defined in the obvious way, so we obtain a notion of isomorphism, and can pass to isomorphism classes.)

One then shows

Proposition 5.7 *The functor $Y(N)$ is representable by a scheme, and the fibers $Y(N) \times_{\operatorname{Spec}\mathbb{Z}} \mathbb{Q}$, and $Y(N) \times_{\operatorname{Spec}\mathbb{Z}} \mathbb{F}_p$ for p a prime not dividing N, are one-dimensional.*

These modular curves are useful when studying arithmetic properties of elliptic curves. One example is Deligne's proof [12] that the Weil conjectures imply the Ramanujan conjecture which asserts that the coefficients $\tau(n)$ defined by expanding the following infinite product

$$D(q) := q\prod_{n\geq 1}(1-q^n)^{24} =: \sum_{n\geq 0}\tau(n)q^n$$

(which we can consider as a formal power series in q) satisfy the inequality

$$|\tau(p)| \leq 2p^{11/2} \quad \text{for every prime } p.$$

Very roughly, the idea is to relate these coefficients to the trace of Frobenius on certain cohomology groups, as in Grothendieck's approach to the Weil conjectures via "étale cohomology", and then to use the Weil conjectures to obtain estimates on this trace. Since the function $z \mapsto \Delta(z) := D(q^{2\pi i z})$ on the complex upper half-plane is a so-called modular form, it is known that the coefficients $\tau(n)$ can be expressed as eigenvalues of certain operators (Hecke operators) on the cohomology of the modular curve $Y(N) \times_{\operatorname{Spec}\mathbb{Z}} \mathbb{C}$ over $\mathbb{C}$. By a theorem in étale cohomology, for primes p not dividing N, this cohomology over $\mathbb{C}$ can be

identified with the cohomology of $Y(N) \times_{\operatorname{Spec}\mathbb{Z}} \operatorname{Spec}\mathbb{F}$, and since the Hecke operators can be defined in geometric terms, they can be described directly on the fiber over $\mathbb{F}$. As before, $\mathbb{F}$ denotes an algebraic closure of $\mathbb{F}_p$. In fact, it turns out that they are much easier to understand in that case, and are closely related to the Frobenius morphism, thus allowing for the desired connection.

6 Further topics in EGA

6.1 EGA III – Cohomology

Another important topic developed in EGA, Ch. III [EGA III], is the cohomology of coherent sheaves. Sheaves and sheaf cohomology had been introduced by J. Leray in the context of algebraic topology. These methods were soon after applied by Cartan and others to solve several deep problems in complex geometry. In 1955, Serre took the bold step of considering the cohomology of (coherent) sheaves on algebraic varieties with the Zariski topology; he showed that analogues of Cartan's famous theorems A and B for Stein spaces are true for affine schemes.

So what is the point of cohomology? Rather than giving precise statements here, we give a few answers to this question on a fairly abstract level.

- Cohomology theories attach algebraic invariants (groups, vector spaces) to geometric objects. For example, computing the singular homology of $\mathbb{R}^n \setminus \{0\}$, we see that $\mathbb{R}^m \setminus \{0\}$ and $\mathbb{R}^n \setminus \{0\}$ (and hence $\mathbb{R}^m$ and $\mathbb{R}^n$) are not homeomorphic for $m \neq n$.
- The main topic of [EGA III] is sheaf cohomology. It serves to describe the difference between constructing sections of a sheaf, with certain properties, locally, and constructing them globally.
  In the context of Riemann surfaces, the Mittag-Leffler problem is a typical example: Given a discrete set of points on a Riemann surface X, and for each point a principal part, does there exist a meromorphic function on X which at each point has the specified principal part? Locally the problem is trivial (in fact, a local solution is given to start with), but the question of existence of a global solution is non-trivial. The analogue in higher dimension is called the Cousin problem.
- A general framework for many cohomology theories is the problem of describing in which way a certain functor fails to be exact. For instance, the global section functor

$$\Gamma(X,-)\colon \mathscr{F} \mapsto \Gamma(X,\mathscr{F}) := \mathscr{F}(X)$$

  for sheaves of abelian groups on a topological space X is left exact, but not exact: If

$$0 \to \mathscr{F} \to \mathscr{G} \to \mathscr{H} \to 0$$

  is an exact sequence[10] of sheaves of abelian groups, then the sequence

$$0 \to \Gamma(X,\mathscr{F}) \to \Gamma(X,\mathscr{G}) \to \Gamma(X,\mathscr{H})$$

[10] The category of sheaves of abelian groups on a topological space is abelian, so kernels and images exist and we obtain a notion of exact sequence. More explicitly, a sequence of sheaves on a space X is exact if and only if for every $x \in X$ the induced sequence of stalks is exact.

