Zeta functions in algebraic geometry

Mircea Mustaţă

Contents

Foreword

These are lecture notes from a graduate course I taught in Spring 2011. They cover some elementary topics related to Hasse-Weil zeta functions. I hope to add in the near future a second part, largely independent of the first one, covering p-adic and motivic zeta functions.

CHAPTER 1

Introduction: An overview of zeta functions

Zeta functions encode the counting of certain objects of geometric, algebraic, or arithmetic behavior. What distinguishes them from other generating series are special analytic or algebraic properties.

Zeta functions come up in a lot of area of mathematics. The ones we will deal with come in two flavors: local and global. Here *local* means relative to a prime p in $\mathbf{Z}$, or in some ring of integers in a number field. In this case, one expects the zeta function to be a rational function, in a suitable variable. By a global zeta function we mean an object that takes into account all primes. In this case one expects to have a product formula in terms of local factors. The basic example is the well-known factorization of the Riemann zeta function:

$$\zeta(s) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

A good understanding of the local factors of the zeta function can be used to show that the global zeta function is defined in some region $\{s \in \mathbf{C} \mid \mathrm{Re}(s) > \eta\}$, and then there are fundamental questions regarding analytic continuation and the existence of a functional equation. Again, the model is provided by the Riemann zeta function. However, very little is known in a more general setting. The general philosophy is that the analytic properties of the zeta function encode a lot of information about the geometric/arithmetic/algebraic of the object that is studied.

In what follows we give an overview of the types of zeta functions that we will discuss in the following chapters. In all this discussion, we restrict to the simplest possible setting.

1.1. The Hasse-Weil zeta function

This is one of the most famous zeta functions, and it played an important role in the development of algebraic geometry in the twentieth century. It is attached to a variety over a finite field, say $k = \mathbf{F}_q$. Suppose, for simplicity, that $X \subset \mathbf{A}^n_k$ is a closed subvariety defined by the equations $f_1, \dots, f_d$.

For every $m \leq 1$, let

$$N_m := |\{u \in X(\mathbf{F}_{q^m})| = |\{u \in \mathbf{F}^n_{q^m} \mid f_i(u) = 0 \,\text{for all}\, i\}|.$$

The Hasse-Weil zeta function of X is

$$Z(X,t) := \exp\left(\sum_{m \geq 1} \frac{N_m}{m} t^m\right) \in \mathbf{Q}[\![t]\!].$$

A fundamental result is that $Z(X,t)$ is a rational function. This was conjectured by Weil in [We2], who also proved it for curves and abelian varieties in [We1].

The general case was proved by Dwork in [Dwo]. Another proof in the case of smooth projective varieties was later given by Grothendieck and its school using étale cohomology, see [Gro]. Both the methods of Grothendieck and of Dwork have been extremely influential for the development of arithmetic geometry.

When X is a smooth projective variety, $Z_X(t)$ satisfies

- The functional equation.
- A connection with the Betti numbers defined over $\mathbf{C}$.
- An analogue of the Riemann hypothesis.

These three properties, together with the rationality mentioned above, form the Weil conjectures [We2], now a theorem of Grothendieck [Gro] and Deligne [Del3]. See §2.4 for the precise statements.

1.2. The zeta function of an arithmetic variety

Suppose now that $X \subset \mathbf{A}^n_{\mathbf{Z}}$ is defined by the ideal $(f_1, \dots, f_d) \subseteq \mathbf{Z}[x_1, \dots, x_n]$. For every prime p, we may consider $\overline{f_1}, \dots, \overline{f_d} \in \mathbf{F}_p[x_1, \dots, x_n]$ defining $X_p \subseteq \mathbf{A}^n_{\mathbf{F}_p}$, and the corresponding $Z(X_p, t)$. One then defines

$$L_X(s) := \prod_{p \nmid a} Z(X_p, 1/p^s).$$

If $X \subset \mathbf{A}^n_{\mathbf{Q}}$, then we may assume that the equations defining X have coefficients in some localization $\mathbf{Z}[1/a]$, where a is a positive integer. In this case we may still define X_p when p does not divide a, and we obtain L_X as above, by taking the product over those p that do not divide a (this definition on the choice of a, but for us this is not important).

Let us consider the case $X = \operatorname{Spec} \mathbf{Q}$, when we may take $X_p = \operatorname{Spec} \mathbf{F}_p$ for every prime p. Note that

$$Z(X_p, t) = \exp\left(\sum_{e \geq 1} \frac{t^e}{e}\right) = \exp(-\log(1-t)) = (1-t)^{-1}.$$

Therefore $L_X(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s)$ is the Riemann zeta function.

In general, it is not hard to see that L_X is defined in some half-plane $\{s \in \mathbf{C} \mid \operatorname{Re}(s) > \eta\}$ (we will discuss this in Chapter 6, giving a precise value for η, as a consequence of the Lang-Weil estimates, which in turn follow from the Weil conjectures for curves).

It is conjectured that if X is a smooth projective variety over $\mathbf{Q}$, then L_X has an analytic continuation that is a meromorphic function. One also expects that after a suitable normalization (necessary for taking into account the infinite prime and the primes of bad reduction) L_X satisfies a functional equation. Very little is know in this direction. Both properties are known for $\mathbf{P}^n$ and related varieties (such as toric varieties or flag varieties). The case of elliptic curves is known as a consequence of the Taniyama-Shimura conjecture (proved by Wiles [Wil], Taylor-Wiles [TW] and Breuil-Conrad-Diamond-Taylor [BCDT]), which implies that in this case L_X can be described as the L-function attached to a modular form.

1.3. The Igusa zeta function

Suppose now, for simplicity, that p is a prime in $\mathbf{Z}$, and $X \hookrightarrow \mathbf{A}^n_{\mathbf{Z}_p}$ is defined by $f \in \mathbf{Z}_p[x_1, \ldots, x_n]$. The Igusa zeta function of f is defined by

$$Z_f(s) := \int_{\mathbf{Z}_p^n} |f(x)|_p^s dx.$$

This is defined using the p-adic absolute value $|\cdot|_p$ and the Haar measure on $\mathbf{Z}_p$. It is easy to see using the definition that Z_f is analytic in the half-plane $\{s \mid \mathrm{Re}(s) > 0\}$. Let us give some motivation for this definition.

1.3.1. The Archimedean analogue of Z_f. The following analogue in the Archimedean setting (over $\mathbf{R}$ or $\mathbf{C}$) appeared before Igusa's zeta function, in the setting of complex powers. Suppose, for example, that $f \in \mathbf{R}[x_1, \ldots, x_n]$, and we want to define $|f(x)|^s$ for $s \in \mathbf{C}$ as a distribution.

Given a test function Φ, consider the map

$$s \to \int_{\mathbf{R}^n} |f(x)|^s \Phi(x) dx.$$

It is not hard to see that this is well-defined and analytic in the half-space $\{s \in \mathbf{C} \mid \mathrm{Re}(s) > 0\}$. Gelfand conjectured that it has a meromorphic continuation to $\mathbf{C}$.

This conjecture was proved by two methods. The first solution, given independently by Atiyah [Ati] and by Bernstein-Gelfand [BG], used Hironaka's theorem on resolution of singularities. This essentially allows replacing f by a monomial, in which case the assertion can be easily proved via integration by parts. A second proof due to Bernstein [Ber] directly used integration by parts, relying on the existence of what is nowadays called the Bernstein-Sato polynomial of f (in the process of proving the existence of this polynomial, Bernstein established the basics of the algebraic D-module theory).

1.3.2. The Poincaré power series of f. For every $m \geq 0$, let

$$c_m := |\{u \in (\mathbf{Z}/p^m\mathbf{Z})^n \mid f(u) = 0\}|$$

(with the convention $c_0 = 1$). The Poincaré series of f is $P_f := \sum_{m \geq 0} \frac{c_m}{p^{mn}} t^m \in \mathbf{Q}[\![t]\!]$. It was a conjecture of Borevich that P_f is a rational function.

It is not hard to see, using the definition of the Haar measure on $\mathbf{Z}_p^n$ that

$$P_f(t) = \frac{1 - tZ_f(s)}{1 - t},$$

where $t = (1/p)^s$. The usefulness of the integral expression for P_f via Z_f is that allows the use of the same methods employed in the Archimedean case. Using embedded resolution of singularities and the change of variable formula for p-adic integrals, Igusa showed that $Z_f(s)$ is a rational function of $(1/p)^s$, see [Igu]. In particular, this proved Borevich's conjecture about the rationality of P_f.

Note that if $X = V(f)$ is smooth over $\mathbf{Z}_p$, then the information contained in P_f is equivalent with that of $X(\mathbf{F}_p)$. It is remarkable, in fact, that in general the behavior of P_f can be linked to invariants of singularities of f. Since an embedded resolution of singularities comes up in the proof of rationality, it is maybe not too surprising that invariants that come up via resolutions are related to the poles of Z_f. On the other hand, a very interesting open problem in this field, due to Igusa, concerns a relation between these poles and the roots of the Bernstein-Sato

polynomial of f (compare with the Archimedean case; note, however, that there is no analogue of integration by parts in the p-adic setting).

One can define a global analogue of Igusa's zeta function, though this has been a lot less studied. Suppose that f is a polynomial with coefficients in $\mathbf{Z}$ (or, more generally, in a ring of integers in some number field). For every prime p, we may consider the image f_p of f in $\mathbf{Z}_p[x_1, \ldots, x_n]$, and the corresponding zeta function $Z_{f_p}(s)$. If a_p is the constant coefficient of the power series in $(1/p)^s$ representing $Z_{f_p}(s)$, then one can define

$$Z(s) := \prod_{p \text{ prime}} \left(a_p^{-1} Z_{f_p}(s)\right).$$

All non-trivial results concerning Z are due to du Sautoy and Grunewald [dSG]. They showed that this function has a rational abscissa of convergence, and that it can be meromorphically continued to the left of this abscissa. However, it is known that even in simple examples, Z does not have a meromorphic continuation to $\mathbf{C}$. It is also not clear how properties of the singularities of f can be recast into analytic properties of Z.

1.4. Motivic versions of the above (local) zeta functions

Both the Hasse-Weil zeta functions and the Igusa zeta functions have motivic versions. In this setting, *motivic* means working with coefficients in the Grothendieck ring of varieties over a field k. Recall that this is the quotient $K_0(\mathrm{Var}/k)$ of the free abelian group on the set of isomorphism classes of varieties over k, by the relations

$$[X] = [Y] + [X \smallsetminus Y],$$

where Y is a closed subvariety of X.

The motivic analogue of the Hasse-Weil zeta function was introduced by Kapranov [Kap]. If k is any field, and X is a variety over k, let $\mathrm{Sym}^n(X)$ denote the n^{th} symmetric product of X. Kapranov's zeta function is

$$Z_{\mathrm{mot}}(X, t) := \sum_{n \geq 0} [\mathrm{Sym}^n(X)] t^n \in K_0(\mathrm{Var}/k)[\![t]\!].$$

If k is a finite field, then there is a ring homomorphism $K_0(\mathrm{Var}/k) \to \mathbf{Z}$, that takes $[V]$ to $|V(k)|$. One can show that the induced map $K_0(\mathrm{Var}/k)[\![t]\!] \to \mathbf{Z}[\![t]\!]$ takes $Z_{\mathrm{mot}}(X, t)$ to $Z(X, t)$. Kapranov proved in [Kap] that if X is any curve, then $Z_{\mathrm{mot}}(X, t)$ is a rational function. On the other hand, Larsen and Lunts [LL1] showed that if X is a smooth complex surface, then $Z_{\mathrm{mot}}(X, t)$ is rational if and only if X has negative Kodaira dimension. However, it is still open whether $Z_{\mathrm{mot}}(X, t)$ is always rational when inverting the class $\mathbf{L}$ of $\mathbf{A}^1$ in $K_0(\mathrm{Var}/k)$.

Igusa's zeta function also has a motivic version, due to Denef and Loeser, see [DL]. The idea is to replace $\mathbf{Z}_p$ by $\mathbf{C}[\![t]\!]$ (in this case f is a polynomial with complex coefficients). The space of integration $\mathbf{Z}_p^n$ is replaced by $(\mathbf{C}[\![t]\!])^n$, and p-adic integrals by the so-called motivic integrals. Once the framework of motivic integration is in place, the results about Igusa's zeta function extend to this framework without much effort.

1.5. Zeta functions in group theory

1.5.1. Subgroup growth zeta functions. Let G be a finitely generated group. For every $n \geq 1$, put $a_n(G) := |\{H \leq G \mid [G : H] = n\}$, and let

$$\zeta_G(s) = \sum_{n \geq 1} \frac{a_n(G)}{n^s}.$$

This is a global type of zeta function.

The following facts are known:

- If G is solvable, then ζ_G is analytic in a half-plane of the form
$$\{s \mid \mathrm{Re}(s) > \alpha(G)\}.$$
- If G is nilpotent, then there is a product formula
$$\zeta_G(s) = \prod_{p \text{ prime}} \zeta_{G,p}(s),$$
where $\zeta_{G,p}(s) = \sum_{n \geq 0} \frac{a_{p^n}(G)}{p^{ns}}$. Furthermore, each $\zeta_{G,p}$ is a rational function of $(1/p)^s$.

