Algebraic Geometry: Arithmetic Techniques

University of Toronto 2018

Michael Groechenig

Contents

1 Basic algebraic geometry

1.1 Affine varieties over algebraically closed fields

We denote by $\bar{k}$ an algebraically closed field.

Definition 1.1. *For a subset $S \subset \bar{k}[t_1, \ldots, t_n]$ we let $V(S) = \{x \in \bar{k}^n | F(x) = 0 \ \forall F \in S\}$.*

It is clear that an inclusion $S_1 \subset S_2$ yields $V(S_2) \subset V(S_1)$. Without loss of generality we can assume S to be an ideal, as shown by the following lemma.

Lemma 1.2. *Let $I \subset \bar{k}[t_1, \ldots, t_n]$ be the ideal generated by $S \subset \bar{k}[t_1, \ldots, t_n]$. Then we have $V(S) = V(I)$.*

Proof. If $x \in \bar{k}^n$ is a common zero of $f \in S$ then also for every $g \in I = (S)$. This shows $V(S) \subset V(I)$. On the other hand, the inclusion $S \subset I$ implies $V(I) \subset V(S)$. □

Corollary 1.3. *Let $S \subset \bar{k}[t_1, \ldots, t_n]$ be an arbitrary subset. Then there exists a* finite *subset $T \subset \bar{k}[t_1, \ldots, t_n]$, such that $V(S) = V(T)$.*

Proof. As above we denote by $I = (S)$ the ideal generated by S. The ring $\bar{k}[t_1, \ldots, t_n]$ is Noetherian, that is, every ideal is finitely generated (see Hilbert's basis theorem [Row06, Theorem 7.18]). We conclude that there exists a finite subset $T \subset \bar{k}[t_1, \ldots, t_n]$, such that $I = (T)$. According to Lemma 1.2 we have $V(S) = V(I) = V(T)$. □

Definition 1.4. *A subset $X \subset \bar{k}^n$ is called an* affine variety *if there exists an ideal $I \subset \bar{k}[t_1, \ldots, t_n]$, such that $X = V(I)$.*

By the corollary above, an affine variety is defined by finitely many equations.

Definition 1.5. *The subset $\bar{k}^n \subset \bar{k}^n$ is an affine variety (it corresponds to $I = \{0\}$), it will be referred to as* affine n-space *and denoted by $\mathbb{A}^n_{\bar{k}}$.*

Henceforth, we denote by $X \subset \mathbb{A}^n_{\bar{k}}$ a fixed affine variety.

Definition 1.6. *A function $f \colon X \longrightarrow \mathbb{A}^1_{\bar{k}}$ is called* regular *if there exists a polynomial $F \in \bar{k}[t_1, \ldots, t_n]$, such that for all $x \in X$ we have $f(x) = F(x)$.*

It is clear that the sum and product of two regular functions is again regular. In particular we see that the set of regular functions on X has a ring structure where the unit is given by the constant function $x \mapsto 1$.

Definition 1.7. *We denote the ring*[1] *of regular functions on X by $\mathcal{O}(X)$.*

[1] In these lecture notes the word ring exclusively refers to commutative and unital rings.

Definition 1.8. *For a subset $Z \subset \bar{k}^n$ we denote by I_Z the subset*

$$\{f \in \bar{k}[t_1, \ldots, t_n] | f(x) = 0 \ \forall x \in Z]\} \subset \bar{k}[t_1, \ldots, t_n].$$

A direct computation shows that I_Z is an ideal.

Lemma 1.9. *For an affine variety $X \subset \mathbb{A}^n_{\bar{k}}$ we have $\mathcal{O}(X) \simeq \bar{k}[t_1, \ldots, t_n]/I_X$.*

Proof. We denote by $\mathsf{Fun}(X)$ the ring of arbitrary maps $X \longrightarrow \bar{k}$. There is a ring homomorphism

$$\Phi \colon \bar{k}[t_1, \ldots, t_n] \longrightarrow \mathsf{Fun}(X)$$

which sends a polynomial $F \in \bar{k}[t_1, \ldots, t_n]$ to the map $f \colon x \mapsto F(x)$. By definition, the image of Φ is the ring of regular functions $\mathcal{O}(X)$. We conclude that $\mathcal{O}(X)$ is a quotient of $\bar{k}[t_1, \ldots, t_n]$. □

The following statement might seem obvious, but is far from being a tautology.

Proposition 1.10. *The ring of regular functions on $\mathbb{A}^n_{\bar{k}}$ is isomorphic to $\bar{k}[t_1, \ldots, t_n]$.*

We'll give the full proof below, but let's see first what goes into it. We already know that $\mathcal{O}(\mathbb{A}^n_{\bar{k}})$ is a quotient of $\bar{k}[t_1, \ldots, t_n]$. Let I be the kernel of the quotient map. We want to show that I is the zero ideal. This amounts to the assertion that non-zero polynomial induces a non-zero regular function.

Proposition 1.11 (Weak Nullstellensatz)**.** *The assertion $V(I) = \emptyset$ is equivalent to $I = \bar{k}[t_1, \ldots, t_n]$.*

Proof. We prove the contrapositive: $V(I) \neq \emptyset$ is equivalent to $1 \notin I$. It is clear that if $\exists x \in V(I)$ then $1 \notin I$ (as 1 corresponds to the constant function with value 1 which is nowhere zero).

Lemma 1.12. *Let I be an ideal, such that $1 \notin I$, then there exists a maximal ideal $\mathfrak{m} \supset I$.*

We leave the proof of this lemma as an exercise to the reader. It's an application of Zorn's lemma (and hence the axiom of choice). The quotient ring $K = \bar{k}[t_1, \ldots, t_n]/\mathfrak{m}$ is a field. We have a ring homomorphism $\bar{k} \longrightarrow L$ (which is injective, because $\bar{k}$ is a field). The field extension $L/\bar{k}$ is finitely generated by the images of $t_1, \ldots, t_n$.

Lemma 1.13 (Proposition 7.9 in [AM94] or Theorem 5.11 in [Row06])**.** *A field extension L/K which is finitely generated as a ring extension (that is, L is a quotient of a polynomial ring $K[t_1, \ldots, t_n]$) is* finite*: the field L is a finite-dimensional K-vector space.*

We deduce from this that $L/\bar{k}$ is a finite field extension. However, by assumption $\bar{k}$ is algebraically closed, and therefore the only finite over-field of $\bar{k}$ is $\bar{k}$ itself.

Therefore, we have a morphism $\phi \colon \bar{k}[t_1, \ldots, t_n] \longrightarrow \bar{k}[t_1, \ldots, t_n]/I \longrightarrow \bar{k}$. Let us denote by $x_i \in \bar{k}$ the image $\phi(t_i)$. By definition, this □

Remark 1.14. *The weak Nullstellensatz is the reason for us to work with algebraically closed fields. For $k = \mathbb{R}$ the polynomial $t^2 + 1$ generates a proper ideal I satisfying $V(t^2 + 1) = \emptyset$. We'll see below (1.22) that for algebraically closed fields $\bar{k}$ we get a perfect correspondence between (so-called reduced ideals) and affine varieties $X \subset \mathbb{A}^n_{\bar{k}}$.*

We can now turn to the proof of the proposition above.

Proof of Proposition 1.10. Let $F \in \bar{k}[t_1, \ldots, t_n]$ be a polynomial, such that the induced map $\bar{k}^n \longrightarrow \bar{k}$ is the zero map. We consider $G = F + 1$. By assumption, $V(G) = \emptyset$. By virtue of the Weak Nullstellensatz 1.11 we have $(G) = \bar{k}[t_1, \ldots, t_n]$. In particular, there exists a polynomial $H \in \bar{k}[t_1, \ldots, t_n]$, such that $GH = 1$. This implies that G is a constant, and hence $G = 1$. We conclude $F = 0$. □

A more prominent application of the Weak Nullstellensatz is the *Nullstellensatz*. For an ideal $J \subset R$ we write $\sqrt{J}$ to denote the *radical* of J, that is the ideal given by the subset $\{x \in R | \exists n \in \mathbb{N} : \ x^n \in I\}$. Recall the ideal I_Z for a subset $Z \subset \bar{k}^n$ introduced in Definition 1.8.

Theorem 1.15 (Nullstellensatz)**.** *For an ideal $J \subset \bar{k}[t_1, \ldots, t_n]$ one has*

$$I_{V(J)} = \sqrt{J}.$$

Proof. We use the *Rabinowitsch trick* to reduce the theorem to the weak version 1.11. Let $I \subset \bar{k}[t_1, \ldots, t_n]$ an ideal. Since $\bar{k}[t_1, \ldots, t_n]$ is Noetherian there exist finitely many generators $I = (F_1, \ldots, F_m)$. Let $G \in \bar{k}[t_1, \ldots, t_n]$ be a polynomial, such that G vanishes on $V(I)$.

We introduce an auxiliary variable t_0. The $(n+1)$-variable polynomials $F_0 = 1 - t_0 G$, F_1, ... F_m have the property that $V(F_0, \ldots, F_n) = \emptyset$. By the weak Nullstellensatz 1.11 we have $1 \in (F_0, \ldots, F_m)$. In particular there exist polynomials $H_0, \ldots, H_m$, such that

$$\sum_{i=0}^{m} H_i F_i = 1.$$

We substitute $t_0 = \frac{1}{G}$ and obtain the following identity in $\bar{k}(t_1, \ldots, t_n)$:

$$\sum_{i=1}^{m} H_i(\frac{1}{G}, t_1, \ldots, t_m) F_i = 1.$$

There exists a positive integer r, such that $G^r H_i(\frac{1}{G}, t_1, \ldots, t_m)$ belongs to $\bar{k}[t_1, \ldots, t_m]$ for all $i = 1, \ldots, m$. This yields

$$\sum_{i=1}^{m} G^r H_i(\frac{1}{G}, t_1, \ldots, t_m) F_i = G^r,$$

and we conclude $G^r \in I$ and thus $G \in \sqrt{I}$. □

Definition 1.16. *If I is an ideal, such that $\sqrt{I} = I$ we say that I is* reduced*.*

The Nullstellensatz establishes a 1 : 1-correspondence between affine subvarieties $X \subset \mathbb{A}^n_{\bar{k}}$ and reduced ideals.

Corollary 1.17 (The dictionary I)**.** *There is a bijection*

$$\{X \subset \mathbb{A}^n_{\bar{k}} \,|\textit{affine variety}\} \xleftrightarrow{1:1} \{I \subset \bar{k}[t_1, \ldots, t_n] | \textit{reduced ideal}\},$$

which is defined as

$$X \mapsto I_X,$$

respectively

$$I \mapsto V(I).$$

Proof. It suffices to check $V(I_X) = X$ and $I_{V(I)} = I$. We know that $X = V(I)$ for some ideal I. By definition we have $I_X \supset I$, and therefore $X \subset V(I_X) \subset V(I) = X$. This establishes the first equality. Vice versa, let I be a reduced ideal. By Theorem 1.15 we have $I_{V(I)} = \sqrt{I} = I$. □

Definition 1.18. *A map $f\colon Y \longrightarrow X$ between two varieties $X \subset \mathbb{A}^n_{\bar{k}}$ and $Y \subset \mathbb{A}^m_{\bar{k}}$ is called a* morphism *(or a* regular map*), if for every $i = 1, \ldots, n$ the composition of f with the projection to the i-th coordinate $\mathbb{A}^n_{\bar{k}} \longrightarrow \mathbb{A}^1_{\bar{k}}$*

$$Y \longrightarrow \mathbb{A}^1_{\bar{k}}$$

is a regular function. We write $\mathbf{Mor}(Y, X) \subset \mathsf{Map}(Y, X)$ to denote the set of morphisms from Y to X.

Definition 1.19. *Let $f\colon Y \longrightarrow X$ be an injective morphism of affine varieties. We say that Y is a subvariety of X, if the composition $f(Y) \subset X \subset \bar{k}^n$ is an affine variety.*

Lemma 1.20. *Let $f\colon Y \longrightarrow X$ be a morphism. Then we have for every regular function $g \in \mathcal{O}(X)$ that $g \circ f$ is a regular function on Y. We denote the induced ring homomorphism $\mathcal{O}(X) \longrightarrow \mathcal{O}(Y)$ by f^*.*

Proof. We know that this is true for the projections $e_i\colon \mathbb{A}^n_{\bar{k}} \longrightarrow \mathbb{A}^1_{\bar{k}}$. Let us denote the composition $e_i \circ f$ by h_i. There exists a unique ring homomorphism $\Phi\colon \bar{k}[t_1, \ldots, t_n] \longrightarrow \mathcal{O}(X)$ sending $t_i \mapsto h_i$ (this is just the universal property of polynomial rings).

Let's turn to the general case. By assumption, there exists a polynomial $G \in \bar{k}[t_0, \ldots, t_n]$, such that $g \in \mathcal{O}(X)$ is induced by G. We claim that $\Phi(G)$ is a regular function, satisfying

$$\Phi(G)(y) = g(f(y))$$

for all $y \in Y$. This is true as we have $g(f(y)) = G(f(y)) = \Phi(G)(y)$. □

Definition 1.21. *(a) Let R be a ring. An R-*algebra *consists of a ring S and a ring homomorphism $R \longrightarrow S$. A morphism of R-algebras $S_1 \longrightarrow S_2$ corresponds to a commutative diagram*

$$\begin{array}{ccc} R & \longrightarrow & S_1 \\ & \searrow & \downarrow \\ & & S_2. \end{array}$$

(b) We say that an R-algebra S is finitely generated *if there exists a surjection of R-algebras $R[t_1, \ldots, t_n] \twoheadrightarrow S$.*

(c) An ring (respectively an R-algebra) S is called reduced*, if there are no nilpotent elements, that is, $\sqrt{0} = (0)$.*

Theorem 1.22 (The dictionary II)**.** *(a) The category of affine $\bar{k}$-varieties and morphisms, $\mathsf{Aff}_{\bar{k}}$ is equivalent of the opposite category of finitely generated reduced $\bar{k}$-algebras $\mathsf{Alg}^{\mathrm{red,fg}}_{\bar{k}}$: that is, for every pair of affine varieties X, Y we have isomorphisms*

$$\mathbf{Mor}(Y, X) \simeq \mathsf{Hom}_{\bar{k}}(\mathcal{O}(X), \mathcal{O}(Y)),$$

which respect identities and composition.

(b) A point $x \in X$ corresponds to a maximal ideal $\mathfrak{m} \subset \mathcal{O}(X)$.

(c) Subvariety $Y \subset X$ correspond to reduced quotients $\mathcal{O}(X) \twoheadrightarrow \mathcal{O}(Y)$, and thus to reduced ideals $I \subset \mathcal{O}(X)$.

Proof. We have already constructed a map $\mathbf{Mor}(Y, X) \longrightarrow \mathsf{Hom}(\mathcal{O}(X), \mathcal{O}(Y))$, $f \mapsto f^*$ which sends identities to identities and respects composition (see Lemma 1.20).

Let $X \subset \mathbb{A}^n$, in order to show injectivity of $f \mapsto f^*$, assume that we have $f, g \in \mathbf{Mor}(Y, X)$, such that $f^* = g^*$. Let $e_i \colon \mathbb{A}^n_{\bar{k}} \longrightarrow \mathbb{A}^1_{\bar{k}}$ be the regular function given by projection to the i-th component. We then have by assumption $f^* e_i = g^* e_i$. That is, $e_i \circ f = e_i \circ g$. That is, $f = g$ as maps.

Vice versa, we can use a similar trick to show surjectivity. Let $\varphi \colon \mathcal{O}(X) \longrightarrow \mathcal{O}(Y)$ be an abstract $\bar{k}$-algebra homomorphism. We denote by $f \colon X \longrightarrow \mathbb{A}^n_{\bar{k}}$ the function corresponding to $(\varphi(e_1), \ldots, \varphi(e_n)) \colon Y \longrightarrow \mathbb{A}^n_{\bar{k}}$. By construction we have $f(Y) \subset X$, hence f is a well-defined morphism from Y to X. It remains to show $f^* = \varphi$. By construction we have $f^*(e_i) = \varphi(e_i)$ for all $i = 1, \ldots, n$. Since these elements generate the ring $\mathcal{O}(X)$ we conclude $f^* = \varphi$. This proves (a).

Points $x \in X$ correspond to morphisms $\mathbb{A}^0_{\bar{k}} \longrightarrow X$. By (a), they correspond to $\bar{k}$-algebra homomorphisms $\mathcal{O}(X) \longrightarrow \mathcal{O}(\mathbb{A}^0_{\bar{k}}) = \bar{k}$. Every such homomorphism is surjective, as $\bar{k} \subset \mathcal{O}(X)$. Their kernel is therefore a maximal ideal $\mathfrak{m} \subset \mathcal{O}(X)$. Vice versa, given a maximal ideal $\mathfrak{m}$, the quotient ring $\mathcal{O}(X)/\mathfrak{m}$ is a finitely generated field extension of $\bar{k}$. By Zariski's lemma 1.13 it is equal to $\bar{k}$.

The inclusion of a subvariety $Y \subset X \subset \mathbb{A}^n_{\bar{k}}$ gives rise to a commutative diagram

$$\begin{array}{ccc} \bar{k}[t_1, \ldots, t_n] & \twoheadrightarrow & \mathcal{O}(X) \\ & \searrow & \downarrow \\ & & \mathcal{O}(Y). \end{array}$$

The ring homomorphisms originating from $\bar{k}[t_1, \ldots, t_n]$ are surjective, hence the downward arrow $\mathcal{O}(X) \longrightarrow \mathcal{O}(Y)$ is a surjection too.

Vice versa, if $\mathcal{O}(X) \longrightarrow \mathcal{O}(Y)$ is surjective, the composition $\bar{k}[t_1, \ldots, t_n] \longrightarrow \mathcal{O}(Y)$ is surjective, which shows that $Y \longrightarrow \mathbb{A}^n_{\bar{k}}$ is a subvariety. We conclude that $Y \longrightarrow X$ is a subvariety. This proves (c). □

Corollary 1.23. *Let $x \in X$ and $\mathfrak{m}_x \subset \mathcal{O}(X)$ be the corresponding maximal ideal. Then one has*

$$\mathfrak{m}_x = \{f \in \mathcal{O}(X) | f(x) = 0\}.$$

Proof. By the dictionary, the subvariety $x \colon \mathbb{A}^0_{\bar{k}} \longrightarrow X$ corresponds to an ideal $I \subset \mathcal{O}(X)$ which is the kernel of the surjective map

$$x^* \, \mathcal{O}(X) \twoheadrightarrow \bar{k}.$$

By definition, the map x^* sends $\mathcal{O}(X)$ to $f \circ x = f(x)$. We conclude $\mathfrak{m}_x = \{f \in \mathcal{O}(X) | f(x) = 0\}$. □

1.2 Affine varieties over non-algebraically closed fields

When the coefficients of a system of equations belong to a subfield $k \subset \bar{k}$ it makes sense to expect that the induced $\bar{k}$-variety is deduced from an object one should refer to as a k-variety. The naive analogue of our previous approach to define k-varieties as subsets of k^n fails, as there are systems of equations without any k-solutions. Instead we take one's cue from the dictionary.

Scholia 1.24. *The dictionary allows us to change our viewpoint on affine varieties. Rather than viewing them as subsets of $\bar{k}^n$ we can define the category $\mathsf{Aff}_{\bar{k}}$ as the opposite category of $\mathsf{Alg}_{\bar{k}}^{\mathrm{red,fg}}$.*

A k-algebra R is said to be *geometrically reduced* if the base change $R \otimes_k \bar{k}$ is reduced. We denote the corresponding category by $\mathsf{Alg}_k^{g-\mathrm{red,fg}}$.

Definition 1.25. *(a) We define the category of k-varieties to be the opposite category of $\mathsf{Alg}_k^{g-\mathrm{red,fg}}$.*

(b) We refer to the set of maximal ideals $\mathfrak{m}$ of $R \in \mathsf{Alg}_k^{\mathrm{red,fg}}$ as $\mathsf{MSpec}\, R$. We also write $\mathsf{MSpec}\, R$ to denote the k-variety corresponding to X.

(c) If we have a morphism of k-varieties $Y \longrightarrow X$, such that the corresponding map or rings $R_1 \twoheadrightarrow R_2$ is surjective, we say that Y is a subvariety of X.

The carefulness of restricting oneself to geometrically reduced k-algebras is only needed when working with non-perfect fields. Henceforth, we assume that k is perfect.

Inspired by the dictionary we treat a maximal ideal $\mathfrak{m} \in \mathsf{MSpec}\, R$ as a point of $X = \mathsf{MSpec}\, R$.

Definition 1.26. *Let $X = \mathsf{MSpec}\, R$ and $I \subset R$ an ideal. We denote by $V(I) = \{\mathfrak{m} \in \mathsf{MSpec}\, R | I \subset \mathfrak{m}\}$.*

Lemma 1.27. *Let $Y \subset X$ be a subvariety corresponding to a surjection of rings $R_1 \twoheadrightarrow R_2$ with kernel I. Then the set of points in Y corresponds to $V(I)$.*

Proof. This is a direct consequence of the following statement in commutative algebra. Let $\pi\colon R_1 \twoheadrightarrow R_2$ be a surjection of rings. Then we have a bijection

$$\{\mathfrak{m} \in \mathsf{MSpec}\, R_2\} \overset{1:1}{\longleftrightarrow} \{\mathfrak{m} \in \mathsf{MSpec}\, R_1 | \mathfrak{m} \supset I\},$$

where we send $\mathfrak{m} \in \mathsf{MSpec}\, R_2$ to $\pi^{-1}(\mathfrak{m})$. We leave the proof to the reader. □

Despite of the suggestive nature of the terminology "point", we alert the readers that the points of a k-variety might be unlike what they have seen before, and in fact, defy geometric intuition. The following lemma shows that the points of affine k-space do not correspond to k^n as one might naively expect from the case of algebraically closed fields.

Lemma 1.28. *We denote by $\mathbb{A}_k^n$ the k-variety given by the maximal spectrum of the ring $k[t_1, \ldots, t_n]$. Let $\bar{k}$ be an algebraic closure of k, then there is a bijection*

$$\mathsf{MSpec}\, k[t_1, \ldots, t_n] \overset{1:1}{\longleftrightarrow} \bar{k}^n / \mathsf{Aut}(\bar{k}/k).$$

Proof. For a maximal ideal $\mathfrak{m} \subset k[t_1, \ldots, t_n]$ we write $L_\mathfrak{m}$ for the field $k[t_1, \ldots, t_n]/\mathfrak{m}$. By virtue of Zariski's Lemma 1.13 $L_\mathfrak{m}$ is a finite field extension of k. We choose an embedding $L_\mathfrak{m} \hookrightarrow \bar{k}$. The set of such embeddings is acted on transitively by $\mathsf{Aut}(\bar{k}/k)$. By composing with the quotient map $k[t_1, \ldots, t_n] \longrightarrow L_\mathfrak{m}$ we obtain a ring homomorphism $\phi_\mathfrak{m} k[t_1, \ldots, t_n] \longrightarrow \bar{k}$ which corresponds to a tuple $(x_1, \ldots, x_n) \in \bar{k}^n$. A different choice of an embedding into $\bar{k}$ yields an n-tuple differing from this one by an element of $\mathsf{Aut}(\bar{k}/k)$. This concludes the proof. □

Definition 1.29. *Let $x \in X = \mathsf{MSpec}\, R$ be a point of an affine k-variety corresponding to a maximal ideal $\mathfrak{m} \subset R$. We define $k_x = R/\mathfrak{m}$ and call it the* residue field *at x. The degree of the finite field extension k_x/k (Zariski!) will be denoted by*

$$\deg(x) = [k_x : k].$$

Let $x \in \mathbb{A}^n_k$ be a point, such that k_x/k is Galois. Then the degree $\deg(x)$ equals the length of the corresponding Galois orbit in $\bar{k}^n$ (see Lemma 1.28).

One way to restore geometric intuition is to define points differently, using the following formal trick.

Definition 1.30. *Let R be a k-algebra and $X = \mathsf{MSpec}\, R$ an affine k-variety. The set of* R-points *of X is defined to be the set of ring homomorphisms $\mathcal{O}(X) \longrightarrow R$, and is denoted by $X(R)$.*

In the case of affine n-space $\mathbb{A}^n_k$ one has $\mathbb{A}^n_k(R) = \mathsf{Hom}(k[t_1, \ldots, t_n], R) = R^n$. In particular, we see that the set of k-points $\mathbb{A}^n_k(k)$ is in bijection with k^n. If L/k is a finite field extension, then the set of L-points corresponds to a pair (x, i), where $x \in X$ and $i \colon k_x \hookrightarrow L$.

Later it will prove useful to have a notion of R-points for arbitrary k-algebras R, even for R non-reduced.

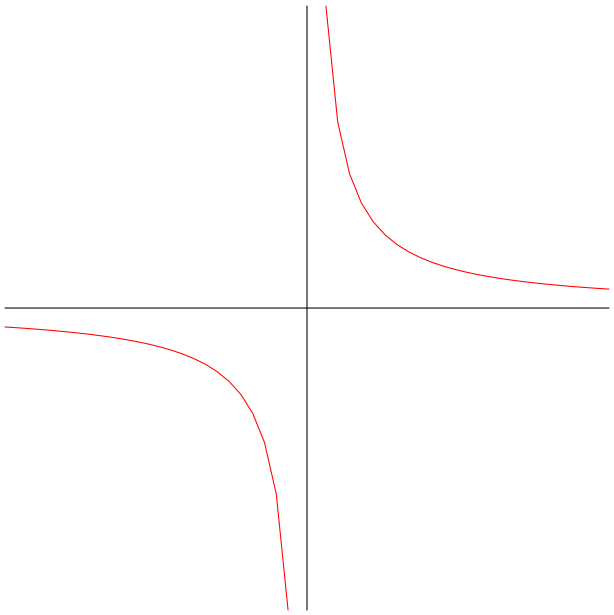
Definition 1.31. *We denote $\mathsf{MSpec}\, k[t_1, \ldots, t_n]$ by $\mathbb{A}^n_k$. A morphism $f \colon X \longrightarrow \mathbb{A}^1_k$ is called a* regular function *on X. We denote the set of regular functions by $\mathcal{O}(X)$.*

Exercise 1.32. *Show that for $X = \mathsf{MSpec}\, R$ we have a bijection $\mathcal{O}(X) \simeq R$.*

In particular, we conclude that $\mathcal{O}(X)$ is a ring.

1.3 The Zariski topology

Consider the affine k-variety corresponding to the k-algebra $k[t, t^{-1}]$. We denote it by $\mathbb{G}_{m,k} = \mathsf{MSpec}\, k[t, t^{-1}]$. Equivalently we may say that this k-variety corresponds to the equation $st = 1$.



(1)

Over an algebraically closed field $\bar{k}$, this variety is given by the subset $\bar{k}^2$ consisting of tuples (x, y), such that $xy = 1$. In particular, $x \neq 0$ and $y = x^{-1}$. This shows that we have a bijection between the set of points of $\mathbb{G}_{m,\bar{k}}$ and $\bar{k}^\times = \bar{k} \setminus \{0\}$.

Let us describe the set of points of $\mathbb{G}_{m,k}$ for k a field. A maximal ideal $\mathfrak{m} \subset k[t, t^{-1}]$ gives rise to a maximal ideal $\mathfrak{m}' = \mathfrak{m} \cap k[t] \subset k[t, t^{-1}]$. Vice versa, given $\mathfrak{m}' \in \mathsf{MSpec}\, k[t]$ we can consider $R[t, t^{-1}]\mathfrak{m}' \subset k[t, t^{-1}]$. The latter is a maximal ideal, if and only if $t \notin \mathfrak{m}'$. We see that $\mathsf{MSpec}\, k[t, t^{-1}] = \mathsf{MSpec}\, k[t] \setminus \{(t)\}$. Geometrically, this corresponds to removing the subvariety $V(t)$ from $\mathbb{A}^1_k$, that is, the origin $\{0\}$.

Similarly, for a k-algebra R the set of R-points $\mathbb{G}_{m,k}(R)$ agrees with $\mathsf{Hom}(k[t, t^{-1}], R) \simeq R^\times$, that is, the set of units in R. For $R = k$ we have $\mathbb{G}_{m,k}(k) = k^\times = k \setminus \{0\}$.

Definition 1.33. *Let X be an affine variety. A subset $U \subset X$ is said to be Zariski open, if $X \setminus U \subset X$ is a subvariety.*

Exercise 1.34. *(a) Show that Zariski open subsets of $|X|$ define a topology on X.*

(b) For $f \in \mathcal{O}(X)$ we denote by $U(f) \subset X = \mathsf{MSpec}\, \mathcal{O}(X)$ the subset $\{\mathfrak{m} \in X | f \notin \mathfrak{m}\}$. Show that

$$\{U(f) | f \in \mathcal{O}(X)\}$$

defines a basis for the Zariski topology.

The Zariski open subsets $U(f)$ are important as they are themselves affine varieties. For a ring R and an element $f \in R$ we denote by R_f the localisation $R[f^{-1}] = R[t]/(tf - 1)$.

Lemma 1.35. *Let $X = \mathsf{MSpec}\, R$ be an affine variety, and let $i\colon \mathsf{MSpec}\, R_f \longrightarrow \mathsf{MSpec}\, R$ be the morphism corresponding to the canonical ring homomorphism from R to the localisation R_f. Then, i is injective and its image agrees with the Zariski open subset $U(f)$.*

Proof. We claim that the map $\mathfrak{m} \mapsto R_f\mathfrak{m}$ gives rise to a bijection

$$U(f) \overset{1:1}{\longleftrightarrow} \mathsf{MSpec}\, R_f.$$

First of all let us check that $R_f\mathfrak{m}$ is a maximal ideal in R_f.

Claim 1.36. *The ideal $R_f\mathfrak{m} \subset R_f$ is maximal.*

Proof. One has $1 \in R_f\mathfrak{m}$ if and only if $f^n \in \mathfrak{m}$ for some positive integer n. Since maximal ideals are reduced, this is the case if and only if $f \in \mathfrak{m}$. We have $U(f) = \{\mathfrak{m} \in \mathsf{MSpec}(R) | f \notin \mathfrak{m}\}$, and therefore we may conclude $1 \notin R_f\mathfrak{m}$.

The quotient $R_f/R_f\mathfrak{m}$ contains $R/\mathfrak{m} = L$ as a subfield. By definition, one has $R_f/R_f\mathfrak{m} = L[f^{-1}]$. However, the element in L induced by $f \in R$ is already invertible (as it is non-zero). This shows $R_f/R_f\mathfrak{m} = L$, and therefore the quotient is a field, and we conclude that $R_f\mathfrak{m}$ is a maximal ideal. □

This shows that the map $U(f) \longrightarrow \mathsf{MSpec}\, R_f$ is well-defined.

Claim 1.37. *We denote by $\mathfrak{m}'$ an element of $\mathsf{MSpec}\, R_f$. The map $\mathfrak{m}' \mapsto \mathfrak{m}' \cap R$ defines an inverse to $\mathfrak{m} \mapsto R_f\mathfrak{m}$.*

Proof. It is clear that for $\mathfrak{m} \in U(f)$ we have $(R_f\mathfrak{m}) \cap R \supset \mathfrak{m}$. Since $\mathfrak{m}$ is a maximal ideal, and $1 \notin R_f\mathfrak{m}$, we infer $(R_f\mathfrak{m}) \cap R = \mathfrak{m}$.

Vice versa, given $\mathfrak{m}' \in \mathsf{MSpec}\, R_f$ we certainly have $R_f(\mathfrak{m}' \cap R) \subset \mathfrak{m}$. Let $y \in \mathfrak{m}'$, we write $y = \frac{x}{f^r}$ for $r > 0$. We conclude that $f^r y \in R$, and therefore that $x \in R_f(\mathfrak{m}' \cap R)$. This shows $R_f(\mathfrak{m}' \cap R) \supset \mathfrak{m}$. □

By combining the two assertions above we conclude the proof. □

Zariski open subsets of the form $U(f)$ are often referred to as *standard (affine) open subsets*. Every open subset is a union of finitely many Zariski open subsets. For a Zariski open subset we can write $U = X \setminus V(I)$ where $I \subset \mathcal{O}(X)$ is an ideal. Since the k-algebra $\mathcal{O}(X)$ is Noetherian, we may write $I = (f_1, \ldots, f_n)$ and therefore $U = \bigcup_{i=1}^n U(f_i)$.

Definition 1.38. *We refer to the underlying topological space of an affine variety by $|X|$.*

The statement below looks like another property of Noetherian rings, but works for arbitrary rings actually.

Proposition 1.39. *The topological space $|X|$ is* quasi-compact. *That is, for every open covering $|X| = \bigcup_{j\in J} U_j$ there exists a finite subset $J_0 \subset J$, such that $X = \bigcup_{i\in J_0} U_j$.*

Proof. Let $I_j \subset \mathcal{O}(X)$ be an ideal, such that $U_j = X \setminus V(I_j)$ for all $j \in J$. By assumption we have $\bigcap_{j\in J} V(I_j) = \emptyset$. One has $\bigcap_{j\in J} V(I_j) = V(I)$ where I denotes the ideal generated by $\{I_j\}_{j\in J}$. Since $V(I) = \emptyset$, we conclude $1 \in I$. This implies that there exists a finite linear combination

$$f_1 g_1 + \cdots + f_n g_n = 1$$

with f_i arbitrary and $g_i \in I_{j_i}$ for $i = 1, \ldots, n$. This shows $V(I_{j_1} + \cdots + I_{j_n}) = \emptyset$ and therefore that $U_{j_1}, \ldots, U_{j_n}$ cover X. □

Using that a Zariski open subset is a finite union of standard affine open subsets (which are quasi-compact), we deduce the following statement.