is exact, but the arrow on the right is not surjective in general. The *cohomology groups* $H^i(X,-)$ give us an exact sequence, called the *long exact cohomology sequence*

$$\begin{aligned}0 \to &\Gamma(X,\mathscr{F}) \to \Gamma(X,\mathscr{G}) \to \Gamma(X,\mathscr{H}) \\ \to &H^1(X,\mathscr{F}) \to H^1(X,\mathscr{G}) \to H^1(X,\mathscr{H}) \\ \to &H^2(X,\mathscr{F}) \to H^2(X,\mathscr{G}) \to H^2(X,\mathscr{H}) \to \cdots\end{aligned}$$

which can be viewed as a precise description in which way the functor $\Gamma(X,-)$ fails to be right exact. The functors $H^i(X,-)$ are called the *right derived functors* of $\Gamma(X,-)$.

The notion of derived functor was also developed by Grothendieck [24]. Later, Grothendieck's student J. L. Verdier, introduced the notion of *derived category*, a more abstract and much more powerful approach. For [EGA III], this notion did not become available in time, however.

One of the most important results in [EGA III] is the coherence of higher direct images of coherent sheaves under proper morphisms (loc. cit. §3). We have not defined the notion of coherent sheaf ([EGA I] Ch. 0, (5.3.1)) so we will not give a precise statement. A special case is that for a projective k-scheme X, k a field, the cohomology spaces $H^i(X,\mathscr{O}_X)$ are finite-dimensional k-vector spaces. The statement is analogous to the corresponding result in complex analysis which has been proved by Grauert in 1960. In contrast, for affine $X = \operatorname{Spec} R$, $\Gamma(X,\mathscr{O}_X) = R$, and Serre proved that $H^i(X,\mathscr{O}_X) = 0$ for all $i > 0$, [49], [EGA III] Thm. 1.3.1.

6.2 EGA IV – Local properties of schemes and morphisms

The fourth chapter [EGA IV] of EGA, titled *Étude locale des schémas et des morphismes de schémas*, *Local study of schemes and morphisms of schemes*, consists of four parts and with about 1100 pages is the longest of the four chapters. Many of the results given there can be viewed as belonging to commutative algebra. Of course, this is to be expected since "by definition" commutative algebra is the theory of affine schemes. Important topics are the notion of smoothness, and related notions (derivations, differentials, regular rings), flat morphisms and their fibers, dimension theory, and techniques of reduction to the noetherian case. All of these topics are technically quite demanding, so that we forego a more detailed treatment in this note.

Example 6.1 Using the difficult results on dimension theory, we can sketch an EGA powered[11] proof of the above-mentioned theorem (Example 2.2) that every smooth cubic surface in $\mathbb{P}^3_k$, k an algebraically closed field of characteristic 0, contains precisely 27 lines of $\mathbb{P}^3_k$. As it turns out, the key step is to prove that every (smooth) cubic surface contains at least one line.

A cubic surface is given by a homogeneous polynomial in 4 variables of degree 3, i.e., by the 20 coefficients of such a polynomial (which must not all vanish simultaneously). Two polynomials define the same surface if and only if they differ by a unit in k. We see that the entirety of cubic surfaces is parameterized by $P := \mathbb{P}^{19}(k)$. (Here it is easy to find a parameter space since we do not pass to isomorphism classes, but rather want to fix the

[11] This is not to say that the proof is given in EGA — examples and applications of the theoretical machinery are almost non-existent there.

embedding into $\mathbb{P}^3_k$.) Of course, not all those cubic surfaces are smooth, but for the moment we include the non-smooth ones in our considerations.

Next, recall the Grassmann variety (Section 4.4). Specifically, let $G := \mathrm{Grass}_{2,4}$ be the variety of planes in k^4. Equivalently, we can view a plane in k^4 as a line in $\mathbb{P}^3(k)$; this is the point of view used below.

Let

$$Z(k) := \{(\ell, f) \in G(k) \times P(k);\ \ell \subset V_+(f)\},$$

the set of pairs (ℓ, f) consisting of a line in $\mathbb{P}^3_k$ and a cubic polynomial f such that the line ℓ is contained in the cubic surface defined by f. The suggestive notation indicates that this set is in fact the set of k-valued points of a closed subscheme $Z \subset G \times_{\mathrm{Spec}\, k} P$. The projections give us morphisms

$$G \xleftarrow{\alpha} Z \xrightarrow{\beta} P$$

Showing that every cubic surface contains a line amounts to showing that β is surjective.