A key point in the study of $\zeta_{G,p}(s)$ is the fact that it can be computed by a p-adic integral, very similar to the ones that come up in the definition of Igusa zeta functions. A fundamental problem concerns the behavior of $\zeta_{G,p}$ when p varies. In general, it turns out that this can be rather wild. Some of the key results in the understanding of this variation of $\zeta_{G,p}$ are due to du Sautoy and Grunewald [**dSG**]. For some recent developments concerning functional equations in this context, see [**Voll**].

Similar zeta functions can be defined to measure the rate of growth of other algebraic subobjects. For example, this can be done for Lie subalgebras of a Lie algebra that is finitely generated as an abelian group over $\mathbf{Z}$, or for ideals in a ring that is finitely generated as an abelian group over $\mathbf{Z}$. The corresponding zeta functions have similar properties with the ones measuring the rate of growth of subgroups, see [**dSG**].

1.5.2. Representation zeta functions. Given a group G, let $r_n(G)$ denote the number of equivalence classes of n-dimensional representations of G (with suitable restrictions: for example, the representations are assumed to be rational if G is an algebraic group). The representation zeta function of G is

$$\zeta_G^{\mathrm{rep}}(s) = \sum_{n \geq 1} \frac{r_n(G)}{n^s}.$$

An interesting example is given by $G = SL_n(\mathbf{Z})$. One can show that if $n \geq 3$, then

$$\zeta^{\mathrm{rep}}_{SL_n(\mathbf{Z})}(s) = \zeta^{\mathrm{rep}}_{SL_n(\mathbf{C})}(s) \cdot \prod_{p \text{ prime}} \zeta^{\mathrm{rep}}_{SL_n(\mathbf{Z}_p)}(s).$$

It is somewhat surprising that in the few known examples, the dependence on p of the p-factors of the representation zeta function is better behaved than in the case of the subgroup growth zeta functions. Again, a key ingredient in the study of the the p-factors is given by p-adic integration. We refer to [**AKOV**] for some interesting new results on representation zeta functions.

CHAPTER 2

Basics of Hasse-Weil zeta functions

In this chapter we introduce the Hasse-Weil zeta function, prove some elementary properties, and give the statements of the Weil conjectures. Before doing this, we review some basic facts about finite fields and varieties over finite fields.

2.1. Review of finite fields

Recall that if k is a finite field, then $|k| = p^e$ for some $e \geq 1$, where $p = \mathrm{char}(k)$. Furthermore, two finite fields with the same cardinality are isomorphic. We denote a finite field with $q = p^e$ elements (where p is a prime positive integer) by $\mathbf{F}_q$.

Let us fix $k = \mathbf{F}_q$. Given a finite field extension K/k, if $r = [K : k]$, then $|K| = q^r$. Conversely, given any $r \geq 1$, there is a field extension $k \hookrightarrow K$ of degree r. Furthermore, if $k \hookrightarrow K'$ is another such extension, then the two extensions differ by an isomorphism $K \simeq K'$. More generally, if $[K' : k] = s$, then there is a morphism of k-algebras $K \to K'$ if and only if $r|s$.

If $\overline{k}$ is an algebraic closure of k, then we have an element $\sigma \in G(\overline{k}/k)$ given by $\sigma(x) = x^q$. This is called the *arithmetic Frobenius element*, and its inverse in $G(\overline{k}/k)$ is the *geometric Frobenius element*. There is a unique subextension of k of degree r that is contained in $\overline{k}$: this is given by $K = \{x \in \overline{\mathbf{F}_q} \mid \sigma^r(x) = x\}$.

In fact, the Galois group $G(K/k)$ is cyclic or order r, with generator $\sigma|_K$. Furthermore, we have canonical isomorphisms

$$G(\overline{k}/k) \simeq \mathrm{projlim}_{K/k \text{ finite}} G(K/k) \simeq \mathrm{projlim}_{r \in \mathbf{Z}_{>0}} \mathbf{Z}/r\mathbf{Z} =: \widehat{\mathbf{Z}},$$

with σ being a topological generator of $G(\overline{k}/k)$.

2.2. Preliminaries: varieties over finite fields

By a variety over a field k we mean a reduced scheme of finite type over k (possibly reducible). From now on we assume that $k = \mathbf{F}_q$ is a finite field. Recall that there are two notions of points of X in this context, as follows.

Note that X is a topological space. We denote by X_{cl} the set of closed points of X (in fact, these are the only ones that we will consider). Given such $x \in X_{\mathrm{cl}}$, we have the local ring $\mathcal{O}_{X,x}$ and its residue field $k(x)$. By definition, $k(x)$ is isomorphic to the quotient of a finitely generated k-algebra by a maximal ideal, hence $k(x)$ is a finite extension of k by Hilbert's Nullstellensatz. We put $\deg(x) := [k(x) : k]$.

On the other hand, we have the notion of K-valued points of X. Recall that if $k \to K$ is a field homomorphism, the the set of K-valued points of X is

$$X(K) := \mathrm{Hom}_{\mathrm{Spec}\, k}(\mathrm{Spec}\, K, X) = \bigsqcup_{x \in X} \mathrm{Hom}_{k-\mathrm{alg}}(k(x), K).$$

We will always consider the case when the extension K/k is algebraic. In this case, if $\phi\colon \mathrm{Spec}\, K \to X$ is in $X(K)$, the point $x \in X$ that is the image of the unique point

in $\operatorname{Spec} K$ is closed: indeed, we have $\dim \overline{\{x\}} = \operatorname{trdeg}(k(x)/k) = 0$. In particular, we see that if K/k is a finite extension of degree r, then

$$X(K) = \bigsqcup_{\deg(x)|r} \operatorname{Hom}_{k-\mathrm{alg}}(k(x), K). \tag{2.1}$$

Note that if $\deg(x) = e|r$, then $\operatorname{Hom}_{k-\mathrm{alg}}(k(x), K)$ carries a transitive action of $G(\mathbf{F}_{q^r}/\mathbf{F}_q) \simeq \mathbf{Z}/r\mathbf{Z}$. The stabilizer of any element is isomorphic to $G(\mathbf{F}_{q^r}/\mathbf{F}_{q^e})$, hence

$$|\operatorname{Hom}_{k-\mathrm{alg}}(k(x), K)| = e.$$

In particular, this proves the following

PROPOSITION 2.1. *If X is a variety over the finite field k, and K/k is a field extension of degree r, then*

$$|X(K)| = \sum_{e|r} e \cdot |\{x \in X_{\mathrm{cl}} \mid \deg(x) = e\}.$$

REMARK 2.2. It is clear that if $X = Y_1 \cup \ldots \cup Y_m$, where each Y_i is a locally closed subset of X, then $X(K) = Y_1(K) \cup \ldots \cup Y_m(K)$. Furthermore, if the former union is disjoint, then so is the latter one.

REMARK 2.3. Suppose that X is affine, and consider a closed embedding $X \hookrightarrow \mathbf{A}^n_k$ defined by the ideal $(F_1, \ldots, F_d) \subseteq k[x_1, \ldots, x_n]$. If K/k is a field extension, then we have an identification

$$X(K) = \{(u_1, \ldots, u_n) \in K^n \mid f_i(u_1, \ldots, u_n) = 0 \text{ for } 1 \leq i \leq d\}.$$

In particular, we see that if K/k is finite, then $X(K)$ is finite. The formula in Proposition 2.1 now implies that for every $e \geq 1$, there are only finitely many $x \in X$ with $\deg(x) = e$. Of course, by taking an affine open cover of X, we deduce that these assertions hold for arbitrary varieties over k.

It is often convenient to think of K-valued points in terms of an algebraic closure of the ground field. Suppose that $\overline{k}$ is a fixed algebraic closure of k, and let us write $\mathbf{F}_{q^r}$ for the subfield of $\overline{k}$ of degree r over k. Let $\overline{X} = X \times_{\operatorname{Spec} k} \operatorname{Spec} \overline{k}$. This is a variety over $\overline{k}$ (the fact that $\overline{X}$ is reduced follows from the fact that X is reduced and k is perfect; however, we will not need this). Note that by definition we have $\overline{X}(\overline{k}) = X(\overline{k})$.

Consider the Frobenius morphism $\operatorname{Frob}_{X,q} \colon X \to X$ on X. This is the identity on X, and the morphism of sheaves of rings $\mathcal{O}_X \to \mathcal{O}_X$ is given by $u \to u^q$ (since $u^q = u$ for every $u \in k$, we see that $\operatorname{Frob}_{X,q}$ is a morphism of schemes over k. In particular, it induces a morphism of schemes over $\overline{k}$:

$$\operatorname{Frob}_{\overline{X},q} = \operatorname{Frob}_{X,q} \times \mathrm{id} \colon \overline{X} \to \overline{X}.$$

Note that this is a functorial construction. In particular, if X is affine and if we consider a closed immersion $X \hookrightarrow \mathbf{A}^N_k$, then $\operatorname{Frob}_{\overline{X},q}$ is induced by $\operatorname{Frob}_{\mathbf{A}^N_{\overline{k}},q}$. This is turn corresponds to the morphism of $\overline{k}$-algebras

$$\overline{k}[x_1, \ldots, x_N] \to \overline{k}[x_1, \ldots, x_N], \ x_i \to x_i^q,$$

hence on $\overline{k}$-points it is given by $(u_1, \ldots, u_N) \to (u_1^q, \ldots, u_N^q)$. We conclude that the natural embedding

$$X(\mathbf{F}_{q^r}) \hookrightarrow X(\overline{k}) = \overline{X}(\overline{k})$$

identifies $X(\mathbf{F}_{q^r})$ with the elements of $\overline{X}(\overline{k})$ fixed by $\mathrm{Frob}_{\overline{X},q}^r$. Indeed, this is clear when $X = \mathbf{A}_k^N$ by the previous discussion, and the general case follows by considering an affine open cover, and by embedding each affine piece in a suitable affine space.

In other words, if $\Delta, \Gamma_r \subset \overline{X} \times \overline{X}$ are the diagonal, and respectively, the graph of $\mathrm{Frob}_{\overline{X},q}^r$, then $X(\mathbf{F}_{q^r})$ is in natural bijection with the closed points of $\Gamma_r \cap \Delta$. The following proposition shows that when X smooth, this is a transverse intersection.

PROPOSITION 2.4. *If X is smooth over $k = \mathbf{F}_q$, then the intersection $\Gamma_r \cap \Delta$ consists of a reduced set of points.*

Note that since k is perfect, X is smooth over k if and only if it is nonsingular.

PROOF. We have already seen that the set $\Gamma_r \cap \Delta$ is finite, since it is in bijection with $X(\mathbf{F}_{q^r})$. In order to show that it is a reduced set, let us consider first the case when $X = \mathbf{A}_{\mathbf{F}_q}^n$. In this case, if $R = \overline{k}[x_1, \ldots, x_n, y_1, \ldots, y_n]$, then $\Delta \subset \operatorname{Spec} R$ is defined by $(y_1 - x_1, \ldots, y_n - x_n)$ and Γ_r is defined by $(y_1 - x_1^q, \ldots, y_r - x_r^q)$. Therefore $\Gamma_r \cap \Delta$ is isomorphic to $\prod_{i=1}^n \operatorname{Spec} k[x_i]/(x_i - x_i^q)$, hence it is reduced (note that the polynomial $x_i^q - x_i$ has no multiple roots).