Corollary 1.40. *We denote by $U \subset |X|$ the underlying topological space of a Zariski open subset. It is quasi-compact.*

1.4 Smooth varieties

Let $k = \mathbb{C}$ be the field of complex numbers. The *standard topology* on $\mathbb{C}$ refers to the metric topology defined with respect to the metric $d(z, w) = |z - w|$. This terminology is necessary since we could also identify $\mathbb{C}$ with $\mathbb{A}^1_{\mathbb{C}}$ and work with the Zariski topology.

An affine $\mathbb{C}$-variety corresponds to a subset $X \subset \mathbb{C}^n$ defined by the common set of zeroes of finitely many polynomials. The subset topology on X produces an interesting topological space X^{an}, called the *analytification* of X. The topological spaces arising by this construction are always Hausdorff and second-countable (since $\mathbb{C}^n$ has this property).

Under some additional assumption on X one can show that X^{an} has the structure of a complex manifold. Let us recall what this means: there exists a covering of X by open subsets $\{U_i\}_{i \in I}$, such that there are homeomorphisms

$$\phi_i \colon U_i \xrightarrow{\simeq} U_i' \subset \mathbb{C}^{n_i},$$

where U_i' is an open subset of $\mathbb{C}^{n_i}$, and for every pair $i, j \in I^2$ we have that the *change-of-coordinates map*

$$\begin{array}{ccc} \phi_i(U_i \cap U_j) & \xrightarrow{\phi_{ij}} & \phi_j(U_i \cap U_j) \\ & {\scriptstyle \phi_i^{-1}} \searrow \quad \nearrow {\scriptstyle \phi_j} & \\ & U_i \cap U_j & \end{array}$$

is *holomorphic*. In particular, we by exchanging i and j we see that the change of coordinates map is inverse to ϕ_{ji}, that is, it is a biholomorphic map.

We refer the reader to Griffiths and Harris's [GH94, Chapter 2] for an overview of the theory of complex manifolds and an *analytic* viewpoint on *algebraic* geometry.

Theorem 1.41 (Jacobi criterion or Implicit Function Theorem, see p. 18 of [GH94])**.** *Let $m \geq n$ and $f = (f_1, \ldots, f_m)$, such that for every $x \in \mathbb{C}^n$, such that $f(x) = 0$ for all $i = 1, \ldots, n$, the matrix*

$$\left(\frac{\partial f_i}{\partial t_j}(x) \right)_{i,j}$$

has full rank. Then the topological space $f^{-1}(0)$ can be endowed with the structure of a complex manifold.

Recall that the matrix above has *full rank* if the induced linear map of vector spaces is *surjective*.

Corollary 1.42. *Let $X = V(I)$ be a $\mathbb{C}$-variety, such that $I = (f_1, \ldots, f_n)$, such that the polynomials satisfy the condition of Theorem 1.41 (note: this is still in the realm of algebra, since the f_i are polynomials). Then the analytification X^{an} can be endowed with the structure of a complex manifold.*

We call complex affine varieties with this property *smooth*. Since the Jacobi criterion makes sense for arbitrary fields, this motivates the following definition.

Definition 1.43. *Let X be an affine k-variety, we say that X is smoooth, if there exists a covering by Zariski open subsets $X_\alpha \subset X$ with $\mathcal{O}(X_\alpha) \simeq k[t_1, \ldots, t_n]/(f_1, \ldots, f_m)$, such that for $x \in X$ the matrix*

$$\left(\frac{\partial f_i}{\partial t_j}(x)\right)_{i,j}$$

has full rank.[2]

1.5 Smooth and étale morphisms

For a complex manifold X and a point $x \in X$ one defines a complex vector space, called the tangent space T_xX. We recall its definition for the convenience of the reader: let U_ε denote the ε-neighbourhood of 0 in $\mathbb{C}$. We consider the set of holomorphic maps

$$\gamma \colon U_{\varepsilon_\gamma} \longrightarrow X,$$

such that $\gamma(0) = x$. We say that $\gamma_1 \sim \gamma_2$ if there exists a chart (U, ϕ) containing $x \in X$, such that for $0 < \varepsilon < \min(\varepsilon_{\gamma_1}, \varepsilon_{\gamma_2})$ we have that the maps $g_1 = \phi \circ \gamma_1$ and $g_2 = \phi \circ \gamma_2$ satisfy $g_1'(0) = g_2'(0)$.[3] The set of equivalence classes is denoted by T_xX. It carries a unique structure of a vector space: we define addition as follows: $\gamma_1 + \gamma_2 \sim \gamma_3$ if and only if for an appropriate chart (U, ϕ) as above we have $(\phi \circ \gamma_1)'(0) + (\phi \circ \gamma_2)'(0) = (\phi \circ \gamma_3)'(0)$. Multiplication with complex scalars is defined similarly.

In the theory of complex manifolds one defines two types of holomorphic maps $f \colon Y \longrightarrow X$ which deserve particular attention.

Definition 1.44. *We say that ...*

(a) ... f is a submersion*, if for every $y \in Y$ the differential $d_y f$ is* surjective*.*

(b) ... f is a local equivalence*, if for every $y \in Y$ the differential $d_y f$ is an* isomorphism*.*

These maps deserve particular praise, since the structure of their fibres is well-behaved. The Jacobi-criterion 1.41 implies the following corollary:

Corollary 1.45. *Let $f \colon Y \longrightarrow X$ be a submersion of complex manifolds, then for every $x \in X$ the preimage $f^{-1}(x)$ is a complex manifold.*

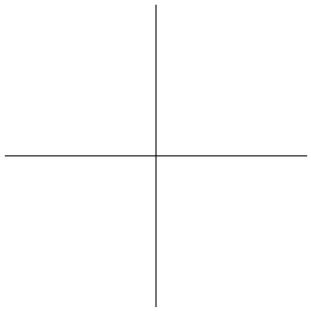
Example 1.46. *Consider the map $f \colon \mathbb{C}^2 \longrightarrow \mathbb{C}$ which sends (x, y) to xy. The fibre over $c \in \mathbb{C} \setminus \{0\}$ can be identified with $\{(x, y) | xy = c\} \simeq \mathbb{C}^\times$. For $c = 0$ we see that*

$$f^{-1}(0) = \{(x, y) | xy = 0\} = \{(x, 0) | x \in \mathbb{C}\} \cup \{(0, y) | y \in \mathbb{C}\}.$$

[2] We think of $x \in X_\alpha$ as a map $\mathcal{O}(X_\alpha) \longrightarrow k_x$ where $k_x = \mathcal{O}(X_\alpha)/\mathfrak{m}$. The matrix above is defined over the field k_x.

[3] The map g_i is a holomorphic map from an open subset of $\mathbb{C}$ to an open subset of $\mathbb{C}^n$. Therefore, the derivative is well-defined.

This space no longer admits the structure of a complex manifold, as removing the origin $(0,0)$ *produces a disconnected topological space. The intersection with* $\mathbb{R}^2$ *reveals a singularity:*



(2)

The Jacobi matrix of the map is given by $(y \;\; x)$*, consistently to the picture above, it vanishes at the origin* $(0,0)$*.*

Inspired by our discussion of complex manifolds we first define the analogue of the tangent space T_xX of a k-variety, and then introduce the analogues of submersions (= *smooth morphisms*) and local equivalences (=*étale morphisms*). For our definition of tangent spaces we make use of the concept of R-points for a non-reduced ring.

Definition 1.47. *(a) For a ring* R *we denote by* $R[\varepsilon]$ *the ring* $R[t]/(t^2)$*. There is a surjection* $\pi\colon R[\varepsilon] \longrightarrow R$ *given by* $\varepsilon \mapsto 0$*.*

(b) A k*-algebra homomorphism* $R_1 \xrightarrow{\phi} R_2$ *gives rise to a map* $X(R_1) \longrightarrow X(R_2)$ *(we send* $\mathcal{O}(X) \longrightarrow R_1$ *to the composition* $\mathcal{O}(X) \longrightarrow R_2$*).*

(c) Let X *be an affine* k*-variety* L/k *a field extension and* $x \in X(L)$ *an* L*-point. We denote by* T_xX *the set of* $L[\varepsilon]$*-points of* X*, such that the induced* L*-point is* x*, that is,* T_xX *is the fibre of the map* $X(L[\varepsilon]) \longrightarrow X(L)$ *over* x*. We call* T_xX *the* tangent space *at* x*.*

The ring $L[\varepsilon]$ consists of finite Taylor series over L of first order. The relation $\varepsilon^2 = 0$ ensures that higher order phenomena (which don't play a role for tangent spaces) are ignored.

Example 1.48. *For an arbitrary* k*-algebra we have an isomorphism* $\mathbb{A}^n_k(R) = R^n$*. For a field* $L \supset k$ *we can understand the map* $\mathbb{A}^n_k(L[\varepsilon]) \longrightarrow \mathbb{A}^n_k(L)$ *as follows:*

$$\begin{array}{ccc} \mathbb{A}^n_k(L[\varepsilon]) & \xrightarrow{\simeq} & L[\varepsilon]^n \\ \downarrow & & \downarrow \pi \\ \mathbb{A}^n_k(L) & \xrightarrow{\simeq} & L^n. \end{array}$$

For $x \in \mathbb{A}^n_k(L) \simeq L^n$*, the tangent space is therefore given by the fibre* $\pi^{-1}(x) = (\varepsilon)^n \simeq L^n$*. We conclude that for every point of affine* n*-space, the tangent space is an* n*-dimensional vector space.*

In order to gain intuition for the general case we fix a presentation for the k-algebra of regular functions

$$\mathcal{O}(X) = k[t_1, \ldots, t_n]/(f_1, \ldots, f_m)$$

of an affine k-variety. Let L/k be a field extension, and consider a k-algebra homomorphism

$$\phi\colon\ \mathcal{O}(X) \longrightarrow L[\varepsilon].$$

A k-algebra homomorphism $\phi\colon\ \mathcal{O}(X) \longrightarrow L[\varepsilon]$ is specified by the images $\gamma_i = \phi(t_i)$. These images correspond to n-tuples of elements $(\gamma_1, \ldots, \gamma_n) \in L[\varepsilon]^n$, satisfying the condition

$$f_i(\gamma_1, \ldots, \gamma_n) = 0$$

for all $i = 1, \ldots, m$. We write $\gamma_j = x_j + \varepsilon \cdot v$ with x_j and v_j in L. Let v be the column vector with entries v_j. A direct computation shows

$$(f_1, \ldots, f_m)(\gamma_1, \ldots, \gamma_n) = (f_1, \ldots, f_m)(x_1, \ldots, x_n) + \varepsilon \cdot \left(\frac{\partial f_i}{\partial t_j}(x)\right) v.$$

This expression vanishes if and only if the constant term and the coefficient of ε vanishes. That is, if one has $(f_1, \ldots, f_m)(x_1, \ldots, x_n) = 0$ and $\left(\frac{\partial f_i}{\partial t_j}(x)\right) v = 0$. We conclude the following:

Corollary 1.49. *The tangent space T_xX is isomorphic to the kernel of*

$$\left(\frac{\partial f_i}{\partial t_j}(x)\right) : L^m \longrightarrow L^n.$$

In particular it carries a natural structure of an L-vector space.

We keep going and produce another corollary.

Corollary 1.50. *A k-variety X is smooth, if and only if the function $x \mapsto \dim T_xX$ is* Zariski locally constant*.*

Proof. By definition, X is smooth if and only if the rank of $\left(\frac{\partial f_i}{\partial t_j}(x)\right)$ is a locally-constant function on X. This is equivalent to the dimensions of the kernels, that is, T_xX to be locally constant. □

The vector space structure on T_xX can also be defined *intrinsically*, that is, without fixing a presentation $\mathcal{O}(X) = k[t_1, \ldots, t_n]/(f_1, \ldots, f_m)$. At first we recall the following definition from commutative algebra

Definition 1.51. *Let R be a k-algebra and M an R-module. A k-linear* derivation $\delta\colon R \longrightarrow M$ *is a k-linear map, such that for every $f, g \in R$ we have*

$$\delta(fg) = \delta(f)g + f\delta(g).$$

Derivations arise naturally when studying tangent spaces. In the theory of manifolds one can define tangent spaces at x as vector spaces of derivations of the ring of germs of functions. The same construction also applies to affine k-varieties.

Construction 1.52. *Let $\phi\colon\ \mathcal{O}(X) \longrightarrow L[\varepsilon]$ be a ring homomorphism corresponding to an element of T_xX. As above we write $\phi = x + v\varepsilon$, where $v\colon\ \mathcal{O}(X) \longrightarrow L$ is a map. The sum $x + v$ is a ring homomorphism if and only if $v(f + g) = v(f) + v(g)$ and $v(fg) = fv(g) + v(f)g$. We call such a map an* L*-valued derivation. This allows us to identify T_xX with the L-vector space of derivations $\mathcal{O}(X) \longrightarrow L$, where we view L as an $\mathcal{O}(X)$-module via the surjection $\mathcal{O}(X) \twoheadrightarrow L$.*

We can now define the algebraic analogue of *submersions*. Unfortunately this goes hand in hand with an often confusing change in terminology.

Definition 1.53. *(a) A morphism of smooth affine k-varieties $f\colon Y \longrightarrow X$ is* smooth *if for every $y \in Y$ the induced map of tangent spaces $df\colon T_yY \longrightarrow T_X$ is a surjection.*

(b) It is said to be étale *if d_yf is an isomorphism for all $y \in Y$.*

Despite of the similarity between the definition of smooth and étale morphisms with their counterparts in the theory of manifolds, their behaviour is fundamentally different in the realm of algebraic geometry.

Exercise 1.54. *The inverse function theorem fails for algebraic varieties and the Zariski topology.*

(a) Let $\mathbb{G}_{m,k} = \mathsf{MSpec}\ k[t,t^{-1}]$ and let $f\colon \mathbb{G}_{m,k} \longrightarrow \mathbb{G}_{m,k}$ be the morphism corresponding to the k-algebra homomorphism

$$k[t,t^{-1}] \longrightarrow k[t,t^{-1}],\ \ t \mapsto t^n.$$

Show that f is étale if n is coprime to the characteristic of k (or k has characteristic 0).

(b) Prove that there do not exist non-empty Zariski open subsets $U, V \subset \mathbb{G}_m$, such that $f(U) = V$ and $f|_U\colon U \longrightarrow V$ is an isomorphism.

1.6 Projective varieties

So far we have worked only with local aspects of algebraic geometry. This is comparable with studying analysis only open subsets of Euclidean spaces rather than manifolds. Just like a manifold is a patchwork of local pieces, each of which looks like an open set in $\mathbb{R}^n$, an *abstract variety* is assembled from affine varieties by glueing them along Zariski open subsets.

We will not define abstract k-varieties here, for the sake of keeping this introduction short. However we will discuss the most important class of examples: projective k-varieties. As in the case of affine varieties, we begin by introducing this new concept over algebraically closed fields first.

Definition 1.55. *Let $\bar{k}$ be an algebraically closed field. We define $\mathbb{P}^n_{\bar{k}}$ to be the set $(\bar{k}^{n+1} \setminus 0)/\bar{k}^\times$. The equivalence class of the point $(z_0, \ldots, z_n)$ will be denoted by $[z0 : \cdots : z_n]$ (homogeneous coordinates).*

The set $\mathbb{P}^n_{\bar{k}}$ admits an interesting stratification. For $0 \leq i \leq n$ we define

$$V_i = (\mathbb{P}^n_{\bar{k}})_i = \{[z_0 : \cdots : z_n] | z_0 = \cdots = z_{i-1} = 0\}.$$

We have $V_0 = \mathbb{P}^n_{\bar{k}}$, while V_1 is in bijection with $\mathbb{P}^{n-1}_{\bar{k}}$, and more generally V_i is in bijection with $\mathbb{P}^{n-i}_{\bar{k}}$. Furthermore, we observe that

$$\mathbb{P}^n_{\bar{k}} \setminus V_1 = \{[z_0 : \cdots : z_n | z_0 \neq 0]\} \simeq \{(x_1, \ldots, x_n) \in \bar{k}^n\} = \mathbb{A}^n_{\bar{k}},$$

where we send $[z_0 : \cdots : z_n]$ to $(\frac{z_1}{z_0}, \ldots, \frac{z_n}{z_0})$. A similar computation shows

$$V_i \setminus V_{i-1} = \mathbb{A}^{n-i}.$$

We conclude that the set $\mathbb{P}^n_{\bar{k}}$ is in bijection with the disjoint union

$$\mathbb{A}^n_{\bar{k}} \sqcup \cdots \sqcup \mathbb{A}^0_{\bar{k}}\,.$$

In the case of $\mathbb{P}^1_{\bar{k}}$ one recovers $\mathbb{P}^1_{\bar{k}} = \mathbb{A}^1_{\bar{k}} \sqcup \{\infty\}$, a space reminiscent of the Riemann sphere.

In order to arrive at a more geometric object, than just a plain set, we observe that $\mathbb{P}^n_{\bar{k}}$ can be covered by "affine charts", similar to the theory of manifolds.

Definition 1.56. *For $i = 0, \ldots, n$ we let $U_i \subset \mathbb{P}^n_{\bar{k}}$ be the subset*

$$U_i = \{[z_0 : \cdots : z_n] | z_i \neq 0\}.$$

We denote by $\phi_i \colon U_i \longrightarrow \mathbb{A}^n_{\bar{k}}$ the bijection $[z_0 : \cdots : z_n] \mapsto (\frac{z_0}{z_i}, \ldots, \frac{z_{i-1}}{z_i}, \frac{z_{i+1}}{z_i}, \ldots, \frac{z_n}{z_i})$.

For $k = \mathbb{C}$ this construction would be the starting point to show that the analytification of $\mathbb{P}^n_{\mathbb{C}}$ has the structure of a complex manifold. More generally, one can use these "charts" to construct the structure of an abstract $\bar{k}$-variety on $\mathbb{P}^n_{\bar{k}}$. We will not follow this approach for now, but still keep referring to the pair (U_i, ϕ_i) in order to introduce notions like morphisms between projective varieties, tangent spaces, and smoothness. A good example of this is the following definition of regular maps from affine $\bar{k}$-varieties to $\mathbb{P}^n_{\bar{k}}$.

Definition 1.57. *Let X be an affine $\bar{k}$-variety. A map (of sets) $f \colon X \longrightarrow \mathbb{P}^n_{\bar{k}}$ is called* regular *or a* morphism*, if there exists a Zariski-open covering $X = \bigcup_{i \in J} W_j$, such that for every $j \in J$*

(a) there exists an $i(j) \in \{0, \ldots, n\}$ with $f(W_j) \subset U_{i(j)}$,

(b) the map $f|_{W_j} \colon W_j \longrightarrow U_{i(j)} = \mathbb{A}^n_{\bar{k}}$ is a regular map of affine $\bar{k}$-varieties.

Definition 1.58. *A polynomial $F \in \bar{k}[t_0, \ldots, t_n]$ is said to be* homogeneous of degree d*, if for every $\lambda \in \bar{k}$ we have*

$$F(\lambda t_0, \ldots, \lambda t_n) = \lambda^d F(t_0, \ldots, t_n).$$

Equivalently, F is homogeneous of degree d, if it is a $\bar{k}$-linear combination of degree d monomials.

Example 1.59. *The polynomial $t_0^2 + 2t_0t_1$ is homogenous of degree 2. The polynomial $t_0^3 + t_2$ is not homogeneous.*

A homogeneous polynomial $F(t_0, \ldots, t_n)$ has a well-defined zero set in $\mathbb{P}^n_{\bar{k}}$. Indeed, for $(x_0, \ldots, x_n) \in \bar{k}^n$ we have $F(x_0, \ldots, x_n) = 0$ if and only if $F(\lambda x_0, \ldots, \lambda x_n) = 0$.

Definition 1.60. *Let $F_0, \ldots, F_m \in \bar{k}[t_0, \ldots, t_n]$ be homogeneous polynomials with $\deg F_i = d_i$. We define $V(F_1, \ldots, F_m) \subset \mathbb{P}^n_{\bar{k}}$ to be the subset*

$$\{[x_0 : \cdots : x_n] \in \mathbb{P}^n_{\bar{k}} \,|F_i(x_0, \ldots, x_n) = 0 \ \forall i\}.$$

A subset $X \subset \mathbb{P}^n_{\bar{k}}$ of this form is called a projective variety*.*

For a polynomial $F \in \bar{k}[t_0, \ldots, t_n]$ in $n+1$ variables we denote by $d_i(F)$ the polynomial in n variables obtained by substituting $t_i = 1$. Let $X \subset \mathbb{P}^n_{\bar{k}}$ be a projective variety, defined by a system of homogenous equations $F_1, \ldots, F_m$. For every $i = 0, \ldots, n$ we denote by $X_i = X \cap U_i$. Recall that we have a bijection $U_i \simeq \mathbb{A}^n_{\bar{k}} = \bar{k}^n$. With respect to this identification, $X_i \subset \bar{k}^n$ is the affine $\bar{k}$-variety defined by the system of equations

$$X_i = V\left(d_i(F_1), \ldots, d_i(F_m)\right) \subset \mathbb{A}^n_{\bar{k}}\,.$$

By definition, we have $X = \bigcup_{i=1}^n X_i$; the projective variety X is obtained by "glueing" the affine pieces X_i. In analogy with Definition 1.57 we define morphisms between projective varieties.

Definition 1.61. *Let y be an affine $\bar{k}$-variety and $X \subset \mathbb{P}^n_{\bar{k}}$ a projective $\bar{k}$-variety. A map (of sets) $f\colon Y \longrightarrow X$ is called* regular *or a* morphism*, if there exists a Zariski-open covering $X = \bigcup_{i\in J} W_j$, such that for every $j \in J$*

(a) there exists an $i(j) \in \{0, \dots, n\}$ with $f(W_j) \subset X_{i(j)}$,

(b) the map $f|_{W_j}\colon W_j \longrightarrow X_{i(j)} \subset \mathbb{A}^n_{\bar{k}}$ is a regular map of affine $\bar{k}$-varieties.

We don't have to stop here. Building on the construction above we can define morphisms from projective varieties to projective and even affine varieties.

Definition 1.62. *Let $f\colon Y \longrightarrow X$ be a map of sets where $Y \subset \mathbb{P}^n_{\bar{k}}$ is a projective $\bar{k}$-variety and X is either an affine $\bar{k}$-variety or a projective $\bar{k}$-variety. We say that f is regular (or a morphism), if for every $i = 0, \dots, n$ the restriction $f|_{Y_i}\colon Y_i \longrightarrow X$ is regular.*

This definition allows us to define a category whose objects are either affine or projective $\bar{k}$-varieties. There are several classical examples of morphisms of projective varieties. At first we observe that there are hardly any interesting morphisms from a projective variety to affine spaces. We refer to a morphism $X \longrightarrow \mathbb{A}^1_{\bar{k}}$ as a *regular function*.

Lemma 1.63. *Let $f\colon \mathbb{P}^1_{\bar{k}} \longrightarrow \mathbb{A}^1_{\bar{k}}$ be a regular function. Then f is constant.*

Proof. We denote by $f_i \in \bar{k}[t]$ the restriction $f|_{U_i}\colon \mathbb{A}^1_{\bar{k}}$ $(i = 0, 1)$. With respect to the bijection $\phi_i\colon U_i \simeq \mathbb{A}^1_{\bar{k}}$ one has

$$\phi_i(U_0 \cap U_1) = \mathbb{G}_m\,.$$

The diagram

$$\begin{array}{ccc} U_0 \cap U_1 & \xrightarrow{\phi_0} & \mathbb{G}_m \\ \big\downarrow & & \big\downarrow{\scriptstyle t\mapsto t^{-1}} \\ U_0 \cap U_1 & \xrightarrow{\phi_1} & \mathbb{G}_m \end{array}$$

commutes. We obtain the relation $f_0(t^{-1}) = f_1(t)$. Since f_1 is a polynomial, we obtain $\deg f_0 = 0$. Hence, f is a constant. □

We leave it to the reader to generalise this result to regular functions on $\mathbb{P}^n_{\bar{k}}$ (using a similar argument). More generally one can show that regular functions on a projective variety are locally constant. Taking this for granted we deduce that a morphism $f\colon Y \longrightarrow X$ from a projective variety Y to an affine variety X factors through finitely many points. In order to arrive at interesting examples we need to study morphisms with a projective target.

Example 1.64 (Veronese embedding I)**.** *Let $f\colon \mathbb{P}^1_{\bar{k}} \longrightarrow \mathbb{P}^3_{\bar{k}}$ be the map sending $[z_0\colon z_1] \mapsto [z_0^2 : z_0z_1 : z_1^2]$.*

This is the first non-trivial case of a family of maps form projective spaces to (higher-dimensional) projective spaces.

Example 1.65 (Veronese embedding II)**.** *Let $V_{n,d}$ be the $\bar{k}$-vector space of homogenous degree d polynomials in the variables $t_0, \dots, t_n$. This is a vector space of dimension $\binom{n+d}{n}$. We choose a basis $h_0, \dots, h_{\binom{n+d}{n}}$ and define a map*

$$v_{n,d}\colon \mathbb{P}^n \longrightarrow \mathbb{P}^{\binom{n+d}{n}-1},\ \ [z_0 : \cdots : z_n] \mapsto [h_0(z_0, \dots, z_n), \dots, h_{\binom{n+d}{d}}(z_0, \dots, z_n)].$$

.

We can also define tangent spaces of points of projective varieties, and hence introduce the notion of smooth and étale morphisms.

Definition 1.66. *Let X be a projective variety and $x \in X$ a point. We define T_xX to be the $\bar{k}$-vector space T_xX_i, where $X_i \subset X$ is chosen to be one of the affine charts containing $x \in X$.*

Note that x might be contained in X_i and X_j for $i \neq j$. In this case one observes that $X_i \cap X_j$ is a standard affine open inside X_i and insider X_j, and therefore we get a canonical isomorphism $T_xX_i = T_xX_j$.

Definition 1.67. *A projective $\bar{k}$-variety X is* smooth *if for all $i = 0, \ldots, n$ the affine varieties X_i are smooth.*

Henceforth, we shall say $\bar{k}$-variety when we mean either an affine or projective $\bar{k}$-variety. We remark that many sources consider more general classes of varieties (including quasi-affine and non-projective examples).

Definition 1.68. *(a) A morphism of smooth $\bar{k}$-varieties $f\colon Y \longrightarrow X$ is* smooth *if for every $y \in Y$ the induced map of tangent spaces $df\colon T_yY \longrightarrow T_X$ is a surjection.*

(b) It is said to be étale *if d_yf is an isomorphism for all $y \in Y$.*

We conclude this subsection by giving a quick overview of the theory of projective k-varieties for non-algebraically closed fields k.

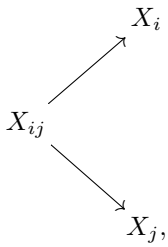
Definition 1.69. *(a) Let $\bar{X} \subset \mathbb{P}^n_{\bar{k}}$ be a projective k-variety. We say that $\bar{X}$ is* defined over $k \subset \bar{k}$ *if there exists a system of homogenous polynomials $F_0, \ldots, F_m \in k[t_0, \ldots, t_n]$, such that X agrees with*

$$\{[z_0 : \cdots : z_n] \in \mathbb{P}^n_{\bar{k}} \,|F_i(z_0, \ldots, z_n) = 0 \;\forall i = 0, \ldots, n\}.$$

(b) For every $i = 0, \ldots, n$ we obtain an affine k-variety

$$X_i = \mathsf{MSpec}\, k[t_1, \ldots, t_n]/(d_i(F_0), \ldots, d_i(F_m)).$$

We also have affine k-varieties X_{ij}, such that



and the induced $\bar{k}$-variety $\bar{X}_{ij}$ is isomorphic to $\bar{X}_i \cap \bar{X}_j$.

(c) We define a topological space $|X|$ as the union $\bigcup_{i=0}^n |X_i|$ where $|X_i| \cap |X_j| = |X_{ij}|$.[4]

[4]Formally, one defines $|X|$ as a pushout in the category of topological spaces.

(d) For $x \in X$ there exists $i = 0, \ldots, n$, such that $x \in X_i$. We write $\deg(x)$ *for the* degree *of $x \in X_i$ (see Definition 1.29).*

(e) For a field extension L/k we define $X(L)$ to be the intersection $\bar{X} \cap (k^{n+1} \setminus 0)/k^\times$. In other words, $X(k)$ is the set of points in $\bar{X}$ whose homogenous coordinates belong to k.

Recall that our base field k is always assumed to be perfect. Let $\bar{X} \subset \mathbb{P}^n_{\bar{k}}$ be a projective variety. There is a criterion for X to be defined over k in terms of Galois actions.

Proposition 1.70 (11.28 in [Spr26])**.** *The subvariety $\bar{X} \subset \mathbb{P}^n_{\bar{k}}$ is defined over $k \subset \bar{k}$ if and only if $\gamma(\bar{X}) = \bar{X}$ for all $\gamma \in \mathrm{Gal}(\bar{k}/k)$.*

The proof of this proposition is based on the technique of *Galois descent*. In fact, *loc. cit.* proves a more general assertion which also applies to subvarieties of affine space, and more generally to $\bar{k}$-subvarieties of $\bar{k}$-varieties which are defined over k.

We can use the definition above of projective varieties defined over k as the objects in a category of k-varieties. In order to define morphisms in this category one could proceed as follows.

To a map $f\colon Y \longrightarrow X$ of projective $\bar{k}$-varieties we associate its graph

$$\Gamma_f = \{(y, f(y) | y \in Y)\} \subset Y \times X \subset \mathbb{P}^n \times \mathbb{P}^m .$$

The product $\mathbb{P}^n \times \mathbb{P}^m$ is embedded into $\mathbb{P}^{nm+n+m}$ by means of the so-called *Segree embedding*.

Example 1.71 (Segre embedding)**.** *There is a map from $\mathbb{P}^n \times \mathbb{P}^m \longrightarrow \mathbb{P}^{nm+n+m}$ given by*

$$([z_0 : \cdots : z_n], [w_0 : \cdots : w_m]) \mapsto [z_0 w_0 : \cdots : z_0 w_m : z_1 w_0 : \cdots : z_1 w_m : \cdots z_n w_0 : \cdots z_n w_m].$$

One then says that $f\colon Y \longrightarrow X$ is *defined over k*, if the subset $\Gamma_f \subset \mathbb{P}^{nm+n+m}$ is a projective $\bar{k}$-variety defined over k.

2 Weil cohomology theories

The goal of this section is to state the Weil conjectures and to discuss the main ingredient of their proof: étale cohomology. Henceforth we denote by $k = \mathbb{F}_q$ a finite field with q elements, and let $\bar{k}$ be its algebraic closure.

2.1 Zeta functions

Let X be a k-variety. According to our conventions this refers to either an affine k-variety, or a projective $\bar{k}$-variety defined over k. Readers familiar with more general notions of k-varieties (or the theory of k-schemes) won't have any troubles generalising the contents of this subsection to the notion they have in mind.

For a finite field k, and an affine k-variety $X \subset \mathbb{A}^n_k$ it is clear that $X(k) \subset k^n$ is a finite set. Since every projective variety is a union of finitely many affine varieties, this finiteness property also holds for projective k-varieties.

Definition 2.1. *We let $N_r(X) = \#X(\mathbb{F}_{q^r})$ be the number of $\mathbb{F}_{q^r}$-points of X.*

This sequence of numbers is an important invariant of a k-variety. If two k-varieties are isomorphic, then they must have the same "point-counts".

Example 2.2. *We have* $N_r(\mathbb{A}^n_k) = q^{rn}$, $N_r(\mathbb{G}_{m,k}) = q^r - 1$ *and* $N_r(\mathbb{P}^n_k) = \frac{q^{nr+r}-1}{q^r-1}$.

Whenever one has an infinite series describing the solutions to an enumerative problem, it is a wise idea to capture this information in form of a generating series. This is precisely the purpose of the zeta function of X.

Definition 2.3. *We define a formal power series in a variable* T*, called the* zeta function *of* X*:*

$$Z(X,T) = \exp\left(\sum_{r=1}^{\infty} \frac{N_r}{r} T^r\right).$$

In order to get a feeling for this definition we take a look at the simplest example: a point, or 0-dimensional projective space $\mathbb{P}^0_k$. In this case, we have $N_r = 1$ for all $r \geq 1$. The zeta function therefore agrees with

$$Z(\mathbb{P}^0_k, T) = \exp\left(\sum_{r=1}^{\infty} \frac{1}{r} T^r\right) = \exp\left(-\log(1-T)\right) = (1-T)^{-1}.$$

This computation is the starting point of a generalisation to higher-dimensional projective spaces. It is based on the following lemma.

Lemma 2.4. *Let* X *be a* k*-variety, and* $Y \subset X$ *a closed* k*-subvariety with open compliment* U*. Then we have*

$$Z(X,T) = Z(Y,T) \cdot Z(U,T).$$

Proof. It is clear that $N_r(X) = N_r(Y) + N_r(U)$. We therefore have

$$Z(X,T) = \exp\left(\sum_{r=1}^{\infty} \frac{N_r(X)}{r} T^r\right) = \exp\left(\sum_{r=1}^{\infty} \frac{N_r(Y)}{r} T^r\right) \cdot \exp\left(\sum_{r=1}^{\infty} \frac{N_r(U)}{r} T^r\right),$$

and the right hand side agrees with $Z(Y,T) \cdot Z(U,T)$. □

Corollary 2.5. *We have* $Z(\mathbb{A}^n_k, T) = (1-q^nT)^{-1}$ *and* $Z(\mathbb{P}^n_k, T) = \prod_{i=0}^n (1-q^iT)^{-1}$.