First, look at the map α: It is easy to see that the fibers of α are all isomorphic, and have dimension 15. Now dimension theory tells us that $\dim Z = \dim G + 15 = 19$. So Z has the same dimension as P.

The morphism β is proper because G is proper over k and Z is closed in the product $G \times P$, so the image of β is closed. If β were not surjective, then the image would be a proper closed subscheme of P, and hence would have dimension $< \dim P = \dim Z$. Another theorem of dimension theory then yields that all non-empty fibers of β have dimension ≥ 1. At this point it is enough to show the existence of *one* cubic surface which contains a line, and contains only finitely many lines. Since we can just pick one surface to our liking to check this, this is an easy task. For further details see [6], [23] Ch. 16.

7 Some results building on EGA

7.1 The proof of the Weil Conjectures

Let us briefly come back to the Weil conjectures which we discussed in Section 2.7. With the notion of schemes over arbitrary (i.e., not necessarily algebraically closed) fields, we can describe the setup a little more cleanly: Let X be a smooth projective scheme over the finite field $\mathbb{F}_q$. For $m \geq 1$, we denote by N_m the number of $\mathbb{F}_q$-valued points of X (Example 4.1): $N_m := \#X(\mathbb{F}_q)$. From the N_m, we define the zeta function of X as in (2) above.

We fix an algebraic closure $\mathbb{F}$ of $\mathbb{F}_q$. The Frobenius automorphism $x \mapsto x^q$ on $\mathbb{F}$ induces the "relative Frobenius morphism" $F\colon \mathbb{A}^n(\mathbb{F}) \to \mathbb{A}^n(\mathbb{F})$, $(x_i)_i \mapsto (x_i^q)_i$. If $Z \subseteq \mathbb{A}^n_{\mathbb{F}_q}$ is a closed subscheme, then F restricts to a morphism $Z_{\mathbb{F}} \to Z_{\mathbb{F}}$, where $Z_{\mathbb{F}} := Z \times_{\mathrm{Spec}\, \mathbb{F}_q} \mathrm{Spec}\, \mathbb{F}$ is the base change. The set of fixed points is naturally identified with $Z(\mathbb{F}_q)$. (Note that although F induces a bijection on $\mathbb{A}^n_{\mathbb{F}_q}(\mathbb{F})$, the morphism F is not an isomorphism, because the inverse map is not given by polynomials.)

Let us denote by $|X|$ the set of closed points of the scheme X. Then it is easy to see that we can write the zeta function as an "Euler product"

$$Z(X,T) = \prod_{x \in |X|} (1 - T^{[\kappa(x):\mathbb{F}_q]})^{-1}.$$

Recall that we defined T as q^{-s} for a complex variable s, and $q^{[\kappa(x):\mathbb{F}_q]} = \#\kappa(x)$. Therefore, this formula is the direct analogue of the Euler product expansion

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} = \prod_{x\in|\operatorname{Spec}\mathbb{Z}|} (1-(\#\kappa(x))^{-s})^{-1}$$

of the Riemann ζ-function, where we write the set of prime numbers as the set $|\operatorname{Spec}\mathbb{Z}|$ of closed points of $\operatorname{Spec}\mathbb{Z}$ in order to emphasize the similarity.

The rationality of the zeta function was first proved by B. Dwork in 1960, using p-adic methods. By 1964, the methods invented by Grothendieck and developed by him with M. Artin and J.-L. Verdier (étale cohomology and the Lefschetz trace formula) had become sufficiently mature to prove the rationality of the zeta function and its functional equation. This follows up on the general idea of Weil that one should try to construct a suitable cohomology theory. With the Lefschetz trace formula, the number of fix points of a map can be computed as a trace on cohomology. This principle can be used to describe the number of $\mathbb{F}_q$-valued points of a scheme X: For $X = \operatorname{Spec}\mathbb{F}_p[X_1,\dots,X_n]/(f_1,\dots,f_m)$ (and similarly in more general cases) we can identify $X(\mathbb{F}_q)$ with the set of fixed points in $V(f_1,\dots,f_m)\subset\mathbb{F}^n$ of the Frobenius F, as mentioned above. Since only finitely many cohomology groups are non-zero, the rationality of the zeta function follows directly from the Lefschetz fixed point formula. The functional equation follows from Poincaré duality for étale cohomology.

At this point, it remained to prove the third part of the Weil conjectures, the "Riemann hypothesis". Grothendieck had outlined a path to proving it as a consequence of a number of conjectures which came to be known as the standard conjectures. However, as of today, those conjectures are still open to a large part.