For an arbitrary smooth variety X, let us consider $u \in X(\mathbf{F}_{q^e})$, and let $x \in X$ be the corresponding closed point. If $t_1, \ldots, t_n$ form a regular system of parameters of $\mathcal{O}_{X,x}$, it follows that $(t_1, \ldots, t_n)$ define an étale map $U \to \mathbf{A}^n$, where U is an open neighborhood of x. Note that the restriction to $\overline{U} \times \overline{U}$ of Δ and Γ_r are the inverse images via $\overline{U} \times \overline{U} \to \mathbf{A}_{\overline{k}}^n \times \mathbf{A}_{\overline{k}}^n$ of the corresponding subsets for $\mathbf{A}_{\overline{k}}^n$. Since the inverse image of a smooth subscheme by an étale morphism is smooth, we deduce the assertion in the proposition for X from the assertion for $\mathbf{A}_k^n$. □

EXERCISE 2.5. Let X and $\overline{X}$ be as above. The group $G = G(\overline{k}/k)$ acts on the right on $\operatorname{Spec} \overline{k}$, by algebraic automorphisms.

i) Show that G has an induced right action on $\overline{X}$, by acting on the second component of $X \times_{\operatorname{Spec} k} \operatorname{Spec} \overline{k}$. Of course, these automorphisms are not of schemes over $\overline{k}$.

ii) Let $\tau \colon \overline{X} \to \overline{X}$ be the action of the arithmetic Frobenius element. Describe τ when $X = \mathbf{A}_k^n$. Show that $\tau \circ \mathrm{Frob}_{\overline{X},q} = \mathrm{Frob}_{\overline{X},q} \circ \tau$, and they are equal to the absolute q-Frobenius morphism of $\overline{X}$ (recall: this is the identity on $\overline{X}$, and the morphism of sheaves of rings $\mathcal{O}_{\overline{X}} \to \mathcal{O}_{\overline{X}}$ is given by $u \to u^q$).

iii) We also have a natural left action of G on $X(\overline{k})$ that takes (g, ϕ) to $\phi \circ g$ (where we identify g with the corresponding automorphism of $\operatorname{Spec} \overline{k}$). Show that the arithmetic Frobenius acts on $X(\overline{k}) = \overline{X}(\overline{k})$ by the map induced by $\mathrm{Frob}_{\overline{X},q}$.

iv) The canonical projection $\overline{X} \to X$ induces a map $\overline{X}_{\mathrm{cl}} \to X_{\mathrm{cl}}$. Show that this is identified via $X(\overline{k}) = \overline{X}(\overline{k}) = \overline{X}_{\mathrm{cl}}$ with the map described at the beginning of this section, that takes a $\overline{k}$-valued point of X to the corresponding closed point of X.

v) We similarly have a left action of $G(\mathbf{F}_{q^r}/\mathbf{F}_q)$ on $X(\mathbf{F}_{q^r})$. Show that the fibers of the map $X(\mathbf{F}_{q^r}) \to X_{\mathrm{cl}}$ that takes an $\mathbf{F}_{q^r}$-valued point to the corresponding closed point of X are precisely the orbits of the $G(\mathbf{F}_{q^r}/\mathbf{F}_q)$-action.

2.3. The Hasse-Weil zeta function

2.3.1. The exponential and the logarithm power series. Recall that the exponential formal power series is given by

$$\exp(t) = \sum_{m \geq 0} \frac{t^n}{n!} \in \mathbf{Q}[\![t]\!].$$

We will also make use of the logarithm formal power series, defined by

$$\log(1+t) = \sum_{m \geq 1} \frac{(-1)^{m+1} t^m}{m} \in \mathbf{Q}[\![t]\!].$$

In particular, we may consider $\exp(u(t))$ and $\log(1+u(t))$ whenever $u \in t\mathbf{Q}[\![t]\!]$.

We collect in the following proposition some well-known properties of the exponential and logarithm formal power series. We will freely use these properties in what folows.

PROPOSITION 2.6. *The following properties hold:*

i) *We have* $\exp(t)' = \exp(t)$ *and* $\log(1+t)' = (1+t)^{-1}$.
ii) $\exp(s+t) = \exp(s) \cdot \exp(t)$ *in* $\mathbf{Q}[\![s,t]\!]$. *In particular, we have* $\exp(u+v) = \exp(u) \cdot \exp(v)$ *for every* $u, v \in t\mathbf{Q}[\![t]\!]$.
iii) $\exp(mt) = \exp(t)^m$ *for every* $m \in \mathbf{Z}$. *In particular,* $\exp(mu) = \exp(u)^m$ *for every* $u \in t\mathbf{Q}[\![t]\!]$.
iv) $\log(\exp(u)) = u$ *and* $\exp(\log(1+u)) = 1+u$ *for every* $u \in t\mathbf{Q}[\![t]\!]$.
v) $\log((1+u)(1+v)) = \log(1+u) + \log(1+v)$ *for every* $u, v \in t\mathbf{Q}[\![t]\!]$.
vi) $\log((1+u)^m) = m \cdot \log(1+u)$ *for every* $m \in \mathbf{Z}$ *and every* $u \in t\mathbf{Q}[\![t]\!]$.

PROOF. The proofs are straightforward. i) and ii) follow by direct computation, while iii) is a direct consequence of i). It is enough to prove the assertions in iv) for $u = t$. The first assertion now follows by taking formal derivatives of the both sides. Note that we have two ring homomorphisms $f, g \colon \mathbf{Q}[\![t]\!] \to \mathbf{Q}[\![t]\!]$, $f(u) = \log(1+u)$ and $g(v) = \exp(v) - 1$. They are both isomorphisms by the formal Inverse Function theorem, and $f \circ g = \mathrm{Id}$ by the first equality in iv). Therefore $g \circ f = \mathrm{Id}$, which is the second equality in iv). The assertions in v) and vi) now follow from ii) and iii) via iv). □

2.3.2. The definition of the Hasse-Weil zeta function. Suppose that X is a variety over a finite field $k = \mathbf{F}_q$. For every $m \geq 1$, let $N_m = |X(\mathbf{F}_{q^m})|$[1]. The Hasse-Weil zeta function of X is

$$Z(X,t) = \exp\left(\sum_{m \geq 1} \frac{N_m}{m} t^m\right) \in \mathbf{Q}[\![t]\!]. \tag{2.2}$$

The following proposition gives a product formula for $Z(X,t)$ that is very useful in practice.

PROPOSITION 2.7. *For every variety* X *over* $\mathbf{F}_q$, *we have*

$$Z(X,t) = \prod_{x \in X_{\mathrm{cl}}} (1 - t^{\deg(x)})^{-1}. \tag{2.3}$$

[1] If k' is a finite extension of k of degree m, then the set $X(k')$ depends on this extension. However, any two extension of k of the same degree differ by a k-automorphism, hence $|X(k')|$ only depends on $|k'|$.

In particular, $Z(X,t) \in \mathbf{Z}[\![t]\!]$.

By making $t = p^{-s}$, we see that the above formula is analogous to the product formula for the Riemann zeta function.

PROOF. Let us put $a_r := |\{x \in X_{\mathrm{cl}} \mid [k(x) : \mathbf{F}_q] = r\}|$ for every $r \geq 1$. Therefore the right-hand side of (2.3) is equal to $\prod_{r\geq 1}(1-t^r)^{-a_r}$. It is clear that this product is well-defined in $\mathbf{Z}[\![t]\!]$.

Recall that by Proposition 2.1, we have $N_m = \sum_{r|m} r \cdot a_r$. It follows from definition that

$$\log(Z(X,t)) = \sum_{m\geq 1} \frac{N_m}{m} t^m = \sum_{m\geq 1}\sum_{r|m} \frac{r\cdot a_r}{m} t^m = \sum_{r\geq 1} a_r \cdot \sum_{\ell \geq 1} \frac{t^{\ell r}}{\ell} = \sum_{r\geq 1} (-a_r)\cdot \log(1-t^r)$$

$$= \sum_{r\geq 1} \log(1-t^r)^{-a_r} = \log\left(\prod_{r\geq 1}(1-t^r)^{-a_r}\right).$$

The formula (2.3) now follows applying exp on both sides. □

REMARK 2.8. Suppose that $q = (q')^m$. If X is a variety over $\mathbf{F}_q$, we may consider X as a variety over $\mathbf{F}_{q'}$, in the natural way. For every closed point $x \in X$, we have $\deg(k(x)/\mathbf{F}_{q'}) = m \cdot \deg(k(x)/\mathbf{F}_q)$. It follows from Proposition 2.7 that $Z(X/\mathbf{F}_{q'}, t) = Z(X, \mathbf{F}_q, t^m)$.

REMARK 2.9. One can interpret the formula in Proposition 2.7 by saying that $Z(X,t)$ is a generating function for the effective 0-cycles on X. Recall that the group of 0-cycles $Z_0(X)$ is the free abelian group generated by the (closed) points of X. Given a 0-cycle $\alpha = \sum_{i=1}^r m_i x_i$, its degree is $\deg(\alpha) = \sum_{i=1}^r m_i \deg(x_i)$. A 0-cycle $\sum_i m_i x_i$ is *effective* if all m_i are nonnegative. With this terminology, we see that the formula in Proposition 2.7 can be rewritten as

$$Z(X,t) = \prod_{x\in X_{\mathrm{cl}}} (1 + t^{\deg(x)} + t^{2\deg(x)} + \ldots),$$

and multiplying we obtain

$$Z(X,t) = \sum_{\alpha} t^{\deg(\alpha)}, \tag{2.4}$$

where the sum is over all effective 0-cycles on X.

2.3.3. Examples and elementary properties. We start with the example of the affine space.

EXAMPLE 2.10. Let $k = \mathbf{F}_q$, and $X = \mathbf{A}^n_k$. It is clear that for every finite extension k'/k we have $X(k') = (k')^n$, hence $|X(k')| = |k'|^n$. We conclude that

$$Z(\mathbf{A}^n, t) = \exp\left(\sum_{m\geq 1} \frac{q^{mn}}{m} t^m\right) = \exp\left(-\log(1-q^n t)\right) = \frac{1}{(1-q^n t)}.$$

EXAMPLE 2.11. More generally, note that for every two varieties X and Y, we have $X\times Y(k') = X(k')\times Y(k')$. In particular, if $X = \mathbf{A}^n$, we have $|\mathbf{A}^n \times Y(\mathbf{F}_{q^m})| = |Y(\mathbf{F}_{q^m})| q^{mn}$, hence

$$Z(\mathbf{A}^n \times Y, t) = \exp\left(\sum_{m\geq 1} \frac{|Y(\mathbf{F}_{q^m})| q^{mn}}{m} t^m\right) = Z(Y, q^n t).$$

PROPOSITION 2.12. *If X is a variety over $\mathbf{F}_q$, and Y is a closed subvariety of X, then $Z(X,t) = Z(Y,t) \cdot Z(U,t)$, where $U = X \setminus Y$.*

PROOF. It is clear that for every $m \geq 1$ we have $|X(\mathbf{F}_{q^m})| = |Y(\mathbf{F}_{q^m})| + |U(\mathbf{F}_{q^m})|$. The assertion in the proposition is an immediate consequence of this and of the fact that $\exp(u+v) = \exp(u) \cdot \exp(v)$ for every $u, v \in t\mathbf{Q}[\![t]\!]$. □

COROLLARY 2.13. *The zeta function of the projective space is given by*

$$Z(\mathbf{P}^n_{\mathbf{F}_q}, t) = \frac{1}{(1-t)(1-qt)\cdots(1-q^n t)}.$$

PROOF. The assertion follows from Example 2.10 by induction on n, using Proposition 2.12, and the fact that we have a closed embedding $\mathbf{P}^{n-1}_{\mathbf{F}_q} \hookrightarrow \mathbf{P}^n_{\mathbf{F}_q}$, whose complement is isomorphic to $\mathbf{A}^n_{\mathbf{F}_q}$. □

PROPOSITION 2.14. *Let X be a variety over $k = \mathbf{F}_q$, and let k'/k be a field extension of degree r. If $X' = X \times_{\operatorname{Spec} k} \operatorname{Spec} k'$, then*

$$Z(X', t^r) = \prod_{i=1}^{r} Z(X, \xi^i t),$$

where ξ is a primitive root of order r of 1.

PROOF. Let us put $N'_m := |X'(\mathbf{F}_{q^{rm}})|$ and $N_m = |X(\mathbf{F}_{q^m})|$, hence $N'_m = N_{mr}$. By definition, it is enough to show that

$$\sum_{m \geq 1} \frac{N_{mr}}{m} t^{mr} = \sum_{i=1}^{r} \sum_{\ell \geq 1} \frac{N_\ell}{\ell} \xi^{i\ell} t^\ell.$$

This is a consequence of the fact that $\sum_{i=1}^{r} \xi^{i\ell} = 0$ if r does not divide ℓ, and it is equal to r, otherwise. □

2.4. The statements of the Weil conjectures

Suppose that X is a smooth, geometrically connected, projective variety, of dimension n, defined over a finite field $k = \mathbf{F}_q$. We put $Z(t) = Z(X,t)$.

CONJECTURE 2.15 (Rationality). *$Z(t)$ is a rational function, i.e. it lies in $\mathbf{Q}(t)$.*

CONJECTURE 2.16 (Functional equation). *If $E = (\Delta^2)$ is the self-intersection of the diagonal $\Delta \hookrightarrow X \times X$, then*

$$Z\left(\frac{1}{q^n t}\right) = \pm q^{nE/2} t^E Z(t).$$

CONJECTURE 2.17 (Analogue of Riemann hypothesis). *One can write*

$$Z(t) = \frac{P_1(t) \cdot P_3(t) \cdots P_{2n-1}(t)}{P_0(t) \cdot P_2(t) \cdots P_{2n}(t)},$$

with $P_0(t) = 1 - t$, $P_{2n}(t) = 1 - q^n t$, and for $1 \leq 2n-1$, we have $P_i(t) \in \mathbf{Z}[t]$,

$$P_i(t) = \prod_j (1 - \alpha_{i,j} t),$$

with $\alpha_{i,j}$ algebraic integers with $|\alpha_{i,j}| = q^{i/2}$.

Note that the conditions in the above conjecture uniquely determine the P_i.