Proof. We have $N_r(\mathbb{A}^n_k) = q^{rn}$, and therefore

$$Z(\mathbb{A}^n_k, T) = \exp\left(\sum_{r=1}^{\infty} \frac{1}{r} (q^nT)^r\right) = \exp\left(-\log(1-q^nT)\right) = (1-q^nT)^{-1}.$$

We deduce the assertion about the zeta function of $\mathbb{P}^n_k$ by using inductively that $\mathbb{P}^n_k$ contains $\mathbb{P}^{n-1}_k$ as a closed subvariety, with compliment $\mathbb{A}^n_k$:

$$\mathbb{P}^{n-1}_k(k) = \{[z_0 : \cdots : z_n] | z_i \in k \text{ and } z_0 = 0\} \subset \mathbb{P}^n_k(k) \supset \{[z_0 : \cdots : z_n] | z_i \in k \text{ and } z_0 \neq 0\} \simeq \mathbb{A}^n_k(k).$$

This concludes the proof. □

Proposition 2.6 (Product formula)**.** *We have an identity of formal power series*

$$Z(X,T) = \prod_{x \in |X|} \frac{1}{1 - T^{\deg(x)}}.$$

Proof. The infinite product on the right hand side is a well-defined element of $\mathbb{Z}[[T]]$, since its a product of formal series with constant coefficient 1. Let us denote the resulting element of $\mathbb{Z}[[T]]$ by $W(X,T)$ for the duration of the proof. Since the constant coefficient of $Z(X,T)$ and $W(X,T)$ are equal to 1, it suffices to show

$$Td\log Z(X,T) = Td\log W(X,T).$$

By virtue of the the definition the left hand side equals

$$Td\log Z(X,T) = \sum_{r\geq 1} N_r T^r.$$

For the right hand side we obtain

$$Td\log W(X,T) = \sum_{x\in|X|} Td\log(1-T^{\deg(x)})^{-1} = \sum_{x\in|X|} T\frac{d}{dT}\sum_{m\geq 0}\frac{T^{m\cdot\deg(x)}}{m} = \sum_{x\in|X|}\sum_{m\geq 0}\deg(x)T^{m\cdot\deg(x)}.$$

We have seen for affine n-space that the set of point $|X|$ can be identified with the quotient of $X(\bar{k})/\operatorname{Gal}(\bar{k}/k)$. Furthermore, the fibre of $X(\bar{k})\longrightarrow|X|$ over $x\in X$ has $\deg(x)$-many points. The same reasoning applies to arbitrary affine and projective k-varieties. This allows us to deduce the equality

$$N_r(X) = \sum_{d|r}\sum_{\deg(x)=d} d,$$

and we conclude $Td\log Z(X,T) = Td\log W(X,T)$. □

In the special case of $\mathbb{A}^1_{\mathbb{F}_q}$ we obtain an equality resembling another famous product formula.

Corollary 2.7. *We have an identity of infinite power series*

$$\frac{1}{1-qT} = \prod_f \frac{1}{1-T^{\deg(x)}},$$

where f runs over the set of monic irreducible polynomials in $\mathbb{F}_q[T]$.

The right left hand side of this equation is the zeta function of $\mathbb{A}^1_{\mathbb{F}_q}$. Recall that the ring $\mathbb{F}_q[T]$ has many qualitative similarities to the ring $\mathbb{Z}$ of integers. It is a Euclidean domain which implies that every ideal is principal and that prime ideals are in bijection with irreducible elements. For the Riemann zeta function we have the product formula

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}}.$$

This time the product ranges over all primes p. The right hand side is a convergent infinite product if $\mathsf{Re}\ s > 1$.

Remark 2.8. *For a ring R which is finitely generated over the integers, and a maximal ideal $\mathfrak{m}\subset R$ we denote by $q_\mathfrak{m}$ the cardinality of the field $R/\mathfrak{m}$. One can use an infinite product*

$$\zeta_R(s) = \prod_{\mathfrak{m}\in\mathsf{MSpec}\,R}\frac{1}{1-q_\mathfrak{m}^{-s}}$$

as an ansatz *to define the zeta function $\zeta_R(s)$. If $R = \mathbb{Z}$ we obtain the Riemann zeta function. For $R = \mathcal{O}_K$ the ring of integers inside a number field K, the ansatz yields the Dedkind zeta function $\zeta_R(s) = \zeta_K(s)$.*

These classical examples are wonderfully complemented by geometry. For an affine k-variety X and $R = \mathcal{O}(X)$ its ring of regular functions, we obtain

$$\zeta_R(s) = Z(X, q^{-s}).$$

Indeed, one has $q_{\mathfrak{m}} = q^{\deg(\mathfrak{m})}$. More generally, the theory of schemes allows one to associate to any finite type scheme X over $\operatorname{Spec}\mathbb{Z}$ *a zeta function $\zeta_X(s)$.*

2.2 The Frobenius morphism and Lefschetz's fixed point formula

In the last subsection we defined the zeta function $Z(X,T) \in \mathbb{Q}[[T]]$ of a variety X defined over a finite field $k = \mathbb{F}_q$. Since the definition uses the fact that a variety has only a finite number N_r of rational points defined over $\mathbb{F}_{q^r}$, this looks like a concept which only makes sense over finite fields. The goal of this subsection is to describe analogues of zeta functions for pairs (X, α), where X is a variety defined over an algebraically closed field, and α is an endomorphism of X. The link with zeta functions as we know them is provided by the *Frobenius morphism*.

Recall that we fix a finite field $k = \mathbb{F}_q$ with algebraic closure $\bar{k}$. Furthermore, we specify an inclusion of $\mathbb{F}_{q^r} \subset \bar{k}$ for all $r \geq 1$. Let X be a k-variety, we denote by $\bar{X}$ the corresponding $\bar{k}$-variety.

Lemma 2.9 (Frobenius morphisms)**.** *There exists a morphism $\mathsf{Fr}_q \colon \bar{X} \longrightarrow \bar{X}$ of $\bar{k}$-varieties, such that for a positive integer $r \geq 1$ the fixed points of $\mathsf{Fr}_q^r \colon X(\bar{k}) \longrightarrow X(\bar{k})$ agree precisely with the subset $X(\mathbb{F}_{q^r})$.*

Proof. Let us construct such a morphism for $\mathbb{A}^n_{\bar{k}}$ first. Here it is clear what we have to do. We choose $\mathsf{Fr}_q \colon \mathbb{A}^n_{\bar{k}} \longrightarrow \mathbb{A}^n_{\bar{k}}$ to be the regular map

$$(x_1, \ldots, x_n) \mapsto (x_1^q, \ldots, x_n^q).$$

If $\bar{X} \subset \mathbb{A}^n_{\bar{k}}$ is equal to $V(f_1, \ldots, f_m)$ where $f_i \in k[t_0, \ldots, t_n]$, the morphism above sends $\bar{X}$ to itself, since we have

$$\mathsf{Fr}_q^*(f_i)(t_1, \ldots, t_n) = f_i(t_1^q, \ldots, t_n^q) = f_i(t_1, \ldots, t_n)^q.$$

In the last step we have used that $\mathbb{F}_q \subset \bar{k}$ is the subfield fixed by the Frobenius automorphism $\varphi_q \colon \lambda \mapsto \lambda^q$.[5]

Similarly, if $\bar{X} \subset \mathbb{P}^n_{\bar{k}}$ is a projective variety defined over k, we can define $\mathsf{Fr}_q \colon \mathbb{P}^n_{\bar{k}} \longrightarrow \mathbb{P}^n_{\bar{k}}$ by the formula

$$[z_0 : \cdots : z_n] \mapsto [z_0^q : \cdots : z_n^q],$$

and observe that it restricts to a regular self-map of $\bar{X}$. □

A priori our proof of existence of a so-called *Frobenius morphism* $\bar{X} \longrightarrow \bar{X}$ depends on a chosen embedding onto affine or projective space. However, one can show that the resulting self-map of $\bar{X}$ is well-defined. We content ourselves with a proof of this statement for affine varieties. The projective case follows from this one by using that every projective variety is a union of affine varieties.

[5] This field automorphism goes by the name *arithmetic Frobenius*.

Lemma 2.10. *Let X be an affine k-variety with ring of regular functions $\mathcal{O}(X)$. Let $F_q\colon \mathcal{O}(X)\longrightarrow\mathcal{O}(X)$ be the map sending $f\mapsto f^q$. This is a k-algebra homomorphism. The base change*

$$\varphi_q\colon \otimes\,\mathrm{id}_{\bar{k}}\colon \mathcal{O}(\bar{X})=\mathcal{O}(X)\otimes_k\bar{k}\longrightarrow\mathcal{O}(\bar{X})=\mathcal{O}(X)\otimes_k\bar{k}$$

agrees with $\mathsf{Fr}_q^*\colon \mathcal{O}(\bar{X})\longrightarrow\mathcal{O}(\bar{X})$ constructed in Lemma 2.9.

Proof. The map $\varphi_q\colon \mathcal{O}(X)\longrightarrow\mathcal{O}(X)$ is a ring homomorphism, since k is of characteristic p and $\mathcal{O}(X)$ is a k-algebra. This implies $(f+g)^q=f^q+f^q$. Furthermore, for $f\in k=\mathbb{F}_q$ we have $f^q=f$ which implies $\varphi(fg)=\varphi(f)\varphi(g)=f\varphi(g)$, and therefore that φ is a k-algebra homomorphism.

A k-algebra homomorphism of affine k-algebras $\alpha\colon R_1\longrightarrow R_2$ yields a commutative diagram

$$\begin{array}{ccc} R_1 & \xrightarrow{\varphi_q} & R_1 \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha} \\ R_2 & \xrightarrow{\varphi_q} & R_2. \end{array}$$

The Dictionary 1.22 implies that we have a well-defined map $F_q\colon \bar{X}\longrightarrow\bar{X}$, and furthermore, for every morphism $g\colon Y\longrightarrow X$ of affine k-varieties, we obtain a commutative diagram

$$\begin{array}{ccc} \bar{Y} & \xrightarrow{F_q} & \bar{Y} \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g} \\ \bar{X} & \xrightarrow{F^q} & \bar{X} \end{array}$$

Since an affine k-variety can be embedded into an affine n-space, it suffices to show for $\mathbb{A}^n_{\bar{k}}$ the equality $F_q=\mathsf{Fr}_q$. In this case, $\mathcal{O}(\mathbb{A}^n_k)=k[t_1,\ldots,t_n]$ and φ_q equals the map $t_i\mapsto t_i^q$. This concludes the proof. □

The existence Frobenius morphism changes our viewpoint of zeta funtions as being a purely characteristic p phenomenon. The following definition makes sense in greater generality.

Definition 2.11. *Let $\mathbb{K}$ be an algebraically closed field (of arbitrary characteristic), and X a $\mathbb{K}$-variety together with a morphism*

$$\alpha\colon X\longrightarrow X,$$

such that for every integer $r\geq 1$ there is only a finite number of fixed points $N_r=N_r(X,\alpha)$ of α_r. We define $Z(X,\alpha;T)=\exp(\sum_{r\geq 1}\frac{N_r}{r}T^r)\in\mathbb{Q}[[T]]$ and refer to it as the zeta function *of (X,α).*

In particular we can now work with the field of complex numbers $\mathbb{K}=\mathbb{C}$. This allows one to use geometric methods to study examples. Let's take a look at endomorphisms of the Riemann sphere $\mathbb{P}^1_{\mathbb{C}}$. We denote by n a positive integer and $\phi_n\colon \mathbb{P}^1_{\mathbb{C}}\longrightarrow\mathbb{P}^1_{\mathbb{C}}$ the morphism given by $[z:w]\mapsto[z^n:w^n]$.

Example 2.12. *The morphism ϕ_n always fixes $0=[0:1]$ and $\infty=[0:1]$. For the subset $\mathbb{C}^\times=\mathbb{P}^1_{\mathbb{C}}\setminus\{0,\infty\}$ we have $\phi_n(z)=z$ if and only if $z^{n-1}=1$. That is, if and only if z is a root of unity of order $n-1$. The total number of fixed points N_n of ϕ_n is therefore $n+1$. This shows that we have*

$$Z(\mathbb{P}^1_{\mathbb{C}},\phi_n;T)=\exp\left(\sum_{r\geq 1}\frac{n^r+1}{r}T^r\right)=\exp\left(\sum_{r\geq 1}\frac{1}{r}T^r\right)\cdot\exp\left(\sum_{r\geq 1}\frac{n^r}{r}T^r\right)=\frac{1}{(1-T)(1-nT)}.$$

We observe that we have an equality of zeta functions $Z(\mathbb{P}^1_{\mathbb{C}}, \alpha_q; T) = Z(\mathbb{P}^1_{\mathbb{F}_q}, T)$. The zeta functions associated to complex varieties with endomorphisms therefore stand a chance of being a good model for zeta functions of varieties over finite fields. The upshot is that over the complex numbers we have topology at our disposal which allows one to prove interesting facts about the zeta functions $Z(X, \alpha; T)$. An important tool is given by singular cohomology.

Let us denote by Top the category of topological spaces. In cohomology theory one constructs a sequence of functors

$$(H^i)_{i\geq 0} \colon \mathsf{Top}^{\mathsf{op}} \longrightarrow \mathsf{Vect}_{\mathbb{Q}},$$

from the (opposite of the) category of topological spaces to the category of $\mathbb{Q}$-vector spaces. In particular, one associates to a space X a rational vector space $H^i(X, \mathbb{Q})$ and to every continuous map $f \colon Y \longrightarrow X$ a linear map $f^* \colon H^i(X, \mathbb{Q}) \longrightarrow H^i(Y, \mathbb{Q})$. We refer the reader to Hatcher's [Hat, Chapter 3] for a detailed account of singular cohomology theory.

Example 2.13. *For a d-dimensional sphere S^d one has $H^i(S^d, \mathbb{Q}) = 0$, if $i \neq 0, d$ and $H^i(S^d, \mathbb{Q}) \simeq \mathbb{Q}$ for $i = 0, d$. For a self-map $f \colon S^d \longrightarrow S^d$ one obtains an endomorphism f^* of $H^d(S^d, \mathbb{Q})$. This corresponds to a number* $\deg(f)$ *which is called the degree of f.*[6]

The importance of cohomology in the study of zeta functions is due to the following theorem by Lefschetz:

Theorem 2.14 (Lefschetz's fixed point formula)**.** *Let X be a compact manifold with a continuous self-map $f \colon X \longrightarrow X$. If f has only a finite number $N(f)$ of fixed points, then*

$$N(f) = \sum_{i\geq 0} (-1)^i \,\mathsf{Tr}\left(f^* \colon H^i(X, \mathbb{Q}) \longrightarrow H^i(X, \mathbb{Q})\right).$$

Exercise 2.15. *Prove the Lefschetz fixed point formula for a self-map $f \colon S \longrightarrow S$ of a finite set S. That is, denoting by*

$$f^* \colon \mathbb{Q}^S \longrightarrow \mathbb{Q}^S$$

the induced linear map, show that one has

$$\#\mathsf{Fix}(f) = \mathsf{Tr}\ f^*.$$

Let's take a look at our maps $\phi_n \colon \mathbb{P}^1_{\mathbb{C}} \longrightarrow \mathbb{P}^1_{\mathbb{C}}$. Since $\mathbb{P}^1_{\mathbb{C}}$ is homeomorphic to S^2 we obtain precisely two non-trivial maps

$$H^i(\phi_n) \colon \mathbb{Q} \longrightarrow \mathbb{Q}$$

for $i = 0, 2$.

Lemma 2.16. *We have $H^0(\phi_n) = \mathrm{id}_{H^0(S^2, \mathbb{Q})}$.*

First proof. Let P be a topological space consisting of a single point. We denote by $i \colon P \longrightarrow S^2$ the map sending this point to $\infty \in S^2 \simeq (\mathbb{P}^1_{\mathbb{C}})^{\mathsf{an}}$. One has that $H^0(i) \colon H^0(S^2) \longrightarrow H^0(P)$ is an isomorphism. This follows for example from the cellular cohomology complex of the CW-complex S^2 with P being the unique 0-cell, and $S^2 \setminus \{\infty\}$ the unique 2-cell (see [Hat, p. 203] and [Hat, p.

[6] A priori this is a rational number, however since cohomology also exists over $\mathbb{Z}$ it can be shown to be an integer.

137] for a more detailed account of cellular homology). The commutative diagram of topological spaces

$$\begin{array}{ccc} P & & \\ \downarrow & \searrow & \\ S^2 & \xrightarrow{\phi_n} & S^2 \end{array}$$

commutes. We therefore obtain a commutative diagram of abelian groups

$$\begin{array}{ccc} H^0(P) & & \\ {\scriptstyle H^0(i)}\uparrow & \nwarrow^{H^0(i)} & \\ H^0(S^2) & \xleftarrow{H^0(\phi_n)} & H^0(S^2). \end{array}$$

Since $H_0(i)$ is an isomorphism, we deduce $H_0(\phi_n) = \mathrm{id}_{H_0(S^2,\mathbb{Q})}$. □

Second proof. We give another prove of the first assertion which is more elementary as it uses the definition of singular cohomology. It will follow from the following claim and the fact that S^2 has a unique connected component. For a topological space X we denote by $\pi_0(X)$ the set of path-connected components. It is clear that we have a functor

$$\pi_0 \colon \mathsf{Top} \longrightarrow \mathsf{Set},$$

which sends X to $\pi_0(X)$ and a continuous map $f \colon Y \longrightarrow X$ to $\pi_0(f) \colon \pi_0(Y) \longrightarrow \pi_0(X)$ (well-defined since images of path-connected spaces are path connected). We also have a functor

$$\mathsf{Map}(-, \mathbb{Q}) \colon \mathsf{Set}^{\mathsf{op}} \longrightarrow \mathsf{AbGrp}$$

sending a set S to the set of maps $S \longrightarrow \mathbb{Q}$ which we denote by $\mathbb{Q}^S$.

Claim 2.17. *We have a natural isomorphism of functors*

$$H^0 \simeq \mathsf{Map}(\pi_0, \mathbb{Q}) \colon \mathsf{Top} \longrightarrow \mathsf{AbGrp}\,.$$

That is, for a topological space X we have a linear isomorphism $\beta_X \colon H^0(X) \xrightarrow{\simeq} \mathbb{Q}^S$, such that for a continuous map $f \colon Y \longrightarrow X$ the diagram

$$\begin{array}{ccc} H^0(X) & \xrightarrow{H^0(f)} & H^0(Y) \\ {\scriptstyle \beta_X}\downarrow & & \downarrow{\scriptstyle \beta_Y} \\ \mathbb{Q}^{\pi_0(X)} & \longrightarrow & \mathbb{Q}^{\pi_0(Y)} \end{array} \tag{3}$$

commutes.

Proof. By definition, $H^0(X, \mathbb{Q})$ is the kernel of a linear map of vector spaces

$$C^0(X, \mathbb{Q}) \xrightarrow{\delta} C^1(X, \mathbb{Q}).$$

Their definition is as follows: $C^0(X,\mathbb{Q})$ is the rational vector space of set-theoretic maps $c\colon X\longrightarrow\mathbb{Q}$. We denote by PX the set of continuous maps $\sigma\colon[0,1]\longrightarrow X$ and let $C^1(X,\mathbb{Q})$ be the rational vector space of set-theoretic maps $c_1\colon PX\longrightarrow\mathbb{Q}$. The so-called coboundary map $\delta\colon C^0(X,\mathbb{Q})\longrightarrow C^1$ is given by

$$\delta(c)\colon\sigma\mapsto c(\sigma(1))-c(\sigma(0)).$$

We therefore see that $c\in\ker\delta$ if and only if $c\colon X\longrightarrow\mathbb{Q}$ is constant on pathconnected components. In other words, if and only if we have a factorisation

$$\begin{array}{ccc} X & & \\ \downarrow & \searrow^{c} & \\ \pi_0(X) & \longrightarrow & \mathbb{Q}\,. \end{array}$$

This shows $H^0(X,\mathbb{Q})=\ker\delta\simeq\mathbb{Q}^{\pi_0(X)}$. For the second assertion we remark that

$$H^0(f)\colon H^0(X,\mathbb{Q})\longrightarrow H^0(Y,\mathbb{Q})$$

is given by the map $\ker_{\delta_X}\longrightarrow\ker\delta_Y$ sending $c\colon X\longrightarrow\mathbb{Q}$ to the composition $c\circ f$. The commutative diagram

$$\begin{array}{ccccc} Y & \xrightarrow{f} & X & & \\ \downarrow & & \downarrow & \searrow^{c} & \\ \pi_0(Y) & \xrightarrow{\pi_0(f)} & \pi_0(X) & \longrightarrow & \mathbb{Q} \end{array}$$

yields that the diagram (3) commutes. □

The proof now simply follows from the fact that $\#\pi_0(S^2)=1$. Therefore, we have that the map $\pi_0(\phi_n)\colon\pi_0(S^2)\longrightarrow\pi_0(S^2)$ is the identity morphism. □

Lemma 2.18. *We have* $H^2(\phi_n)=n\cdot\mathrm{id}_{H^2(S^2,\mathbb{Q})}$ *and thus* $\mathsf{Tr}(H^2(\phi_n))=n$.

Proof. We will deduce this from the Mayer–Vietoris sequence [Hat, p. 149 & p. 203] associated to the covering

$$(\mathbb{P}^1_{\mathbb{C}})^{\mathsf{an}}=\mathbb{C}\cup(\mathbb{P}^1_{\mathbb{C}})^{\mathsf{an}}\setminus\{0\}.$$

This long exact sequences relates the cohomology groups of $(\mathbb{P}^1_{\mathbb{C}})^{\mathsf{an}}$, $\mathbb{C}$ and $\mathbb{C}^\times$. We have the following excerpt for every $i\geq 0$:

$$H^{i-1}(\mathbb{C},\mathbb{Q})\oplus H^{i-1}(\mathbb{C},\mathbb{Q})\longrightarrow H^{i-1}(\mathbb{C}^\times,\mathbb{Q})\longrightarrow H^i((\mathbb{P}^1_{\mathbb{C}})^{\mathsf{an}},\mathbb{Q})\longrightarrow H^i(\mathbb{C},\mathbb{Q})\oplus H^i(\mathbb{C},\mathbb{Q})\longrightarrow H^i(\mathbb{C}^\times,\mathbb{Q}).$$

The topological space $\mathbb{C}$ is contractible, that is, homotopy equivalent to a point. We deduce $H^i(\mathbb{C},\mathbb{Q})=0$ for $i>0$ and $H^0(\mathbb{C},\mathbb{Q})=\mathbb{Q}$. The Mayer–Vietoris sequence therefore implies $H^i((\mathbb{P}^1_{\mathbb{C}})^{\mathsf{an}},\mathbb{Q})\simeq H^{i-1}(\mathbb{C}^\times,\mathbb{Q})$ for $i\geq 1$.

We leave it to the reader as an exercise to check that one has a commutative diagram

$$\begin{array}{ccc} H^i((\mathbb{P}^1_{\mathbb{C}})^{\mathsf{an}},\mathbb{Q}) & \xrightarrow{\phi_n} & H^i((\mathbb{P}^1_{\mathbb{C}})^{\mathsf{an}},\mathbb{Q}) \\ \downarrow & & \downarrow \\ H^{i-1}(\mathbb{C}^\times,\mathbb{Q}) & \xrightarrow{\phi_n} & H^{i-1}(\mathbb{C}^\times,\mathbb{Q}). \end{array}$$

It suffices therefore to understand the maps $H^1(\phi_n)\colon H^1(\mathbb{C}^\times,\mathbb{Q}) \longrightarrow H^1(\mathbb{C}^\times,\mathbb{Q})$. We observe that the topological space $\mathbb{C}^\times$ is homeomorphic to $S^1 \times \mathbb{R}^\times$, and therefore homotopy equivalent to S^1. This shows that we have a commutative diagram

$$\begin{array}{ccc} H^1(\mathbb{C}^\times,\mathbb{Q}) & \xrightarrow{H^1(\phi_n)} & H^1(\mathbb{C}^\times,\mathbb{Q}) \\ \simeq\downarrow & & \downarrow\simeq \\ H^1(S^1,\mathbb{Q}) & \xrightarrow{H^1(\phi_n)} & H^1(S^1,\mathbb{Q}), \end{array}$$

which allows us to trade $\mathbb{C}^\times$ for the easier space $S^1 \subset \mathbb{C}^\times$. In order to compute the induced map in cohomology of the self-map $\phi_n\colon S^1 \longrightarrow S^1$, we use cellular cohomology (see [Hat, p. 203]).

On the left hand copy of S^1 we consider the cell decomposition with the set of 0-cells being the set of n-th roots of unity $\mu_n \subset S^1$. On the right hand side we can put S^1 with the standard CW decomposition where we have a single 0-cell at $1 \in S^1$. It is clear that with respect to these cell decompositions, the map $\phi_n\colon (S^1)_{\text{left}} \longrightarrow (S^1)_{\text{right}}$ is a map of CW-complexes. In terms of the cellular cohomology complexes, we obtain

$$\begin{array}{ccc} \mathbb{Q}^n & \xrightarrow{\delta} & \mathbb{Q}^n \\ {\scriptstyle\phi_n^*}\downarrow & & \downarrow{\scriptstyle\phi_n^*} \\ \mathbb{Q} & \xrightarrow{\delta} & \mathbb{Q}\,. \end{array}$$

The vertical morphisms are given by the linear map corresponding to the row vector $\phi_n^* = (1\ \cdots\ 1)$. By definition, we have $H^1(S^1,\mathbb{Q}) = \operatorname{coker}\delta = \mathbb{Q}^n \,/\, \mathsf{im}(\delta)$ (respectively $\mathbb{Q} \,/\, \mathsf{im}(\delta)$). The cokernel of δ can be identified with $\mathbb{Q}$ by virtue of the map $\mathbb{Q}^n \longrightarrow \mathbb{Q}$ given by the column matrix

$$\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} :\ \mathbb{Q}^n \longrightarrow \mathbb{Q}\,.$$

The induced map of ϕ_n on $H^1(S^1,\mathbb{Q}) = \operatorname{coker}\delta$ is therefore $\sum_{i=1}^n 1 = n$. □

In summary, all we have done so far is verifying the Lefschetz fixed point formula for $\phi_n\colon (\mathbb{P}^1_{\mathbb{C}})^{\mathsf{an}}$. Indeed, we have

$$\mathsf{Tr}(H^0(\phi_n)) + \mathsf{Tr}(H^2(\phi_n)) = n + 1 = \#\,\mathsf{Fix}(\phi_n).$$

We now turn to a more serious application of the Lefschetz fixed point formula. We will study zeta functions of pairs (M,α) where M is a compact manifold and α a continuous self-map $M \longrightarrow M$, such that every power α^r has a finite number of fixpoints N_r. As before, we denote by

$$Z(M,\alpha;T) = \exp\Big(\sum_{r\geq 1} \frac{N_r}{r} T^r\Big) \in \mathbb{Q}[[T]]$$

the *zeta function* of (M,α). The case we care most about is where the pair (M,α) arises by analytification of a smooth projective variety X and a regular endomorphism α.

Proposition 2.19. *We have an identity of formal power series*

$$Z(X,T) = \frac{\prod_{i\geq 0} \det(1 - T \cdot H^{2i+1}(\alpha))}{\prod_{i\geq 0} \det(1 - T \cdot H^{2i}(\alpha))}.$$

In particular, the zeta function $Z(M,\alpha;T)$ equals the Taylor series expansion of the rational function *in T (with integral coefficients).*

Proof. We apply the Lefschetz fixed point formula 2.14. We have

$$N_r = \sum_{i\geq 0} (-1)^i \,\mathsf{Tr}(H^i(\alpha^n)) = \sum_{i\geq 0} (-1)^i \,\mathsf{Tr}(H^i(\alpha)^r),$$

and thus

$$Z(M,\alpha;T) = \exp\left(\sum_{r\geq 1} \frac{\sum_{i\geq 0}(-1)^i \,\mathsf{Tr}(H^i(\alpha^r))}{r} T^r\right) = \prod_{i\geq 0} \exp\left((-1)^i \sum_{r\geq 1} \frac{\mathsf{Tr}(H^i(\alpha)^r)}{r} T^r\right).$$

Lemma 2.20. *Let $\phi\colon V \longrightarrow V$ be a $\mathbb{K}$-linear endomorphism of a finite-dimensional $\mathbb{K}$-linear vector space V. Then, we have an identity of formal power series*

$$\exp\left(\sum_{r\geq 1} \frac{\mathsf{Tr}(\phi^r)}{r} T^r\right) = \frac{1}{\det(1 - T \cdot \phi)} \in \mathbb{K}[[T]].$$

Proof. Without loss of generality we may replace $\mathbb{K}$ by a field extension to verify this equality. In particular we may assume that $\mathbb{K}$ is algebraically closed. We may then assume that $V = \mathbb{K}^m$ and ϕ is represented by a triangular matrix

$$\begin{pmatrix} \lambda_1 & \cdots & & \\ 0 & \lambda_2 & \cdots & \\ & & \ddots & \\ 0 & \cdots & 0 & \lambda_m \end{pmatrix}.$$

We conclude the identity

$$\mathsf{Tr}(\phi^r) = \sum_{i=1}^m \lambda_i^r$$

and therefore

$$\exp\left(\sum_{r\geq 1} \frac{\sum_{i=1}^m \lambda_i^r}{r} T^r\right) = \prod_{i=1}^m (1 - \lambda_i \cdot T)^{-1} = \frac{1}{\det(1 - T \cdot \phi)}.$$

□

Using this lemma we finish the computation above:

$$Z(M,\alpha;T) = \prod_{i\geq 0} \exp\left((-1)^i \sum_{r\geq 1} \frac{\mathsf{Tr}(H^i(\alpha)^r)}{r} T^r\right),$$

and the right hand side agrees with

$$\frac{\prod_{i\geq 0}\det(1-T\cdot H^{2i+1}(\alpha))}{\prod_{i\geq 0}\det(1-T\cdot H^{2i}(\alpha))}.$$

This concludes the proof. □

We don't stop here. Cohomology has more in store in for us. But at first we need to recall the cup product and Poincaré duality. For a topological space M we have a bilinear map

$$H^i(M,\mathbb{Q})\times H^j(M,\mathbb{Q})\longrightarrow H^{i+j}(M,\mathbb{Q}),\ \ (\alpha,\beta)\mapsto \alpha\cup\beta.$$

This bilinear map is compatible with the functoriality of cohomology. That is, for a continuous map $f\colon M\longrightarrow N$ we have

$$H^{i+j}(f)(\alpha\cup\beta)=H^i(f)(\alpha)\cup H^j(f)(\beta).$$

We refer the reader to [Hat, Sect. 3.2] for an overview of the cup product.

Theorem 2.21 (Poincaré duality)**.** *Let M be a compact orientable manifold of dimension d. Then we have $H^d(M,\mathbb{Q})\simeq\mathbb{Q}$ and a perfect pairing*

$$H^i(M,\mathbb{Q})\times H^{d-i}(M,\mathbb{Q})\longrightarrow H^d(M,\mathbb{Q}),\ \ (\alpha,\beta)\mapsto\alpha\cup\beta.$$

Corollary 2.22 (Functional equation)**.** *Let M be a compact orientable manifold of even dimension d, together with a continuous endomorphism α, such that every power α^r has a finite number of fixed points. Then we have*

$$Z(M,\alpha;T)=c\cdot T^{\chi(M)}\cdot Z(M,\alpha,\frac{1}{n^dT}),$$

where $\chi(M)=\sum_{i\geq 0}(-1)^i\,\mathsf{rk}\,H^i(M,\mathbb{Q})$ denotes the Euler characteristic of M and $c\in\mathbb{Q}$ is a constant, and $n=\mathsf{Tr}(H^d(\alpha))$.

Proof. Let $P_i(T)$ be the polynomial $\det(1-T\cdot H^i(\alpha))$. We then have

$$P_i(\frac{1}{nT})=c_iT^{\mathsf{rk}\,H^i(X,\mathbb{Q})}P_{d-i}(1-T\cdot H^{d-i}(\alpha)). \tag{4}$$

Taking the product of these identities we obtain the functional equation.

Equation (4) follows from the fact that we have a perfect pairing

$$H^i(M,\mathbb{Q})\times H^{d-i}(M,\mathbb{Q})\longrightarrow H^d(M,\mathbb{Q}),\ \ (x,y)\mapsto x\cup y,$$

and equation $H^i(\alpha)(x)\cup H^{d-i}(\alpha)(y)=H^d(\alpha)(x\cup y)=n(x\cup y)$.

Lemma 2.23. *Let V,W be finite-dimensional $\mathbb{K}$-vector spaces (where $\mathbb{K}$ has characteristic 0), and $b\colon V\times W\longrightarrow\mathbb{K}$ a perfect pairing. Assume that we have endomorphisms $f\in\mathsf{End}(V)$, $g\in\mathsf{End}(W)$, and $n\in\mathbb{K}^\times$, such that we have*

$$b\,(f(x),g(y))=nb(x,y)$$

for all $x\in V$ and $y\in W$. Then

$$\det(1-T\cdot g)=\frac{(-1)^{\dim V}n^{\dim V}T^{\dim V}}{\det(f)}\cdot\det\left(1-\frac{f}{nT}\right).$$

Proof. Without loss of generality we assume that $\mathbb{K}$ is algebraically closed (or at least contains all eigenvalues of f and g). We prove the formula above by induction on $\dim V$. In the base case $\dim V = 1$ we can identity f and g with their eigenvalues in $\mathbb{K}$, and compute

$$1 - T \cdot g = -\frac{nT}{f} \cdot \left(1 - \frac{f}{nT}\right),$$

using the identity $fg = n$.