The first proof of the "Riemann hypothesis" was given by Deligne in 1974. By now there are also several other proofs and further extensions of this part of the Weil conjectures. In addition to the original papers [13], [14], see [22], [31] for more detailed accounts in a form accessible with a good basic knowledge of algebraic geometry. See [25] App. C and Oort's article [43] for surveys.

It is quite amazing what one can get out of cohomology theories such as étale cohomology. In the meantime, several other cohomology theories have been developed and/or studied in the context of algebraic geometry (crystalline, de Rham, ...), and have been put to good use in fascinating ways. This also gave a way to apply algebro-geometric methods to problems in representation theory (such as the proof of the Kazhdan-Lusztig conjectures; for recent results in this field see Williamson's article [58] and the references there). The search for even more powerful cohomology theories continuous with exciting developments in the last few years (and more to come?), see Scholze's report [48].

While the Weil conjectures state a certain regularity for the numbers of points over $\mathbb{F}_{q^m}$ of a smooth projective variety over the finite field $\mathbb{F}_q$, one can ask a similar question for a scheme X over $\operatorname{Spec}Z$. By forming the fiber product $X\times_{\operatorname{Spec}\mathbb{Z}}\operatorname{Spec}\mathbb{F}_p$, we obtain a scheme over the finite field $\mathbb{F}_p$, and can count its number of points over extension fields of $\mathbb{F}_p$, and combining these for all p, form the Hasse-Weil zeta function of X. Again, one expects that this zeta function has "nice properties". The Langlands program makes more precise predictions, but in this generality, many problems are not yet well understood. (See Section 7.3 for the case of elliptic curves.)

7.2 Mori's Bend and Break

As another spectacular application of methods which became available only through Grothendieck's algebraic geometry, we mention the results by S. Mori [39] who used characteristic p methods in order to prove a conjecture by R. Hartshorne about projective varieties over the complex numbers, and went on to apply this method to obtain far-reaching results about algebraic varieties of dimension 3.

Let k be an algebraically closed field. Hartshorne's conjecture is a statement to the effect that certain algebraic varieties (namely connected smooth projective k-schemes with "ample tangent bundle") are necessarily isomorphic to projective space $\mathbb{P}^n_k$. The key step is to show sufficient conditions under which a proper k-scheme X contains "rational curves", i.e., when there exist scheme morphisms $\mathbb{P}^1_k \to X$ with finite fibers. The image of such a morphism is then called a rational curve. The existence of such curves is easier to show if k has positive characteristic, because one can then make use of the Frobenius endomorphism.

To get back to characteristic 0 from the positive characteristic case, we start with X over an algebraically closed k of characteristic 0. There exists a subring $A \subset k$ which is a finitely generated $\mathbb{Z}$-algebra, together with an A-scheme $\mathfrak{X}$ such that the base change $\mathfrak{X} \times_{\operatorname{Spec} A} \operatorname{Spec} k$ is isomorphic to X. The existence of such an A is clear, because in the (finitely many) defining equations of X inside some projective space, only finitely many elements of k occur. In the actual proof, one will want to choose A with some additional properties. We can then compare X with other fibers of the family $\mathfrak{X}$ over $\operatorname{Spec} A$, in particular, with those over residue class fields of A of positive characteristic. Mori shows that the existence of sufficiently many rational curves of small degree (think, roughly: defined by polynomials of small degree) in the positive characteristic fibers implies the existence of rational curves in the fiber X over k.

The above argument using the Frobenius morphism shows that there exist rational curves in positive characteristic, but we actually need to find such curves of small degree. Here the so-called "bend-and-break" method comes in: Applying methods of deformation theory, Mori proves that in the case of large degree, the curve sits in a family of rational curves n X and that this family also contains curves which are a union of several rational curves, necessarily of smaller degree. This is called "bend and break": If we bend the curve, i.e., move it in that family, it must eventually break up as a union of curves. Hence one concludes that there exist sufficiently many rational curves of small degree to ensure the existence of rational curves in characteristic 0.

7.3 Elliptic curves, continued

In Section 2, we have mentioned elliptic curves and the group structure on them. These curves also encode deep arithmetic information: Consider an elliptic curve E over the rational numbers $\mathbb{Q}$ (or over a number field K, i.e., a finite extension field of $\mathbb{Q}$). Explicitly, this means that E is defined by a cubic equation in Weierstra form

$$E:\ y^2 = x^3 + ax + b \quad \text{with } a,b \in K,$$

where the right hand side has only simple zeros, and where once again we write down only the affine part of E, but implicitly understand E as a smooth projective curve $E \subset \mathbb{P}^2_k$. So for the set of solutions in any extension field L of K, we have

$$E(L) = \{(x,y) \in L^2;\ y^2 = x^3 + ax + b\} \sqcup \{O\}.$$

It is easy to check that the description of the group law can be carried out over K, i.e., E is a group scheme over K. Concretely, we obtain that $E(K)$ is an abelian group with neutral element O, and if L/K is a field extension, then $E(K) \subseteq E(L)$ is a subgroup.