CONJECTURE 2.18. *Assuming Conjecture 2.17, define the "i^{th} Betti number of X" as $b_i(X) := \deg(P_i(t))$. In this case, the following hold:*

i) $E = \sum_{i=0}^{2n} (-1)^i b_i(X)$.
ii) *Suppose that R is a finitely generated $\mathbf{Z}$-subalgebra of the field $\mathbf{C}$ of complex numbers, $\widetilde{X}$ is a smooth projective scheme over $\operatorname{Spec} R$, and $P \in \operatorname{Spec} R$ is a prime ideal such that $R/P = \mathbf{F}_q$ and $\widetilde{X} \times_{\operatorname{Spec} R} \operatorname{Spec} R/P = X$. Then*

$$b_i(X) = \dim_{\mathbf{Q}} H^i \left((\widetilde{X} \times_{\operatorname{Spec} R} \operatorname{Spec} \mathbf{C})^{\text{an}}, \mathbf{Q} \right).$$

As we will see in §4.3, one can in fact formulate Conjecture 2.18 without assuming Conjecture 2.17. We will give in the next chapter the proofs of the above conjectures in the case of curves. In Chapter 4 we will give a brief introduction to ℓ-adic cohomology, and explain how this formalism allows one to prove Conjectures 2.15, 2.16, and 2.18 (where in Conjecture 2.15 one just has to assume that X is of finite type over $\mathbf{F}_q$). The harder Conjecture 2.17 was proved by Deligne [**Del3**], and a later proof was given by Laumon [**Lau**], but both these proofs go far beyond the scope of our notes. On the other hand, the first proof of Conjecture 2.15, for arbitrary schemes of finite type over $\mathbf{F}_q$, was obtained by Dwork [**Dwo**] using p-adic analysis. We present his proof in Chapter 8.

2.5. Comments on the conjectures

REMARK 2.19. Let X be an arbitrary variety over $k = \mathbf{F}_q$, and let $Y \hookrightarrow X$ be a closed subvariety, and $U = X \smallsetminus Y$. It follows from Proposition 2.12 that $Z(X,t) = Z(Y,t) \cdot Z(U,t)$. Therefore if two of $Z(X,t)$, $Z(Y,t)$ and $Z(U,t)$ are known to be rational, then the third one is rational, too.

REMARK 2.20. The above remark implies that if we assume resolution of singularities over finite fields, then a positive answer to Conjecture 2.15 for smooth projective varieties implies the rationality of $Z(X,t)$ for every variety X over a finite field. Indeed, suppose by induction on dimension that the assertion is known for varieties of dimension $< n$. Remark 2.19 and the induction hypothesis imply that if X and Y are varieties of dimension n that have dense open subsets U, respectively V, that are isomorphic, then $Z(X,t)$ is rational if and only if $Z(Y,t)$ is rational. Given any n-dimensional variety X, there is a projective variety Y such that there are U and V as above. Furthermore, if we have resolution of singularities over our ground field, then we may assume that Y is also smooth. Therefore $Z(Y,t)$ is rational by Conjecture 2.15 (note that the irreducible components Y_i of Y are disjoint, hence $Z(Y,t) = \prod_i Z(Y_i,t)$, any we apply Conjecture 2.15 to each Y_i).

REMARK 2.21. In a similar vain, in order to prove that $Z(X,t)$ is rational for every variety X, it is enough to prove it in the case when X is an irreducible hypersurface in $\mathbf{A}^n_{\mathbf{F}_q}$. Indeed, arguing as in the previous remark we see that we may assume that X is affine and irreducible, in which case it is birational (over $\mathbf{F}_q$) with a hypersurface in an affine space.

REMARK 2.22. There is the following general formula in intersection theory: if $i\colon Y \hookrightarrow X$ is a closed embedding of nonsingular varieties of pure codimension r,

then $i^*(i_*(\alpha)) = c_r(N_{Y/X}) \cap \alpha$ for every $\alpha \in A^*(X)$, where $N_{Y/X}$ is the normal bundle of Y in X.

In particular, if X is smooth, projective, of pure dimension n, and $\Delta\colon X \hookrightarrow X \times X$ is the diagonal embedding, then $N_{X/X\times X} = T_X$, and therefore

$$(\Delta^2) = \deg(c_n(T_X)).$$

EXAMPLE 2.23. Let us check the Weil conjectures when $X = \mathbf{P}^n_{\mathbf{F}_q}$. As we have seen in Corollary 2.23, we have

$$Z(\mathbf{P}^n, t) = \frac{1}{(1-t)(1-qt)\cdots(1-q^nt)}. \tag{2.5}$$

In particular, it is clear that Conjectures 2.15 and 2.17 hold in this case. It follows from (2.5) that

$$Z(X, 1/q^nt) = \frac{1}{\left(1-\frac{1}{q^nt}\right)\left(1-\frac{1}{q^{n-1}t}\right)\cdots\left(1-\frac{1}{t}\right)} = (-1)^{n+1}t^{n+1}q^{n(n+1)/2}Z(X,t).$$

Hence in order to check Conjecture 2.16, it is enough to show that $E = n+1$. The Euler exact sequence

$$0 \to \mathcal{O}_{\mathbf{P}^n} \to \mathcal{O}_{\mathbf{P}^n}(1)^{\oplus(n+1)} \to T_{\mathbf{P}^n} \to 0$$

implies $c(T_{\mathbf{P}^n}) = c(\mathcal{O}_{\mathbf{P}^n}(1)^{\oplus(n+1)}) = (1+h)^{n+1}$, where $h = c_1(\mathcal{O}_{\mathbf{P}^n}(1))$. This implies that $\deg(c_n(T_{\mathbf{P}^n})) = n+1$.

Since $H^*(\mathbf{P}^n_{\mathbf{C}}, \mathbf{Q}) \simeq \mathbf{Q}[t]/(t^{n+1})$, with $\deg(t) = 2$, the assertions in Conjecture 2.18 also follow.

REMARK 2.24. Let X be a variety over $\mathbf{F}_q$, and suppose we know that $Z(X,t)$ is rational. Let us write $Z(X,t) = \frac{f(t)}{g(t)}$, with $f, g \in \mathbf{Q}[t]$. After dividing by the possible powers of t, we may assume that $f(0), g(0) \neq 0$, and after normalizing, that $f(0) = 1 = g(0)$.

We write $f(t) = \prod_{i=1}^r(1-\alpha_i t)$ and $g(t) = \prod_{j=1}^s(1-\beta_j t)$. If $N_m = |X(\mathbf{F}_{q^m})|$, then

$$\sum_{m\geq 1}\frac{N_m}{m}t^m = \sum_{i=1}^r \log(1-\alpha_i t) - \sum_{j=1}^s \log(1-\beta_j t),$$

hence $N_m = \sum_{j=1}^s \beta_j^m - \sum_{i=1}^r \alpha_i^r$ for every $m \geq 1$.

2.6. Two examples: computing the Betti numbers for Grassmannians and full flag varieties

One can use the above Conjecture 2.18 to compute the Betti numbers of smooth complex projecive varieties. We illustrate this by computing the Poincaré polynomials for Grassmannians and full flag varieties. For a famous example, in which the Weil conjectures are used to compute the Betti numbers of the Hilbert schemes of points on smooth projective surfaces, see [Göt2].

Recall that both the Grassmannian and the flag variety can be defined over $\mathbf{Z}$. More precisely, if $1 \leq r \leq n-1$, there is a scheme $\mathrm{Gr}(r,n)$ defined over $\operatorname{Spec}\mathbf{Z}$, such that for every field K, the K-valued points of $\mathrm{Gr}(r,n)$ are in bijection with the r-dimensional subspaces of K^n. Similarly, we have a scheme $\mathrm{Fl}(n)$ defined over $\operatorname{Spec}\mathbf{Z}$ such that for every field K, the K-valued points of $\mathrm{Fl}(n)$ are in bijection with the full flags on K^n, that is, with the n-tuples of linear subspaces $V_1 \subset V_2 \subset \ldots \subset V_n = K^n$,

with $\dim(V_i) = i$ for every i. It is well-known that both $\mathrm{Gr}(r,n)$ and $\mathrm{Fl}(n)$ are smooth, geometrically connected, and projective over $\operatorname{Spec}\mathbf{Z}$. For every field K, we put $\mathrm{Gr}(r,n)_K = \mathrm{Gr}(r,n) \times \operatorname{Spec} K$ and $\mathrm{Fl}(n)_K = \mathrm{Fl}(n) \times \operatorname{Spec} K$.

Recall that the Poincaré polynomial of a complex algebraic variety X is given by $P_X(y) = \sum_{i=0}^{2\dim(X)} (-1)^i \dim_{\mathbf{Q}} H^i(X(\mathbf{C})^{\mathrm{an}}, \mathbf{Q}) y^i$. In order to compute the Poincaré polynomials of $\mathrm{Gr}(r,n)_{\mathbf{C}}$ and $\mathrm{Fl}(n)_{\mathbf{C}}$, we need to compute the zeta functions $Z(\mathrm{Gr}(r,n)_{\mathbf{F}_q}, t)$ and $Z(\mathrm{Fl}(n)_{\mathbf{F}_q}, t)$. Therefore we need to determine the numbers $a_q(r,n)$ and $b_q(n)$ of r-dimensional linear subspaces of $\mathbf{F}_q^n$, respectively, of full flags on $\mathbf{F}_q^n$.

In fact, we first compute $b_q(n)$, and then use this to compute $a_q(r,n)$. In order to give a full flag in $\mathbf{F}_q^n$, we first need to give a line L_1 in $\mathbf{F}_q^n$, then a line L_2 in $\mathbf{F}_q^n/L_1$, and so on. This shows that

$$b_q(n) = |\mathbf{P}^{n-1}(\mathbf{F}_q)| \cdot |\mathbf{P}^{n-2}(\mathbf{F}_q)| \cdots |\mathbf{P}^1(\mathbf{F}_q)|,$$

and therefore

(2.6)

$$b_q(n) = \frac{(q^n-1)(q^{n-1}-1)\cdots(q-1)}{(q-1)^n} = (1+q)(1+q+q^2)\cdots(1+q+\ldots+q^{n-1}).$$

We now compute $a_q(r,n)$. Note that the natural action of $GL_n(\mathbf{F}_q)$ on $\mathbf{F}_q^n$ induces an action on $\mathrm{Gr}(r,n)(\mathbf{F}_q)$. This action is transitive, and the stabilizer of the subspace W generated by $e_1, \ldots, e_r$ (where $e_1, \ldots, e_n$ is the standard basis of $\mathbf{F}_q^n$) is the set of matrices

$$\{A = (a_{i,j}) \in GL_n(\mathbf{F}_q) \mid a_{i,j} = 0 \,\text{for}\, r+1 \le i \le n, 1 \le j \le r\}.$$

If $A = (a_{i,j}) \in M_n(\mathbf{F}_q)$ is such that $a_{i,j} = 0$ for $r+1 \le i \le n$ and $1 \le j \le r$, then A is invertible if and only if the two matrices $(a_{i,j})_{i,j\le r}$ and $(a_{i,j})_{i,j\ge r+1}$ are invertible. We conclude that the number of elements in the stabilizer of W is

$$|\mathrm{GL}_r(\mathbf{F}_q)| \cdot |\mathrm{GL}_{n-r}(\mathbf{F}_q)| \cdot |M_{r,n-r}(\mathbf{F}_q)|. \tag{2.7}$$

In order to compute $|\mathrm{GL}_r(\mathbf{F}_q)|$, we use the transitive action of $GL_r(\mathbf{F}_q)$ on $\mathrm{Fl}(r)(\mathbf{F}_q)$ induced by the natural action on $\mathbf{F}_q^r$. The stabilizer of the flag

$$\langle e_1 \rangle \subset \langle e_1, e_2 \rangle \subset \ldots \subset \mathbf{F}_q^n$$

is the set of upper triangular matrices in $GL_r(\mathbf{F}_q)$, and there are $(q-1)^r q^{r(r-1)/2}$ such matrices. We conclude that

$$|\mathrm{GL}_r(\mathbf{F}_q)| = b_q(r) q^{r(r-1)/2} (q-1)^r = q^{r(r-1)/2}(q^r-1)(q^{r-1}-1)\cdots(q-1).$$

We now deduce from (2.7) that

$$a_q(r,n) = \frac{|GL_n(\mathbf{F}_q)|}{|\mathrm{GL}_r(\mathbf{F}_q)| \cdot |\mathrm{GL}_{n-r}(\mathbf{F}_q)| \cdot q^{r(n-r)}} = \frac{(q^n-1)\cdots(q-1)}{(q^r-1)\cdots(q-1)(q^{n-r}-1)\cdots(q-1)}$$

$$= \frac{(q^n-1)\cdots(q^{n-r+1}-1)}{(q^r-1)\cdots(q-1)}. \tag{2.8}$$

The expression in (2.8) is called the *Gaussian binomial coefficient*, and it is denoted by $\binom{n}{r}_q$ (there are many analogies with the usual binomial coefficients; in any case, note that $\lim_{q\to 1} \binom{n}{r}_q = \binom{n}{r}$).