We assume by induction that the equation has verified for vector spaces of rank r. For the induction step we consider V and W to be of rank $r+1$, and observe that f and g can't be the zero maps (since $n \neq 0$). Let v be an eigenvector of f corresponding to a non-zero eigenvalue λ. The annihilator $v^\perp \subset W$ is then of rank r. It is preserved by g, since for $y \in V' = v^\perp$ we have

$$0 = nb(v, y) = b(fv, gy) = \lambda b(v, gy).$$

We conclude that there exists $w \in W \setminus V'$, such that $b(v, w) = 1$ and w is an eigenvector for g for an eigenvalue μ (automatically non-zero). As before we see that $W' = w^\perp \subset V$ is a subspace of rank r, preserved by f. The pairing b restricts to a perfect pairing $V^\times W' \longrightarrow \mathbb{K}$; $f' = f|_{V'}$ and $g' = g|_{W'}$ still satisfy the assumptions of the lemma. Using the induction hypothesis and the rank 1 case we obtain

$$\det(1-T\cdot g) = \det(1-T\cdot g')(1-\mu T) = \frac{(-1)^{\dim V'} n^{\dim V'} T^{\dim V'}}{\det(f')} \cdot \det\left(1 - \frac{f'}{nT}\right) \cdot \frac{-nT}{\lambda} \cdot \left(1 - \frac{\lambda}{nT}\right).$$

We conclude the proof by observing that the right hand side equals $\frac{(-1)^{\dim V} n^{\dim V} T^{\dim V}}{\det(f)} \cdot \det\left(1 - \frac{f}{nT}\right)$. □

Applying the lemma above to $H^i(\alpha)$ and $H^{d-i}(\alpha)$ and the cup product pairing, we obtain the requested functional equation. □

Remark 2.24. *Compare the functional equation above to the one satisfied by the Riemann zeta function*

$$\xi(s) = \xi(1-s)$$

where $\xi(s) = \frac{1}{2}\pi^{-\frac{s}{2}} s(s-1)\Gamma(\frac{s}{2})\zeta(s)$.

Exercise 2.25. *Let* $\mathbb{T} = S^1 \times S^1$ *be the manifold given by a 2-torus. Let* $m, n \in \mathbb{N}$ *be positive integers, and let*

$$\alpha \colon \mathbb{T} \longrightarrow \mathbb{T}, \quad (z, w) \mapsto (z^m, w^n).$$

Compute the zeta function $Z(\mathbb{T}, \alpha; T)$ *(as an element of* $\mathbb{Q}(T)$*).*

2.3 The Weil conjectures

Inspired by the computations of $Z(M, \alpha; T)$ using the Lefschetz trace formula we engage in the following phantasy:

Phantansy 2.26. *A* cohomology theory *for smooth varieties over* $\bar{k} = \bar{\mathbb{F}}_p$*, that is, a sequence of functors*

$$\left(H^i\right)_{i\in\mathbb{N}} : (\mathsf{Var}_{\bar{k}}^{\mathrm{sm,proj}})^{\mathsf{op}} \longrightarrow \mathsf{Vect}_{\mathbb{Q}},$$

such that we have

(a) cup products*: $H^i(\bar{X}) \times H^j(\bar{X}) \longrightarrow H^{i+j}(\bar{X})$, compatible with pullback of cohomology classes,*

(b) Poincaré duality*: let d be the dimension of $\bar{X}$ and assume $\bar{X}$ is connected, then $H^i(\bar{X}) = 0$ for $i > 2d$, there exists an isomorphism $H^{2d}(\bar{X}) \simeq \mathbb{Q}$, and $H^i(\bar{X}) \times H^{2d-i}(\bar{X}) \longrightarrow H^{2d}(\bar{X})$ is a perfect pairing.*

(c) Lefschetz fixed point formula*: let X be a k-model for $\bar{X}$ and $\mathsf{Fr}_X \colon \bar{X} \longrightarrow \bar{X}$ the induced Frobenius morphism. Then we have*

$$\#X(\mathbb{F}_q) = \sum_{i \geq 0} (-1)^i \operatorname{\mathsf{Tr}}(H^i(\mathsf{Fr}_X)).$$

(d) we have $H^{2d}(\mathsf{Fr}_X) = q^d \cdot \mathrm{id}$ and $H^0(\mathsf{Fr}_X) = \mathrm{id}$.

The same computations lead us to the first two statements in Weil's conjectures:

Weil Conjectures 2.27. *Let X be a smooth and projective variety over $\mathbb{F}_q$ of dimension d.*

(a) The zeta function $Z(X,T) \in \mathbb{Q}[[T]]$ is the Taylor series expansion of a rational function*, that is, an element of $\mathbb{Q}(T)$.*

(b) It satisfies the functional equation

$$Z(X, \frac{1}{q^d T}) = \pm q^{\frac{d\chi}{2}} T^\chi Z(X,T),$$

where $\chi = \sum_{i=0}^{2d} (-1)^i \operatorname{\mathsf{rk}} H^i(X)$.

(c) We have the "Riemann hypothesis"*:*

$$Z(X,T) = \frac{\prod_{i=0,\ odd}^{2d} P_i(T)}{\prod_{j=0,\ even}^{2d} P_j(T)},$$

where $P_i(T) \in \mathbb{Q}[T]$ is a polynomial satisfying

$$P_i(\alpha) = 0 \Rightarrow |\alpha| = q^{\frac{i}{2}}.$$

In the following subsections we will study our first non-trivial example of zeta functions of varieties over finite fields: elliptic curves. This example brings good and bad news for our phantasy: we will show that the Weil conjectures hold for elliptic curves; but will be forced to acknowledge that Phantasy 2.26 is too optimistic.

2.4 A crash course on elliptic curves

A *curve* X over an algebraically closed field $\mathbb{K}$ is a smooth projective $\mathbb{K}$-variety of dimension 1 (that is, all tangent spaces have dimension 1). If $\mathbb{K} = \mathbb{C}$ have the *analytification* functor from 1.4 which assigns to X a compact complex manifold X^{an} of dimension 1.

Complex manifolds of dimension 1 are also referred to as Riemann surfaces. The topological space underlying X^{an} is a compact orientable surface, and therefore up to homeomorphism classified by its genus g. We hurry to add that there's a whole family of different complex structures on any given orientable topological surface, unless the genus is 0.

Definition 2.28. *A $\mathbb{K}$-curve of genus 1 is said to be an* elliptic curve.

So far we have only given a definition of the genus of a curve for $\mathbb{K} = \mathbb{C}$. We will make good for this in Definition **??** below, and first study elliptic curves over the field of complex numbers.

Proposition 2.29. *Let $E/\mathbb{C}$ be an elliptic curve, then there exists a biholomorphic map $E^{\mathsf{an}} \simeq \mathbb{C}/\Gamma$, where $\Gamma = \mathbb{Z} \oplus \tau\mathbb{Z}$ with $\mathsf{Im}\,\tau > 0$.*

In particular, we see that E^{an} is a group object in the category of complex manifolds. The group structure in induced by $+\colon \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C}$.

Definition 2.30. *Let $\mathbb{K}$ be an arbitrary field. A group object in the category of smooth projective $\mathbb{K}$-curves, is said to be an* elliptic curve.

Since E is a group object, there exists a neutral element 0, presented by a morphism $0\colon \mathbb{P}^0_{\mathbb{K}} \longrightarrow E$. In particular, $0 \in E(\mathbb{K})$ is a $\mathbb{K}$-rational point. We denote the group structure by $+\colon E \times E \longrightarrow E$.

Definition 2.31. *We let $\mathsf{End}(E)$ be the set of endomorphisms of $f\colon E \longrightarrow E$, satisfying $f(0) = 0$.*[7] *One defines a structure of an abelian group on this set by defining*

$$f_1 + f_2 = \mathsf{add} \circ (f_1, f_2),$$

where $\mathsf{add}\colon E \times E \longrightarrow E$ denotes the group structure. Furthermore, composition of endomorphisms gives rise to a multiplication

$$f_1 \cdot f_2 = f_1 \circ f_2$$

which distributes over $+$. Therefore, we have a non-commutative ring structure on $\mathsf{End}(E)$.

The non-commutative ring $\mathsf{End}(E)$ has additional properties which play an important role in the proof of the Weil conjectures for elliptic curves:

Lemma 2.32. *There exists a function $\deg\colon \mathsf{End}(E) \longrightarrow \mathsf{End}(E)$, such that*

(a) $\deg([n]) = n^2$, *where $[n]$ denotes the endomorphism $[n]\colon x \mapsto n \cdot x$,*

(b) $\deg$ *is a positive-definite quadratic form, in particular we have $\deg f = 0$ if and only if $f = 0$.*

Proof. See [Sil86, Corollary III.6.3] □

Corollary 2.33. *The natural map $\mathbb{Z} \longrightarrow \mathsf{End}(E)$, sending an integer n to the endomorphism $[n]\colon x \mapsto n \cdot x$, is injective.*

Lemma 2.34. *Let E be an elliptic curve over an algebraically closed field $\mathbb{K}$, and $f \in \mathsf{End}(E)$, such that $f\colon E \longrightarrow E$ is étale. Then*

$$\deg f = \#f^{-1}(0).$$

Proof. See [Sil86, Theorem III.4.10(c)]. □

Lemma 2.35. *There exists an involution $f \mapsto \widehat{f}$, such that*

(a) $\widehat{f}_1 + \widehat{f}_2 = \widehat{f_1 + f_2}$,

[7] One can show that this assumption implies that f respects the group structure on E.

(b) $\widehat{f_1}\widehat{f_2} = \widehat{f_2 f_1}$,

(c) $\widehat{[n]} = [n]$ *for* $n \in \mathbb{Z}$,

(d) $f\widehat{f} = [\deg f] = \widehat{f}f$.

Proof. See [Sil86, Theorems III.6.1, III.6.2]. □

Proof. We have $\deg[n] = n^2 \geq 0$, whenever $n \neq 0$. This shows $[n] \neq 0$ in this case. □

If $\bar{E}$ is an elliptic curve over $\bar{k}$ with a model over the finite field k, there is an important element in $End(\bar{E})$ often called the *Lang isogeny*.

Lemma 2.36. *The isogeny* $\mathrm{id}_X - \mathsf{Fr}_X$ *is étale.*

Proof. See [Sil86, Corollary III.5.5]. □

2.5 The Weil conjectures for elliptic curves

We fix a finite field $k = \mathbb{F}_q$ with algebraic closure $\bar{k}$, and an elliptic curve E defined over k. For $r \geq 1$ we denote by N_r the number of $\mathbb{F}_{q^r}$-rational points of E. As always, we define the zeta function

$$Z(E,T) = \exp\left(\sum_{r\geq 1} \frac{N_r}{r} T^r\right).$$

Theorem 2.37 (Hasse)**.** *The zeta function* $Z(E,T)$ *equals the Taylor series expansion of a rational function*

$$\frac{P(T)}{(1-T)(1-qT)},$$

where $P(T) \in \mathbb{Q}[T]$ *is a polynomial of degree* 2*, such that* $P(T) = (1-\alpha T)(1-\bar{\alpha})T$ *in* $\mathbb{C}[T]$ *with* $|\alpha| = \sqrt{q}$.

The Riemann hypothesis for elliptic curves implies the following non-trivial estimate.

Corollary 2.38 (Hasse, conjectured by E. Artin)**.** *One has the inequality*

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

Proof. The formula for the zeta function

$$Z(E,T) = \frac{(1-\alpha T)(1-\bar{\alpha}T)}{(1-T)(1-qT)}$$

yields

$$N_r = q^r + 1 - (\alpha^r + \bar{\alpha}^r).$$

This shows

$$|q^r + 1 - N_r| \leq 2|\alpha| = 2\sqrt{q^r}.$$

For $r = 1$ this implies the claim. □

Let us take a look at the meaning of the *Hasse bound*, for $p > 2$. The affine elliptic curve $E \setminus 0$ is the zero set of the so-called Weierstrass embedding:

$$y^2 = f(x),$$

where f is a cubic polynomial of degree 3. We therefore see that the number $\frac{N_r - 1}{2}$ roughly speaking counts the number of $x \in \mathbb{F}_{q^r}$, such that $f(x)$ is a square in $\mathbb{F}_q$ (for $f(x) \neq 0$ there will be precisely two possible values of y, for $f(x) = 0$ only one). Half the elements of $\mathbb{F}_q^\times$ are squares. If one assumes that $(f(x))_{x \in \mathbb{F}_{q^r}}$ is a random sequence, then we expect the expectation value of N_r to be $q+1$. The Hasse bound now confirms this heuristic model, by describing the variance of this random sequence $(f(x))_{x \in \mathbb{F}_{q^r}}$.

Proof of Theorem 2.37. Let $\bar{E}$ be the induced elliptic curve over $\bar{k}$. We consider the rationalisation

$$\mathsf{End}(\bar{E})_{\mathbb{Q}} = \mathsf{End}(\bar{E}) \otimes \mathbb{Q}$$

of the non-commutative ring $\mathsf{End}(\bar{E})$. We denote by $f = \mathsf{Fr}_X \in \mathsf{End}(\bar{E})$ be the Frobenius endomorphism (since $0 \in E$ is a k-rational point, one has $\mathsf{Fr}_X(0) = 0$, and therefore Fr is indeed an endomorphism of the elliptic curve). One has $\deg f = q$ (see [Sil86, Proposition II.2.11(c)]), and therefore $f\widehat{f} = q = \widehat{f}f$.

We define a subring

$$\mathbb{K} = \mathbb{Q}[f, \widehat{f}] \subset \mathsf{End}(\bar{E})_{\mathbb{Q}},$$

since it is generated by f and $\widehat{f}$, the equation

$$f\widehat{f} = \deg f = q = \widehat{f}f$$

implies that $\mathbb{K}$ is commutative and $f^{-1} = \frac{\widehat{f}}{q} \in \mathbb{K}$.

According to Lemma 2.34 and Lemma 2.36

$$N_1 = \deg(1 - f) = (1 - f)(1 - \widehat{f}) = (1 - f)(1 - qf^{-1}),$$

which can be rearranged to the quadratic equation

$$N_1 f = (1 - f)(f - q).$$

This shows that $\mathbb{K} = \mathbb{Q}[f] = \mathbb{Q}(f)$ is a field extension of $\mathbb{Q}$ of degree 2.

More generally, Lemma 2.34 and 2.36 imply the formula

$$N_r = \deg(1 - f^r) = (1 - f^r)(1 - \widehat{f}^r).$$

We can further simplify this, by using again $f\widehat{f} = q$. This shows

$$N_r = q + 1 - (f^r + \widehat{f}^r).$$

This yields the identity

$$Z(E, T) = \frac{(1 - fT)(1 - \widehat{f}T)}{(1 - T)(1 - qT)}.$$

in $\mathbb{K}[[T]]$. Let $P(T) = (1 - fT)(1 - \widehat{f}T) \in \mathbb{K}[T]$. Since $P(T) = Z(X, T)(1 - T)(1 - qT) \in \mathbb{Q}[[T]]$, we deduce $P(T) \in \mathbb{Q}[T]$.

In order to conclude the proof we choose an embedding $\sigma\colon \mathbb{K} \hookrightarrow \mathbb{C}$, and denote $\sigma(f)$ by $\alpha \in \mathbb{C}$. We claim that $\bar{\alpha} = \sigma(\widehat{f})$, that is, we claim that $P(T)$ has two complex-conjugate zeroes. This follows from the inequality:

Claim 2.39. $P(x) \geq 0,\ \forall x \in \mathbb{R}$.

Proof. It suffices to show $P(\frac{m}{n}) \geq 0$ for every rational number $\frac{m}{n} \in \mathbb{Q}$. We have

$$P(\frac{m}{n}) = (1 - \frac{m}{n}f)(1 - \frac{m}{n}\widehat{f}) = \deg(1 - \frac{m}{n}f) = \frac{\deg(n - mf)}{n^2} \geq 0,$$

where we used positivity of the quadratic form given by the degree (see Lemma 2.32). □

The equality $|\alpha|^2 = \alpha\bar{\alpha} = q$ implies $|\alpha| = \sqrt{q}$, and thus concludes the proof of the theorem. □

Exercise 2.40. *(a) Prove the functional equation for $Z(E,T)$, where E/k is an elliptic curve over a finite field k.*

(b) Prove the formula

$$\mathsf{res}_{T=1} Z(E,T) = \frac{\#E(k)}{q-1}.$$

(c) Recall that $N_r = \#E(\mathbb{F}_{q^r})$. We define $N'_r = N_r - (q^r + 1)$. Show that there exists a recursive relation

$$N'_{r+2} + x \cdot N'_{r+1} + y \cdot N'_r = z.$$

Conclude that the values of N_1 and N_2 completely determine the zeta function $Z(E,T)$.

2.6 Serre's counterexample

Now that we have seen the Weil conjectures confirmed for a non-trivial class of varieties, it is time to come back to the phantasmagoric idea 2.26 which led us there.

Definition 2.41. *An elliptic curve E over a finite field k is said to be* supersingular, *if $\mathsf{End}(E) \otimes \mathbb{R}$ is isomorphic to the quaternion algebra $\mathbb{H}$.*

The terminology *"supersingular"* is misleading: a supersingular elliptic curve is still a smooth variety, and therefore certainly not singular at all. However, these elliptic curves are very special, due to their large ring of endomorphisms. Using the degree map deg and the involution $f \mapsto \widehat{f}$ one can show that for an elliptic curve E/k the possibly non-commutative ring $\mathsf{End}(E) \otimes \mathbb{R}$ is either isomorphic to $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$ (see [Sil86, III.9]).

Remark 2.42 (Serre)**.** *There cannot exist a functor*

$$H^1 \colon (\mathsf{Var}_{\bar{k}})^{\mathsf{op}} \longrightarrow \mathsf{Vect}_{\mathbb{Q}},$$

such that $\mathsf{rk}\, H^1(E) = 2$ for all elliptic curves. Otherwise, for E supersingular, we obtain a $\mathbb{H}$-vector space $H^1(E) \otimes \mathbb{R}$ of real dimension 2. This is impossible, since the dimension of every quaternionic vector space is divisible by 4.

Despite of this observation, it would be a mistake to abandon Phantasy 2.26 completely. As long as we drop the assumption that the cohomology $H^i(\bar{X})$ of a $\bar{k}$-variety is a rational vector space, there is still some wiggle room. The following modification of Phantasy 2.26 is sufficient.

Definition 2.43. *Let $\mathbb{K}$ field of characteristic 0. A* Weil cohomology theory[8] *for smooth varieties over $\bar{k} = \bar{\mathbb{F}}_p$ is a sequence of functors*

$$\big(H^i\big)_{i\in\mathbb{N}} : (\mathsf{Var}_{\bar{k}}^{\mathrm{sm,proj}})^{\mathsf{op}} \longrightarrow \mathsf{Vect}_{\mathbb{K}},$$

such that we have

(a) cup products*: $H^i(\bar{X}) \times H^j(\bar{X}) \longrightarrow H^{i+j}(\bar{X})$, compatible with pullback of cohomology classes,*

(b) Poincaré duality*: let d be the dimension of $\bar{X}$ and assume $\bar{X}$ is connected, then $H^i(\bar{X}) = 0$ for $i > 2d$, there exists an isomorphism $H^{2d}(\bar{X}) \simeq \mathbb{K}$, and $H^i(\bar{X}) \times H^{2d-i}(\bar{X}) \longrightarrow H^{2d}(\bar{X})$ is a perfect pairing.*

(c) Lefschetz fixed point formula*: let X be a k-model for $\bar{X}$ and $\mathsf{Fr}_X \colon \bar{X} \longrightarrow \bar{X}$ the induced Frobenius morphism. Then we have*

$$\#X(\mathbb{F}_q) = \sum_{i\geq 0} (-1)^i \,\mathsf{Tr}(H^i(\mathsf{Fr}_X)).$$

(d) we have $H^{2d}(\mathsf{Fr}_X) = q^d \cdot \mathrm{id}$ and $H^0(\mathsf{Fr}_X) = \mathrm{id}$.

Serre's counterexample proves that there cannot be a Weil cohomology theory over $\mathbb{Q}$. However, we may replace $\mathbb{Q}$ by a sufficiently big field extension $\mathbb{K}$, such that the additional endomorphisms of supersingular elliptic curves no longer cause any problems.

In order to get an idea for which fields $\mathbb{K}$ a Weil cohomology theory exists we take a closer look at the endomorphism ring of a supersingular elliptic curve.

Definition 2.44. *A* quaternion algebra over $\mathbb{Q}$ *is a non-commutative unital $\mathbb{Q}$-algebra $\mathcal{H}$, such that there exist elements $\alpha, \beta \in \mathcal{H}$, satisfying the assumptions*

(a) the quadruple $(1, \alpha, \beta, \alpha\beta)$ is a basis of $\mathcal{H}$,

(b) we have $\alpha^2, \beta^2 \in \mathbb{Q}_{<0}$,

(c) and $\alpha\beta = -\beta\alpha$.

The following assertion follows from [Sil86, Corollary III.9.4]:

Proposition 2.45. *Let $\bar{k}$ the algebraic closure of a finite field k. For a supersingular elliptic curve $\bar{E}/\bar{k}$ we have that $\mathsf{End}(\bar{E})_{\mathbb{Q}}$ is a quaternionic algebra over $\mathbb{Q}$.*

One has that $\mathsf{End}(\bar{E}) \hookrightarrow \mathsf{End}(\bar{E}) \otimes \mathbb{Q}$, since $\mathsf{End}(\bar{E})$ doesn't have zero divisors (this follows from properties of the degree map $\deg \colon \mathsf{End}(\bar{E}) \longrightarrow \mathbb{Z}$). A subalgebra $\mathcal{H}' \subset \mathcal{H}$ with the property $\mathcal{H}' \otimes \mathbb{Q} = \mathcal{H}$ is called *an order* in a quaternionic $\mathbb{Q}$-algebra.

Definition 2.46. *Let $\mathcal{H}$ be a quaternionic algebra over $\mathbb{Q}$ and $\mathbb{K} \,/\, \mathbb{Q}$ a field of characteristic 0. We say that $\mathcal{H}$ is $\mathbb{K}$-split, if there exists a 2-dimensional $\mathbb{K}$-vector space V with an $\mathcal{H}$-module structure.*

[8] The literature contains several variants of this definition. Some authors ask for additional axioms.

Equivalently, $\mathcal{H}$ is $\mathbb{K}$-split, if $\mathcal{H} \otimes_{\mathbb{Q}} \mathbb{K}$ is isomorphic to $M_{2\times 2}(\mathbb{K}) = \mathsf{End}(\mathbb{K}^2)$. It is clear that fields $\mathbb{K}$, such that for all supersingular elliptic curves $\bar{E}/\bar{k}$ the quaternionic algebra $\mathsf{End}(\bar{E})_{\mathbb{Q}}$ is $\mathbb{K}$-split, are precisely the fields which circumvent Serre's counterexample. For all practical intents and purposes, the fields $\mathbb{Q}_\ell$ of ℓ-adic numbers are the easiest example of such a field, for which a Weil cohomology theory can be constructed. Here we denote by ℓ a prime which is different from p. This notation is convenient, as it turns out that $\mathsf{End}(\bar{E})_{\mathbb{Q}}$ is not $\mathbb{Q}_p$-split.

Definition 2.47. *Let ℓ be a prime number.*

(a) We denote by $v_\ell \colon \mathbb{Q} \longrightarrow \mathbb{Z}$ the function, such that we have for all $x \in \mathbb{Q}$

$$x = \ell^{v_\ell(x)} \frac{a}{b},$$

which $a, b \in \mathbb{Z}$ coprime to ℓ.

(b) One defines $|-|_\ell \colon \mathbb{Q} \longrightarrow \mathbb{R}$ to be the norm $|x|_\ell = \ell^{-v_\ell(x)}$.

(c) The completion of $\mathbb{Q}$ with respect to $|-|_\ell$ is a normed field denoted by $\mathbb{Q}_\ell$.

(d) The closure of $\mathbb{Z}$ with respect to $|-|_\ell$ is denoted by $\mathbb{Z}_\ell$.

Theorem 2.48 (Grothendieck et al)**.** *For $\ell \neq p$ there exists a Weil cohomology theory taking values in $\mathbb{Q}_\ell$-vector spaces.*

Grothendieck's construction of étale cohomology was truly spectacular. The next subsections are devoted to a description of the main ideas underlying the construction of *ℓ-adic cohomology*. But first we mention modern response to Serre's objection.

Conjecture 2.49 (Scholze)**.** *There exists a Weil cohomology theory $(H^i)_{i\geq 0}$ taking values in* complex *vector spaces with the following extra structure: $H^i(X)$ is* endowed with an antilinear involution *j, such that $j^2 = (-1)^i \cdot \mathrm{id}$.*

It is not difficult to produce Weil cohomology theories taking values in complex vector spaces.[9] The interesting feature of Scholze's conjecture is the presence of the involution j. In the case of an elliptic curve $\bar{E}$, its degree 1 cohomology $H^1(\bar{E})$ would be a 2-dimensional complex vector space with an antilinear operator j satisfying $j^2 = -1$. That is, $H^1(\bar{E})$ is a 4-dimensional real vector space, endowed with operators i, j, satisfying the relations $ij = -ji$, $i^2 = -1$ and $j^2 = -1$. We conclude that $H^1(\bar{E})$ has the structure of a quaternionic vector space. In the case of a supersingular elliptic curve, the action of $\mathbb{H}$ on this space would be simply given by right multiplication.

The conjecture above can be found as Conjecture 9.5 in Scholze's ICM address [Sch]. In fact, there Scholze proposes the existence of an even more general Weil cohomology theory, taking values in a $\mathbb{Q}$-linear category constructed by Kottwitz.

2.7 The fundamental group revisited

Subsequently we discuss the definition of étale cohomology. As a warm-up we start with a discussion of fundamental groups. The reason is the following lemma.

[9] For instance we can use ℓ-adic cohomology and tensor along an embedding of fields $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$.

Lemma 2.50. *Let X be a path-connected topological space, $x \in X$ a point. For every abelian group A there is an equivalence*

$$H^1_{sing}(X, A) = \mathsf{Hom}(\pi_1(X, x), A).$$

This suggests that in order to produce an algebraic analogue of H^1, it is sufficient to define an algebraic analogue of the fundamental group.[10]

We define the category $Cov(X)$ whose objects are connected covering spaces $\pi : Y \longrightarrow X$. Morphisms $Y \longrightarrow Y'$ are given by a commutative diagram of coverings

$$\begin{array}{ccc} Y & \longrightarrow & Y' \\ & \searrow & \downarrow \\ & & X, \end{array}$$

and denote by

$$\mathbf{Fib}_x : Cov(X) \longrightarrow Set$$

the functor sending Y to the set $\pi^{-1}(x)$ and refer to it as the fibre functor at x. The group of natural self-transformations of the fibre functor $Aut(\mathbf{Fib}_x)$ is given by the collection of compatible automorphisms of $\pi^{-1}(Y)$; i.e., for every $Y \in Cov(X)$ a permutation σ_Y of the set $\mathbf{Fib}_x(Y) = \pi^{-1}(x)$, s.t. for every morphism of coverings $\phi : Y \longrightarrow Y'$ we have a commutative diagram

$$\begin{array}{ccc} \mathbf{Fib}_x(Y) & \xrightarrow{\phi} & \mathbf{Fib}_x(Y') \\ \downarrow{\scriptstyle \sigma_Y} & & \downarrow{\scriptstyle \sigma_{Y'}} \\ \mathbf{Fib}_x(Y) & \xrightarrow{\phi} & \mathbf{Fib}_x(Y'). \end{array}$$

Theorem 2.51. *There is a natural automorphism $\pi_1(X, x) \simeq Aut(\mathbf{Fib}_x)$.*

Proof. Every element of $\pi_1(X, x)$ can be pictured as a closed path in X based at x. Every such path can be lifted to a non-necessarily closed path in a covering space Y, depending only on the choice of a starting point given an element in $\pi^{-1}(x) = \mathbf{Fib}_x(Y)$. This construction obiously yields a compatible system of permutations of the set $\pi^{-1}(x)$. We have therefore obtained a natural morphism $\pi_1(X, x) \longrightarrow Aut(\mathbf{Fib}_x)$ and to conclude the proof we have to verify that it is an isomorphism.

Let $\widetilde{X}$ denote a universal covering space of X. We recall that up to the choice of a base point $\tilde{x} \in \pi^{-1}(x)$ there exists an identification of $\mathbf{Fib}_x(\widetilde{X})$ with $\pi_1(X)$, by means of the above construction. Moreover there exists an identification of $\pi_1(X)$ with the group of deck transformations $Aut(\widetilde{X}/X)$.

Let now σ be the permutation of $\mathbf{Fib}_x(\widetilde{X})$ otained by restricting an arbitrary element of $Aut(\mathbf{Fib}_x)$ to $\widetilde{X}$. By the discussion in the paragraph above, we have to show that $\sigma(\tilde{x})$ determines σ uniquely. Every other element in $\mathbf{Fib}_x(\widetilde{X})$ can be uniquely written as $\tilde{x}\gamma$, where $\gamma \in \pi_1(X, x)$.[11] Moreover, γ can be also viewed as a deck transformation of the universal covering space $\widetilde{X}$. By naturality of the permutation σ (definition of natural self-transformation of a functor), we obtain

$$\sigma(\tilde{x}\gamma) = \sigma((\tilde{x})\gamma) = \sigma(\tilde{x})\gamma,$$

which allows us to conclude the proof. □

[10] The following two subsections are based on the notes of a talk the author gave in Lausanne in 2013.

[11] It is helpful to write the action of $\pi_1(X, x)$ as a right action.

If the topological spaces X and Y can be endowed with the structure of differentiable manifold, the notion of covering can be expressed in terms of these extra structure.

Recall that a C^∞-map $f : Y \longrightarrow X$ between C^∞-manifolds is called a *local diffeomorphism* if for every $x \in X$ and every $y \in f^{-1}(x)$, the differential $df_y : T_yY \longrightarrow T_xX$ is an isomorphism.

The proof of the proposition below is left to the reader. It will turn out to be the key ingredient in algebraising the topological invariant π_1.

Proposition 2.52. *Let $\pi : Y \longrightarrow X$ be a local diffeomorphism between C^∞-manifolds, which is additionally proper (i.e. preimages of compact subsets are compact), then π is a covering morphism with finite fibres. Moreover, all finite coverings of a differentiable manifold X arise in this way: i.e. every covering Y inherits the structure of a differentiable manifold, rendering the map π to be étale, and a covering map between manifolds has finite fibres if and only if it is proper.*

Proposition 2.52 gives a geometric characterisation of finite covering maps, it is therefore an interesting question how far we can go by only using finite covering spaces. A more precise question being: let $Cov^{fin}(X) \subset Cov(X)$ be the full subcategory of finite connected covering spaces, and

$$\mathbf{Fib}_x^{fin} : Cov^{fin}(X) \longrightarrow Set^{fin}$$

the restriction of the fibre functor. How does

$$\pi_1^{fin}(X, x) := Aut(\mathbf{Fib}_x^{fin})$$

relate to the fundamental group $\pi_1(X, x) = Aut(\mathbf{Fib}_x)$? The next definition contains a construction from abstract group theory, which allows us to formulate the answer.

Definition 2.53. *Let G be an abstract group, we denote by $F(G)$ the set of normal, finite-index subgroups N of G, i.e. G/N being a finite group. The set $F(G)$ is inductively ordered and the inverse limit of the finite quotients G/N, i.e.*

$$\widehat{G} := \{([g_N]_N)_{N \in F(G)} | [g_N]_N \in G/N, \text{ and } [g_{N'}]_N = [g_N]_N \text{ for } N' \subset N\},$$

is called the pro-finite completion *of G.*

It is important to know that pro-finite groups are more than just groups. The inverse limit construction endows them naturally with a topology (the subset topology of the product topology).[12] Moreover, by Tychonov's theorem, pro-finite groups are actually compact.

Example 2.54. *One has $\widehat{\mathbb{Z}} = \prod_{p \text{ prime}} \mathbb{Z}_p$.*

The relevance of this abstract notion to the determination of π_1^{fin} is due to a simple observation in the theory of covering spaces. Every finite-index subgroup N of $\pi_1(X, x)$ corresponds to a finite covering space $Y \longrightarrow X$ by virtue of the fundamental theorem of covering theory. If N is moreover assumed to be a normal subgroup, it corresponds to finite regular covering spaces.[13] We hope that these remarks are already convincing enough to believe the statement of the following theorem, for the sake of clarity we have included a proof below.

[12] Finite groups are viewed as topological groups with the trivial topology.

[13] Regularity is equivalent to the natural action of $\pi_1(X, x)$ on $\pi^{-1}(x)$ being transitive.

Theorem 2.55. *The canonical morphism $\pi_1(X,x) \longrightarrow \pi_1^{fin}(X,x)$, obtained by restricting an element of $Aut(Fib_x)$ to the subcategory $Cov^{fin}(X)$, induces an isomorphism*

$$\widehat{\pi_1(X,x)} \simeq \pi_1^{fin}(X,x).$$

Proof. Let $Y_N \longrightarrow X$ be the regular finite covering corresponding to a normal, finite-index subgroup $N \subset \pi_1(X,x)$, a compatible choice of these a collection $(Y_N)_{N \in F(\pi_1(X,x))}$ can be constructed by quotienting a universal covering space $\widetilde{X}$ by N. The group of deck transformations of Y_N is canonically given by $\pi_1(X,x)/N$. The choice of $\tilde{x} \in \mathbf{Fib}_x(\widetilde{X})$ gives rise to a base point x_N in every Y_N, which allows us to identify $\mathbf{Fib}_x(Y_N)$ with $\pi_1(X,x)/N$. Similarly to the proof of Theorem 2.51 we let (σ_N) be a compatible system of permuations of $\mathbf{Fib}_x(Y_N)$. For $y \in \mathbf{Fib}_x(Y_N)$ there exists a $\gamma \in \pi_1(X,x)$, whose class $[\gamma]_N$ is welldefined, s.t. $y = \gamma(y_N)$. As before we see by naturality of (σ_N) that σ_N is given by right multiplication with $\sigma_N(y_N) \in \pi_1(X,x)/N$. This construction associates to (σ_N) the compatible system $(\sigma_N(y_N))_N \in \pi_1(X,x)/N$, which can be seen to give an inverse $\widehat{\pi_1(X,x)} \longrightarrow \pi_1^{fin}(X,x)$. □

2.8 The étale fundamental group

Proposition 2.52 contained a characterisation of finite covering maps of manifolds as proper local diffeomorphisms. The analogue of a local diffeomorphism in the category of varieties is an *étale morphism* (see Definition 1.53).

Also the notion of properness of a morphism is wonderfully captured by Grothendieck's approach to algebraic geometry (see chapter II.4 in [Har77]). Nonetheless it can be shown that for étale maps, properness is equivalent to the simpler notion of being *finite* (this is essentially exercise III.11.2 in [Har77]).