The Mordell-Weil Theorem states that the abelian group $E(K)$ is a finitely generated abelian group, i.e., isomorphic to a product $\mathbb{Z}^r \times G$ with G a finite abelian group. The integer $r =: r(E)$ is called the (algebraic) rank of E. There are still many open questions about ranks of elliptic curve, for instance: Does every non-negative integer occur as the rank of an elliptic curve? Given an elliptic curve, by a cubic equation, say, how to determine its rank?

To simplify the discussion, let us specialize to the case that E is defined over $\mathbb{Q}$. By a change of coordinates, we can replace E by an isomorphic elliptic curve which is given by an equation with integer coefficients, and this equation defines a closed subscheme $\mathscr{E} \subset \mathbb{P}^2_{\mathbb{Z}}$. In particular, for each prime number p, we can consider the base change $\mathscr{E}_p := \mathscr{E} \times_{\operatorname{Spec}\mathbb{Z}} \mathbb{F}_p$, a closed subscheme of $\mathbb{P}^2_{\mathbb{F}_p}$. For all but finitely many p, this is an elliptic curve over $\mathbb{F}_p$: The smoothness over the generic point of $\operatorname{Spec}\mathbb{Z}$, i.e., the smoothness of E over $\mathbb{Q}$, extends to an open subset of $\operatorname{Spec}\mathbb{Z}$. On the other hand, we can clearly not expect that this is true for all p, because the reduction of a separable polynomial in $\mathbb{Z}[X]$ might have multiple zeros in $\mathbb{F}_p$. In fact, one can show that there does not exist any elliptic curve over $\mathbb{Z}$ (in the sense of Def. 5.4).

Whenever $\mathscr{E}_p$ is an elliptic curve, we can count the number of points over $\mathbb{F}_p$ (and its finite extension fields), and we have the zeta function as discussed above. As we have stated above (Example 2.5), the only important piece of information given by the zeta function is the number of points of $\mathscr{E}_p$ over the ground field $\mathbb{F}_p$. It is useful to combine these numbers for all the different primes, and this is usually done by defining the (incomplete[12]) L-function of E over $\mathbb{Q}$:

$$L(E/\mathbb{Q},s) := \prod_p \frac{1}{1-(p+1-\#\mathscr{E}_p(\mathbb{F}_p))p^{-s}+p^{1-2s}},$$

where the product ranges over all p such that $\mathscr{E}_p$ is an elliptic curve. We view this as a function in the complex variable s. The product converges if the real part of s is $> \frac{3}{2}$, and we obtain a holomorphic function in this region of the complex plane.

Theorem 7.1 (Wiles, Taylor, ...) *The function $L(E/\mathbb{Q},s)$ extends to a holomorphic function on the entire complex plane.*

This theorem is a consequence of the more precise statement (conjectured by Y. Taniyama, G. Shimura, A. Weil) that every elliptic curve over $\mathbb{Q}$ is *modular*, which entails very strong "symmetry conditions" on the L-function of E. By previous work of G. Frey and K. Ribet, the modularity of elliptic curves yields a proof of Fermat's Last Theorem. The proof of the modularity theorem relies on the combination of many advanced techniques in algebraic geometry. Moduli spaces play a prominent role: As the terminology indicates, the property of being modular is related to the modular curves we discussed above; it is equivalent to the existence of a non-constant morphism $X_0(N) \to E$, where $X_0(N)$ is a variant of the modular curves $Y(N)$ which we introduced above. One of the important points of the proof uses the "functorial point of view", in particular the formalism of deformation theory,

[12] The "incomplete" refers to the fact that we omit the primes where $\mathscr{E}_p$ is not an elliptic curve from the discussion; incorporating them in a suitable way leads to a more elegant theory. Even for the incomplete L-function, our discussion is a little over-simplified: To be consistent with the usual terminology, one should be a little more careful with the choice of the equation for $\mathscr{E}$ over $\mathbb{Z}$. Nevertheless, our definition is good enough for the needs of the following discussion. Generalizations of this construction are available for elliptic curves over general number fields.

in a non-geometric setting: Wiles studies deformation functors of "Galois representations" and the rings representing these functors. See the proceedings volume [11] for background material and further references.

It is conjectured that the modularity, and in particular the existence of a holomorphic continuation of the L-function also hold for elliptic curves over arbitrary number fields. By now, this is known for all so-called CM fields K, see [48] Thm. 5.3.