Exercise 2.25. Prove the following properties of Gaussian binomial coefficients:

i) $\binom{n}{r}_q = q^r \binom{n-1}{r}_q + \binom{n-1}{r-1}_q$ (generalized Pascal identity).
ii) Using i) and induction on n, show that if $\lambda_{n,r}(j)$ denotes the number of partitions of j into $\leq n-r$ parts, each of size $\leq r$, then

$$\binom{n}{r}_q = \sum_{j=0}^{r(n-r)} \lambda_{n,r}(j) q^j. \tag{2.9}$$

A variety X over $\mathbf{F}_q$ is called of *polynomial count* if there is a polynomial $P \in \mathbf{Z}[y]$ such that the number of $\mathbf{F}_{q^m}$-valued points of X is $P(q^m)$ for every $m \geq 1$. It follows from (2.6) that $\mathrm{Fl}(n)_{\mathbf{F}_q}$ is of polynomial count. Similarly, $\mathrm{Gr}(r,n)_{\mathbf{F}_q}$ is of polynomial count by (2.8) and part ii) in the above exercise.

LEMMA 2.26. *Suppose that X is a variety over $\mathbf{F}_q$, and $P(y) = a_d y^d + a_{d-1} y^{d-1} + \ldots + a_0$, with all $a_i \in \mathbf{Z}$, is such that $|X(\mathbf{F}_q^m)| = P(q^m)$ for every $m \geq 1$. In this case the zeta function of X is given by*

$$Z(X,t) = \prod_{i=0}^{d} (1 - q^i t)^{-a_i}.$$

PROOF. We have

$$\sum_{m \geq 1} \frac{N_m}{m} t^m = \sum_{i=0}^{n} a_i \sum_{m \geq 1} \frac{q^{mi}}{m} t^m = \sum_{i=0}^{n} -a_i \log(1 - q^i t).$$

Therefore by taking exp we get the formula in the lemma. □

REMARK 2.27. In the context of the lemma, if X is smooth and projective, then the analogue of the Riemann hypothesis implies that $a_i \geq 0$ for all i. In this context, we have $b_i(X) = 0$ for i odd, and $b_{2i}(X) = a_i$ for $1 \leq i \leq n$.

By combining Lemma 2.26 with Conjecture 2.18, our computations for the flag variety and the Grassmannian give the following.

COROLLARY 2.28. *The Poincaré polynomial of $\mathrm{Fl}(n)_{\mathbf{C}}$ is $\prod_{i=1}^{n}(1+y^2+\ldots+y^{2i})$, and the Poincaré polynomial of $\mathrm{Gr}(r,n)_{\mathbf{C}}$ is $\sum_{i=0}^{r(r-n)} \lambda_{n,r}(i) y^{2i}$.*

CHAPTER 3

The Weil conjectures for curves

In this chapter we consider a smooth projective curve X defined over $k = \mathbf{F}_q$. Let $\overline{k}$ denote an algebraic closure of k and $\overline{X} = X \times_{\operatorname{Spec} k} \operatorname{Spec} \overline{k}$. If $\pi\colon \overline{X} \to X$ is the natural projection, then for every quasicoherent sheaf $\mathcal{F}$ on X, we have canonical isomorphisms $H^i(X, \mathcal{F}) \otimes_k \overline{k} \simeq H^i(\overline{X}, \pi^*(\mathcal{F}))$.

We always assume that X is geometrically connected, that is, $\overline{X}$ is connected. In this case $\overline{X}$ is a smooth, irreducible, projective curve over $\overline{k}$. Since $H^0(\overline{X}, \mathcal{O}_{\overline{X}}) = \overline{k}$, we get $H^0(X, \mathcal{O}_X) = k$. Recall that the *genus* of X is $g := h^1(X, \mathcal{O}_X) = h^1(\overline{X}, \mathcal{O}_{\overline{X}})$.

Our goal in this chapter is to prove the Weil conjectures in this setting. As we have seen in Chapter 2, $Z(X, t)$ can be viewed as a generating function for effective 0-cycles on X. Since X is a curve, a 0-cycle is the same as a Weil divisor on X. We start by recalling a few generalities about divisors and line bundles on X.

A divisor on X is a finite formal combination $\sum_{i=1}^r a_i P_i$, where $a_i \in \mathbf{Z}$ and P_i is a closed point of X. One says that D is effective if $a_i \geq 0$ for all i. Note that every such divisor is automatically Cartier since X is nonsingular. The *degree* of D is $\deg(D) := \sum_i a_i \cdot [k(P_i) : k]$. The line bundle associated to D is denoted by $\mathcal{O}_X(D)$. The degree map induces a morphism of abelian groups $\deg\colon \operatorname{Pic}(X) \to \mathbf{Z}$.

Given a line bundle L on X, the set of effective divisors D on X with $\mathcal{O}_X(D) \simeq L$ is in bijection with the quotient of $H^0(X, L) \smallsetminus \{0\}$ by the action of the invertible elements in $H^0(X, \mathcal{O}_X)$ via multiplication. By assumption, $H^0(X, \mathcal{O}_X) = k$, hence this space of divisors is nonempty if and only if $H^0(X, L) \neq 0$, and in this case it is in bijection with $\mathbf{P}^{h^0(L)-1}(\mathbf{F}_q)$, hence it has $\frac{q^{h^0(L)}-1}{q-1}$ elements.

The Riemann-Roch theorem says that for every divisor D on X,

$$\chi(X, \mathcal{O}_X(D)) = \deg(D) - g + 1. \tag{3.1}$$

Furthermore, recall that if $\deg(\mathcal{O}_X(D)) \geq 2g - 1$, then $H^1(X, \mathcal{O}_X(D)) = 0$, in which case $h^0(X, \mathcal{O}_X(D)) = \deg(D) - g + 1$. We will also make use of Serre duality: if $\omega_X = \Omega_{X/k}$ is the canonical line bundle on X, then for every line bundle L on X we have $h^1(X, L) = h^0(X, \omega_X \otimes L^{-1})$. Note that $\deg(\omega_X) = 2g - 2$. All the above assertions can be proved by passing to $\overline{k}$, and using the familiar results over algebraically closed fields, see [Har, Chapter IV.1].

There is a variety $J(X)$ defined over k, with the following property: for every field extension k' of k, the k'-valued points of $J(X)$ are in natural bijection with the line bundles of degree zero on $X \times_{\operatorname{Spec} k} \operatorname{Spec} k'$. In particular, the number h of line bundles on X of degree zero is equal to $|J(X)(k)|$, hence it is finite (and, of course, positive). Note that if $\operatorname{Pic}^m(X)$ denotes the set of line bundles on X of degree m, then $\operatorname{Pic}^m(X)$ is either empty, or it has h elements (we will see below that $\operatorname{Pic}^m(X)$ is never empty).

3.1. Rationality of the zeta function

We first prove the first of the Weil conjectures. In fact, we will prove the following more precise statement below. In this section and the next one, we follow [Lor, Chapter 8].

THEOREM 3.1. *If X is a smooth, geometrically connected, projective curve of genus g over $\mathbf{F}_q$, then*

$$Z(X,t) = \frac{f(t)}{(1-t)(1-qt)},$$

where $f \in \mathbf{Z}[t]$ is a polynomial of degree $\leq 2g$, with $f(0) = 1$ and $f(1) = h$, where $h = |J(X)(\mathbf{F}_q)|$.

PROOF. It follows from Proposition 2.7 that

$$Z(X,t) = \prod_{x \in X_{\mathrm{cl}}} \frac{1}{1 - t^{\deg(x)}} = \sum_{D \geq 0} t^{\deg(D)},$$

where the last sum is over the effective divisors D on X. We will break this sum into two sums, depending on whether $\deg(D) \geq 2g-1$ or $\deg(D) \leq 2g-2$.

Let $e > 0$ be the positive integer such that $\deg(\mathrm{Pic}(X)) = e\mathbf{Z}$. For every m such that $e|m$, we have

$$|\{L \in \mathrm{Pic}(X) \mid \deg(L) = m\}| = h.$$

As we have seen, if $h^0(X,L) \geq 1$, then the number of effective divisors D with $\mathcal{O}_X(D) \simeq L$ is $\frac{q^{h^0(L)}-1}{q-1}$. In particular, if m is a nonegative integer with $m \geq 2g-1$, then for every $L \in \mathrm{Pic}(X)$ with $\deg(L) = m$, we have exactly $\frac{q^{m-g+1}-1}{q-1}$ effective divisors D with $\mathcal{O}_X(D) \simeq L$.

Let d_0 be the smallest nonnegative integer such that $d_0 e \geq 2g-1$. We deduce that

$$Z(X,t) = \sum_{D \geq 0, \deg(D) \leq 2g-2} t^{\deg(D)} + \sum_{d \geq d_0} h \frac{q^{de-g+1}-1}{q-1} t^{de}. \tag{3.2}$$

Note that the first sum in (3.2) is a polynomial in t^e of degree $\leq (2g-2)/e$. Since $\sum_{d \geq d_0} t^{de} = \frac{t^{d_0 e}}{1-t^e}$ and $\sum_{d \geq d_0} q^{de} t^{de} = \frac{(qt)^{d_0 e}}{1-(qt)^e}$, the second sum in (3.2) is equal to

$$\frac{h}{(q-1)} \cdot \left(q^{1-g} \cdot \frac{(qt)^{d_0 e}}{1-(qt)^e} - \frac{t^{d_0 e}}{1-t^e} \right). \tag{3.3}$$

We conclude that we may write

$$Z(X,t) = \frac{f(t^e)}{(1-t^e)(1-q^e t^e)}, \tag{3.4}$$

where f is a polynomial with rational coefficients of degree $\leq \max\{2 + \frac{2g-2}{e}, d_0 + 1\}$. In fact, since $Z(X,t)$ has integer coefficients, we see that f has integer coefficients, as well.

This already shows that $Z(X,t)$ is a rational function. We now show the more precise assertions in the statement of the theorem. Note first that the expression in (3.3) implies that

$$\lim_{t \to 1} (t-1) Z(X,t) = -\frac{h}{q-1} \cdot \lim_{t \to 1} \frac{t-1}{1-t^e} = \frac{h}{e(q-1)}. \tag{3.5}$$

In particular, we see that $Z(X,t)$ has a pole of order one at $t=1$.

We now show that, in fact, $e=1$. Consider $X' = X \times_{\operatorname{Spec}\mathbf{F}_q} \operatorname{Spec}\mathbf{F}_{q^e}$. We have seen in Proposition 2.14 that

$$Z(X',t^e) = \prod_{i=1}^{e} Z(X,\xi^i t),$$

where ξ is an e^{th} primitive root of 1. It follows from the formula in (3.4) that $Z(X',t^e) = Z(X,t)^e$. On the other hand, applying what we have proved so far to X', we see that $Z(X',t)$ has a pole of order one at $t=1$, and therefore $Z(X',t^e)$ has the same property. This implies that $e=1$. If $g \geq 0$, then $d_0 = 2g-1$, so that $\deg(f) \leq 2g$. On the other hand, $d_0 = 0$ if $g=0$, and the formula in (3.3) shows that $f=h$ in this case. The remaining assertions in the theorem now follow from (3.4) and (3.5). □

For future reference, we state explicitly the following result that was showed during the proof of Theorem 3.1.

COROLLARY 3.2. *If X is a smooth, geometrically connected, projective curve over $\mathbf{F}_q$, then all $\operatorname{Pic}^m(X)$ have the same (nonzero) number of elements.*

3.2. The functional equation

In our setting, if Δ is the diagonal in $\overline{X} \times \overline{X}$, then (Δ^2) can be computed via the adjunction formula: if $\ell_1 = \overline{X} \times \text{pt}$ and $\ell_2 = \text{pt} \times \overline{X}$, then $(\ell_1^2) = 0 = (\ell_2^0)$, $(\ell_1 \cdot \ell_2) = 1$, and $(\Delta \cdot \ell_1) = 1 = (\Delta \cdot \ell_2)$. Therefore we have

$$2g-2 = (\Delta \cdot (\Delta + (2g-2)\ell_1 + (2g-2)\ell_2)) = (\Delta^2) + 2(2g-2).$$

Hence $(\Delta^2) = 2-2g$, and the statement of the second Weil conjecture for curves becomes the following.

THEOREM 3.3. *If X is a smooth, geometrically connected, projective curve over $\mathbf{F}_q$, then*

$$Z(X,1/qt) = q^{1-g}t^{2-2g}Z(X,t).$$

PROOF. As we will see, the key ingredient in the proof is Serre duality. If $g=0$, it follows from Theorem 3.1 that $Z(X,t) = \frac{h}{(1-t)(1-qt)}$, and the formula in the theorem is straightforward in this case. Hence from now on we may assume that $g \geq 1$. We follow the approach to $Z(X,t) = \sum_{D \geq 0} t^D$ used in the previous section.