Definition 2.56. *A map between two affine varieties $f : \operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ is called* finite*, if the induced map of rings $A \longrightarrow B$ endows B with the structure of a finitely generated A-module. A map between two varieties $f : Y \longrightarrow X$ is called* finite*, if there exists a covering $X = \bigcup_{i \in I} U_i$, s.t. each $f^{-1}(U_i)$ is affine, and the restriction $f : f^{-1}(U_i) \longrightarrow U_i$ is finite.*

Motivated by Theorem 2.55 we define the category $Cov^{\text{ét}}(X)$ to be the category of (connected) finite étale covering spaces $\pi : Y \longrightarrow X$ with morphisms being given by a finite étale map $Y \longrightarrow Y'$ sitting in a commutative diagram

$$\begin{array}{ccc} Y & \longrightarrow & Y' \\ & \searrow & \downarrow \\ & & X. \end{array}$$

For every geometric point x of X, i.e. for every map $\operatorname{Spec} F^{sep} \longrightarrow X$, where F^{sep} is a separably closed field, there is a fibre functor

$$\mathbf{Fib}_x^{\text{ét}} : Cov^{\text{ét}}(X) \longrightarrow Set,$$

sending Y to the fibre $Hom_X(\operatorname{Spec} \bar{F}, Y)$.

Definition 2.57. *The étale fundamental group of a variety X at a geometric point x, is defined to be the group of natural self-transformations of the fibre functor $\mathbf{Fib}_x^{\acute{e}t}$, i.e.*

$$\pi_1^{\acute{e}t}(X,x) := Aut(\mathbf{Fib}_x^{\acute{e}t}).$$

For later use we record the following lemma, which will be useful in constructing representations of the étale fundamental group.

Lemma 2.58. *Let X be a variety and $\pi : Y \longrightarrow X$ a finite étale covering. We say that π is regular (or Galois), if the action of $\pi_1^{ét}(X,x)$ on $\mathbf{Fib}_x^{ét}(Y)$ is transitive. Under these circumstances, the group of deck transformations $Aut(Y/X)$, i.e. the automorphism group of Y in the category $Cov^{ét}(X)$, is a surjective image of $\pi_1^{ét}(X,x)$.*

In case that X is a complex variety, and $x \in X(\mathbb{C})$ we would like to state a comparison theorem relating $\pi_1^{\text{ét}}(X,x)$ with $\pi_1^{fin}(X,x)$. In order to achieve this it suffices to construct a natural equivalence of categories

$$Cov^{fin}(X^{an}) \simeq Cov^{\text{ét}}(X),$$

respecting fibre functors. This follows from the following theorem, see [SGA71, Exp. XII Thm. 5.1].

Theorem 2.59 (Riemann Existence Theorem)**.** *Let X be a complex variety, then there exists a canonical equivalence of finite étale coverings of X and finite coverings of X^{an}.*

Corollary 2.60 (Comparison theorem for $\pi_1^{\text{ét}}$)**.** *Let X be a complex variety and $x \in X(\mathbb{C})$ a $\mathbb{C}$-point, then there is a canonical equivalence*

$$\pi_1^{ét}(X,x) \simeq \pi_1\widehat{(X^{an}}, x).$$

Proof. The Riemann Existence Theorem 2.59 shows that there is an equivalence of categories $Cov^{\text{ét}}(X,x) \simeq Cov^{fin}(X^{an},x)$, respecting fibre functors. In particular we obtain an equivalence of the groups of natural self-transformations

$$\pi_1^{\text{ét}}(X,x) = Aut(\mathbf{Fib}_x^{\text{ét}}) \simeq Aut(\mathbf{Fib}_x^{fin}) = \pi_1^{fin}(X^{an},x).$$

Since we have seen in Theorem 2.55 that $\pi_1^{fin}(X^{an},x) \simeq \pi_1\widehat{(X^{an}}, x)$, finishing the proof of the theorem. □

As an example, we compute the étale fundamental group of an elliptic curve $E = \mathbb{C}/\Gamma$ over $\mathbb{C}$ without referring to the universal covering space. Recall that $\Gamma \subset \mathbb{C}$ is a *lattice*, that is, a subgroup of $\mathbb{C}$, such that the natural map

$$\Gamma \otimes \mathbb{R} \longrightarrow \mathbb{C}$$

is an isomorphism.

Proposition 2.61. *Let $E = \mathbb{C}/\Gamma$ be a complex elliptic curve. There is an isomorphism*

$$\pi_1^{ét}(E,0) \simeq \widehat{\Gamma}.$$

Proof. It follows from part (a) and (b) of the exercise below that a finite covering space $E' \longrightarrow E$ is equivalent to

$$\mathbb{C}/\Gamma' \longrightarrow \mathbb{C}/\Gamma$$

where $\Gamma' \subset \Gamma$ is a lattice in $\mathbb{C}$ contained in Γ. Furthermore, every subgroup $\Gamma' \subset \Gamma$ of finite index, is a lattice. Indeed, the natural map

$$\Gamma' \otimes \mathbb{R} = \Gamma \otimes \mathbb{R} \longrightarrow \mathbb{C}$$

is an isomorphism. This establishes a bijection between finite covering spaces E' of E up to isomorphism and finite index subgroups $\Gamma' \subset \Gamma$. We deduce that the deck transformation group of E'/E is given by Γ/Γ'. As before, one infers the existence of an isomorphism $\mathsf{Aut}(\mathsf{Fix}_0) = \widehat{\Gamma}$. $\square$

Exercise 2.62. *We consider a complex elliptic curve $E/\mathbb{C}$. Let $\pi\colon E' \longrightarrow E$ be a finite covering space. Show that E' has a natural structure of a complex manifold (to be precise, a Riemann surface), such that:*

(a) the map π is a holomorphic map between complex manifolds,

(b) the complex manifold E' is an elliptic curve,

(c) there exists a positive integer n, such that we have a holomorphic map $E \longrightarrow E'$, such that the diagram

$$\begin{array}{ccc} E & \longrightarrow & E' \\ & \searrow^{[n]} & \downarrow \\ & & E \end{array}$$

commutes. Here, we denote by $[n]\colon E \longrightarrow E$ the map sending $x \in E$ to nx.

This exercise shows, that the inverse system

$$\left(E \xrightarrow{[n]} E \right)_{n \geq 1},$$

where we order integers by divisibility, behaves like a universal profinite space of E. This inverse system is defined in purely algebraic terms. Using it, and the analogue of exercise (c) above, one can show the following:

Theorem 2.63. *Let $\mathbb{K}$ be an algebraically closed field of characteristic 0, and $E/\mathbb{K}$ an elliptic curve. Then, one has $\pi_1^{\acute{e}t}(E,0) \simeq (\widehat{\mathbb{Z} \times \mathbb{Z}})$.*

There is a variant of the same result over characteristic p fields. It is necessary to avoid coverings of degree divisible to p. This corresponds to considering the coprime-to-p part of $\pi_1^{\text{ét}}$ and $(\widehat{\mathbb{Z} \times \mathbb{Z}})$.

Theorem 2.64 (SGA)**.** *Let $\bar{k}$ be an algebraically closed field of characteristic $p > 0$, and $\bar{E}/\bar{k}$ an elliptic curve. Then, one has $\pi_1^{\acute{e}t}(\bar{E},0)' \simeq (\widehat{\mathbb{Z} \times \mathbb{Z}})'$.*[14]

An elementary account of the proof of these theorems is given in [Kun].

2.9 Torsors and $H^1_{\text{ét}}$

Let A be a finite abelian group. In this subsection we define $H^1_{\text{ét}}(X,A)$ for X a k-variety. We will see that the field of complex numbers, and A finite, our definition agrees with singular cohomology $H^1_{\text{sing}}(X^{\mathsf{an}}, A)$. However, using the same definition for $A = \mathbb{Z}, \mathbb{Q}$, one obtains a meaningless (and often trivial) answer without any connection to singular cohomology.

Before delving into the construction of $H^1(X,A)$ let us remark how we can use it as the starting point of the construction of a Weil cohomology theory (ℓ-adic cohomology).

[14] The $'$ indicates that we only consider normal subgroups of index coprime to p.

Construction 2.65. *Assume that we already know how to define $H^i_{ét}(X, A)$ for A a finite abelian group. For a prime number ℓ we define a $\mathbb{Z}_\ell$-module*

$$H^i_{ét}(X, \mathbb{Z}_\ell) = \varprojlim_{n \geq 0} H^i(X, \mathbb{Z}/\ell^n\,\mathbb{Z}),$$

and a $\mathbb{Q}_\ell$-vector space

$$H^i_{ét}(X, \mathbb{Q}_\ell) = H^i(X, \mathbb{Z}_\ell) \otimes \mathbb{Q}\,.$$

This definition is justified by the following comparison result over the complex numbers.

Proposition 2.66. *Let $X/\,\mathbb{C}$ be a smooth projective variety. Assume that for a finite abelian group A we already have constructed isomorphisms $H^i_{ét}(X, A) \simeq H^i_{\mathrm{sing}}(X^{\mathsf{an}}, A)$. Then, we have an isomorphism $H^i_{ét}(X, \mathbb{Q}_\ell) \simeq H^i_{\mathrm{sing}}(X^{\mathsf{an}}, \mathbb{Q}_\ell)$.*

Proof. The analytification X^{an} is a compact complex manifold. In particular, its singular homology group $H^{\mathrm{sing}}_i(X, A)$ are finitely generated abelian groups. These groups govern the other cohomology group $H^i(X, A)$ for all abelian groups A:

Theorem 2.67 (Universal coefficient theorem, Theorem 3.2 in [Hat])**.** *Let Z be a topological space. Then, we have $H^i_{\mathrm{sing}}(Z, A) \simeq \mathsf{Hom}(H^{\mathrm{sing}}_i(Z, \mathbb{Z}), A) \oplus \mathsf{Ext}(H^{\mathrm{sing}}_{i-1}(X, \mathbb{Z}), A)$.*

The abelian group $\mathsf{Ext}(H^{\mathrm{sing}}_{i-1}(X, \mathbb{Z}), A)$ is finite, if A is finite. For $A = F$ a field, one can show that $\mathsf{Ext}(H^{\mathrm{sing}}_{i-1}(X, \mathbb{Z}), F) = 0$ (see [Hat, p. 207]). Furthermore, one has the relation

$$\mathsf{Ext}(\mathbb{Z}/\ell^n\,\mathbb{Z}, \mathbb{Z}/\ell^m\,\mathbb{Z}) = \mathbb{Z}/\ell^{\min(m,n)}\,\mathbb{Z}\,.$$

This implies that the inverse limit $\varprojlim \mathsf{Ext}(H^{\mathrm{sing}}_{i-1}(X, \mathbb{Z}), \mathbb{Z}/\ell^n\,\mathbb{Z})$ equals the ℓ-primary part of $H^{\mathrm{sing}}_{i-1}(X, \mathbb{Z})$ (that is, the set of elements annihilated by a power of ℓ). We conclude

$$\varprojlim H^i_{\mathrm{sing}}(Z, \mathbb{Z}_\ell) \simeq \mathsf{Hom}(H^{\mathrm{sing}}_i(Z, \mathbb{Z}), \mathbb{Z}_\ell) \oplus H^{\mathrm{sing}}_{i-1}(X, \mathbb{Z})[\ell^\infty].$$

Since the factor on the right hand side is a fixed torsion group, it disappears when tensoring with $\mathbb{Q}$. We infer an isomorphism

$$H^i_{\mathrm{ét}}(X, \mathbb{Q}_\ell) \simeq H^i_{\mathrm{sing}}(X^{\mathsf{an}}, \mathbb{Q}_\ell),$$

which concludes the proof. □

We now turn to the algebraic construction of $H^i(X, A)$ for A a finite abelian group. At first we need to specify what it means for A to act on a variety Y. An A-action on Y is a group homomorphism $\alpha\colon A \longrightarrow \mathsf{Aut}(Y)$. A morphism $Y \longrightarrow X$ is said to be A-invariant, if for all $a \in A$ we have

$$\pi \circ \alpha(a) = \pi,$$

that is, the diagram

$$\begin{array}{ccc} Y & \xrightarrow{\alpha(a)} & Y \\ & {\scriptstyle\pi}\searrow & \downarrow{\scriptstyle\pi} \\ & & X \end{array}$$

commutes.

Definition 2.68. *Let X be a smooth k-variety. An* étale A-torsor *is a triple (Y, π, α), where*

(a) Y is a smooth k-variety endowed with an A-action α,

(b) $\pi\colon Y \longrightarrow X$ a finite étale morphism ***of degree*** *$\#A$ which is A-invariant,*

(c) the natural map $\phi\colon A \longrightarrow \mathsf{Aut}_A(\bar{Y}/\bar{X})$ an isomorphism between A and the group of deck transformations commuting with A (where $\bar{Y} \longrightarrow \bar{X}$ denotes the induced morphism of $\bar{k}$-varieties).

Even the simplest example can be helpful in order to understand the definition of torsors.

Example 2.69. *Let $\bar{k}$ be an algebraically closed field and $X = \mathbb{A}^0_{\bar{k}}$ a point. An A-torsor over X corresponds to a set S*

$$\bigsqcup_{s\in S} \mathbb{A}^0_{\bar{k}} \longrightarrow \mathbb{A}^0_{\bar{k}}$$

with an A-action $\alpha\colon A \times S \longrightarrow S$, such that we have an isomorphism

$$A \simeq \mathsf{Aut}_A(S) = \{f\colon S \longrightarrow S | f(as) = af(s).\}$$

Claim 2.70. *For $s \in S$ one has $S = A \cdot s$.*

Proof. Let $f_a\colon S \longrightarrow S$ be the map given by $t \mapsto a \cdot t$ for $t \in A \cdot s$, and $t \mapsto t$ otherwise. This is a bijection satisfying $f_a(bt) = bf_a(t)$ for all $b \in A$, that is, $f_a \in \mathsf{Aut}_A(S)$. By assumption, $A = \mathsf{Aut}_A(S)$, and therefore $f_a(t) = a \cdot t$ for all $t \in S$. This implies $A \cdot s = S$. □

We conclude that an A-torsor on the point $\mathbb{A}^0_{\bar{k}}$ corresponds to a set S with an A-action α which is transitive and faithful. In particular, S is non-canonically equivalent to A, as a set with A-action.

For non-algebraically closed fields k (as always we assume perfect), this example gets more interesting.

Example 2.71. *Let k'/k be a Galois extension with finite abelian Galois group A. Then,*

$$\mathsf{MSpec}\, k' \longrightarrow \mathsf{MSpec}\, k$$

is an A-torsor. Indeed, the map above is étale (the tangent spaces are 0-dimensional[15]), and by definition, A acts on k' through field automorphisms. Therefore, A acts on the k-variety $\mathsf{MSpec}\, k'$. We have $\mathsf{Aut}(\mathsf{MSpec}\, k'/\mathsf{MSpec}\, k) = \mathsf{Aut}(k'/k) = A$. In particular, all deck transformations commute with the A-action, and thus $\mathsf{MSpec}\, k'/\mathsf{MSpec}\, k$ is an A-torsor.

The third example finally has some geometric relevance.

Exercise 2.72. *Let $\bar{k}$ be an algebraically closed field, and n a positive integer which is invertible in $\bar{k}$.[16] In Exercise 1.54 we verified that the map*

$$\phi_n\colon \mathbb{G}_{m,\bar{k}} \longrightarrow \mathbb{G}_{m,\bar{k}}$$

given by the ring homomorphism $\bar{k}[t, t^{-1}] \longrightarrow \bar{k}[t, t^{-1}]$ sending t to t^n, is étale. Let us denote by μ_n the group of n-th roots of unity, that is, $\lambda \in \bar{k}$ satisfying

$$\lambda^n = 1.$$

Show that the map $\phi_n\colon \mathbb{G}_{m,\bar{k}} \longrightarrow \mathbb{G}_{m,\bar{k}}$ is a μ_n-torsor.

[15] This argument only makes sense for a perfect field k

[16] In other words, n is coprime to the characteristic p of $\bar{k}$.

Definition 2.73. *Let X be a smooth k-variety. The set of isomorphism classes of A-torsors on X is denoted by $H^1_{\acute{e}t}(X, A)$.*

It remains to prove that for a complex variety, this reproduces singular cohomology.

Lemma 2.74. *For X a connected smooth complex variety and A a finite abelian group one has a natural isomorphism $H^1_{\acute{e}t}(X, A) \simeq H^1_{\mathrm{sing}}(X^{\mathsf{an}}, A)$.*

Proof. The Riemann Existence Theorem 2.59 yields an isomorphism between $H^1_{\text{ét}}(X, A)$ and the set of isomorphism classes $T(A)$ of covering spaces $\pi\colon Z \longrightarrow X^{\mathsf{an}}$, endowed with an A-action, such that π is A-invariant and $A \longrightarrow \mathsf{Aut}_A(Z/X^{\mathsf{an}})$ is an isomorphism.

We claim that every $(Z/X^{\mathsf{an}}) \in T(A)$ gives rise to a morphism $\pi_1(X^{\mathsf{an}}, x) \longrightarrow A$. To see this, we choose an arbitrary connected component Z'/X^{an} of Z. By construction, there exists a subgroup $B \subset A$, such that Z'/X^{an} is a B-torsor. In particular, $B \subset \mathsf{Aut}(Z'/X^{\mathsf{an}})$. Since $\pi^{-1}(x)$ has as many elements as B, we conclude from the theory of covering spaces that $B = \mathsf{Aut}(Z'/X^{\mathsf{an}})$.

The homomorphism $\pi_1(X^{\mathsf{an}}, x) \longrightarrow A$ is defined to be the composition

$$\pi_1(X^{\mathsf{an}}, x) \twoheadrightarrow B \hookrightarrow A.$$

A direct verification shows that it is independent of the chosen connected component $Z' \subset Z$.

Vice versa, given a homomorphism $\rho\colon \pi_1(X^{\mathsf{an}}, x) \longrightarrow A$ one can construct the corresponding A-torsor as follows:

$$Z = (\widetilde{X} \times A)/\pi_1(X^{\mathsf{an}}, x),$$

where $\pi_1(X^{\mathsf{an}}, x)$ acts through the inverse of its usual action on the universal covering space $\widetilde{X}$, and through the homomorphism $\rho\colon \pi_1(X^{\mathsf{an}}, x) \longrightarrow A$ on A:

$$\gamma \cdot (\widetilde{x}, a) = (\gamma^{-1}\widetilde{x}, \rho(\gamma)).$$

A direct computation shows that we constructed mutually inverse bijections

$$T(A) \simeq \mathsf{Hom}(\pi_1(X^{\mathsf{an}}, x), A).$$

The right hand side can be identified with $H^1_{\mathrm{sing}}(X^{\mathsf{an}}, A)$. □

Dangerous Bend 2.75. *If the group order $\#A$ is divisible by the characteristic p of $\bar{k}$, strange things can happen. For instance, we will see that*

$$H^1(\mathbb{A}^1_{\bar{k}}, \mathbb{Z}/p\,\mathbb{Z}) = \mathbb{Z}/p\,\mathbb{Z}\,.$$

A non-trivial torsor is given by the so-called Artin-Schreier map

$$\mathbb{A}^1_{\bar{k}} \longrightarrow \mathbb{A}^1_{\bar{k}}, \quad \lambda \mapsto \lambda^p - \lambda.$$

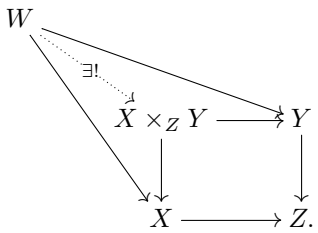
2.10 Fibre products and equalisers

Definition 2.76. *Let C be a category, and $f\colon X \to Z$, $g\colon Y \to Z$ two morphisms. Consider the category of diagrams*

$$\begin{array}{ccc} W & \longrightarrow & Y \\ \downarrow & & \downarrow \\ X & \longrightarrow & Z. \end{array}$$

If it exists, we denote the top left corner (W) of the final object in this category by $X \times_Z Y$, and call it the fibre product of the two morphisms f and g.

By the definition of final objects, we see that whenever we have a commutative diagram as above, there exists a unique morphism $W \to X \times_Z Y$, such that the resulting diagram



commutes.

Example 2.77. *For a topological space X, and inclusions of open subsets $U \hookrightarrow X$, $V \hookrightarrow X$, we have that the fibre product $U \times_X V$ in the category $\mathsf{Open}(X)$, respectively Top, is given by the inclusion of the open subset $U \cap V \hookrightarrow X$.*

Proposition 2.78. *Let $Y \longrightarrow X$ be an étale morphism of smooth k-varieties, and $Z \longrightarrow Y$ an arbitrary morphism of smooth varieties. Then the fibre product $W = Y \times_X Z$ is a smooth variety, and the map $Y \times_X Z \longrightarrow Z$ is étale.*

Proof. See [Mil80, Proposition 3.3(c)]. □

2.11 Grothendieck topologies

Definition 2.79. *Let C be a category. A* Grothendieck topology $\mathcal{T}$ *on C consists of a collection of sets of morphisms (called* coverings*) $\{U_i \to U\}_{i \in I}$ for each object $U \in \mathsf{C}$, satisfying:*

(a) For every isomorphism $U' \to U$, the singleton $\{U' \to U\}$ is a covering.

(b) Coverings are preserved by base change, i.e. if $\{U_i \to U\}_{i \in I}$ is a covering, and $V \to U$ a morphism in C, then $\{U_i \times_U V \to V\}_{i \in I}$ is well-defined, and a covering.

(c) Given a covering $\{U_i \to U\}$, and for each $i \in I$ a covering $\{U_{ij} \to U_i\}_{j \in J_i}$, then

$$\{U_{ij} \to U\}_{(i,j) \in \prod_{i \in I} J_i}$$

is a covering.

Originally, Grothendieck topologies were called *pre*topologies. A pair $(\mathsf{C}, \mathcal{T})$ is called a *site*. An example everyone is familiar with is given by topological spaces.

Example 2.80. *For the category $\mathsf{Open}(X)$, for X a topological space, we have a natural choice for a Grothendieck topology. We define $\mathcal{T}(X)$ to be the collection of all $\{U_i \subset U\}$, such that $\bigcup_{i \in I} U_i = U$.*

Definition 2.81. *Let* C *be a category. A functor* $F\colon \mathsf{C}^{\mathsf{op}} \to \mathsf{Set}$ *is called a* presheaf. *The category of presheaves will be denoted by* $\Pr(\mathsf{C})$. *If* $(\mathsf{C}, \mathcal{T})$ *is a site, a presheaf is called a* sheaf, *if for every* $\{U_i \to U\}_{i\in I}$ *the diagram*

$$F(U) \to \prod_{i\in I} F(U_i) \rightrightarrows \prod_{(i,j)\in I^2} F(U_i \times_U U_j)$$

is an equaliser. We denote the full subcategory of sheaves by $\mathrm{Sh}_{\mathcal{T}}(\mathsf{C})$.

We fix a topological space X. As we have seen above, there is a category, denoted by $\mathsf{Open}(X)$, whose objects are open subsets $U \subset X$, and morphisms are inclusions $U \subset V$.

Example 2.82. *A (set-valued)* presheaf *on* X *is a functor* $F\colon \mathsf{Open}(X)^{\mathsf{op}} \to \mathsf{Set}$.

In more concrete terms, we associate to every open subset $U \subset X$ a set $F(U)$, as well as a restriction map

$$r_U^V\colon F(V) \to F(U)$$

for every inclusion $U \subset V$. Moreover, the conditions

(a) $r_U^U = \mathrm{id}_{F(U)}$,

(b) $r_U^V \circ r_V^W = r_U^W$ for triples of open subsets $U \subset V \subset W$,

are satisfied.

If Y is a topological space, we denote by $\underline{Y}_X$ the presheaf on X, which associates to an open subset $U \subset X$ the set of continuous functions $U \to Y$, i.e.,

$$\underline{Y}_X(U) = \mathsf{Hom}_{\mathsf{Top}}(U, Y).$$

The restriction maps r_U^V are given by

$$f \mapsto f|_U,$$

i.e., sending a continuous map $f\colon V \to Y$ to the composition $f \circ i$, where $i\colon U \hookrightarrow V$ denotes the inclusion.

If $U = \bigcup_{i\in I} U_i$ is an open covering, we have for every pair of open subsets U_i, U_j two maps

$$U_i \hookleftarrow U_i \cap U_j \hookrightarrow U_j.$$

Hence, for every presheaf F we have a pair of restriction maps

$$F(U_i) \to F(U_i \cap U_j) \leftarrow F(U_j).$$

Taking a product over all pairs $(i, j) \in I^2$, and relabelling indices, we obtain

$$\prod_{i\in I} F(U_i) \rightrightarrows \prod_{(i,j)\in I^2} F(U_i \cap U_j).$$

Example 2.83. *A presheaf* F *is called a* sheaf, *if for every open subset* $U \subset X$, *and every open covering* $U = \bigcup_{i\in I} U_i$, *we have that*

$$F(U) \to \prod_{i\in I} F(U_i) \rightrightarrows \prod_{(i,j)\in I^2} F(U_i \cap U_j)$$

is an equaliser diagram.

Unravelling the definition of equalisers, we see that a presheaf is a sheaf, if and only if for every $U = \bigcup_{i\in I} U_i$ as above, the following condition is satisfied: given a collection of local sections $s_i \in F(U_i)$, which agree on overlaps, i.e. satisfy $r^{U_i}_{U_i\cap U_j}(s_i) = r^{U_j}_{U_i\cap U_j}(s_j)$ for all pairs of indices, there exists a unique section $s \in F(U)$, such that $r^U_{U_i}(s) = s_i$.

Lemma 2.84. *The presheaf $\underline{Y}_X$ is a sheaf.*

Concrete proof. If $f_i\colon U_i \to Y$ are continuous functions, such that $f_i|_{U_i\cap U_j} = f_j|_{U_i\cap U_j}$ for all pairs of indices, then there is a well-defined map of sets $f\colon U \to Y$, which sends $x \in U$ to $f_i(x)$, if $x \in U_i$. Since continuity is a local property, i.e. continuity at a point $x \in X$ depends only on the restriction $f|_{U_i}$, for $x \in U_i$, we see that f is a continuous function. □

Abstract proof. We can represent U as a co-equaliser

$$\coprod_{(i,j)\in I^2} U_i \cap U_j \rightrightarrows \coprod_{i\in I} U_i \to U,$$

i.e., as a colimit in the category Top of topological spaces. The universal property of colimits implies that $\mathsf{Hom}_{\mathsf{Top}}(-, Y)$ sends a co-equaliser to an equaliser. □

Definition 2.85. *Let X be a smooth k-variety. We denote by $(X)_{ét}$ the so-called* small étale site *of X. The objects of the underlying category consists of étale morphisms of k-varieties $Y \longrightarrow X$. Morphisms are given by commutative diagram of étale morphisms*

$$\begin{array}{ccc} Z & \longrightarrow & Y \\ & \searrow & \downarrow \\ & & X. \end{array}$$

The Grothendieck topology is defined as follows: a finite collection $\{U_i \xrightarrow{f_i} U\}$ of étale morphisms is said to be a covering family, if and only $\bigcup_{i\in I} f_i(U_i) = U$.

An important class of sheaves is given by so-called *representable sheaves*.

Definition 2.86. *Let X and Y be k-varieties. We denote by $\underline{Y}_X$ the presheaf on $(X)_{ét}$ which assigns to an étale morphism $U \longrightarrow X$ the set $\mathbf{Mor}(U, Y)$.*

It is an important consequence of faithfully flat descent theory that this presheaf is in fact a sheaf. We defer the proof in Subsection 2.15.

Theorem 2.87. *The presheaf $\underline{Y}_X$ is an étale sheaf.*

An important special case is $Y = \mathbb{A}^1_k$. In this case, $\underline{\mathbb{A}^1_k}$ is the sheaf of regular functions: it assigns to $U \longrightarrow X$ the set of $f\colon U \longrightarrow \mathbb{A}^1_k$. This sheaf is our first example of a *sheaf in abelian groups*.

2.12 Sheaf cohomology: an axiomatic approach

Henceforth, we shall work under the following assumptions: let $(\mathsf{C}, \mathcal{T})$ be a small site,[17] such that there exists a *final* object $X \in \mathsf{C}$. We remark that this assumption is satisfied by $\mathsf{Open}(X)$, where X is a topological space. Another example is given by $(X)_{\text{ét}}$, the small étale site of X, where X is a smooth k-variety.

Another convention we're going to introduce is that: sheaves will be sheaves of abelian groups. That is, we assume that $\mathcal{F}(U)$ is an abelian group for every $U \in \mathsf{C}$ and for every morphism $V \longrightarrow U$, the corresponding map $\mathcal{F}(U) \longrightarrow \mathcal{F}(V)$ is a homomorphism.

For a presheaf $\mathcal{F}$ on C we'll also suggestively write $\Gamma(X, \mathcal{F}) = \mathcal{F}(X)$, and refer to this abelian group as the group of *global sections* of $\mathcal{F}$.

Definition 2.88. *A sequence $\mathcal{F} \xrightarrow{f} \mathcal{G} \xrightarrow{g} \mathcal{H}$ of sheaves is said to be exact at $\mathcal{G}$, if and only if for every $U \in \mathsf{C}$ and every $s \in \mathcal{G}(U)$, such that $g_U(s) = 0$, ther exists a covering $\{U_i \longrightarrow U\}_{i \in I} \in \mathcal{T}$, such that there are sections $t_i \in \mathcal{F}(U_i)$ satisfying $t_i = f_{U_i}(t_i) = s|_{U_i}$.*

A special case of the above definitions are exact sequences of the form

$$0 \longrightarrow \mathcal{F} \xrightarrow{f} \mathcal{G},$$

which amount to the map f being *locally injective*. We will see that locally injective maps of sheaves are actually injective. Another special case is given by exact sequences

$$\mathcal{F} \xrightarrow{g} \mathcal{G} \longrightarrow 0.$$

This amounts to g being *locally surjective*. It is not true that a locally surjective map of sheaves is surjective, as shown by the following example.

Example 2.89. *Let $X = \mathbb{C}^\times$ with the standard topology. We denote by $\mathcal{O}$ the sheaf of holomorphic functions on X, and by $\mathcal{O}^\times$ the sheaf of invertible holomorphic functions (that is, they are nowhere zero). The sequence*

$$0 \longrightarrow 2\pi i\,\mathbb{Z} \longrightarrow \mathcal{O} \xrightarrow{\exp} \mathcal{O}^\times \longrightarrow 0$$

is exact. However, the induced map between global sections $\mathcal{O}(X) \longrightarrow \mathcal{O}^\times(X)$ is not surjective, as the function $\mathrm{id}_{\mathbb{C}^\times}$ cannot be expressed as the exponential of a holomorphic function.

The most general statement we can make is the following:

Lemma 2.90. *Let $0 \longrightarrow \mathcal{F} \xrightarrow{f} \mathcal{G} \xrightarrow{g} \mathcal{H} \longrightarrow 0$ be a short exact sequence of sheaves. The sequence of abelian groups*

$$0 \longrightarrow \Gamma(X, \mathcal{F}) \longrightarrow \Gamma(X, \mathcal{G}) \longrightarrow \Gamma(X, \mathcal{H})$$

is exact.

Proof. We claim that exactness at $\Gamma(X, \mathcal{F})$ is equivalent to injectivity of the map $\mathcal{F}(X) \longrightarrow \mathcal{G}(X)$. The assumption $f_X(s) = 0$ implies $0 = f_X(s)|_{U_s} = f_U(s|_U) = 0$ for every object U of the site. By assumption, there exists a covering $\{U_i \longrightarrow X\}_{i \in I}$, such that $s|_{U_i} = 0$ for all $i \in I$. Hence, we have

[17] *Small* is a technical term, it means that there's an actual set of objects, and not just a class.

$s|_{U_x} = 0$ for every $x \in X$. The sheaf property implies now that $s = 0$, since the two sections s and 0 both solve the glueing problem for $0 \in \mathcal{F}(U_{xy})$ for $(x, y) \in X^2$.

Exactness at $\Gamma(X, \mathcal{G})$ can be shown as follows: let $s \in \mathcal{G}(X)$, such that $g(s) = 0$. By assumption there exists a covering $\{U_i \longrightarrow X\}_{i \in I}$, and sections $t_i \in \mathcal{F}(U_i)$, such that $f(t_i) = s|_{U_i}$. We claim that the glueing condition is satisfied, that is $t_i|_{U_{ij}} = t_j|_{U_{ij}}$ for all $(i, j) \in I^2$, where $U_{ij} = U_i \times_U U_j$. This is true, since $f(t_i|U_{ij}) = s|_{U_{ij}} = f(t_j|_{U_{ij}})$, but f is injective, which implies what we want. Therefore, there exists a section $t \in \mathcal{F}(X)$, such that $f(t)|_{U_i} = s|_{U_i}$ for all $i \in I$. We conclude that $f(t) = s$. □

Definition 2.91. *A sheaf $\mathcal{I}$ is called* injective*, if the following is true: let $\mathcal{F} \hookrightarrow \mathcal{G}$ be an injective morphism of sheaves, and $f\colon \mathcal{F} \longrightarrow \mathcal{I}$ a morphism of sheaves. Then there exists a morphism $\mathcal{G} \longrightarrow \mathcal{I}$, such that the diagram*

$$\begin{array}{ccc} \mathcal{F} & \hookrightarrow & \mathcal{G} \\ {\scriptstyle f}\downarrow & \swarrow_{\exists} & \\ \mathcal{I} & & \end{array}$$

commutes.

We emphasise that injectivity is a property, and not a universal property! We are now ready to state the third axiom of sheaf cohomology, and prove the existence of such a theory.