As mentioned above, one would like to understand the ranks of the finitely generated abelian groups $E(\mathbb{Q})$. With the L-function at hand, we can state the Conjecture of Birch and Swinnerton-Dyer, one of the Clay Millenium Problems, see [57]:

Conjecture 7.2 (Birch, Swinnerton-Dyer) Let E be an elliptic curve over $\mathbb{Q}$. Then the rank of E is equal to the order of the zero of the L-function $L(E/\mathbb{Q},s)$ at $s=1$.

Note that the conjecture talks about the value of the L-function at $s=1$, a point which is not covered by the defining expression as an infinite product above, but requires the analytic continuation. In particular, the conjecture says that $E(\mathbb{Q})$ is finite whenever $L(E/\mathbb{Q},1)\neq 0$. This statement has been proved by B. Gross, D. Zagier and V. Kolyvagin.

As a side note, and taking the occasion to mention another famous theorem that heavily relies on EGA style algebraic geometry: For a curve C over a number field K of genus ≥ 2, the set $C(K)$ is finite. This was conjectured by L. Mordell and proved by G. Faltings [20]. See the proceedings volume [10] for an English translation of Faltings's paper and for background material bridging the gap between EGA and the proof by Faltings.

Many other questions are still open, e.g.: Are there elliptic curves with arbitrarily high rank? No elliptic curve with rank > 28 is currently known.

Finally, let us mention that the groups $E(K)$ for K a finite field, and $a,b\in K$ defining an elliptic curve, give rise to several applications to real life: elliptic curve cryptography; factorization of large integers via elliptic curves; the elliptic curve primality test. See Washington's book [54] and the references given there.

8 Miscellaneous remarks and further reading

We conclude this note with some remarks. The presence of a foundational text of the size, and meticulous and detailed style of writing of EGA has clearly made a large impact on the field of algebraic geometry. While there are by now numerous textbooks with introductions to algebraic geometry (e.g., [41], [25], [23]), and also the encyclopedic Stacks Project [52], EGA remains a standard reference for most of the results which it covers. Altogether for the volumes of EGA more than 2,700 citations are listed on MathSciNet.

There are basically no examples in EGA, and little to motivate the definitions. This is also reflected by the places above where references to EGA are given, and those where none are given. For instance, only the very simplest examples of representable functors beyond $\mathbb{P}^n$ are actually discussed (Grassmannians, and even that only in the new edition [EGA I_n] of the first volume). In view of this style, for beginners in most cases other paths into this subject are more suitable. Cf. the discussion [35] on MATH OVERFLOW.

In the Springer edition [EGA I_n] of the first volume of EGA (and already, with minor differences, in the original edition), there is a list of planned chapters which includes, beyond the Chapters I–IV which have actually appeared, titles for Chapters V to XII — for Chapter XII, the given title is *Cohomologie étale des schémas*, étale cohomology of schemes. For Chapter V, there exist pre-notes which were edited by P. Blass and J. Blass [18].

Many survey papers and other texts similar to this one have been written over the course of the last fifty years, mostly focusing more on the work of Grothendieck as a whole and/or his life, than on EGA. See for instance the articles by Deligne [15], Cartier [8], McLarty [37], [38], Barbieri Viale [5], Illusie and Raynaud [27], and the book [47] edited by Schneps.

Biographical information about Alexander Grothendieck can be found in the articles by Jackson [28] and Scharlau [45] and in the much more comprehensive books [46] by Scharlau. See also [4].

For the history of algebraic geometry, see for example the texts [16], [17] by Dieudonné.

Éléments de Géométrie Algébrique (EGA)

[EGA I] A. Grothendieck, rédigé avec la collaboration de J. Dieudonné, Éléments de Géométrie Algébrique. I. Le langage des schémas, Publ. math. de l'IHES **4**, no. 2, 5–228, 1960

[EGA II] A. Grothendieck, rédigé avec la collaboration de J. Dieudonné, Éléments de Géométrie Algébrique. II. Étude globale élémentaire de quelques classes de morphismes, Publ. math. de l'IHES **8**, 5–222, 1961

[EGA III] A. Grothendieck, rédigé avec la collaboration de J. Dieudonné, Éléments de Géométrie Algébrique. III. Étude cohomologique des faisceaux cohérents, Publ. math. de l'IHES **11**, 5–167, 1961; **17**, 5–91, 1963

[EGA IV] A. Grothendieck, rédigé avec la collaboration de J. Dieudonné, Éléments de Géométrie Algébrique. IV. tude locale des schmas et des morphismes de schmas, Publ. math. de l'IHES **20**, 5–259, 1964; **24**, 5–231, 1965; **28**, 5–255, 1966; **32**, 5–361, 1967

[EGA I_n] A. Grothendieck, J. Dieudonné, Éléments de Géométrie Algébrique I, Springer, 1971

Scans of the chapters of EGA published in Publ. Math. de l'IHES are available at the NUMDAM project, `www.numdam.org`.