Recall that for every line bundle $L \in \operatorname{Pic}(X)$ with $h^0(L) \geq 1$, the effective divisors D with $\mathcal{O}(D) \simeq L$ form the $\mathbf{F}_q$-points of a projective space $\mathbf{P}^{h^0(L)-1}$, hence there are $\frac{q^{h^0(L)}-1}{q-1}$ such divisors. Using the fact that $h^0(L) = \deg(L) - g + 1$ when $\deg(L) \geq 2g-1$ and Corollary 3.2, we conclude that

(3.6)
$$Z(X,t) = \sum_{m=0}^{2g-2} \left(\sum_{L \in \operatorname{Pic}^m(X)} \frac{q^{h^0(L)}-1}{q-1} \right) t^m + \sum_{m \geq 2g-1} h \frac{q^{d-g+1}-1}{q-1} t^d = S_1 + S_2,$$

where

$$S_1 = \sum_{m=0}^{2g-2} \sum_{L \in \operatorname{Pic}^m(X)} \frac{q^{h^0(L)}}{q-1} t^m, \quad S_2 = -\frac{h}{q-1} \cdot \frac{1}{1-t} + \frac{hq^{1-g}(qt)^{2g-1}}{(q-1)(1-qt)}. \tag{3.7}$$

Note that

$$S_2(1/qt) = -\frac{h}{q-1}\cdot\frac{qt}{1-qt} - \frac{hq^{1-g}t^{2-2g}}{(q-1)(1-t)}$$

$$= q^{1-g}t^{2-2g}\cdot\left(\frac{hq^g t^{2g-1}}{(q-1)(1-qt)} - \frac{h}{(q-1)(1-t)}\right) = q^{1-g}t^{2-2g}S_2(t).$$

On the other hand, $L \to \omega_X \otimes L^{-1}$ gives a bijection between the set of line bundles on X of degree in $[0, 2g-2]$, and Serre duality plus Riemann-Roch gives $h^0(\omega_X \otimes L^{-1}) = h^0(L) - (\deg(L) - g + 1)$. Therefore

$$S_1(1/qt) = \sum_{m=0}^{2g-2}\left(\sum_{L\in \mathrm{Pic}^m(X)}\frac{q^{h^0(L)}}{q-1}\right)\left(\frac{1}{qt}\right)^m$$

$$= \sum_{m=0}^{2g-2}\left(\sum_{L\in \mathrm{Pic}^m(X)}\frac{q^{h^0(\omega_X\otimes L^{-1})}}{q-1}\right)\left(\frac{1}{qt}\right)^{2g-2-m}$$

$$= \sum_{m=0}^{2g-2}\left(\sum_{L\in \mathrm{Pic}^m(X)}\frac{q^{h^0(L)-m+g-1}}{q-1}\right)(qt)^{m+2-2g}$$

$$= t^{2-2g}q^{1-g}\sum_{m=0}^{2g-2}\left(\sum_{L\in \mathrm{Pic}^m(X)}\frac{q^{h^0(L)}}{q-1}\right)t^m = q^{1-g}t^{2-2g}S_1(t).$$

This completes the proof of the theorem. □

Remark 3.4. With the notation in Theorem 3.1, we write $f(t) = \prod_{i=1}^{2g}(1-\omega_i t)$, with $\omega_i \in \mathbf{C}$, possibly zero. We have

$$Z(X, 1/qt) = \frac{\prod_{i=1}^{2g}\left(1-\frac{\omega_i}{qt}\right)}{\left(1-\frac{1}{qt}\right)\left(1-\frac{1}{t}\right)} = \frac{qt^2(qt)^{-2g}\prod_{i=1}^{2g}(qt-\omega_i)}{(1-t)(1-qt)}$$

$$= q^{1-g}t^{2-2g}\cdot\frac{\prod_{i=1}^{2g}(1-\omega_i t)}{(1-t)(1-qt)},$$

where the last equality is a consequence of Theorem 3.3. Therefore $\prod_{i=1}^{2g}(t-\omega_i/q) = q^{-g}\cdot\prod_{i=1}^{2g}(1-\omega_i t)$.

The first consequence is that $\omega_i \neq 0$ for all i, that is, $\deg(f) = 2g$. Furthermore, we see that $\prod_{i=1}^{2g}\omega_i = q^g$, and the multiset $\{\omega_1, \ldots, \omega_{2g}\}$ is invariants under the map $x \to q/x$.

Remark 3.5. Note that the assertion in the fourth Weil conjecture in now clear in our setting. Indeed, we have $B_0 = B_2 = 1$ and $B_1 = 2g$. Recall that $E = 2-2g$, hence $E = B_0 - B_1 + B_2$. Furthermore, if X is the closed fiber of a smooth projective curve $\widetilde{X}$ over a finite type $\mathbf{Z}$-algebra R, then $\widetilde{X}_{\mathbf{C}} := \widetilde{X}\times_{\mathrm{Spec}\,R}\mathrm{Spec}\,\mathbf{C}$ is a smooth connected complex curve of genus g. Its Betti numbers are $b_0 = b_2 = 1$, and $b_1 = 2g$ (the formula for b_1 is a consequence of Hodge decomposition: $b_1(\widetilde{X}_{\mathbf{C}}) = h^0(\Omega_{\widetilde{X}_{\mathbf{C}}}) + h^1(\mathcal{O}_{\widetilde{X}_{\mathbf{C}}}) = 2g$). This proves all the assertions in the fourth Weil conjecture for X.

3.3. The analogue of the Riemann hypothesis

We use the notation for the zeta function $Z(X,t)$ introduced in Remark 3.4:

$$Z(X,t) = \frac{\prod_{i=1}^{2g}(1-\omega_i t)}{(1-t)(1-qt)}. \tag{3.8}$$

The following proves the analogue of the Riemann hypothesis in our setting.

THEOREM 3.6. *With the above notation, every ω_i is an algebraic integer, and $|\omega_i| = q^{1/2}$ for every i.*

REMARK 3.7. If we show that $|\omega_i| \leq q^{1/2}$ for every i, since the multiset $\{\omega_1, \ldots, \omega_{2g}\}$ is invariant by the map $x \to q/x$ (see Remark 3.4) we conclude that we also have $|\omega_i| \geq q^{1/2}$, hence $|\omega_i| = q^{1/2}$ for every i. The fact that the ω_i are algebraic integers is clear: since $\prod_{i=1}^{2g}(1-\omega_i t) = (1-t)(1-qt)Z(X,t)$ has integer coefficients, it follows that all elementary symmetric functions $s_j = s_j(\omega_1, \ldots, \omega_{2g})$ are integers, and ω_i is a root of $t^{2g} + \sum_{j=1}^{2j}(-1)^j s_j t^{2g-j}$.

Before proving Theorem 3.6 we make some general considerations that are very useful in general when considering zeta functions of curves. Let $N_m = |X(\mathbf{F}_{q^m})|$, and let $a_m \in \mathbf{Z}$ be defined by

$$N_m = 1 - a_m + q^m. \tag{3.9}$$

It follows from the definition of the zeta function and from (3.8) that

$$\sum_{m\geq 1}\frac{N_m}{m}t^m = \sum_{i=1}^{2g}\log(1-\omega_i t) - \log(1-t) - \log(1-qt) = \sum_{m\geq 1}\frac{1}{m}\cdot\left(1 + q^m - \sum_{i=1}^{2g}\omega_i^m\right)t^m, \tag{3.10}$$

hence $a_m = \sum_{i=1}^{2g}\omega_i^m$ for every $m \geq 1$. The following lemma rephrases the condition in Theorem 3.6 as an estimate for the integers a_m. This estimate, in fact, is responsible for many of the applications of the Weil conjectures in the case of curves.

LEMMA 3.8. *With the above notation, we have $|\omega_i| \leq g^{1/2}$ for every i if and only if $|a_m| \leq 2gq^{m/2}$ for every $m \geq 1$.*

PROOF. One implication is trivial: since $a_m = \sum_{i=1}^{2g}\omega_i^m$, if $|\omega_i| \leq q^{1/2}$ for every i, it follows that $|a_m| \leq 2g^{m/2}$. For the converse, note that

$$\sum_{m\geq 1} a_m t^m = \sum_{i=1}^{2g}\sum_{m\geq 1}\omega_i^m t^m = \sum_{i=1}^{2g}\frac{\omega_i t}{1-\omega_i t}. \tag{3.11}$$

If $|a_m| \leq 2gq^{m/2}$ for all m, then for $t \in \mathbf{C}$ with $|t| < q^{-1/2}$ we have

$$|\sum_{m\geq 1} a_m t^m| \leq 2g\sum_{m\geq 1}(q^{1/2}|t|)^m = \frac{2gq^{1/2}|t|}{1-q^{1/2}|t|}. \tag{3.12}$$

Note that (3.11) implies that the rational function $\sum_{m\geq 1} a_m t^r$ has a pole at $t = 1/\omega_i$. The estimate in (3.12) implies that $1/|\omega_i| \geq q^{-1/2}$, as required. □

We can now prove the main result of this section.

PROOF OF THEOREM 3.6. As it follows from Remark 3.7 and Lemma 3.8, it is enough to show that $|N_m - (q^m+1)| \le 2gq^{m/2}$ for every m. In fact, if we prove this for $m=1$, then we may apply this to $X \times_{\operatorname{Spec}\mathbf{F}_q} \operatorname{Spec}\mathbf{F}_{q^m}$ in order to get the bound for $|N_m - (q^m+1)|$.

We recall the description of N_1 given in Proposition 2.4. Consider the smooth projective surface $S = \overline{X} \times \overline{X}$, where $\overline{X} = X \times_{\operatorname{Spec}\mathbf{F}_q} \operatorname{Spec}\overline{\mathbf{F}}_q$. We have two divisors on S, the diagonal Δ and the graph Γ of the morphism $\mathrm{Frob}_{\overline{X},q}$ on $\overline{X}$. The two divisors intersect transversely, and the number of intersection points is $(\Gamma\cdot\Delta) = |X(\mathbf{F}_q)|$.

It is an elementary consequence of the Hodge index theorem (see Proposition 3.9 below) that if $\ell_1 = \overline{X}\times\mathrm{pt}$ and $\ell_2 = \mathrm{pt}\times\overline{X}$, then for every divisor D on S we have

$$(D^2) \le 2(D\cdot\ell_1)\cdot(D\cdot\ell_2). \tag{3.13}$$

Let us apply this for $D = a\Delta + b\Gamma$. Note that $(\Delta\cdot\ell_1) = (\Delta\cdot\ell_2) = 1$, while $(\Gamma\cdot\ell_1) = q$ and $(\Gamma\cdot\ell_2) = 1$.

We now compute (Γ^2) and (Δ^2) via the adjunction formula. Note that the canonical class K_S on S is numerically equivalent to $(2g-2)(\ell_1+\ell_2)$. Since both Δ and Γ are smooth curves of genus g, we have

$$2g-2 = (\Delta\cdot(\Delta+K_S)) = (\Delta^2) + 2(2g-2),$$

$$2g-2 = (\Gamma\cdot(\Gamma+K_S)) = (\Gamma^2) + (q+1)(2g-2).$$

Therefore $(\Delta^2) = -(2g-2)$ and $(\Gamma^2) = -q(2g-2)$.

Applying (3.13) for $D = a\Delta + b\Gamma$ gives

$$-a^2(2g-2) - qb^2(2g-2) + 2abN_1 \le 2(a+bq)(a+b).$$

After simplifying, we get

$$ga^2 - ab(q+1-N_1) + gqb^2 \ge 0.$$

Since this holds for all integer (or rational) a and b, it follows that $(q+1-N_1)^2 \le 4qg^2$. Therefore $|N_1 - (q+1)| \le 2gq^{1/2}$, as required. This completes the proof of Theorem 3.6. □

The following proposition is [**Har**, Exercise V.1.9].

PROPOSITION 3.9. *Let C_1 and C_2 be smooth projective curves over an algebraically closed field, and let $S = C_1\times C_2$. If $\ell_1 = C_1\times\mathrm{pt}$ and $\ell_2 = \mathrm{pt}\times C_2$, then for every divisor D on S we have*

$$(D^2) \le 2(D\cdot\ell_1)(D\cdot\ell_2).$$

PROOF. Recall that the Hodge index theorem says that if E is a divisor on S such that $(E\cdot H) = 0$, where H is ample, then $(E^2)\le 0$ (see [**Har**, Theorem 1.9]).

We apply this result for the ample divisor $H = \ell_1+\ell_2$, and for $E = D - (b\ell_1 + a\ell_2)$, where $a = (D\cdot\ell_1)$ and $b = (D\cdot\ell_2)$. Note that $(E\cdot H) = 0$, hence $(E^2)\le 0$. Since $(E^2) = (D^2) - 2ab$, we get the assertion in the proposition. □

EXAMPLE 3.10. Consider the case when X is an elliptic curve (that is, $g=1$). In this case it follows from Theorem 3.6 and Remark 3.4 that

$$Z(X,t) = \frac{(1-\alpha t)(1-\beta t)}{(1-t)(1-qt)} = \frac{1-at+qt^2}{(1-t)(1-qt)},$$

where $|\alpha| = |\beta| = q^{1/2}$, and $a \in \mathbf{Z}$. Note that $|X(\mathbf{F}_{q^m})| = (1 + q^m) - 2\mathrm{Re}(\alpha^m)$. In particular, $a = (1 + q) - |X(\mathbf{F}_q)|$.