Definition 2.92 (Sheaf cohomology)**.** *A* sheaf cohomology theory *is a collection of functors*

$$H^i(X, -)\colon \mathrm{Sh}(X) \longrightarrow \mathsf{AbGrp}$$

for $i \geq 0$, such that:

(A1) $H^0(X, \mathcal{F}) = \Gamma(X, \mathcal{F})$ as functors,

(A2) for every short exact sequence of sheaves $0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow 0$ we have a long exact sequence

$$\cdots \longrightarrow H^i(X, \mathcal{F}) \longrightarrow H^i(X, \mathcal{G}) \longrightarrow H^i(X, \mathcal{H}) \longrightarrow H^{i+1}(\mathcal{F}) \longrightarrow \cdots .$$

And for every commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{F}_1 & \longrightarrow & \mathcal{G}_1 & \longrightarrow & \mathcal{H}_1 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{F}_2 & \longrightarrow & \mathcal{G}_2 & \longrightarrow & \mathcal{H}_2 & \longrightarrow & 0 \end{array}$$

we have a commutative diagram whose rows are the aforementioned long exact sequences.

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & H^i(X, \mathcal{F}_1) & \longrightarrow & H^i(X, \mathcal{G}_1) & \longrightarrow & H^i(X, \mathcal{H}_1) & \longrightarrow & H^{i+1}(X, \mathcal{F}_1) \longrightarrow \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \cdots & \longrightarrow & H^i(X, \mathcal{F}_2) & \longrightarrow & H^i(X, \mathcal{G}_2) & \longrightarrow & H^i(X, \mathcal{H}_2) & \longrightarrow & H^{i+1}(X, \mathcal{F}_2) \longrightarrow \cdots \end{array}$$

(A3) If $\mathcal{I}$ is an injective sheaf, then $H^i(X, \mathcal{I}) = 0$ for $i \geq 1$.

2.13 Existence of sheaf cohomology

What does (A3) of the definition of sheaf cohomology buy us? Every sheaf $\mathcal{F}$ can be embedded into an injective sheaf $\mathcal{I}$. Therefore, there exists a short exact sequence

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{I} \longrightarrow \mathcal{I}\,/\,\mathcal{F} \longrightarrow 0.$$

Assuming that there is a theory of sheaf cohomology satisfying the axioms (A1-3), we obtain for $i \geq 0$ an exact sequence

$$\cdots \longrightarrow H^i(X,\mathcal{I}) \longrightarrow H^i(X,\mathcal{I}\,/\,\mathcal{F}) \longrightarrow H^{i+1}(\mathcal{F}) \longrightarrow 0 = H^{i+1}(X,\mathcal{I}),$$

where we use that $H^{i+1}(X,\mathcal{I}) = 0$, since $\mathcal{I}$ is injective. This implies

$$H^1(X,\mathcal{F}) \simeq \operatorname{coker}(H^0(X,\mathcal{I}) \longrightarrow H^0(X,\mathcal{I}\,/\,\mathcal{F})),$$

and for $i \geq 1$:

$$H^{i+1}(X,\mathcal{F}) \simeq H^i(X,\mathcal{I}\,/\,\mathcal{F}).$$

We will turn this observation into an inductive definition. For this to make sense, we have to verify the resulting higher cohomology groups, are independent of the choice of the embedding $\mathcal{F} \hookrightarrow \mathcal{I}$.

Lemma 2.93. *The following defines a functor $H^1(X,-)\colon \operatorname{Sh}(X) \longrightarrow \mathsf{AbGrp}$. For every $\mathcal{F} \in \operatorname{Sh}(X)$ we choose an embedding $\mathcal{F} \hookrightarrow \mathcal{I}$, where $\mathcal{I}$ is an injective sheaf, and define*

$$H^1(X,\mathcal{F}) = \operatorname{coker}(H^0(X,\mathcal{I}) \longrightarrow H^0(X,\mathcal{I}\,/\,\mathcal{F})).$$

For a morphism $\mathcal{F} \xrightarrow{f} \mathcal{G}$ we choose a commutative diagram

$$\begin{array}{ccc} \mathcal{F} & \hookrightarrow & \mathcal{I} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \exists} \\ \mathcal{G} & \hookrightarrow & \mathcal{J} \end{array}$$

and define $H^1(f)$ to be the map

$$\begin{array}{ccccccc} H^0(X,\mathcal{I}) & \longrightarrow & H^0(X,\mathcal{I}\,/\,\mathcal{F}) & \longrightarrow & H^1(X,\mathcal{F}) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle H^1(f)} & & \\ H^0(X,\mathcal{J}) & \longrightarrow & H^0(X,\mathcal{J}\,/\,\mathbb{G}) & \longrightarrow & H^1(X,\mathcal{G}) & \longrightarrow & 0. \end{array}$$

The resulting functor is independent (up to a unique natural isomorphism) of the chosen embeddings $\mathcal{F} \longrightarrow \mathcal{I}$.

Proof. We begin the proof by verifying that the resulting map $H^1(f)$ is independent of the choices. That is, if we have two morphisms g and h giving rise to a commutative diagram

$$\begin{array}{ccc} \mathcal{F} & \hookrightarrow & \mathcal{I} \\ {\scriptstyle f}\downarrow & & {\scriptstyle g}\downarrow\downarrow{\scriptstyle h} \\ \mathcal{G} & \hookrightarrow & \mathcal{J} \end{array}$$

we want to prove that the induced maps $\alpha, \beta\colon H^1(X,\mathcal{F}) \longrightarrow H^1(X,\mathcal{G})$ agree. We will show that $\alpha - \beta = 0$.

$$\begin{array}{ccccccc} H^0(X,\mathcal{I}) & \longrightarrow & H^0(X,\mathcal{I}/\mathcal{F}) & \longrightarrow & H^1(X,\mathcal{F}) & \longrightarrow & 0 \\ {\scriptstyle g}\downarrow\downarrow{\scriptstyle h} & & {\scriptstyle g}\downarrow\downarrow{\scriptstyle h} & & {\scriptstyle \alpha}\downarrow\downarrow{\scriptstyle \beta} & & \\ H^0(X,\mathcal{J}) & \longrightarrow & H^0(X,\mathcal{J}/\mathcal{F}) & \longrightarrow & H^1(X,\mathcal{F}) & \longrightarrow & 0. \end{array}$$

The map $g - h\colon \mathcal{I} \longrightarrow \mathcal{I}$ satisfies $(g-h)|_{\mathcal{F}} = 0$ by definition. Therefore, we obtain a factorisation as indicated by the dotted arrow

$$\begin{array}{ccc} \mathcal{I} & \longrightarrow & \mathcal{I}/\mathcal{F} \\ {\scriptstyle g-h}\downarrow & \swarrow & \downarrow \\ \mathcal{J} & \longrightarrow & \mathcal{J}/\mathcal{G}, \end{array}$$

and we see that $g-h\colon H^0(X,\mathcal{I}/\mathcal{F}) \longrightarrow H^0(X,\mathcal{I}/\mathcal{F})$ factors through $H^0(X,\mathcal{J})$. Since $H^1(X,\mathcal{G}) = \operatorname{coker}(H^0(X,\mathcal{J}) \longrightarrow H^0(X,\mathcal{J}/\mathcal{G}))$, we obtain $\alpha - \beta = 0$.

Applying this to the commutative diagram

$$\begin{array}{ccc} \mathcal{F} & \hookrightarrow & \mathcal{I} \\ {\scriptstyle \mathrm{id}_{\mathcal{F}}}\downarrow & & {\scriptstyle g}\downarrow\downarrow{\scriptstyle \mathrm{id}_{\mathcal{I}}} \\ \mathcal{F} & \hookrightarrow & \mathcal{I}, \end{array}$$

we see that $H^1(\mathrm{id}_{\mathcal{F}})$ is the identity map of $H^1(X,\mathcal{F})$. Applying the observation to

$$\begin{array}{ccc} \mathcal{F} & \hookrightarrow & \mathcal{I} \\ \downarrow & & \downarrow \\ \mathcal{F} & \hookrightarrow & \mathcal{J} \\ \downarrow & & \downarrow \\ \mathcal{F} & \hookrightarrow & \mathcal{I}, \end{array}$$

(and also switching the roles of $\mathcal{I}$ and $\mathcal{J}$) we see that the abelian group $H^1(X,\mathcal{F})$ is independent of the chosen embedding $\mathcal{F} \hookrightarrow \mathcal{I}$.

It remains to see that for composable morphisms of sheaves $\mathcal{F} \xrightarrow{f} \mathcal{G} \xrightarrow{g} \mathcal{H}$ we have $H^1(g \circ f) = H^1(g) \circ H^1(f)$. Consider the commutative diagram

$$\begin{array}{ccc} \mathcal{F} & \hookrightarrow & \mathcal{I} \\ {\scriptstyle f}\downarrow & & \vdots\,\exists\downarrow \\ \mathcal{G} & \hookrightarrow & \mathcal{J} \\ {\scriptstyle g}\downarrow & & \vdots\,\exists\downarrow \\ \mathcal{H} & \hookrightarrow & \mathcal{K}. \end{array}$$

We know that the induced maps $H^1(f), H^1(g), H^1(g\circ)$ are independent of the chosen extensions presented by the dashed arrows. Therefore $H^1(g\circ f) = H^1(g)\circ H^1(f)$, because we can simply form the composition of two successive extension. □

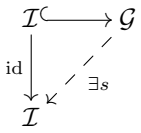
The next lemma can be understood as a consistency check of the third axiom of sheaf cohomology (A3). The condition $H^1(X,\mathcal{I}) = 0$ for an injective sheaf $\mathcal{I}$ implies in particular (using the long exact sequence) that every short exact sequence of sheaves $0 \longrightarrow \mathcal{I} \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow 0$ gives rise to a short exact sequence of global sections. This can be verified directly, and will be used in the proof of existence of sheaf cohomology.

Lemma 2.94. *Let $0 \longrightarrow \mathcal{I} \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow 0$ be a short exact sequence of sheaves, such that $\mathcal{I}$ is injective. Then the sequence of global sections*

$$0 \longrightarrow \Gamma(X,\mathcal{I}) \longrightarrow \Gamma(X,\mathcal{G}) \longrightarrow \Gamma(X,\mathcal{H}) \longrightarrow 0$$

is exact.

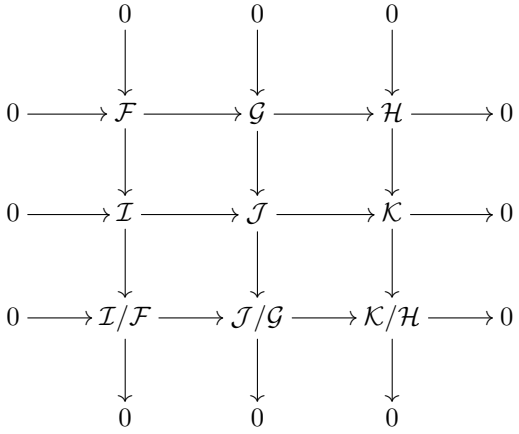
Proof. Using injectivity of $\mathcal{I}$, we obtain a morphism of sheaves $r\colon\ \mathcal{G} \longrightarrow \mathcal{I}$, such that



commutes. This implies that the short exact sequence $0 \longrightarrow \mathcal{I} \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow 0$ splits, that is $\mathcal{G} \simeq \mathcal{I}\oplus\mathcal{H} = \mathcal{I}\times\mathcal{H}$. But $H^0(X,\mathcal{I}\oplus\mathcal{H}) \simeq H^0(X,\mathcal{I}) \oplus H^0(X,\mathcal{H})$, and therefore we see that the map $H^0(X,\mathcal{G}) \longrightarrow H^0(X,\mathcal{H})$ is indeed surjective, and the sequence above thus exact. □

Lemma 2.95. *For every short exact sequence of sheaves $0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow 0$ we have a long exact sequence $0 \longrightarrow H^0(X,\mathcal{F}) \longrightarrow H^0(X,\mathcal{G}) \longrightarrow H^0(X,\mathcal{H}) \longrightarrow H^1(X,\mathcal{F}) \longrightarrow H^1(X,\mathcal{G}) \longrightarrow H^1(X,\mathcal{H})$, where $H^1(X,-)$ is the functor defined in Lemma 2.93.*

Proof. It is left as an exercise to show that there exist embeddings into injective sheaves $\mathcal{F} \hookrightarrow \mathcal{I}$, $\mathcal{G} \hookrightarrow \mathcal{J}$, and $\mathcal{H} \hookrightarrow \mathcal{K}$, such that we have the following commutative diagram with exact rows and exact columns.



Applying the functor $H^0(X,-)$ to the lower two rows we obtain the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(X,\mathcal{I}) & \longrightarrow & H^0(X,\mathcal{J}) & \longrightarrow & H^0(X,\mathcal{H}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H^0(X,\mathcal{I}/\mathcal{F}) & \longrightarrow & H^0(X,\mathcal{J}/\mathcal{G}) & \longrightarrow & H^0(X,\mathcal{K}/\mathcal{H}). & & \end{array}$$

The first row is exact by virtue of Lemma 2.94. The Snake Lemma gives rise to the required long exact sequence $0 \longrightarrow H^0(X,\mathcal{F}) \longrightarrow H^0(X,\mathcal{G}) \longrightarrow H^0(X,\mathcal{H}) \longrightarrow H^1(X,\mathcal{F}) \longrightarrow H^1(X,\mathcal{G}) \longrightarrow H^1(X,\mathcal{H})$. □

Theorem 2.96. *There exists a unique (up to a unique isomorphism) formalism of sheaf cohomology as in Definition 2.92.*

Proof. We will prove by induction on the degree i, that there exists a family of functors

$$H^i(X,-)\colon \mathrm{Sh}(X) \longrightarrow \mathsf{AbGrp},$$

verifying the axioms $(A1-3)$ up to the given degree. For $i \leq 1$ we know that such a family exists by virtue of Lemma 2.93. In this lemma we verified explicitly that (A1-2) are satisfied, and (A3) holds by definition of the functor $H^1(X,-)$. Indeed, if $\mathcal{I}$ is an injective sheaf, we may consider the trivial embedding $\mathrm{id}_{\mathcal{I}}\colon \mathcal{I} \hookrightarrow \mathcal{I}$, and hence obtain $H^1(X,\mathcal{I}) = \mathrm{coker}(H^1(X,\mathcal{I}) \xrightarrow{\mathrm{id}} H^0(X,\mathcal{I})) = 0$.

For $i \geq 1$ we define $H^{i+1}(X,\mathcal{F}) = H^i(X,\mathcal{I}\,/\,\mathcal{F})$, where $\mathcal{F} \hookrightarrow \mathcal{I}$ is an embedding into an injective sheaf (according to E7, ex. 5 this is always possible). For a morphism of sheaves $\mathcal{F} \xrightarrow{f} \mathcal{G}$ we choose a commutative diagram

$$\begin{array}{ccc} \mathcal{F} & \hookrightarrow & \mathcal{I} \\ {\scriptstyle f}\downarrow & & \vdots \\ \mathcal{G} & \hookrightarrow & \mathcal{J}. \end{array} \tag{5}$$

as in our construction of the functor $H^1(X,-)$ in Lemma 2.93. We will use the same strategy as in *loc. cit.* to verify that the induced map

$$\begin{array}{ccc} H^{i+1}(X,\mathcal{F}) & \longrightarrow & H^{i+1}(X,\mathcal{G}) \\ \| & & \| \\ H^i(X,\mathcal{I}\,/\,\mathcal{F}) & \longrightarrow & H^i(X,\mathcal{J}\,/\,\mathcal{G}) \end{array}$$

is independent of the choice of the dashed morphism. Again we denote by $g,h\colon \mathcal{I} \longrightarrow \mathcal{J}$ two morphisms of sheaves, fitting into the commutative diagram (5). Their difference $g-h$ satisfies $(g-h)|_{\mathcal{F}} = 0$ by commutativity. Therefore, we obtain a factorisation

$$\begin{array}{ccc} \mathcal{I} & \longrightarrow & \mathcal{I}\,/\,\mathcal{F} \\ {\scriptstyle g-h}\downarrow & \swarrow & \downarrow{\scriptstyle g-h} \\ \mathcal{J} & \longrightarrow & \mathcal{J}\,/\,\mathcal{G}\,. \end{array} \tag{6}$$

as indicated by the dotted arrow. Applying the functor $H^i(X,-)$, we obtain a commutative diagram

$$\begin{array}{ccc} H^i(X,\mathcal{I}) & \longrightarrow & H^i(\mathcal{I}\,/\,\mathcal{F}) \\ {\scriptstyle g-h}\downarrow & \swarrow & \downarrow{\scriptstyle g-h} \\ H^i(X,\mathcal{J}) & \longrightarrow & H^i(X,\mathcal{J}\,/\,\mathcal{G}). \end{array} \tag{7}$$

By the induction hypothesis we have $H^i(X,\mathcal{J})=0$. Therefore, we see that $g-h$ induces the zero morphism. As in the proof of Lemma 2.93 we conclude that $H^{i+1}(X,-)$ is a functor.

It remains to verify the axioms $(A2-3)$. If $\mathcal{I}$ is an injective sheaf, then we obtain for $i\geq 1$, $H^{i+1}(X,\mathcal{I})=H^i(X,\mathcal{I}\,/\,\mathcal{I})=0$. This shows that our family of functors satisfies (A3).

Let $0\longrightarrow\mathcal{F}\longrightarrow\mathcal{G}\longrightarrow\mathcal{H}\longrightarrow 0$ be a short exact sequence of sheaves. There exists a commutative diagram with exact rows and columns, such that $\mathcal{I}$, $\mathcal{J}$, and $\mathcal{K}$ are injective sheaves.

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{F} & \longrightarrow & \mathcal{G} & \longrightarrow & \mathcal{H} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{I} & \longrightarrow & \mathcal{J} & \longrightarrow & \mathcal{K} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{I}/\mathcal{F} & \longrightarrow & \mathcal{J}/\mathcal{G} & \longrightarrow & \mathcal{K}/\mathcal{H} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array} \tag{8}$$

For $i\geq 2$ we may simply apply the existence of the long exact sequence for $H^{i-1}(X,-)$ and $H^i(X,-)$, to obtain

$$\begin{array}{ccccccccccc} H^{i-1}(X,\mathcal{I}\,/\,\mathcal{F}) & \longrightarrow & H^{i-1}(X,\mathcal{J}\,/\,\mathcal{G}) & \longrightarrow & H^{i-1}(X,\mathcal{K}\,/\mathcal{H}) & \longrightarrow & H^i(X,\mathcal{I}\,/\,\mathcal{F}) & \longrightarrow & H^i(X,\mathcal{J}\,/\,\mathcal{G}) & \longrightarrow & H^i(X,\mathcal{K}\,/\mathcal{H}) \\ \| & & \| & & \| & & \| & & \| & & \| \\ H^i(X,\mathcal{F}) & \longrightarrow & H^i(X,\mathcal{G}) & \longrightarrow & H^i(X,\mathcal{H}) & \longrightarrow & H^{i+1}(X,\mathcal{F}) & \longrightarrow & H^{i+1}(X,\mathcal{G}) & \longrightarrow & H^{i+1}(X,\mathcal{H}). \end{array}$$

For $i=1$ we have to be more careful, because $H^1(X,\mathcal{F})$ is not equal to $H^0(X,\mathcal{I}\,/\,\mathcal{F})$ in general, but rather to $\operatorname{coker}(H^0(X,\mathcal{I})\longrightarrow H^0(X,\mathcal{I}\,/\,\mathcal{F}))$. We obtain the corresponding part of the long exact sequence as follows. Consider the bottom two rows of (8). Lemma 2.93 implies that we have a commutative diagram

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & H^0(X,\mathcal{I}) & \longrightarrow & H^0(X,\mathcal{J}) & \longrightarrow & H^0(X,\mathcal{K}) & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 \\ & & {\scriptstyle\alpha}\downarrow & & {\scriptstyle\beta}\downarrow & & {\scriptstyle\gamma}\downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & H^0(X,\mathcal{I}/\mathcal{F}) & \longrightarrow & H^0(X,\mathcal{J}/\mathcal{G}) & \longrightarrow & H^0(X,\mathcal{K}/\mathcal{H}) & \longrightarrow & H^1(X,\mathcal{I}/\mathcal{F}) & \longrightarrow & H^1(X,\mathcal{J}/\mathcal{G}) & \longrightarrow & H^1(X,\mathcal{K}/\mathcal{H}) \end{array}$$

with exact rows. Taking cokernels of the vertical arrows, a simple diagram chase verifies that the sequence

$$\begin{array}{ccccccccccc}
\operatorname{coker}\alpha & \longrightarrow & \operatorname{coker}\beta & \longrightarrow & \operatorname{coker}\gamma & \longrightarrow & H^1(X,\mathcal{I}/\mathcal{F}) & \longrightarrow & H^1(X,\mathcal{J}/\mathcal{G}) & \longrightarrow & H^1(X,\mathcal{K}/\mathcal{H}) \\
\| & & \| & & \| & & \| & & \| & & \| \\
H^1(X,\mathcal{F}) & \longrightarrow & H^1(X,\mathcal{G}) & \longrightarrow & H^1(X,\mathcal{H}) & \longrightarrow & H^2(X,\mathcal{F}) & \longrightarrow & H^2(X,\mathcal{G}) & \longrightarrow & H^2(X,\mathcal{H})
\end{array}$$

is exact as required. □

2.14 H^1, torsors and the Picard group

Let $\mathcal{F}$ be a sheaf (in abelian groups) on a site $(\mathsf{C},\mathcal{T})$ with initial object X. Elements of $H^1(X,\mathcal{F})$ can still be grasped "geometrically" in terms of objects called *torsors*.

Definition 2.97. *An* $\mathcal{F}$-sheaf *is a sheaf in sets T on $(\mathsf{C},\mathcal{T})$, together with a map $a\colon \mathcal{F}\times T\longrightarrow T$, such that*

(a) for $U\in\mathsf{C}$ the map $a_U\colon \mathcal{F}(U)\times T(U)\longrightarrow T(U)$ defines an action on T.

An $\mathcal{F}$-sheaf *is called an $\mathcal{F}$-torsor, if*

(b) for every $U\in\mathsf{C}$ there exists a $\mathcal{T}$-covering $\{U_i\longrightarrow U\}_{i\in I}$, such that $T(U_i)\simeq\mathcal{F}(U_i)$ as sets with $\mathcal{F}(U_i)$-actions.

Given two $\mathcal{F}$-sheaves (T_1,a_1) and (T_2,a_2), one can build a new $\mathcal{F}$-sheaf $T_1\otimes_{\mathcal{F}}T_2$ which we will refer to as the $\mathcal{F}$-tensor product or *Baer sum*.

Definition 2.98. *We define $T_1\otimes_{\mathcal{F}}T_2$ to be the quotient sheaf of $T_1\times T_2$ by the $\mathcal{F}$-action*

$$\mathcal{F}\times T_1\times T_2\xrightarrow{(a_1,a_2^{-1})}T_1\times T_2.$$

That is, the action which on the level of local sections looks like $\lambda\cdot(t_1,t_2)\mapsto(at_1,a^{-1}t_2)$.

Just like the tensor product of vector spaces, $T_1\otimes_{\mathcal{F}}T_2$ satisfies a universal property with respect to $\mathcal{F}$-bilinear maps.

Definition 2.99. *Let T_1, T_2 and S be $\mathcal{F}$-sheaves. An $\mathcal{F}$-bilinear map is a morphism of sheaves $\varphi\colon T_1\times T_2\longrightarrow S$, such that for local sections we have*

$$\varphi(ft_1,t_2)=\varphi(t_1,ft_2).$$

Similarly one defines trilinear and multilinear maps.

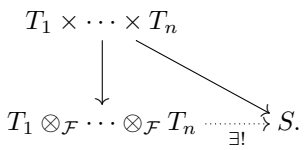
Lemma 2.100. *The canonical map*

$$T_1\times\cdots\times T_n\longrightarrow T_1\otimes_{\mathcal{F}}\cdots\otimes_{\mathcal{F}}T_n$$

is the universal $\mathcal{F}$-multilinear map. That is, for every $\mathcal{F}$-multilinear map of $\mathcal{F}$-sheaves

$$\varphi\colon T_1\times\cdots\times T_n\longrightarrow S$$

there exists a unique $\mathcal{F}$-linear map $T_1 \otimes_{\mathcal{F}} \cdots \otimes_{\mathcal{F}} T_n \longrightarrow S$, such that



Corollary 2.101. *We have canonical isomorphisms $\mathcal{F} \otimes_{\mathcal{F}} \mathcal{F} \simeq \mathcal{F}$ and $(T_1 \otimes_{\mathcal{F}} T_2) \otimes_{\mathcal{F}} T_3 \simeq T_1 \otimes_{\mathcal{F}} (T_2 \otimes_{\mathcal{F}} T_3)$ and $T_1 \otimes_{\mathcal{F}} T_2 \simeq T_2 \otimes_{\mathcal{F}} T_1$.*

Proof. For the first isomorphism it suffices to observe that the multiplication map $\mathcal{F} \times \mathcal{F} \longrightarrow \mathcal{F}$ is universal amongst $\mathcal{F}$-bilinear maps. Similarly, both $(T_1 \otimes_{\mathcal{F}} T_2) \otimes_{\mathcal{F}} T_3$ and $T_1 \otimes_{\mathcal{F}} (T_2 \otimes_{\mathcal{F}} T_3)$ receive a universal $\mathcal{F}$-trilinear map, and both $T_1 \otimes_{\mathcal{F}} T_2$ and $T_2 \otimes_{\mathcal{F}} T_1$ receive a universal $\mathcal{F}$-bilinear map. □

Next, we observe that the tensor product operation preserves $\mathcal{F}$-torsors.

Lemma 2.102. *Let T_1 and T_2 be $\mathcal{F}$-torsors, then $T_1 \otimes_{\mathcal{F}} T_2$ is an $\mathcal{F}$-torsor.*

Proof. Let U be an object of C, there exists a $\mathcal{T}$-covering $\{U_i \longrightarrow U\}_{i \in I}$, such that $T_1|_{U_i} \simeq \mathcal{F}|_{U_i}$. For every $i \in I$ there exists a $\mathcal{T}$-covering $\{U_{ij} \longrightarrow U_i\}_{j \in I_i}$, such that $T_2|_{U_{ij}} \simeq \mathcal{F}|_{U_{ij}}$. By the axioms of a Grothendieck topology, $\{U_{ij} \longrightarrow U\}_{(i,j) \in \bigsqcup I_i}$ is a $\mathcal{T}$-covering of U. Therefore we may assume without loss of generality that $\{U_i \longrightarrow U\}_{i \in I}$ satisfies $T_1|_{U_1} \simeq \mathcal{F}|_{U_i}$ and $T_2|_{U_i} \simeq \mathcal{F}|_{U_i}$ for all $i \in I$.

The tensor product of the trivial torsors $\mathcal{F} \otimes_{\mathcal{F}} \mathcal{F}$ is isomorphic to $\mathcal{F}$ (Corollary 2.101). Since $\mathcal{T}$-torsors are $\mathcal{T}$-locally trivial, the tensor product of $\mathcal{F}$-torsors is again an $\mathcal{F}$-torsor. □

Lemma 2.103. *For an $\mathcal{F}$-sheaf T we denote by $T^\vee$ the $\mathcal{F}$-sheaf $\underline{\mathsf{Hom}}(T, \mathcal{F})$, that is the sheaf of sheaf morphisms $T \longrightarrow \mathcal{F}$. If T is an $\mathcal{F}$-torsor there is a canonical isomorphism $\mathcal{F} \otimes \mathcal{F}^\vee \simeq \mathcal{F}$.*

Proof. We have a canonical $\mathcal{F}$-bilinear map $T \times T^\vee \longrightarrow \mathcal{F}$, since $T^\vee = \underline{\mathsf{Hom}}(T, \mathcal{F})$ (given by evaluation). Hence we get an $\mathcal{F}$-linear map $T \otimes_{\mathcal{F}} T^\vee \longrightarrow \mathcal{F}$. Since an $\mathcal{F}$-linear map of torsors is always an isomorphism, this concludes the proof. □

Definition 2.104. *We define $\mathsf{Tors}(\mathcal{F})$ to be the set of isomorphism classes of $\mathcal{F}$-torsors. Tensor product and duals of $\mathcal{F}$-torsors give rise to a structure of an abelian group on $\mathsf{Tors}(\mathcal{F})$.*

Let

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \xrightarrow{g} \mathcal{H} \longrightarrow 0$$

be a short exact sequence of sheaves. There is a natural map from $\mathcal{H}(X) = H^0(X, \mathcal{H}) \longrightarrow \mathsf{Tors}(\mathcal{F})$. It assigns to a global section $s \in \mathcal{H}(X)$ the $\mathcal{F}$-torsor T_s of local liftings.

Definition 2.105. *We define the sheaf $T_s = g^{-1}(s)$ to be $T_s(U) = \{t \in \mathcal{G}(U) | g(t) = s\}$.*

Exactness of the sequence implies right away that T_s is an $\mathcal{F}$-torsor.

Theorem 2.106. *There exists an isomorphism $H^1(X, \mathcal{F}) \simeq \mathsf{Tors}(\mathcal{F})$, such that the map $s \mapsto T_s = g^{-1}(s)$ corresponds to the boundary map*

$$H^0(X, \mathcal{H}) \longrightarrow H^1(X, \mathcal{F})$$

in the long exact sequence of sheaf cohomology.

Sketch. The proof is divided into two steps.

Claim 2.107. *The abelian group* $\mathsf{Tors}(\mathcal{F})$ *is isomorphic to the abelian group of isomorphism classes of* extensions $\mathsf{Ext}(\underline{\mathbb{Z}}, \mathcal{F})$ *of* $\underline{\mathbb{Z}}$ *by* $\mathcal{F}$*, that is short exact sequences*

$$0 \longrightarrow \mathcal{F} \longrightarrow E \longrightarrow \underline{\mathbb{Z}} \longrightarrow 0,$$

where $\underline{\mathbb{Z}}$ *denotes the sheafification of the constant presheaf* $U \mapsto \mathbb{Z}$.[18]

Proof. Given an extension E as above, one associates to it the $\mathcal{F}$-torsor E_1, that is, the sheaf of local liftings of $1 \in \underline{\mathbb{Z}}(X)$. Vice versa, given an $\mathcal{F}$-torsor T, one constructs E as sheafification of

$$\bigsqcup_{i \in \mathbb{Z}} T^{\otimes i},$$

where $T^{\otimes 0} = \mathcal{F}$ and $T^{-\otimes n} = (T^{\otimes n})^{\vee}$. □

Claim 2.108. *One has a natural isomorphism* $\mathsf{Ext}(\underline{\mathbb{Z}}, \mathcal{F}) \simeq H^1(X, \mathcal{F})$.

In order to see this we recall that $H^1(X, \mathcal{F})$ is defined as the quotient $H^0(X, \mathcal{I} \,/\, \mathcal{F})/H^0(X, \mathcal{I})$ where $\mathcal{F} \hookrightarrow \mathcal{I}$ is an embedding of $\mathcal{F}$ into an injective sheaf $\mathcal{I}$. Let E be an extension of $\underline{\mathbb{Z}}$ by $\mathcal{F}$ as above. By injectivity of $\mathcal{I}$ there exists a map $g_1 \colon E \longrightarrow \mathcal{I}$, such that the left hand square of the diagram below commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{F} & \longrightarrow & E & \longrightarrow & \underline{\mathbb{Z}} & \longrightarrow & 0 \\ & & \downarrow & & \vdots & & \vdots & & \\ 0 & \longrightarrow & \mathcal{F} & \longrightarrow & \mathcal{I} & \longrightarrow & \mathcal{I} \,/\, \mathcal{F} & \longrightarrow & 0. \end{array}$$

By exactness of the first row we get an induced map $s_1 \colon \underline{\mathbb{Z}} \longrightarrow \mathcal{I} \,/\, \mathcal{F}$. It corresponds to a global section $s_1 \in H^0(X, \mathcal{I} \,/\, \mathcal{F})$. Given a different choice of a map $g_1 \colon E \longrightarrow \mathcal{I}$ we obtain an element s_2, such that the difference $s_1 - s_2$ factors through $H^0(X, \mathcal{I})$. The resulting element of $H^1(X, \mathcal{F})$ is therefore well-defined.

Vice versa, given a global section $s \in H^0(X, \mathcal{I} \,/\, \mathcal{F})$, there is a corresponding map $\underline{\mathbb{Z}} \longrightarrow \mathcal{I} \,/\, \mathcal{F}$. We obtain a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{F} & \longrightarrow & \mathcal{I} \times_{\mathcal{I} \,/\, \mathcal{F}} \underline{\mathbb{Z}} & \longrightarrow & \underline{\mathbb{Z}} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{F} & \longrightarrow & \mathcal{I} & \longrightarrow & \mathcal{I} \,/\, \mathcal{F} & \longrightarrow & 0. \end{array}$$

The top row is the sought-for extension of $\underline{\mathbb{Z}}$ by $\mathcal{F}$. □

After a lot of abstract nonsense we finally return to algebraic geometry.

Definition 2.109. *For a smooth* k*-variety* X *one defines the Picard group* $\mathsf{Pic}(X) = H^1_{Zar}(X, \mathbb{G}_m)$.

[18] For the Zariski or small étale site this corresponds precisely to the sheaf of locally constant $\mathbb{Z}$-valued functions.

Elements of the Picard group can also be understood in terms of *line bundles* on X, that is, algebraic vector bundles of rank 1.

By definition, the Picard group $\mathsf{Pic}(X)$ can be identified with the group of $\mathbb{G}_m$-torsors on X, defined with respect to the Zariski topology. However, descent theory (to be discussed subsequently) implies the following:

Theorem 2.110 (Grothendieck's Hilbert 90)**.** *There is an isomorphism* $\mathsf{Pic}(X) = H^1_{\acute{e}t}(X, \mathbb{G}_m)$.

Corollary 2.111. *Let k be a field, then* $H^1_{\acute{e}t}(\mathsf{MSpec}\, k, \mathbb{G}_m) = 0$.