References

1. C. Aholt, B. Sturmfels, R. Thomas, A Hilbert Scheme in Computer Vision, Canadian J. Math. **65**, 2013, 961–988.
2. E. Arbarello, M. Cornalba, P. Griffiths, Geometry of Algebraic Curves, Vol. II, Grundl. math. Wiss. **268**, Springer, 2011
3. M. Artin, Versal deformations and algebraic stacks, Invent. math. **27**, 165–189, 1974
4. Michael Artin, Allyn Jackson, David Mumford, and John Tate (coordinating editors), Alexandre Grothendieck 19282014, Notices of the AMS, Part 1: **63** no. 3, 2016, 242–255; Part 2: **63** no. 4, 2016, 401–413.
5. L. Barbieri Viale, Alexander Grothendieck: Enthusiasm and Creativity, in: C. Bartocci, R. Betti, A. Guerraggio, R. Lucchetti, eds., Mathematical Lives, Springer, 2011
6. A. Beauville, Surfaces algébriques complexes, Astérisque **54**, 1978
7. E. Carlini, M. V. Catalisano, A. Oneto, Waring loci and Strassen conjecture, Advances in Mathematics **314**, 630–662, 2017
8. P. Cartier, A mad day's work: From Grothendieck to Connes and Kontsevich. The evolution of concepts of space and symmetry, Bull. AMS (New Ser.) **38**, No. 4, 389–408, 2001
9. C. Chevalley, Les schémas, Séminaire Henri Cartan **8**, Talk no. 5, 1–6, 1955–1956
10. G. Cornell, J. Silverman, Arithmetic Geometry, Springer, 1986
11. G. Cornell, J. Silverman, G. Stevens, Modular Forms and Fermat's Last Theorem, Springer, 1997
12. P. Deligne, Formes modulaires et représentations ℓ-adiques, Sém. Bourbaki. **355** (Févr. 1969), in: Lecture Notes in Math. **179**, Springer
13. P. Deligne, La conjecture de Weil I, Publ. Math. de l'IHES **43**, 273–308, 1974
14. P. Deligne, La conjecture de Weil: II, Publ. Math. de l'IHES **52**, 137–252, 1980
15. P. Deligne, Quelques idées maîtresses de l'œuvre de A. Grothendieck, in: Matériaux pour l'histoire des mathématiques au XXe siècle: Actes du colloque à la mémoire de Jean Dieudonné, Nice 1996, SMF, 1998
16. J. Dieudonné, The Historical Development of Algebraic Geometry, Amer. Math. Monthly **79**, Issue 8, 827–866, 1972