CHAPTER 4

Weil cohomology theories and the Weil conjectures

Weil realized that the rationality and the functional equation part of the Weil conjectures would follow from the existence of a cohomology theory with suitable properties. Such a cohomology theory is nowadays called a *Weil cohomology theory*. In the first section we describe the axioms of such a cohomology theory, and derive some consequences. These will be used in the second section to deduce the rationality and the functional equation for the Hasse-Weil zeta function. In the last section, we give a brief introduction to the first Weil cohomology over fields of positive characteristic, the ℓ-adic cohomology.

4.1. Weil cohomology theories

In this section we work over a fixed algebraically closed field k. All varieties are defined over k. Recall that given a variety X and $r \in \mathbf{Z}_{\geq 0}$, the group of r-cycles on X is the free abelian group on the set of closed irreducible r-dimensional subvarieties of X. If V is such a variety, then we write $[V]$ for the corresponding element of the cycle group. For a closed subscheme Z of X of pure dimension r, the cycle of Z is $[Z] = \sum_{i=1}^{r} \ell(\mathcal{O}_{Z,Z_i})[Z_i]$, where the Z_i are the irreducible components of Z, and $\mathcal{O}_{Z,Z_i}$ is the zero-dimensional local ring of Z at the generic point of Z_i.

Our presentation of the formalism of Weil cohomology theories follows with small modifications and a few extra details de Jong's note [deJ1]. A Weil cohomology theory with coefficients in the characteristic zero field K is given by the following data:

(D1) A contravariant functor $X \to H^*(X) = \oplus_i H^i(X)$ from nonsingular, connected, projective varieties (over k) to graded commutative[1] K-algebras. The product of $\alpha, \beta \in H^*(X)$ is denoted by $\alpha \cup \beta$.

(D2) For every nonsingular, connected, projective algebraic variety X, a linear *trace* map $\mathrm{Tr} = \mathrm{Tr}_X \colon H^{2\dim(X)}(X) \to K$.

(D3) For every nonsingular, connected, projective algebraic variety X, and for every closed irreducible subvariety $Z \subseteq X$ of codimension c, a *cohomology class* $\mathrm{cl}(Z) \in H^{2c}(X)$.

The above data is supposed to satisfy the following set of axioms.

(A1) For every nonsingular, connected, projective variety X, all $H^i(X)$ have finite dimension over K. Furthermore, $H^i(X) = 0$ unless $0 \leq i \leq 2\dim(X)$.

(A2) (Künneth property) If X and Y are nonsingular, connected, projective varieties, and if $p_X \colon X \times Y \to X$ and $p_Y \colon X \times Y \to Y$ are the canonical

[1] Recall that *graded commutative* means that $\alpha\beta = (-1)^{\deg(\alpha)\deg(\beta)}\beta\alpha$ for every homogeneous elements α and β.

projections, then the K-algebra homomorphism

$$H^*(X) \otimes_K H^*(Y) \to H^*(X \times Y),\ \alpha \otimes \beta \to p_X^*(\alpha) \cup p_Y^*(\beta)$$

is an isomorphsim.

(A3) (Poincaré duality) For every nonsingular, connected, projective variety X, the trace map $\mathrm{Tr}\colon H^{2\dim(X)}(X) \to K$ is an isomorphism, and for every i with $0 \le i \le 2\dim(X)$, the bilinear map

$$H^i(X) \otimes_K H^{2\dim(X)-i}(X) \to K,\ \alpha \otimes \beta \to \mathrm{Tr}_X(\alpha \cup \beta)$$

is a perfect pairing.

(A4) (Trace maps and products) For every nonsingular, connected, projective varieties X and Y, we have

$$\mathrm{Tr}_{X\times Y}(p_X^*(\alpha) \cup p_Y^*(\beta)) = \mathrm{Tr}_X(\alpha)\mathrm{Tr}_Y(\beta)$$

for every $\alpha \in H^{2\dim(X)}(X)$ and $\beta \in H^{2\dim(Y)}(Y)$.

(A5) (Exterior product of cohomology classes) For every nonsingular, connected, projective varieties X and Y, and every closed irreducible subvarieties $Z \subseteq X$ and $W \subseteq Y$, we have

$$\mathrm{cl}(Z \times W) = p_X^*(\mathrm{cl}(Z)) \cup p_Y^*(\mathrm{cl}(W)).$$

(A6) (Push-forward of cohomology classes) For every morphism $f\colon X \to Y$ of nonsingular, connected, projective varieties, and for every irreducible closed subvariety $Z \subseteq X$, we have for every $\alpha \in H^{2\dim(Z)}(Y)$

$$\mathrm{Tr}_X(\mathrm{cl}(Z) \cup f^*(\alpha)) = \deg(Z/f(Z)) \cdot \mathrm{Tr}_Y(\mathrm{cl}(f(Z)) \cup \alpha).$$

(A7) (Pull-back of cohomology classes) Let $f\colon X \to Y$ be a morphism of nonsingular, connected, projective varieties, and $Z \subseteq Y$ an irreducible closed subvariety that satisfies the following conditions:

a) All irreducible components $W_1, \dots, W_r$ of $f^{-1}(Z)$ have pure dimension $\dim(Z) + \dim(X) - \dim(Y)$.

b) Either f is flat in a neighborhood of Z, or Z is *generically transverse* to f, in the sense that $f^{-1}(Z)$ is generically smooth.

Under these assumptions, if $[f^{-1}(Z)] = \sum_{i=1}^r m_i W_i$, then $f^*(\mathrm{cl}(Z)) = \sum_{i=1}^r m_i \mathrm{cl}(W_i)$ (note that if Z is generically transverse to f, then $m_i = 1$ for all i).

(A8) (Case of a point) If $x = \mathrm{Spec}(k)$, then $\mathrm{cl}(x) = 1$ and $\mathrm{Tr}_x(1) = 1$.

A basic example of a Weil cohomology theory is given by singular cohomology in the case $k = \mathbf{C}$, when we may take $K = \mathbf{Q}$. In the last section we will discuss an example of a Weil cohomology theory when $\mathrm{char}(k) = p > 0$, the ℓ-adic cohomology (with $K = \mathbf{Q}_\ell$, for some $\ell \neq p$). Another example, still when $\mathrm{char}(k) > 0$, is given by crystalline cohomology (with $K = W(k)$, the ring of Witt vectors of k).

In the rest of this section we assume that we have a Weil cohomology theory for varieties over k, and deduce several consequences. In particular, we relate the Chow ring of X to $H^*(X)$. We will review below some of the basic definitions related to Chow rings. For our applications in the next section, the main result is the trace formula in Theorem 4.7 below.

PROPOSITION 4.1. *Let X be a smooth, connected, n-dimensional projective variety.*

i) *The structural morphism $K \to H^0(X)$ is an isomorphism.*

ii) *We have* $\mathrm{cl}(X) = 1 \in H^0(X)$.
iii) *If* $x \in X$ *is a closed point, then* $\mathrm{Tr}_X(\mathrm{cl}(x)) = 1$.
iv) *If* $f\colon X \to Y$ *is a generically finite, surjective morphism of degree* d *between smooth, connected, projective varieties,* $\mathrm{Tr}_X(f^*(\alpha)) = d \cdot \mathrm{Tr}_Y(\alpha)$ *for every* $\alpha \in H^{2\dim(Y)}(Y)$. *In particular, if* $Y = X$, *then* f^* *acts as multiplication by* d *on* $H^{2\dim(X)}(X)$.

Proof. Applying condition (A3) with $i = 0$ implies that $\dim_K H^0(X) = 1$, hence the structural morphism of the K-algebra $H^*(X)$ induces an isomorphism $K \simeq H^0(X)$. Applying condition (A7) to the morphism $X \to \operatorname{Spec} k$, as well as condition (A8), we get $\mathrm{cl}(X) = 1 \in H^0(X)$.

Given $x \in X$, let us apply condition (A6) to the morphism $X \to \operatorname{Spec} k$, by taking $Z = \{x\}$ and $\alpha = 1 \in H^0(\operatorname{Spec} k)$. We deduce using also (A8) that $\mathrm{Tr}_X(\mathrm{cl}(x)) = 1$.

If $f\colon X \to Y$ is as in iv), let us choose a general point Q in Y. If the cycle of the fiber $f^{-1}(Q)$ is $[f^{-1}(Q)] = \sum_{i=1}^r m_i P_i$, then by hypothesis $\sum_{i=1}^r m_i = d$. Since f is flat around Q by generic flatness, condition (A7) implies

$$\mathrm{Tr}_X(f^*(\mathrm{cl}(Q))) = \mathrm{Tr}_X(\sum_i m_i \cdot \mathrm{cl}(P_i)) = d \cdot \mathrm{Tr}_Y(\mathrm{cl}(Q)).$$

Since $\mathrm{cl}(Q)$ generates $H^{2\dim(Y)}(Y)$, this proves the assertion in iv). □

We now use Poincaré duality to define push-forwards in cohomology. Let $f\colon X \to Y$ be a morphism between nonsingular, connected, projective varieties, with $\dim(X) = m$ and $\dim(Y) = n$. Given $\alpha \in H^i(X)$, there is a unique $f_*(\alpha) \in H^{2n-2m+i}(Y)$ such that

$$\mathrm{Tr}_Y(f_*(\alpha) \cup \beta) = \mathrm{Tr}_X(\alpha \cup f^*(\beta))$$

for every $\beta \in H^{2m-i}(Y)$. It is clear that f_* is K-linear. The following proposition collects the basic properties of the push-forward map.

Proposition 4.2. *Let* $f\colon X \to Y$ *be a morphism as above.*

i) *(Projection formula)* $f_*(\alpha \cup f^*(\gamma)) = f_*(\alpha) \cup \gamma$.
ii) *If* $g\colon Y \to Z$ *is another morphism, with* Z *smooth, connected, and projective, then* $(g \circ f)_* = g_* \circ f_*$ *on* $H^*(X)$.
iii) *If* Z *is an irreducible, closed subvariety of* X, *then*

$$f_*(\mathrm{cl}(Z)) = \deg(Z/f(Z))\mathrm{cl}(f(Z)).$$

Proof. Properties i) and ii) follow easily from definition, using Poincaré duality. Property iii) is a consequence of (A6). □

Proposition 4.3. *Let* X *and* Y *be nonsingular, connected, projective varieties, and* $p\colon X \times Y \to X$ *and* $q\colon X \times Y \to Y$ *the canonical projections. If* $\alpha \in H^i(Y)$, *then* $p_*(q^*(\alpha)) = \mathrm{Tr}_Y(\alpha)$ *if* $i = 2\dim(Y)$, *and* $p_*(q^*(\alpha)) = 0$, *otherwise.*

Proof. Note that $p_*(q^*(\alpha)) \in H^{i-2\dim(Y)}(X)$, hence it is clear that $p_*(q^*(\alpha)) = 0$ when $i \neq 2\dim(Y)$. On the other hand, if $\alpha \in H^{2\dim(Y)}(Y)$ and $\beta \in H^{2\dim(X)}(X)$, then

$$\mathrm{Tr}_X(p_*(q^*(\alpha)) \cup \beta) = \mathrm{Tr}_{X\times Y}(q^*(\alpha) \cup p^*(\beta)) = \mathrm{Tr}_Y(\alpha)\mathrm{Tr}_X(\beta),$$

where the last equality follows from condition (A4). Therefore $p_*(q^*(\alpha)) = \mathrm{Tr}_Y(\alpha)$. □

Our next goal is to show that taking the cohomology class induces a ring homomorphism from the Chow ring $A^*(X)$ to $H^{2*}(X)$, the even part of the cohomology ring. Before doing this, let us review a few facts about Chow rings. For details and proofs, we refer to [Ful1, Chapters I-VIII].

Let X be an arbitrary variety over k. The Chow group $A_r(X)$ is the quotient of $Z_r(X)$ by the rational equivalence relation. Recall that this equivalence relation is generated by putting $\mathrm{div}_W(\phi) \sim 0$, where W is an $(r+1)$-dimensional closed irreducible subvariety of X, and ϕ is a nonzero rational function of X. We do not give the general definition of $\mathrm{div}_W(\phi)$, but only mention that for W normal, this is the usual definition of the principal divisor corresponding to a rational function. In particular, if ϕ defines a morphism $\widetilde{\phi}\colon W \to \mathbf{P}^1$, then $\mathrm{div}_W(\phi) = [\widetilde{\phi}^{-1}(0)] - [\widetilde{\phi}^{-1}(\infty)]$.