Proof. The only non-empty Zariski open subset of $\mathsf{MSpec}\, k$ is $\mathsf{MSpec}\, k$ itself. Therefore, every Zariski $\mathbb{G}_m$-torsor has to be trivial. □

Lemma 2.112. *We have* $\mathsf{Pic}(\mathsf{MSpec}\, R) = 0$*, if R is a principal ideal domain. In particular,* $H^1_{\acute{e}t}(\mathsf{MSpec}\, R, \mathbb{G}_m) = 0$.

Proof. A $\mathbb{G}_m$-torsor on $X = \mathsf{MSpec}\, R$ can be represented by a Zariski covering $\{U_i \longrightarrow X\}_{i\in I}$ (without loss of generality, by affine varieties $U_i = \mathsf{MSpec}\, R_i$) and a so-called cocycle $(\phi_{ij})_{i,j\in I^2}$, where $\phi_{ij} \colon U_{ij} = U_i \times_X U_j \longrightarrow \mathbb{G}_m$. We can consider $U = \bigsqcup_{i\in I} U_i \longrightarrow X$, and consider the $(\phi_{ij})_{ij}$ as a descent datum for a module M on X. One has $M \otimes_R R_i \simeq R_i$, that is, M is finitely generated and locally free of rank 1. Since R is a principal ideal domain, the classification of R-modules implies that M is a free R-module of rank 1. This implies triviality of the corresponding $\mathbb{G}_m$-torsor. □

2.15 Descent theory

Descending modules

Faithfully flat R-algebras S are flat R-algebras, which reflect if a module is *zero*.

Definition 2.113. *A flat R-algebra S is called* faithfully flat*, if for every R-module M_R we have that $S \otimes_R M_R = 0$ implies that M_R is the zero module.*

A faithfully flat R-algebra S allows us to check that module is zero after tensoring with S. This definition implies directly that many other properties of modules, and morphisms of modules, descend along faithfully flat maps.

Lemma 2.114. *Let $\alpha \colon R \to S$ be a faithfully flat ring homomorphism.*

(a) Let $f \colon M_R \to N_R$ a morphism of R-modules, such that $S \otimes_R M_R \to S \otimes_R M_R$ is an injection (respectively a surjection), then f is an injection (respectively a surjection).

(b) A sequence of R-modules

$$U_R \xrightarrow{f} V_R \xrightarrow{g} W_R,$$

with $g \circ f = 0$ is exact, if and only if the base change

$$S \otimes_R U_R \to S \otimes_R V_R \to S \otimes_R W_R$$

is exact.

(c) If M_R is an R-module, such that $S \otimes_R M_R$ is a finite S-module, then M_R is finite as well.

(d) If $S \otimes_R M_R$ is a finite projective S-module, then M_R is a finite projective R-module.

(e) Flatness of $S \otimes_R M_R$ as S-module implies flatness of M_R as R-module.

Proof. A morphism of modules $f\colon M_R \longrightarrow N_R$ is an injection if and only i $\ker f = 0$ (respectively if $\operatorname{coker} f = N_R/\operatorname{im} f = 0$). Flatness of S implies that $S \otimes_R -$ preserves ker and coker. Therefore, by the assumption that S is faithfully flat, we see that f is an injection (respectively a surjection) if and only if its base change is. This concludes the proof of (a).

Flatness implies that exactness is preserved, therefore it suffices to show that exactness of

$$S \otimes_R U_R \to S \otimes_R V_R \to S \otimes_R W_R$$

implies that

$$U_R \to V_R \to W_R$$

is exact. Since $g \circ f = 0$, we have to show that the induced map

$$\operatorname{coker} f \to \ker g$$

is an isomorphism. We know that this is true after applying the functor $S \otimes_R -$, this implies the assertion, using statement (a).

Assertion (c) follows directly from (a). Choose a finite basis $n_1, \ldots, n_\ell$ for $S \otimes_R M_R$, where each n_i can be written as a sum $m_{i1} \otimes s_{i1} + \cdots m_{ik} \otimes s_{ik}$. We claim that the collection of elements m_{ij} yields a basis for M_R. This is the case, since the corresponding map $(R^{\ell k} \longrightarrow M_R) \otimes_R S$ is a surjection. Hence, by (a) $R^{\ell k} \longrightarrow M_R$ is already a surjection.

The proof of assertion (d) is left as an exercise. Assertion (e) follows from (b). □

So far our treatment of descent theory has focused on qualitative aspects of modules. We have seen that properties like finiteness, flatness, and projectivity descend along faithfully flat map of rings. One can do better. It is possible to describe the datum of an R-module M_R in terms of the S-module $S \otimes_R M_R$, endowed with extra structure, which we will pin down subsequently.

We refer the reader to Vistoli's chapter in [FGI+05, Thm. 4.21] for a more detailed version of the proofs below.

Definition 2.115. *For a ring homomorphism $R \to S$ we define a category $\mathsf{Desc}_{R\to S}$ as the category of pairs (M_S, ϕ), where M_S is an S-module, and ϕ is an isomorphism of $S \otimes_R S$-modules*

$$\phi\colon M_S \otimes_R S \xrightarrow{\cong} S \otimes_R M,$$

which satisfies the identity

$$\begin{array}{ccc} M_S \otimes_R S \otimes_R S & \longrightarrow & S \otimes_R M \otimes_R S \\ & \searrow & \downarrow \\ & & S \otimes_R S \otimes_R M_S \end{array} \tag{9}$$

of $(S \otimes_R S \otimes_R S)$-modules.

Forgetting the isomorphism ϕ (a.k.a. the descent datum), we obtain a forgetful functor

$$\mathsf{Desc}_{R\to S} \to \mathsf{Mod}(R).$$

Base change always factors through this forgetful functor.

Lemma 2.116. *We have a commutative diagram of categories*[19]

$$\begin{array}{ccc} \mathsf{Mod}(R) & \longrightarrow & \mathsf{Desc}_{R\to S} \\ & \searrow^{S\otimes_R -} & \downarrow \\ & & \mathsf{Mod}(S). \end{array}$$

By abuse of language, the resulting functor $\mathsf{Mod}(R) \to \mathsf{Desc}_{R\to S}$ *will also be denoted by* $S \otimes_R -$.

Proof. Let M_R be an R-module. We have to produce an isomorphism ϕ_M of $(S \otimes_R S)$-modules

$$(S \otimes_R M_R) \otimes_R S \xrightarrow{\phi} S \otimes_R (S \otimes_R M_R).$$

There is a natural choice for such a morphism, it sends the element $s_1 \otimes m \otimes s_2$ to $s_1 \otimes s_1 \otimes m$. We now have to check that (9) is satisfied. This amounts to

$$s_1 \otimes m \otimes s_2 \otimes s_3 \mapsto s_1 \otimes s_2 \otimes m \otimes s_3 \mapsto s_1 \otimes s_2 \otimes s_3 \otimes m$$

being the same map as

$$s_1 \otimes m \otimes s_2 \otimes s_3 \mapsto s_1 \otimes s_2 \otimes s_3 \otimes m.$$

This defines the required functor $\mathsf{Mod}(R) \to \mathsf{Desc}_{R\to S}$, such that the diagram above commutes. □

Theorem 2.117 (Faithfully flat descent)**.** *Let* $R \to S$ *be a faithfully flat morphism of rings. The canonical functor*

$$- \otimes_R S \colon \mathsf{Mod}(R) \longrightarrow \mathsf{Desc}_{R\to S}$$

is an equivalence of categories.

Proof. We denote the functor $- \otimes_R S$ by F. Let $G \colon \mathsf{Desc}_{R\to S} \to \mathsf{Mod}(R)$ be the functor, sending (M_S, ϕ) to the R-module

$$G(M_S, \phi) = \{m \in M | \phi(m \otimes 1) = 1 \otimes m\}.$$

We claim that F and G are mutually inverse functors. At first, we construct a natural transformation $\mathrm{id}_{\mathsf{Mod}(R)} \to GF$, i.e. for every R-module M_R a canonical map

$$\tau \colon \mathrm{M} \to G(S \otimes_R M_R).$$

Lemma 2.118. *Let* $R \to S$ *be faithfully flat, and* M_R *an* R*-module. For* $i = 1, 2$ *we denote by* $e_i \colon S \to S \otimes_R S$ *the maps* $e_1(s) = s \otimes 1$*, and* $e_2(s) = 1 \otimes s$*. The sequence*

$$0 \to M_R \xrightarrow{\delta} S \otimes_R M_R \xrightarrow{(e_1 - e_2)\otimes_R \mathrm{id}_M} S \otimes_R S \otimes_R M_R$$

is an exact sequence.

[19] We adopt the convention that a diagram of functors which commutes up to a natural transformation is called commutative. A more precise formulation would be to call such diagrams 2-commutative.

We will prove this lemma at the end of this subsection. For now we note that $\ker((e_1 - e_2) \otimes_R \mathrm{id}_M)$ can be identified with $G(S \otimes_R M_R)$, since we have

$$((e_1 - e_2) \otimes_R \mathrm{id}_M)(s \otimes b) = s \otimes 1 \otimes m - 1 \otimes s \otimes m = \phi_M(s \otimes m \otimes 1) - 1 \otimes s \otimes m.$$

By virtue of the lemma we have that $G(S \otimes_R M_R)$ is isomorphic to M_R.

Vice versa, if (N_S, ϕ) is an object in $\mathsf{Desc}_{R \to S}$, we have to produce a natural morphism

$$\gamma \colon S \otimes_R G(N_S, \phi) \to N_S.$$

By definition, we have that $G(N_S, \phi) \subset N_S$. In particular, we obtain a morphism γ by S-linear extension:

$$s \otimes n \mapsto s \cdot n.$$

As before, we have to check that γ is an isomorphism. In order to see this, we define morphisms of modules $f_i \colon N_S \longrightarrow S \otimes_R N_S$ for $i = 1, 2$. We set $f_1(n) = 1 \otimes n$, and $f_2(n) = \phi(n \otimes 1)$. The morphisms are chosen in a way, such that we have

$$G(N, \phi) = \ker(f_1 - f_2).$$

We then use the following commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & M_R \otimes_R S & \longrightarrow & N \otimes_R S & \xrightarrow{(e_1 - e_2) \otimes_R \mathrm{id}_S} & S \otimes_R M_R \otimes_R S \\ & & \downarrow{\scriptstyle \gamma \circ T} & & \downarrow{\scriptstyle \phi} & & \downarrow \\ 0 & \longrightarrow & N_S & \longrightarrow & S \otimes_R N_S & \xrightarrow{(f_1 - f_2)} & S \otimes_R S \otimes_R N_S. \end{array}$$

Here, T denotes the map exchanging the factors $M_R \otimes_R S \xrightarrow{\cong} S \otimes_R M$. Since the second and third vertical arrow are isomorphisms, so is the first. This implies that $S \otimes_R G(N_S, \phi) \cong N_S$. □

It remains to prove Lemma 2.118. It could be considered at the key technical result which lies at the heart of descent theory. It is also the only place where we will visibly use the assumption that $\alpha \colon R \to S$ is faithfully flat.

Proof of Lemma 2.118. We assume that there exists a ring homomorphism $g \colon S \to R$, such that $g \circ \alpha = \mathrm{id}_R$. In plain language: g is a left inverse. This implies in particular that α is injective, hence deals with exactness at the first node from the left. We have to show that an element in the kernel of $(e_1 - e_2) \otimes \mathrm{id}_M$ lies in the image of δ. Let $s \otimes m$ be in the kernel, i.e. we have $s \otimes m \otimes 1 = 1 \otimes s \otimes m$. Apply the map g to the first factor, which yields the identity

$$g(s) \otimes m = s \otimes m.$$

Since $g(s) \in R$, we can rewrite the left hand side as $1 \otimes g(s)m$. This implies that $s \otimes m \in \mathsf{im}(\delta)$.

If $R \to S$ is a ring homomorphism, we observe that the base change

$$R \otimes_R S \cong S \to S \otimes_R S$$

has a section given by the multiplication map $S \otimes_R S \to S$. This implies directly that the sequence of Lemma 2.118 is exact, after tensoring with $- \otimes_R S$. Since $\alpha \colon R \to S$ is faithfully flat, we conclude from Lemma 2.114(b) that the original sequence is exact as well. □

Descent for ring homomorphisms

Assume that we have a ring homomorphism $\beta\colon S \to T$, and a third ring R. We will see in this paragraph that ring homomorphisms from R to S can be described in terms of the composition $R \to T$, provided that β is faithfully flat. While this is a purely algebraic statement at this point, we will give a geometric interpretation of this result in a later section.

Proposition 2.119. *We have natural maps $e_1\colon T \to T \otimes_S T$, and $e_2\colon T \to T \otimes_S T$. The diagram of sets*

$$\mathsf{Hom}_{\mathsf{Rng}}(R,S) \to \mathsf{Hom}_{\mathsf{Rng}}(R,T) \rightrightarrows \mathsf{Hom}_{\mathsf{Rng}}(R, T \otimes_S T)$$

is an equalizer diagram in the category of sets. I.e., the set of ring homomorphism $g\colon R \to T$, satisfying $e_1 \circ g = e_2 \circ g$, is in bijection with the set of ring homomorphisms $f\colon R \to S$.

Proof. Lemma 2.118 implies that we have an exact sequence

$$0 \to S \xrightarrow{e_1 - e_2} S \otimes_R S,$$

hence an equalizer diagram in the category of rings

$$S \to T \rightrightarrows T \otimes_S T.$$

Since $\mathsf{Hom}_{\mathsf{Rng}}(R,-)$ sends equalizers to equalizers, we obtain the assertion. □

By virtue of the Dictionary 1.22, and the fact that surjective étale morphisms of k-varieties give rise to faithfully flat ring homomorphims, we obtain the following corollary.

Corollary 2.120. *Let X be a smooth k-variety and Y be an arbitrary k-variety. Then, the set-valued presheaf $\underline{Y}_X$ on $(X)_{\acute{e}t}$, which assigns to an étale morphism $U \longrightarrow X$ the set $\mathbf{Mor}(U,Y)$, is a set-valued sheaf.*

2.16 Example: the cohomology of elliptic curves

Let $\bar{k}$ be an algebraically closed field. If $\mathsf{char}(\bar{k})$ is positive, we will denote the corresponding prime number by p, and let ℓ be a prime number, such that $\ell \neq p$.

Recall that an elliptic curve $\bar{E}$ over $\bar{k}$ is a smooth projective $\bar{k}$-variety $\bar{E}$, together with the structure of a commutative group object. That is, we have morphisms

$$m\colon \bar{E} \times \bar{E} \longrightarrow \bar{E},$$

$$\iota\colon \bar{E} \longrightarrow \bar{E},$$

and $e\colon \mathsf{MSpec}\,\bar{k} = \mathbb{A}^0_{\bar{k}} \longrightarrow \bar{E}$, such that the diagrams

$$\begin{array}{ccc} \bar{E}\times\bar{E}\times\bar{E} & \xrightarrow{m\times\mathrm{id}} & \bar{E}\times\bar{E} \\ {\scriptstyle \mathrm{id}\times m}\downarrow & & \downarrow{\scriptstyle m} \\ \bar{E}\times\bar{E} & \xrightarrow{m} & \bar{E} \end{array} \qquad \begin{array}{ccc} \bar{E} & \xrightarrow{(\iota,\mathrm{id})} & \bar{E}\times\bar{E} \\ \downarrow & & \downarrow{\scriptstyle m} \\ \mathsf{MSpec}\,\bar{k} & \xrightarrow{e} & \bar{E} \end{array} \qquad \begin{array}{ccc} \bar{E} & \xrightarrow{(\mathrm{id},e)} & \bar{E}\times\bar{E} \\ & \searrow^{\mathrm{id}_{\bar{E}}} & \downarrow{\scriptstyle m} \\ & & \bar{E} \end{array}$$

commute.[20]

For $\bar{k} = \mathbb{C}$ the field of complex numbers, we have seen that the complex manifold $\bar{E}^{\mathsf{an}}$ associated to $\bar{E}$, is equivalent to $\mathbb{C}/\Gamma$, where $\Gamma = \mathbb{Z} \oplus \tau\,\mathbb{Z}$ with $\mathsf{Im}(\tau) > 0$. The group structure on the complex manifold $\bar{E}^{\mathsf{an}}$ is the one induced by addition of complex numbers.

The singular homology of an elliptic curve, can be identified with the exterior algebra of Γ.

Proposition 2.121. *Let $\bar{E}/\mathbb{C}$ be an elliptic curve. For $i = 0, 1, 2$ we have an isomorphism $H_i^{\mathrm{sing}}(\bar{E}^{\mathsf{an}}, \mathbb{Z}) \simeq \bigwedge^i \Gamma$. All other homology groups vanish.*

Proof. We prove this for $i = 1$ (the other cases being left as an exercises). We have that $\mathbb{C} \longrightarrow \mathbb{C}/\Gamma$ is a universal covering space of $\mathbb{C}/\Gamma$, since $\mathbb{C}$ is simply connected. The deck transformation group of this covering is equal to Γ. This yields an isomorphism $\pi_1(\mathbb{C}/\Gamma, 0) \simeq \Gamma$. The first homology group of a space, is isomorphic to the *abelianisation* of the fundamental group π_1. Since the group Γ is already abelian, we obtain an isomorphism $H_1^{\mathrm{sing}}(\bar{E}^{\mathsf{an}}, \mathbb{Z}) \simeq \Gamma$. □

We remark that as an abstract group, Γ is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$. The Universal Coefficient Theorem implies the following description of the cohomology groups:

$$H^1_{\mathrm{sing}}(\bar{E}^{\mathsf{an}}, \mathbb{Z}/\ell^n\,\mathbb{Z}) \simeq \mathsf{Hom}(\Gamma, \mathbb{Z}/\ell^n\,\mathbb{Z}) \simeq \mathbb{Z}/\ell^n\,\mathbb{Z} \oplus \mathbb{Z}/\ell^n\,\mathbb{Z}\,.$$

In the inverse limit $n \longrightarrow \infty$ we obtain

$$H^1_{\mathrm{sing}}(\bar{E}^{\mathsf{an}}, \mathbb{Z}_\ell) \simeq \mathsf{Hom}(\Gamma, \mathbb{Z}_\ell).$$

As an abstract group, this is isomorphic to $\mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$, however there's no canonical isomorphism. A canonical description can be given in terms of the Tate module. Recall that the notation $\bar{E}[n]$ denotes the group of n-torsion points of $\bar{E}$.

Definition 2.122. *Let $\bar{k}$ be an arbitrary algebraically closed field, and $\bar{E}$ an elliptic curve. We define the* Tate module *of $\bar{E}$ to be*

$$T_\ell \bar{E} = \varprojlim_{n>0} \bar{E}[\ell^n],$$

where the inverse limit is taken with respect to the chain of maps

$$\bar{E}[\ell^{n+1}] \longrightarrow \bar{E}[\ell^n],$$

given by raising an ℓ^{n+1}-torsion point to its ℓ-th power.

The Tate module is a purely algebraic way to define the singular homology of an elliptic curve with $\mathbb{Z}_\ell$-coefficients. We will see later, that this also works for étale cohomology over arbitrary algebraically closed fields.

Lemma 2.123. *Let $\bar{E}/\mathbb{C}$ be an elliptic curve over the complex numbers, such that $\bar{E}^{\mathsf{an}} \simeq \mathbb{C}/\Gamma$. Then we have natural isomorphisms*

$$H_1^{\mathrm{sing}}(\bar{E}^{\mathsf{an}}, \mathbb{Z}_\ell) \simeq T_\ell \bar{E},$$

$$H^1_{\mathrm{sing}}(\bar{E}^{\mathsf{an}}, \mathbb{Z}_\ell) \simeq \mathsf{Hom}(T_\ell \bar{E}, \mathbb{Z}_\ell).$$

[20] There's one diagram missing, corresponding to commutativity. This is left as an exercise to the reader.

Proof. For a positive integer $n > 0$ we have $\bar{E}[n] = (\mathbb{C}/\Gamma)[n] = \frac{1}{n}\Gamma/\Gamma$. The right hand side is naturally isomorphic to $\Gamma/n\Gamma$ (simply multiply with n). Applying this observation to $n = \ell^i$ we obtain $\bar{E}[\ell^i] \simeq \Gamma/\ell^i\Gamma$, and therefore

$$T_\ell \bar{E} \simeq \varprojlim \Gamma/\ell^i\Gamma \simeq \Gamma \otimes \mathbb{Z}_\ell \,.$$

Since $\Gamma \simeq H_1^{\mathrm{sing}}(\bar{E}^{\mathsf{an}}, \mathbb{Z})$ (canonically), we obtain, $T_\ell \bar{E} \simeq H_1^{\mathrm{sing}}(E, \mathbb{Z}) \otimes \mathbb{Z}_\ell \simeq H_1^{\mathrm{sing}}(\bar{E}^{\mathsf{an}}, \mathbb{Z}_\ell)$ from the Universal Coefficient Theorem for singular homology. Dualising (and applying the Universal Coefficient Theorem for cohomology) we obtain $H^1_{\mathrm{sing}}(\bar{E}^{\mathsf{an}}, \mathbb{Z}_\ell) \simeq \mathsf{Hom}(T_\ell \bar{E}, \mathbb{Z}_\ell)$. □

Corollary 2.124. *Every isomorphism of free abelian groups $\bigwedge^2 \Gamma \simeq \mathbb{Z}$ induces an isomorphism $H^1_{\mathrm{sing}}(\bar{E}, \mathbb{Z}_\ell) \simeq T_\ell \bar{E}$.*

Proof. We have a perfect pairing $\Gamma \times \Gamma \longrightarrow \bigwedge^2 \Gamma \simeq \mathbb{Z}$, and therefore we obtain an isomorphism $\Gamma \simeq \mathsf{Hom}(\Gamma, \mathbb{Z})$. This implies $\mathsf{Hom}(T_\ell \bar{E}, \mathbb{Z}_\ell) \simeq \mathsf{Hom}(\Gamma \otimes \mathbb{Z}_\ell, \mathbb{Z}_\ell) \simeq \Gamma \otimes \mathbb{Z}_\ell \simeq T_\ell \bar{E}$. □

We have already seen that $H^i_{\mathrm{sing}}(\bar{E}^{\mathsf{an}}, \mathbb{Z}_\ell) \simeq H^i_{\text{ét}}(\bar{E}, \mathbb{Z}_\ell)$. For $\bar{k} = \mathbb{C}$, the lemma above therefore gives us an explicit description of the étale cohomology groups of an elliptic curve in degree 1, in terms of the Tate module. The next result shows that this works for arbitrary algebraically closed fields.

Proposition 2.125. *Let $\bar{E}/\bar{k}$ be an elliptic curve over an algebraically closed field $\bar{k}$. Let ℓ be a prime number, different from the characteristic of $\bar{k}$. We denote by A the profinite group given by the inverse limit*

$$\varprojlim_{i>0} \mu_{\ell^i},$$

where the transition maps are given by $\mu_{\ell^{i+1}} \longrightarrow \mu_{\ell^i}$, raising a root of unity to its ℓ-th power. Then we have a natural isomorphism of $\mathbb{Z}_\ell$-modules

$$H^1_{\acute{e}t}(\bar{E}, A) \simeq T_\ell \bar{E}.$$

In particular, every isomorphism of profinite groups $A \simeq \mathbb{Z}_\ell$ induces an iso

$$H^1_{\acute{e}t}(\bar{E}, \mathbb{Z}_\ell) \simeq T_\ell \bar{E}.$$

Proof. One has $H^1_{\text{ét}}(\bar{E}, A) \simeq \varprojlim_{i>0} H^1_{\text{ét}}(\bar{E}, \mu_{\ell^i})$. We have seen that there is a natural isomorphism $H^1_{\text{ét}}(\bar{E}, \underline{\mathbb{G}}_m) \simeq \mathsf{Pic}(\bar{E})$. The Kummer sequence

$$0 \longrightarrow \underline{\mu_{\ell^i}} \longrightarrow \underline{\mathbb{G}}_m \xrightarrow{[\ell^i]} \underline{\mathbb{G}}_m \longrightarrow 0$$

yields the long exact sequence

$$H^0_{\text{ét}}(\bar{E}, \underline{G}_m) \xrightarrow{[\ell^i]} H^0_{\text{ét}}(\bar{E}, \underline{\mathbb{G}}_m) \longrightarrow H^1_{\text{ét}}(\bar{E}, \underline{\mu}_{\ell^i}) \longrightarrow \mathsf{Pic}(\bar{E}) \xrightarrow{[\ell^i]} \mathsf{Pic} \longrightarrow \cdots .$$

The first map on the left hand side can be identified with

$$\bar{k}^\times \xrightarrow{[\ell^i]} \bar{k}^\times,$$

since the set of invertible regular functions on $\bar{E}$ equals $\bar{k}^\times$. This map is surjective since $\bar{k}$ is algebraically closed. This shows that

$$H^1_{\text{ét}}(\bar{E}, \underline{\mu}_{\ell^i}) \simeq \ker([\ell^i]\colon \mathsf{Pic}(\bar{E}) \longrightarrow \mathsf{Pic}(\bar{E})).$$

The Picard group of an elliptic curve over an algebraically closed field can be identified with the abstract group $\bar{E} \times \mathbb{Z}$. This yields an isomorphism

$$H^1_{\text{ét}}(\bar{E}, \underline{\mu}_{\ell^i}) \simeq \ker([\ell^i]\colon \bar{E} \longrightarrow \bar{E}) \simeq E[\ell^i].$$

Taking the inverse limit we obtain what we wanted. □

Lemma 2.126. *One has an isomorphism of abstract $\mathbb{Z}_\ell$-modules $T_\ell E \simeq \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell$.*

Proof. Recall that we saw that the endomorphism ring of an elliptic curve $\mathsf{End}(\bar{E})$ is endowed with the following extra structures. There's a degree map

$$\deg\colon \mathsf{End}(E) \longrightarrow \mathbb{N},$$

and an involution $f \mapsto \widehat{f}$, satisfying the properties

(a) $\widehat{(f+g)} = \widehat{f} + \widehat{g}$,

(b) $\widehat{(fg)} = \widehat{g}\widehat{f}$,

(c) $f\widehat{f} = \widehat{f}f = [\deg(f)]$ (were $[n] \in \mathsf{End}(\bar{E})$ denotes the image of $n \in \mathbb{Z}$ under the natural ring homomorphism $\mathbb{Z} \longrightarrow \mathsf{End}(\bar{E})$).

(d) $\deg \mathrm{id}_{\bar{E}} = 1$.

Property (c) and (d) imply $\widehat{\mathrm{id}_{\bar{E}}} = \mathrm{id}_{\bar{E}} = [1]$. Using (a) we deduce that $\widehat{[n]} = (\widehat{[1] + \cdots + [1]}) = [1] + \cdots + [1] = [n]$. By virtue of (c) we have $[\deg[n]] = [n] \cdot [n] = [n^2]$, and therefore $\deg[n] = n^2$.

For an étale morphism of elliptic curves $\bar{E}' \xrightarrow{f} \bar{E}$ one has $\deg f = \#f^{-1}(0)$. If n is coprime to p the map $[n]$ is étale, and we therefore obtain $\#[n]^{-1}(0) = n^2$. Since $[n]$ is the multiplication by n map, the preimage $[n]^{-1}(0)$ agrees with the n-torsion $\bar{E}[n]$.

Claim 2.127. *Let A be a finite abelian group of order n^2, such that for every divisor $d|n$ one has $\#A[d] = d^2$. Then, there exists an abstract isomorphism $A \simeq (\mathbb{Z}/n\mathbb{Z})^2$ of abelian groups.*

The proof of this assertion is left as an exercise. Since these assumptions are met by $\bar{E}[n]$, we deduce that $\bar{E}[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$. In particular, for $\ell \neq p$ we have $\bar{E}[\ell^i] \simeq (\mathbb{Z}/\ell^i\mathbb{Z})^2$. In the limit $i \longrightarrow \infty$ we obtain $T_\ell \bar{E} \simeq (\mathbb{Z}_\ell)^2$. □

Corollary 2.128. *We have* $\dim H^1_{\acute{e}t}(\bar{E}, \mathbb{Q}_\ell) = 2$.

Proof. By virtue of the definition, $H^1_{\text{ét}}(\bar{E}, \mathbb{Q}_\ell) \simeq H^1_{\text{ét}}(\bar{E}, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. This implies the existence of an isomorphism $H^1_{\text{ét}}(\bar{E}, \mathbb{Q}_\ell) \simeq \mathbb{Q}_\ell \oplus \mathbb{Q}_\ell$. □

3 On Deligne's proof

In this section we're going to give an overview of Deligne's proof of the Weil conjectures. At first we take a look at L-functions, and then we turn to the proof of the key lemma of Deligne's argument.

3.1 Local systems

The topological counterpart of local systems are also known as *locally constant sheaves*. Recall that for an abelian group A, one can define a sheaf $\underline{A}_X$ on a topological space X. For an open subset $U \subset X$ one has that $\underline{A}_X(U)$ is the abelian group of continuous maps $U \longrightarrow A$, where A is endowed with the discrete topology.

Definition 3.1. *Let X be a topological space a manifold (or a "nice" topological space), a* local system *L on X is a locally constant sheaf of abelian groups, that is, there exists an open covering $\{U_i\}_{i\in I}$ of X, such that each $L|_{U_i}$ is equivalent to the constant sheaf $\underline{A}_{U_i}$.*

There is an interesting link between locally constant sheaves L and covering spaces. For an A-local system $\mathcal{F}$ on X, there exists a universal local homeomorphism $\pi : Y_{\mathcal{F}} \longrightarrow X$, such that $\mathcal{F}$ can be identified with the sheaf of sections of $Y_{\mathcal{F}}$. This construction is referred to as the *étale space* of the sheaf $\mathcal{F}$. This space is constructed as follows: choose an open covering $\{U_i\}_{i\in I}$ of X, such that each $\mathcal{F}|_{U_i}$ is equivalent to the constant sheaf $\underline{A}_{U_i}$. Define $Y_{\mathcal{F}}$ to be the quotient space

$$Y_{\mathcal{F}} = \left(\bigsqcup_{i\in I} U_i \times \mathcal{F}(U_i) \right) / \sim,$$

where we stipulate that $(x, s) \in U_i \times \mathcal{F}(U_i)$ is equivalent to $(y, t) \in U_j \times \mathcal{F}(U_j)$, if and only if $x = y \in U_i \cap U_j$ and $s|_{U_i\cap U_j} = t|_{U_i\cap U_j}$.

Since $\mathcal{F}$ is assumed to be a local system the étale space $Y_{\mathcal{F}}$ can be seen to be a covering. The condition of L being locally constant translates directly into $Y_L \longrightarrow X$ being locally trivial, since the étale space of the constant sheaf $\underline{A}$ is given by $X \times A$.

We can recover $\mathcal{F}$ from the covering $Y_{\mathcal{F}} \longrightarrow X$ as the *sheaf of (continuous) sections*. We assign to an open subset $U \subset X$ the set of continuous maps $s\colon U \longrightarrow Y_{\mathcal{F}}$, fitting into a commutative diagram

$$\begin{array}{ccc} & & Y_{\mathcal{F}} \\ & \overset{s}{\nearrow} & \downarrow \\ U & \longrightarrow & X. \end{array}$$

This discussion reveals in particular that local systems on a simply connected manifold is trivial (since all covering spaces are), which yields the following useful description of locally constant sheaves.

Proposition 3.2. *Let L be a local system on X and $x \in X$ a base point. If $L_x \simeq A$, A being a fixed abelian group, we call L a local system with fibre A, or an $Aut(A)$-local system. There is a natural equivalence of categories of $Aut(A)$-local systems and representations of the fundamental group*

$$\rho\colon \pi_1(X, x) \longrightarrow \mathsf{Aut}(A).$$

Sketch. We begin by associating a representation $\rho\colon \pi_1(X, x) \longrightarrow \mathsf{Aut}(A)$ to an A-local system. Choose a closed path $\gamma\colon [0, 1] \longrightarrow X$ based at x. By virtue of the definition of A-local systems, there exists an open neighbourhood U_t of $\gamma(t)$ for every $t \in [0, 1]$, such that $L|_{U_t}$ is isomorphic to the constant sheaf $\underline{A}_{U_t}$. □

The proposition above motivates us to replace the topological fundamental group by the étale fundamental group.

Definition 3.3. *Let G be a profinite group and X a smooth k-variety with geometric base point $x \in X(\mathbb{K})$ (where $\mathbb{K}$ is an algebraically closed field containing k). An étale G-local system is a continuous representation*

$$\pi_1^{\acute{e}t}(X,x) \longrightarrow G.$$

Dangerous Bend 3.4. *Unlike the case of local systems on topological spaces, it is not true that continuous representation of étale fundamental groups correspond to sheaves on the small-étale site $(X)_{\acute{e}t}$. This is only the case, if G is a finite group. However, G-local systems can be represented by a* pro-system *of étale sheaves (see the example below).*

Of particular importance to us will be ℓ-adic local systems, which correspond to continuous representations taking values in $GL_n(\mathbb{Z}_\ell)$. This profinite group can be obtained as the inverse limit

$$\varprojlim_{i>0} GL_n(\mathbb{Z}/\ell^i\,\mathbb{Z}).$$

In particular, we see that a continuous representation

$$\rho_i \colon \pi_1^{\text{ét}}(X,x) \longrightarrow GL_n(\mathbb{Z}_\ell)$$

corresponds to a compatible system of representations $\rho_i \colon \pi_1^{\text{ét}}(X,x) \longrightarrow GL_n(\mathbb{Z}/\ell^i\,\mathbb{Z})$.

The representations ρ_i actually correspond to an étale sheaf $\mathcal{F}_i$ on $(X)_{\text{ét}}$, which is étale-locally equivalent to $\underline{\mathbb{Z}/\ell^i\,\mathbb{Z}}$. That is, there exists a finite collection of étale maps $\{U_j \longrightarrow X\}_{j\in I}$, whose images cover all of X, such that $\mathcal{F}_i\,|_{U_j} \simeq \underline{\mathbb{Z}/\ell^i\,\mathbb{Z}}_{U_j}$.