17. J. Dieudonné, History of Algebraic Geometry, Chapman and Hall/CRC, 1985
18. P. Blass, J. Blass; Alexandre Grothendieck's EGA V, Translation and Editing of his 'prenotes', http://www.jmilne.org/math/Documents/EGA-V.pdf
19. D. Edidin, What is . . . a Stack?, Notices of the AMS **50**, no. 4, 458–459, 2003
20. G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. **73** (3), 349–366, 1983
21. B. Fantechi, Stacks for Everybody, in: C. Casacuberta, R. Miró-Roig, J. Verdera, S. Xambó-Descamps, eds., European Congress of Math., Progress in Math. **201**, Birkhäuser, 2001
22. E. Freitag, R. Kiehl, Etale Cohomology and the Weil Conjectures, Erg. Math. u. Ihrer Grenzgeb., 3. Folge, **13**, Springer, 1988
23. U. Görtz, T. Wedhorn, Algebraic Geometry I. Schemes, With Examples and Exercises, Vieweg-Teubner, 2010
24. A. Grothendieck, Sur quelques points d'algèbre homologique, Tohoku Math. J. (2) **9**, 119–221, 1957
25. R. Hartshorne, Algebraic Geometry, Graduate Texts in Math. **52**, Springer, 1977
26. R. Hartshorne, Deformation Theory, Graduate Texts in Math. **257**, Springer, 2010
27. L. Illusie, M. Raynaud, Grothendieck and Algebraic Geometry, Asia Pacific Mathematics Newsletter **5**, no. 1, 1–5, 2015
28. A. Jackson, Comme Appelé du Néant – As If Summoned from the Void: The Life of Alexandre Grothendieck, Part I: Notices AMS **51**, No. 9, 1038–1056, 2004, Part II: Notices AMS **51**, No. 10, 1196–1212, 2004
29. N. Jacobson, A topology for the set of primitive ideals in an arbitrary ring, Proc. Nat. Acad. Sci. USA, **31**, 333–338, 1945
30. N. Katz, B. Mazur, Arithmetic Moduli of Elliptic Curves, Annals of Math. Studies **108**, Princeton Univ. Press, 1985
31. R. Kiehl, R. Weissauer, Weil Conjectures, Perverse Sheaves and ℓ-adic Fourier Transform, Erg. Math. u. Ihrer Grenzgeb., 3. Folge, **42**, Springer, 2001
32. M. Lieblich, L. Van Meter, Two Hilbert Schemes in Computer Vision, Preprint arxiv:1707.09332, 2017
33. D. Lorenzini, An Invitation to Arithmetic Geometry, Grad. Studies in Math. **9**, AMS, 1996
34. S. MacLane, Categories for the working mathematician, Graduate Texts in Math. **5**, Springer, 1978
35. Math Overflow, The importance of EGA and SGA for "students of today", https://mathoverflow.net/questions/3041/the-importance-of-ega-and-sga-for-students-of-today
36. Math Overflow, Existence of fine moduli space for curves and elliptic curves, https://mathoverflow.net/a/11282
37. C. McLarty, The Rising Sea: Grothendieck on simplicity and generality, in: J. J. Gray, K. H. Parshall, eds., Episodes in the History of Modern Algebra (1800–1950), AMS, 2007
38. C. MacLarty, How Grothendieck Simplified Algebraic Geometry, Notices of the A.M.S. **63**, no. 3, 256–265, 2016
39. S. Mori, Projective manifolds with ample tangent bundle, Ann. of Math. **110**, 593–606, 1979
40. D. Mumford, J. Fogarty, F. Kirwan Geometric Invariant Theory, 3rd enl. ed., Springer, 1994
41. D. Mumford, The red book of varieties and schemes, Lecture Notes in Math. **1358**, Springer, 1988
42. D. Mumford, Can one explain schemes to biologists, http://www.dam.brown.edu/people/mumford/blog/2014/Grothendieck.html, 2014
43. F. Oort, The Weil conjectures, Nieuw Archief voor Wiskunde **5/15**, no. 3, 211–219, 2014
44. R. Penner, Moduli spaces and macromolecules, Bull. AMS **53**, 217–268, 2016
45. W. Scharlau, Wer ist Alexander Grothendieck, in: Annual Report 2006 of the Mathematics Research Institute in Oberwolfach, http://www.scharlau-online.de/DOKS/Wer%20ist%20AG.pdf, English translation: Who is Alexander Grothendieck, Notices of the AMS **55** no. 8, 2008, 930–941.
46. W. Scharlau, Wer ist Alexander Grothendieck, Teil 1: Anarchie, 3rd ed., 2011; Teil 3: Spiritualität, 2010.
47. L. Schneps (ed.), Alexandre Grothendieck: A Mathematical Portrait, International Press, 2014.
48. P. Scholze, p-adic Geometry, Report for ICM Rio de Janeiro 2018, Preprint http://www.math.uni-bonn.de/people/scholze/Rio.pdf
49. J. P. Serre, Faisceaux algébriques cohérents, The Annals of Mathematics, 2nd Ser. **61**, No. 2., 197–278, 1955
50. J. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Math. **106**, Springer, 1986
51. J. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Math. **151**, Springer, 1994
52. The Stacks Project Authors, Stacks Project, https://stacks.math.columbia.edu/, 2018
53. B. L. van der Waerden, Einführung in die algebraische Geometrie, Grundl. math. Wiss. **51**, Springer, 1939

54. L. Washington, Elliptic Curves: Number Theory and Cryptography, CRC Press, 2008
55. T. Wedhorn, Manifolds, Sheaves, and Cohomology, Springer Spektrum, 2016
56. A. Weil, Courbes Algébriques et Variétés Abéliennes, Hermann 1948.
57. A. Wiles, The Birch and Swinnerton-Dyer Conjecture, Official Problem Description, Clay Math. Inst., `http://www.claymath.org/sites/default/files/birchswin.pdf`
58. G. Williamson, Parity Sheaves and the Hecke Category, Report for ICM Rio de Janeiro 2018, Preprint `arxiv:1801.00896`
59. O. Zariski, Algebraic geometry. The fundamental ideas of abstract algebraic geometry, Proc. ICM Cambridge 1950, Vol. **2**, AMS, 77–89, 1952