Definition 3.5. *Let $\mathcal{F}$ be a $\mathbb{Z}_\ell$-étale local system on X. We denote by $(\mathcal{F}_i)$ the corresponding compatible family of $\mathbb{Z}/\ell^i$-étale local systems on X, and define*

$$H^i_{\acute{e}t}(X,\mathcal{F}) = \varprojlim_{i>0} H^i_{\acute{e}t}(X,\mathcal{F}_i).$$

3.2 The function sheaf dictionary

In the section part of these notes we consider varieties X over a *finite field* of characteristic p. We emphasis that ℓ and p are always assumed to be coprime.

We denote by $\bar{k}$ a fixed algebraic closure of k, and by $\bar{X}$ the base change of X to $\operatorname{Spec}\bar{k}$. Every element of $Gal(\bar{k}/k)$ induces a *scheme-theoretic automorphism* of X. This implies the existence of an interesting extra structure for the ℓ-adic cohomology, which is not present over the field of complex numbers: the action of the Galois group $\widehat{\mathbb{Z}} = Gal(\bar{k}/k)$ on $H^i_{\acute{e}t}(X,\mathbb{Q}_\ell)$. Since $\widehat{\mathbb{Z}}$ is topologically generated by the Frobenius automorphism $1 \in \widehat{\mathbb{Z}}$, it suffices to study the action of the Frobenius automorphism of an algebraic variety on ℓ-adic cohomology. It can be described in terms of the Frobenius endomorphism.

Definition 3.6. *A Weil ℓ-adic local system on $\bar{X}$ is an ℓ-adic local system L on $\bar{X}$ together with an isomorphism*

$$F_X^* L \simeq L.$$

One can show that an ℓ-adic local system L on X, induces a Weil ℓ-adic local system on $\bar{X}$. In particular, one gets a Frobenius operator

$$H^i(F) \colon H^i_{\text{ét}}(\bar{X},L) \longrightarrow H^i(\bar{X},L).$$

Character sheaves on commutative algebraic groups

We refer the reader to Gaitsgory's [Gai03]. Let A (resp. A_0) be a connected commutative algebraic group variety, defined over a finite field k, and let $A = \mathsf{A}(k)$ be the finite commutative group of k-points. The Frobenius morphism $F : \mathsf{A} \longrightarrow \mathsf{A}$ can be shown to be an isomorphism of group object in varieties. The group A can be identified with the fixed-points of F, or alternatively with the zero fibre of the map

$$L : \mathsf{A} \longrightarrow \mathsf{A},$$

which sends x to $x - Fx$. The map L is called the *Lang isogeny*, and can be shown to be a finite étale covering. In the special case of the additive group $\mathbb{G}_a$, the Lang isogeny is given by the Artin-Schreier map $\mathbb{A}^1 \longrightarrow \mathbb{A}^1$, sending x to $x - x^p$.

Lemma 3.7. *The Lang isogeny L is a regular étale covering, with group of deck transformations canonically equivalent to A.*

Proof. Every non-trivial element of A induces a non-trivial action on A by translation. In particular we have a canonical action of A on A, which by definition of L preserves the Lang isogeny. In particular we see that there is an injection

$$A \hookrightarrow Aut(L),$$

but since each fibre of L can be non-canonically identified with the kernel A of L, we conclude that A acts transitively on the fibres. This implies that L is a regular étale covering, and moreover that $A \simeq Aut(L)$. □

This simple result, combined with Lemma 2.58, yields a construction of associating an Weil ℓ-adic local system on A (preserved by F_{A}) to a representation

$$\rho : A \longrightarrow GL_n(\bar{\mathbb{Q}}_\ell).$$

Lemma 3.8. *To every representation $\rho : A(\mathbb{F}_q) \longrightarrow GL_n(\bar{\mathbb{Z}}_\ell)$ we can naturally associate a Weil ℓ-adic local system L_ρ on A, satisfying $L_{\rho_1 \oplus \rho_2} \simeq L_{\rho_1} \oplus L_{\rho_2}$ and $L_{\rho_1 \otimes \rho_2} \simeq L_{\rho_1} \otimes L_{\rho_2}$.*

Proof. Lemma 3.7 shows that the Lang isogeny $L : \mathsf{A} \longrightarrow \mathsf{A}$ is a finite étale covering with group of deck transformations given by the finite commutative group A. In particular we have a surjection $\pi_1^{\text{ét}}(\mathsf{A}, 0) \twoheadrightarrow A$ by Lemma 2.58. By composing with the representation $\rho : A \longrightarrow GL_n(\bar{\mathbb{Q}}_\ell)$ we obtain a continuous representation of the fundamental group, giving rise to an ℓ-adic local system L_χ. □

Since every representation of the commutative group A decomposes into a sum of 1-dimensional representation (i.e. characters), this case is of particular importance. Applying this construction to the Artin-Schreier morphism, gives rise to interesting local systems on the affine line, usually referred to as *Artin-Schreier sheaves*.[21] Similarly, *Kummer sheaves* on the multiplicative group $\mathbb{G}_m$ and *Hecke eigensheaves* on Jacobians of curves, can be constructed.

In the next subsection we will see how to reconstruct the representation ρ from the ℓ-adic sheaf L_ρ. Since representations of finite groups are governed by their character theory, it suffices to reconstruct the character of ρ, which will simply be given by a function

$$A = \mathsf{A}_0(k) \longrightarrow \bar{\mathbb{Q}}_\ell.$$

[21] This statement is to be contrasted with the analogous situation over the complex numbers, where the affine line, due to its simply-connectedness, does not carry any interesting local systems. As we can see, $\mathbb{A}^1$ is not simply-connected in positive characteristic!

Extracting a function from a sheaf

For a finite field k the absolute Galois group $\mathrm{Gal}(k)$ is abstractly isomorphic to the profinite group $\widehat{\mathbb{Z}}$. The *arithmetic Frobenius* $\varphi \in \mathrm{Gal}(k)$ is given by the field automorphism $\lambda \mapsto \lambda^q$, where $q = \#k$. Its inverse is denoted by Fr and referred to as the *geometric Frobenius*.

Conversely to the process described in the proceeding subsection, we would like to associate a function on $X(k)$ to a local system L on X. In order to do that we let $x : \operatorname{Spec} k \longrightarrow X$ be a k-point of X. This yields a map of étale fundamental groups $\pi_1^{\text{ét}}(\operatorname{Spec} k, \operatorname{Spec} \bar{k}) \longrightarrow \pi_1^{\text{ét}}(X, \operatorname{Spec} \bar{k})$.

Pulling back L to x, we simply obtain a representation of $\rho_x \colon \pi_1^{\text{ét}}(\operatorname{Spec} k) = Gal(\bar{k}/k) = \widehat{\mathbb{Z}}$, which is determined by the action of the Frobenius morphism. The corresponding element $\rho_x(\mathsf{Fr}_x)$ is well-defined up to conjugation.

In analogy with the above character-theoretic construction, we therefore associate the trace of the Frobenius $\rho_x(\mathsf{Fr}_x)$. The corresponding function will be denoted by

$$f_L : X(k) \longrightarrow \bar{\mathbb{Q}}_\ell.$$

The lemma below follows directly from the definition of the Lang isogeny, and establishes a compatibility with the character sheaf construction of Lemma 3.8. The proof of the following lemma is left as an exercise:

Exercise 3.9. *Let $\mathcal{A}$ be a connected commutative group k-variety, and $\chi \colon \mathcal{A}(k) \longrightarrow \mathbb{Z}_\ell^\times$ a character. Then we have $f_{L_\chi} = \chi$.*

This is not the only convenient property of the function-sheaf correspondence.

Lemma 3.10. *The following properties hold for ℓ-adic local systems L_1, L_2 on X, and a map $\pi : Y \longrightarrow X$:*

(a) $f_{L_1 \oplus L_2} = f_{L_1} + f_{L_2}$, *and more generally for short exact sequences*

(b) $f_{L_1 \otimes L_2} = f_{L_1} \cdot f_{L_2}$,

(c) $f_{\pi^* L} = f_L \circ \pi$, *where $\pi^* L$ denotes the local system corresponding to the composition*

$$\pi_1^{\acute{e}t}(Y, \bar{y}) \longrightarrow \pi_1^{\acute{e}t}(X, \pi(\bar{x})) \longrightarrow \mathsf{GL}_n(\mathbb{Z}_\ell).$$

A morphism of varieties $\pi \colon Y \longrightarrow X$ is called *projective*, if there exists a factorisation

$$\begin{array}{ccc} Y & \xrightarrow{\quad i \quad} & \mathbb{P}^N \times X \\ & \searrow \quad \swarrow & \\ & X, & \end{array}$$

where i is a *closed immersion*, that is, the inclusion of a (closed) subvariety. In this case, for every $x \in X(k)$, one has that the fibre $Y_x = Y \times_X, x\, \mathsf{MSpec}\, k$ is a projective k-variety.

Theorem 3.11 (Grothendieck-Lefschetz)**.** *For a projective morphism $\pi : Y \longrightarrow X$ and L an ℓ-adic local system on L, we have an equality of functions*

$$\sum_{y \in Y(k),\ f(y) = x} f_L(y) = \sum_{i \geq 0} (-1)^i \,\mathsf{Tr}(\mathsf{Fr}, H^i(\bar{Y}_x, L)).$$

This result is a powerful analogue of Lefschetz's fixed point formula 2.14. We remark that the right hand side is a finite sum, by virtue of the following important result (see [Mil80, Theorem VI.1.1]):

Theorem 3.12 (Vanishing Theorem)**.** *Let $\bar{X}$ be a $\bar{k}$-variety and $\mathcal{F}$ a constructible sheaf of $\mathbb{Z}_\ell$-modules. Then, $H^i(\bar{X}, \mathcal{F}) = 0$ for $i > 2 \dim \bar{X}$.*

3.3 L-functions

To a local system $\mathcal{F}$ on a k-variety X one can associate the so-called L-function. For the trivial rank 1 local system, the L-function is an old acquaintance of ours: the zeta function. The definition makes use of a characteristic polynomial of a Frobenius operator which is associated to a point $x \in |X|$.

Definition 3.13. *Let F be a rank n local systems on a k-variety X. We denote by $\rho_{\mathcal{F},x} \colon \pi_1^{\acute{e}t}(\mathsf{MSpec}\, k) = \mathbb{Z} \longrightarrow \mathsf{GL}_n(\mathbb{Z}_\ell)$ continuous homomorphism defined by composition*

$$\begin{array}{ccc} \pi_1^{\acute{e}t}(\mathsf{MSpec}\, k, \mathsf{MSpec}\, \bar{k}) & \longrightarrow & \pi_1^{\acute{e}t}(X, \bar{x}) \\ & \searrow & \downarrow \\ & & \mathsf{GL}_n(\mathbb{Z}_\ell), \end{array}$$

where $\bar{x} \in X(\bar{k})$ denotes the $\bar{k}$-point induced by x.

This definition can be extended to a bigger class of "sheaves" (or rather prosystems of sheaves of $\mathbb{Z}_\ell$-modules): so-called *constructible ℓ-adic sheaves*. For a constructible sheaf $\mathcal{F}$ on X one can find an open subset $U \subset X$, such that $\mathcal{F}|_U$ is a local systems, and such that the restriction of $\mathcal{F}$ to $X \setminus U$ is a constructible sheaf. In fact, there exists a finite disjoint union

$$X = \bigsqcup_{i \in I} Z_i,$$

such that $\mathcal{F}|_{Z_i}$ is a local system.

Definition 3.14. *Let $\mathcal{F}$ be a constructible sheaf of $\mathbb{Z}_\ell$-modules on X. We denote by*

$$L(X, \mathcal{F}, T) = \prod_{x \in |X|} \frac{1}{\det(1 - T^{\deg(x)} \rho_{\mathcal{F},x}(F))}$$

the element of $1 + T\,\mathbb{Z}_\ell[[T]] \subset \mathbb{Q}_\ell[[T]]$ given by formally evaluating the infinite product above.

The Grothendieck-Lefschetz Theorem 3.11 implies the following assertion.

Exercise 3.15. *The L-function of a constructible sheaf is the Taylor expansion of a rational function. To be precise, it equals.*

$$L(X, \mathcal{F}, T) = \prod_{i \geq 0} \left(\det(1 - H^i(\mathsf{Fr}) | H^i_{\acute{e}t}(X, \mathcal{F})) \right).$$

3.4 Poincaré duality

Theorem 3.16 (Poincaré duality, no weights)**.** *Let $\bar{X}$ be a smooth projective $\bar{k}$-variety of dimension n where $\bar{k}$ is an algebraically closed field, and $\mathcal{F}$ a constructible sheaf of $\mathbb{Z}_\ell$-modules on $\bar{X}$. Then, we have an abstract isomorphism*

$$H^{2n}(\bar{X}, \mathbb{Q}_\ell) \simeq \mathbb{Q}_\ell,$$

and the induced pairing

$$H^i(\bar{X}) \times H^{2n-i}(\bar{X}) \longrightarrow \mathbb{Q}_\ell$$

is perfect.

Theorem 3.17.

3.5 The key estimate

We follow section 3 in [Del74]. Let k be a finite field, and consider a non-empty affine open subset $U \subset \mathbb{P}^1_k$. We denote by $\bar{U} \subset \mathbb{P}^1_{\bar{k}}$ the base change to the algebraic closure. Let $u \in |U|$ be a point of the k-variety U with residue field k_u. We write $q_u = q^{\deg(u)} = \#k_u$. For a local system $\mathcal{F}$ on U we denote by $F_u = \rho_{\mathcal{F},u}(F)$ the corresponding local Frobenius operator.

Definition 3.18. *Let $\beta \in \mathbb{Z}$ be an integer. We say that a local system $\mathcal{F}$ on U is* pure of weight *β, if for all $u \in U$ we have that the eigenvalues of F_u are algebraic numbers α, such that for every field homomorphism $\sigma\colon \bar{Q} \hookrightarrow \mathbb{C}$ we have $|\sigma(\alpha)| = q_u^{\frac{\beta}{2}}$.*

The trivial local system $\underline{\mathbb{Q}_\ell}$ is of weight 0, because all local Frobenius operators F_u are the identity map. We have already seen a non-trivial class of examples: the Tate twist $\underline{\mathbb{Q}_\ell}(r)$ is pure of weight $-2r$.

An algebraic number α with the property that for every embedding $\sigma\colon \mathbb{Q} \hookrightarrow \mathbb{C}$, the images $\sigma(\alpha)$ have the same absolute value, is called a *Weil number*. This is a special property which isn't shared by all algebraic numbers. It is clear that a root of unity $\zeta^n = 1$ is a Weil number, since $\sigma(\zeta)$ remains a root of unity in $\mathbb{C}$, and therefore has absolute value 1. However, $\alpha = 1 + \sqrt{2}$ is not a Weil number, as there exists an embedding σ exchanging $\pm\sqrt{2}$, and $|\sigma(\alpha)| = |1 - \sqrt{2}| < |1 + \sqrt{2}|$.

Theorem 3.19 (Deligne)**.** *Suppose that the following assumptions are met:*

(a) There exists a non-degenerate alternating *pairing $\psi\colon \mathcal{F} \otimes \mathcal{F} \longrightarrow \underline{\mathbb{Q}_\ell}(-\beta)$, where β is an integer. This implies that $\rho_{\mathcal{F}}\colon \pi_1^{\acute{e}t}(U, \bar{x}) \longrightarrow \mathsf{GL}_n(\mathbb{Q}_\ell)$ factors through the* symplectic group $\mathrm{Sp}(2n, \mathbb{Q}_\ell)$.

(b) The image of $\rho_{\mathcal{F}}$ is an open subgroup *of the topological group* $\mathrm{Sp}(2n, \mathbb{Q}_\ell)$.

(c) For every $u \in U$ the local L-factor

$$\frac{1}{\det(1 - T \cdot F_u)}$$

has rational coefficients.

Then, $\mathcal{F}$ is pure of weight *β.*

The proof of this result will be given at the end of this subsection. We start with a couple of lemmas.

Lemma 3.20. *Let m be a positive integer, we denote by $F_{u,2m}$ the value of the $2m$-fold tensor power of $\rho_{\mathcal{F}}\colon \pi_1^{\acute{e}t}(U,\bar{x}) \longrightarrow \mathsf{GL}_n(\mathbb{Q}_\ell)$ at the local Frobenius F_u.*

(a) The logarithmic derivative $d\log\left(\det(1-T\cdot F_{u,2m})^{-1}\right)$ is a power series in T with non-negative rational coefficients.

(b) The local L-factor $\det(1-T\cdot F_{u,2m})^{-1}$ is a power series in T with non-negative rational coefficients.

Proof. Assertion (a) implies (b): since $\log\left(\det(1-T\cdot F_{u,2m})^{-1}\right)$ doesn't have a constant term, non-negativity of the coefficients of $\log\left(\det(1-T\cdot F_{u,2m})^{-1}\right)$ implies non-negativity of the coefficients of

$$\left(\det(1-T\cdot F_{u,2m})^{-1}\right) = \exp\log\left(\det(1-T\cdot F_{u,2m})^{-1}\right).$$

It therefore remains to prove (a). Recall from Lemma 2.20 that we have

$$\sum_{i=1}^{\infty}\frac{\mathsf{Tr}(F_{u,2m}^r)}{r} = \det(1-T\cdot F_{u,2m})^{-1}.$$

We have $\mathsf{Tr}(F_{u,2m}^r) = \mathsf{Tr}(F_u^r)^{2m}$, in particular the coefficients of the right hand side power series are non-negative integers. This concludes the proof. □

Lemma 3.21. *(a) Let I be a countable set, and let $(f_i)_{i\in I} \in 1+T\,\mathbb{R}_{\geq 0}[[T]] \subset \mathbb{R}[[T]]^\times$, such that*

$$f = \prod_{i\in I} f_i$$

is a well-defined element of $1+T\,\mathbb{R}[[T]]$. Then, the radius of convergence of f is less than the radius of convergence of f_i for all $i\in I$.

(b) Assume that $(f_i)_{i\in I}$ and f are Taylor series expansions of meromorphic functions. Then,

$$\inf(|x| : f(x)=\infty) \leq \inf(|x| : f_i(x)=\infty).$$

Proof. The second assertion follows from the first. We write $f=\sum_{j=0}^{\infty} b_j T^j$ and $f_i = \sum_{j=0}^{\infty} a_{ij}T^j$. By assumption we have

$$b_0 = a_{i0} = 1.$$

Furthermore, the coefficients b_j and a_{ij} are non-negative. The relation $f=\prod_{i\in I} f_i$ implies the inequality $b_j \leq a_{ij}$ for all $i\in I$. This implies the inequality

$$\limsup_{j\longrightarrow\infty}\left(\frac{1}{b_j}\right)^{\frac{1}{j}} \leq \limsup_{j\longrightarrow\infty}\left(\frac{1}{a_{ij}}\right)^{\frac{1}{j}},$$

which amounts to what we wanted to show. □

Lemma 3.22. *For every m there exists a non-negative integer N, such that we have an isomorphism*

$$H_c^2(\bar{U},\mathcal{F}^{\otimes 2m}) \simeq \mathbb{Q}_\ell(-m\beta-1)^N.$$

Proof. By Poincaré duality we have

$$H_c^2(\bar{U}, \mathcal{F}^{\otimes 2m})(1) \simeq H_c^0(\bar{U}, \mathcal{F}^{\vee,\otimes 2m})^\vee.$$

The right hand side agrees with the coinvariants of $\pi_1^{\text{ét}}(\bar{U}, u)$-representation corresponding to $\mathcal{F}^{\otimes 2m}$.

Let V be the standard representation of the symplectic group $\mathrm{Sp} = \mathrm{Sp}(2n, \mathbb{Q}_\ell)$. By virtue of assumption (b) of Theorem 3.19, the right hand side above agrees with the Sp-coinvariants of $V^{\otimes 2m}$. The latter were computed by H. Weyl (see [Wey39, Chapter 6.1]). It follows from Weyl's theory that there exists a set S of partitions of $\{1, \ldots, 2m\}$ into two-element sets

$$\{i_1, j_1\} \sqcup \cdots \sqcup \{i_m, j_m\},$$

such that the maps

$$\mathcal{F}^{\otimes 2m} \longrightarrow \mathbb{Q}_\ell(-m\beta),$$

given by

$$x_1 \otimes \cdots \otimes x_{2m} \mapsto \prod_{\alpha=1}^{m} \psi(x_{i_\alpha}, y_{j_\alpha})$$

give rise to an isomorphism

$$(V^{\otimes 2m})_{\mathrm{Sp}} \xrightarrow{\simeq} (\mathbb{Q}_\ell(-m\beta))^S.$$

We denote the cardinality of S by N, and conclude $H_c^2(\bar{U}, \mathcal{F}^{\otimes 2m})(1) \simeq \mathbb{Q}_\ell(-m\beta)^N$. □

Proof of Theorem 3.19. It follows from the Grothendieck-Lefschetz formula that we have an identity

$$L(X, \mathcal{F}^{\otimes 2m}, T) = \prod_{i=0}^{2} \left(\det(1 - T \cdot F^* | H_c^i(X, \mathcal{F}^{\otimes 2m}))\right)^{(-1)^{i+1}}. \tag{10}$$

The compactly supported cohomology group $H_c^0(X, \mathcal{F}^{\otimes 2m})(1) \simeq H^2(X, \mathcal{F}^{\vee,\otimes 2m})^\vee$ vanishes, since U is assumed to be affine see Theorem 3.17. This implies that the denominator of $L(X, \mathcal{F}^{\otimes 2m}, T)$ equals $\det(1 - T \cdot F^* | H_c^2(X, \mathcal{F}^{\otimes 2m}))$. By virtue of Lemma 3.22 this determinant is equal to $(1 - q^{m\beta+1}T)^N$.

Recall that the Taylor series expansion of $L(X, \mathcal{F}^{\otimes 2m}, T)$ equals an infinite product of the *local L-factors*:

$$L(X, \mathcal{F}^{\otimes 2m}, T) = \prod_{u \in |U|} \frac{1}{\det(1 - T^{\deg(u)} \cdot F_{u,2m})}.$$

Let α be an eigenvalue of F_u, then the corresponding local factor has a pole at $\alpha^{\frac{-2m}{\deg(u)}}$. It follows from the inequality of Lemma 3.21(b) that

$$q^{-m\beta-1} \leq |\alpha|^{\frac{2m}{\deg(u)}}.$$

This is equivalent to the inequality

$$|\alpha| \leq q_u^{\frac{\beta}{2} + \frac{1}{2m}},$$

where we use $q_u = q^{\deg(u)}$. In the limit $m \longrightarrow \infty$ we obtain $|\alpha| \leq q_u^{\frac{\beta}{2}}$.

By assumption (a) of Theorem 3.19, that is, the existence of a non-degenerate alternating pairing

$$\psi\colon \mathcal{F}\otimes\mathcal{F}\longrightarrow\mathbb{Q}_\ell(-\beta),$$

we have that also $\alpha^{-1}q_u^\beta$ is an eigenvalue of F_u. This yields the inequality

$$|\alpha^{-1}q^\beta|\leq q_u^{\frac{\beta}{2}}\Leftrightarrow|\alpha^{-1}|\leq q_u^{-\frac{\beta}{2}}\Leftrightarrow q_u^{\frac{\beta}{2}}\leq|\alpha|.$$

We conclude $|\alpha|=q_u^{\frac{\beta}{2}}$. □

Corollary 3.23. *Let γ be a Frobenius eigenvalue of $H_c^1(\bar{U},\mathcal{F})$ for a local system $\mathcal{F}$ as in Theorem 3.19. Then, for every embedding $\sigma\colon\bar{\mathbb{Q}}\hookrightarrow\mathbb{C}$ we have $|\sigma(\gamma)|\leq q^{\frac{\beta}{2}+1}$.*

Proof. By equation (10) we have that $\sigma(\alpha^{-1})$ is a zero of $L(U,\mathcal{F},T)$. It suffices therefore to show that $L(U,\mathcal{F},T)$ doesn't have a zero for $|T|<q^{-\frac{\beta}{2}-1}$. This is a consequence of convergence of the infinite product

$$L(U,\mathcal{F},T)=\prod_{u\in|U|}\frac{1}{\det(1-T^{\deg(u)}\cdot F_u)}.$$

Let $\alpha_{1,u},\ldots,\alpha_{m,u}$ be a full list of eigenvalues of F_u possibly containing repeating entries, as dictated by algebraic multiplicities of eigenvalues. We can then write

$$\frac{1}{\det(1-T\cdot F_u)}=\prod_{i=1}^{m}\frac{1}{1-T\cdot\alpha_{i,u}}.$$

According to Theorem 3.19 we have $|\alpha_{i,u}|\leq q^{\frac{\beta}{2}}$. For a fixed i the infinite product

$$\prod_{u\in|U|}\frac{1}{1-T^{\deg(u)}\cdot\alpha_{i,u}}$$

converges, if the series $\sum_{u\in|U|}|\alpha_{i,u}T^{\deg(u)}|$ converges absolutely. This series can be estimated as follows:

$$\sum_{u\in|U|}|\alpha_{i,u}T^{\deg(u)}|=\sum_{d\geq1}\#\{u\in|U|:\deg(u)=d\}\cdot|\alpha_{i,u}T^d|<\sum_{d\geq1}q^{d+d\frac{\beta}{2}}|T|^d=\sum_{d\geq1}|q^{1+\frac{\beta}{2}}T|^d.$$

Here we used the fact that $|U|$ has at most q^d point of degree d. The right hand side converges absolutely, if and only if $|T|<q^{-\frac{\beta}{2}-1}$. □

4 p-adic integration

4.1 The p-adic analogue of the Lebesgue measure

On $\mathbb{R}$ there is a unique Borel measure μ which has the following properties:

- $\mu(S)=\mu(S+x)$ for every $x\in\mathbb{R}$ and a Borel measurable subset S,
- $\mu([0,1])=1$.

This measure is also known as the *Lebesgue measure* (however, we point out that there are more Lebesgue measurable subsets than Borel measurable subsets). This is a special case of a *Haar measure* (see [Haa33]).

Theorem 4.1 (Haar)**.** *Let G be a locally compact topological group. There exists a Borel measure μ, such that*

(a) $\mu(gS) = \mu(S)$ for $g \in G$ and $S \subset G$ a Borel measurable subset,

(b) $\mu(K) < \infty$ for $K \subset G$ a compact subset.

Furthermore, if μ_1 and μ_2 are two such measures (which we assume to be non-trivial), then there exists a positive real number λ, such that $\mu_1 = \lambda\mu_2$.

Haar's theorem is a far-reaching generalisation of Lebesgue integration. It also applies to non-commutative topological groups, as long as they are locally compact. In this case, it is important to note that left translation invariance

$$\mu(gS) = \mu(S)$$

does not imply right translation invariance

$$\mu(Sg) = \mu(S).$$

The field $\mathbb{Q}_p$ of p-adic numbers gives rise to a topological group $(\mathbb{Q}_p, +)$. It is locally compact, since $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^m\mathbb{Z}$ is an inverse limit of finite groups, and therefore compact. Since the subset $\mathbb{Z}_p \subset \mathbb{Q}_p$ is also open, one sees that every $x \in \mathbb{Q}_p$ as a compact neighbourhood $x + \mathbb{Z}_p$. We infer the following corollary of Haar's result:

Corollary 4.2. *There exists a unique Haar measure $\mu_{\mathbb{Q}_p}$ on $\mathbb{Q}_p$, such that*

$$\mu_{\mathbb{Q}_p}(\mathbb{Z}_p) = 1.$$

The translation invariance of $\mu_{\mathbb{Q}_p}$ makes it easy to compute the volume of certain subsets of $\mathbb{Q}_p$ which are just as important to the p-adic theory, as intervals are to the real theory.

Definition 4.3. *We denote by $\mathfrak{p}$ subgroup $p\mathbb{Z}_p \subset \mathbb{Z}_p$.*

First of all, we remark that as an abstract topological group we have an isomorphism $\mathbb{Z}_p \simeq p\mathbb{Z}_p$, given by multiplication with p. This shows that $p\mathbb{Z}_p$ is compact. Furthermore, since multiplication by p induces a homeomorphism $\mathbb{Q}_p \longrightarrow \mathbb{Q}_p$ sending the open subset $\mathbb{Z}_p$ to $p\mathbb{Z}_p$, we see that $p\mathbb{Z}_p \subset \mathbb{Z}_p$ is open. The quotient $\mathbb{Z}_p/\mathfrak{p}$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ by means of the canonical projection

$$\mathbb{Z}_p = \varprojlim_m \mathbb{Z}/p^m\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Lemma 4.4. $\mu_{\mathbb{Q}_p}(\mathfrak{p}) = \frac{1}{p}$.

Proof. We have a disjoint decomposition

$$\mathbb{Z}_p = \bigsqcup_{\bar{x} \in \mathbb{Z}/p\mathbb{Z}} x + \mathfrak{p}.$$

This yields

$$1 = \mu(\mathbb{Z}_p) = \sum_{\bar{x} \in \mathbb{Z}/p\mathbb{Z}} \mu(x + \mathfrak{p}) = \sum_{\bar{x} \in \mathbb{Z}/p\mathbb{Z}} \mu(\mathfrak{p}) = p \cdot \mu(\mathfrak{p}),$$

where we used the translation invariance of μ. This shows $\mu(\mathfrak{p}) = \frac{1}{p}$. □

A similar computation yields:

Lemma 4.5. $\mu(\mathfrak{p}^n) = \frac{1}{p^n}$.

We can use these formulae to compute the volume of $\{0\} \subset \mathbb{Q}_p$.

Corollary 4.6. $\mu(\{0\}) = 0$.

Proof. For every $m \geq 1$ we have an inequality

$$\mu(\{0\}) \leq \mu(\mathfrak{p}^m) = \frac{1}{p^m},$$

since $0 \in \mathfrak{p}^m$. This implies the claim. □

We now turn to discussing two generalisations of this measure. First of all, it is clear that we way replace $\mathbb{Q}_p$ by a finite-dimensional $\mathbb{Q}_p$-vector space V. In addition we choose a free $\mathbb{Z}_p$-submodule $\mathcal{V} \subset V$, such that $V = \mathcal{V} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Then, there exists a unique Haar measure μ on V, such that $\mu(\mathcal{V}) = 1$. The following results are proven with the same techniques as above.

Lemma 4.7. *(a) We have* $\mu(\mathfrak{p}^m\mathcal{V}) = \frac{1}{p^m}$.

(b) Let $W \subset V$ *be a* $\mathbb{Q}_p$*-linear subspace of strictly smaller dimension, then* $\mu(W) = 0$.

We can be more general than this: rather than working with $\mathbb{Q}_p$ we can choose a field F endowed with a topology, such that addition and multiplication are continuous, and the underlying topological space F is locally compact. Furthermore, we assume that there exists a compact open subring $\mathcal{O}_F \subset F$, which has a unique maximal ideal $\mathfrak{p}$. Topological fields with these properties are known as *non-archimedean local fields*.

Definition 4.8. *We denote the field* $\mathcal{O}_F/\mathfrak{p}$ *by* k_F *and refer to it as the residue field of* F. *We denote its cardinality by* $q = q_F = |k_F|$.

As before, we observe the existence of a unique Haar measure μ_F on F, such that $\mu_F(\mathcal{O}_F) = 1$.

Lemma 4.9. *One has* $\mu_F(\mathfrak{p}^m) = \frac{1}{q^m}$ *and* $\mu_F(\{0\}) = 0$.

Similarly, for a finite-dimensional F-vector space V with a free $\mathcal{O}_F$-submodule $\mathcal{V}$, such that $V = \mathcal{V} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ there exists a unique Haar measure μ on V, such that $\mu(\mathcal{V}) = 1$.

The choice of $\mathcal{V} \subset V$ is slightly cumbersome, and difficult to keep track off. It turns out that there's a better approach to Haar measures on finite-dimensional vector spaces, in terms of top degree forms.

5 Motivic integration

References

[AM94] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, 1994.

[Del74] P. Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307.

[FGI+05] Barbara Fantechi, Lothar Göttsche, Luc Illusie, Steven L. Kleiman, Nitin Nitsure, and Angelo Vistoli, *Fundamental algebraic geometry*, Mathematical Surveys and Monographs, vol. 123, American Mathematical Society, Providence, RI, 2005, Grothendieck's FGA explained. MR 2222646 (2007f:14001)

[Gai03] D. Gaitsgory, *Informal introduction to geometric Langlands*, An introduction to the Langlands program (Jerusalem, 2001), Birkhäuser Boston, Boston, MA, 2003, pp. 269–281. MR 1990383

[GH94] P. Griffiths and J. Harris, *Principles of Algebraic Geometry*, Wiley Classics Libary, 1994.

[Haa33] Alfred Haar, *Der massbegriff in der theorie der kontinuierlichen gruppen*, Ann. of Math. **34** (1933), no. 1, 147–169.

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52. MR 0463157 (57 #3116)

[Hat] A. Hatcher, *Algebraic topology*, http://pi.math.cornell.edu/ hatcher/AT/AT.pdf.

[Kun] Arnab Kundu, *The étale fundamental group of an elliptic curve*, http://math.uchicago.edu/ may/REU2017/REUPapers/Kundu.pdf.

[Mil80] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. MR 559531 (81j:14002)

[Row06] L. H. Rowen, *Graduate algebra: commutative view*, Graduate Studies in Mathematics, vol. 73, AMS, 2006.

[Sch] P. Scholze, *p-adic geometry*, https://arxiv.org/abs/1712.03708.

[SGA71] *Revêtements étales et groupe fondamental*, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 151, Springer-Verlag, Berlin-New York, 1971. MR 0274458

[Sil86] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, no. 106, Springer, 1986.

[Spr26] T. A. Springer, *Linear Algebraic Groups*, Progress in Mathematics, vol. 9, Birkhäuser, 1926.

[Wey39] H. Weyl, *The classical groups*, Princeton University Press, 1939.