For a proper morphism $f\colon X \to Y$ one defines $f_*\colon Z_r(X) \to Z_r(Y)$ such that for an irreducible variety V of X, $f_*([V]) = \deg(V/f(V))[f(V)]$. One shows that if ϕ is a nonzero rational function on an $(r+1)$-dimensional irreducible closed subvariety W of X, one has $f_*(\mathrm{div}_W(\phi)) = 0$ if $\dim(f(W) < \dim(V)$, and $f_*(\mathrm{div}_W(\phi)) = \mathrm{div}_{f(W)}(N(\phi))$, otherwise, where $N\colon K(f(W)) \to K(W)$ is the norm map. Therefore we get an induced morphism $f_*\colon A_r(X) \to A_r(Y)$. Note that when X is complete, the induced map $\deg\colon A_0(X) \to A_0(\mathrm{Spec}\, k) = \mathbf{Z}$ is given by taking the degree of a cycle. We extend this map by defining it to be zero on $A_i(X)$ with $i \neq 0$.

If X is nonsingular, connected, and $\dim(X) = n$, then one puts $A^i(X) = A_{n-i}(X)$, and $A^*(X) = \oplus_{i=0}^n A^i(X)$ has a structure of commutative graded ring. One denotes by $\alpha \cup \beta$ the product of $\alpha, \beta \in A^*(X)$. If X is complete, and $\alpha_1, \ldots, \alpha_r \in A^*(X)$, then the intersection number $(\alpha_1 \cdot \ldots \cdot \alpha_r)$ is given by $\deg(\alpha_1 \cup \ldots \cup \alpha_r)$.

Taking X to $A^*(X)$ gives, in fact, a contravariant functor from the category of nonsingular quasiprojective[2] varieties to that of graded rings. One defines the pull-back $f^*\colon A^*(Y) \to A^*(X)$ of a morphism $f\colon X \to Y$ of nonsingular varieties in terms of a suitable (refined) intersection product. For us, it is enough to use the following property: if Z is an irreducible subvariety of Y such that $f^{-1}(Z)$ has pure dimension $\dim(Z) + \dim(X) - \dim(Y)$, and either f is flat in a neighborhood of Z, or Z is generically transverse to f, then $f^*([Z]) = [f^{-1}(Z)]$. In fact, one can always reduce to one of these two situations: every f admits the decomposition

$$X \overset{j}{\hookrightarrow} X \times Y \overset{\mathrm{pr}_Y}{\to} Y,$$

where $j = (\mathrm{Id}_X, f)$ is the graph of f. Therefore

$$f^*([Z]) = j^*(\mathrm{pr_Y}^*([Z])) = j^*([X \times Z]).$$

Furthermore, by the Moving Lemma, $[X \times Z]$ is rationally equivalent with a sum $\sum_\ell n_\ell [W_\ell]$, with each W_ℓ generically transverse to j. Therefore $f^*([Z]) = \sum_\ell n_\ell [j^{-1}(W_\ell)]$.

The product of $A^*(X)$ can be described in terms of pull-back, as follows. If Z_1 and Z_2 are irreducible closed subvarieties of X, then

$$[Z_1] \cup [Z_2] = \Delta^*([Z_1 \times Z_2]) \in A^*(X),$$

[2]This assumption is only made for convenience, since we want to use the Moving Lemma, and since we are concerned with projective varieties.

where $\Delta\colon X \hookrightarrow X \times X$ is the diagonal embedding. In particular, suppose that Z_1 and Z_2 are generically transverse, in the sense that all irreducible components $W_1 \ldots, W_r$ of $Z_1 \cap Z_2$ have dimension $\dim(Z_1) + \dim(Z_2) - \dim(X)$, and $Z_1 \cap Z_2$ is generically smooth. In this case $Z_1 \times Z_2$ is generically transverse to Δ, hence $[Z_1] \cup [Z_2] = \sum_{\ell=1}^{r} [W_\ell]$.

Suppose now that we have a Weil cohomology theory for varieties over k. If X is a smooth, connected, projective n-dimensional variety over k, taking the cohomology class induces a group homomorphism $\mathrm{cl}\colon Z_r(X) \to H^{2(n-r)}(X)$. Note that if $f\colon X \to Y$ is a morphism of such varieties, then it follows from Proposition 4.2 iii) that

$$f_*(\mathrm{cl}(\alpha)) = \mathrm{cl}(f_*(\alpha)). \tag{4.1}$$

LEMMA 4.4. *If $\alpha = \sum_{i=1}^{r} n_i[V_i]$ is an r-cycle that is rationally equivalent to zero, then $\sum_i n_i \mathrm{cl}(V_i) = 0$ in $A^{2(n-r)}(X)$.*

PROOF. We may assume that there is an irreducible $(r+1)$-dimensional subvariety W of X, and a nonzero rational function ϕ on W such that $\alpha = \mathrm{div}_W(\phi)$. We have a rational map $\widetilde{\phi}\colon W \dashrightarrow \mathbf{P}^1$ defined by ϕ. Let $\pi\colon W' \to W$ be a projective, generically finite morphism, with W' an integral scheme, such that $\widetilde{\phi} \circ \pi$ is a morphism $\widetilde{\psi}$. After possibly replacing W' by a nonsingular alteration (see [deJ2]), we may assume that W' is nonsingular, connected, and projective. If $d = \deg(W'/W)$ and $\psi = f^*(\phi) \in K(W')$, then we have the equality of cycles $f_*(\mathrm{div}(\psi)) = d \cdot \mathrm{div}(\phi)$. Since $\mathrm{char}(K) = 0$, it follows from (4.1) that it is enough to show that $\mathrm{cl}(\mathrm{div}(\psi)) = 0$ in $H^*(W')$. On the other hand, by construction we have $\mathrm{div}(\psi) = [\widetilde{\psi}^{-1}(0)] - [\widetilde{\psi}^{-1}(\infty)]$, and condition (A7) implies that it is enough to show that $\mathrm{cl}(0) = \mathrm{cl}(\infty) \in H^1(\mathbf{P}^1)$. This follows from assertion iii) in Proposition 4.1. □

The above lemma implies that for every nonsingular, connected, projective n-dimensional variety X, we have a morphism of graded groups $\mathrm{cl}\colon A^*(X) \to H^{2*}(X)$.

PROPOSITION 4.5. *The morphism $\mathrm{cl}\colon A^*(X) \to H^{2*}(X)$ is a ring homomorphism. Furthermore, it is compatible with both f^* and f_*.*

PROOF. Compatibility with f_* follows from (4.1). We next show compatibility with f^*, where $f\colon X \to Y$ is a morphism between nonsingular, connected, projective varieties. Writing f as the composition $X \xhookrightarrow{j} X \times Y \xrightarrow{p_Y} Y$, we note that $f^* = j^* \circ p_Y^*$ both at the level of H^* and at the level of A^*. The fact that taking the cohomology class commutes with both p_Y^* and j^* is a consequence of condition (A7) (and, in the case of j^*, of the Moving Lemma).

We now show that cl is a ring homomorphism. If V and W are irreducible subvarieties of X, and $\Delta\colon X \hookrightarrow X \times X$ is the diagonal embedding, then using the compatibility with pull-back and condition (A5) we get

$$\begin{aligned}\mathrm{cl}([V] \cup [W]) &= \mathrm{cl}(\Delta^*([V \times W])) = \Delta^*(\mathrm{cl}(V \times W)) = \Delta^*(p_X^*(\mathrm{cl}(V)) \cup p_Y^*(\mathrm{cl}(W))) \\ &= \Delta^*(p_X^*(\mathrm{cl}(V))) \cup \Delta^*(p_Y^*(\mathrm{cl}(W))) = \mathrm{cl}(V) \cup \mathrm{cl}(W).\end{aligned}$$

□

COROLLARY 4.6. *If X is a smooth, connected, projective variety, and $\alpha_i \in A^{m_i}(X)$ for $1 \le i \le r$ are such that $m_1 + \ldots + m_r = \dim(X)$, then $(\alpha_1 \cdot \ldots \cdot \alpha_r) = \mathrm{Tr}_X(\mathrm{cl}(\alpha_1) \cup \ldots \cup \mathrm{cl}(\alpha_r))$.*

PROOF. Since the map $\mathrm{cl}\colon A^*(X) \to H^{2*}(X)$ is a ring homomorphism, it is enough to show that for $\alpha \in Z_0(X)$, we have $\deg(\alpha) = \mathrm{Tr}_X(\mathrm{cl}(\alpha))$. By additivity, we may assume $\alpha = P$, in which case it is enough to apply assertion iii) in Proposition 4.1. □

THEOREM 4.7. (*The trace formula*) *If $\phi\colon X \to X$ is an endomorphism of the nonsingular, connected, projective variety X, and if $\Gamma_\phi, \Delta \subset X \times X$ are the graph of ϕ, and respectively, the diagonal, then*

$$(\Gamma_\phi \cdot \Delta) = \sum_{i=0}^{2\dim(X)} (-1)^i \mathrm{trace}(\phi^* | H^i(X)).$$

In particular, if Γ_ϕ and Δ intersect transversely, then the above expression computes $|\{x \in X \mid \phi(x) = x\}|$.

We will apply this result in the next section by taking ϕ to be the Frobenius morphism. On the other hand, by taking ϕ to be the identity, we obtain the following

PROPOSITION 4.8. *If X is a smooth, connected, n-dimensional projective variety, and $\Delta \subset X \times X$ is the diagonal, then*

$$(\Delta^2) = \sum_{i=0}^{2n} (-1)^i \dim_K H^i(X).$$

We give the proof of Theorem 4.7 following [Mil, Chapter VI, §12]. We need two lemmas. With the notation in Theorem 4.7, let $\dim(X) = n$, and let $p, q\colon X \times X \to X$ denote the projections onto the first, respectively second, component.

LEMMA 4.9. *If $\alpha \in H^*(X)$, then $p_*(\mathrm{cl}(\Gamma_\phi) \cup q^*(\alpha)) = \phi^*(\alpha)$.*

PROOF. Let $j\colon X \hookrightarrow X \times X$ be the embedding onto the graph of ϕ, so that $p \circ j = \mathrm{Id}_X$ and $q \circ j = \phi$. Since $j_*(\mathrm{cl}(X)) = \mathrm{cl}(\Gamma_\phi)$, we deduce using the projection formula

$$p_*(\mathrm{cl}(\Gamma_\phi) \cup q^*(\alpha)) = p_*(j_*(\mathrm{cl}(X)) \cup q^*(\alpha)) = p_*(j_*(\mathrm{cl}(X) \cup j^*(q^*(\alpha)))) = p_*(j_*(\phi^*(\alpha)))$$
$$= \phi^*(\alpha).$$

□

LEMMA 4.10. *Let (e_i^r) be a basis of $H^r(X)$ and (f_i^{2n-r}) the dual basis of $H^{2n-r}(X)$ with respect to Poincaré duality, such that $\mathrm{Tr}_X(f_\ell^{2n-r} \cup e_i^r) = \delta_{i,\ell}$. With this notation, we have*

$$\mathrm{cl}(\Gamma_\phi) = \sum_{i,r} p^*(\phi^*(e_i^r)) \cup q^*(f_i^{2n-r}) \in H^{2n}(X \times X).$$

PROOF. We know by the Künneth property that we can write

$$\mathrm{cl}(\Gamma_\phi) = \sum_{\ell,s} p^*(a_{\ell,s}) \cup q^*(f_\ell^{2n-s}),$$

for unique elements $a_{\ell,s} \in H^s(X)$. It follows from Lemma 4.9 and the projection formula that that

$$\phi^*(e_i^r) = \sum_{\ell,s} p_*(p^*(a_{\ell,s}) \cup q^*(f_\ell^{2n-s}) \cup q^*(e_i^r)) = \sum_{\ell,s} a_{\ell,s} \cup p_*(q^*(f_\ell^{2n-s} \cup e_i^r)).$$

Lemma 4.3 implies that $p_*(q^*(f_\ell^{2n-s} \cup e_i^r)$ is zero, unless $r = s$, in which case it is equal to $\mathrm{Tr}_X(f_\ell^{2n-r} \cup e_i^r)$. By assumption, this is zero, unless $i = \ell$, in which case it is equal to 1. We conclude that $\phi^*(e_i^r) = a_{i,r}$. □

Proof of Theorem 4.7. It follows from Lemma 4.10 that

$$\mathrm{cl}(\Gamma_\phi) = \sum_{i,r} p^*(\phi^*(e_i^r)) \cup q^*(f_i^{2n-r}).$$

Applying the same lemma to the identity morphism, and to the dual bases (f_ℓ^s) and $((-1)^s e_\ell^{2n-s})$, we get

$$\mathrm{cl}(\Delta) = \sum_{\ell,s} (-1)^s p^*(f_\ell^s) \cup q^*(e_\ell^{2n-s}).$$

Therefore we obtain

$$(\Gamma_\phi \cdot \Delta) = \mathrm{Tr}_{X\times X}(\mathrm{cl}(\Gamma_\phi) \cup \mathrm{cl}(\Delta))$$

$$= \mathrm{Tr}_{X\times X}\left(\sum_{i,j,r,s} (-1)^{s+s(2n-r)} p^*(\phi^*(e_i^r) \cup f_\ell^s) \cup q^*(f_i^{2n-r} \cup e_\ell^{2n-s})\right)$$

$$= \sum_{i,r} \mathrm{Tr}_X(\phi^*(e_i^r) \cup f_i^{2n-r}) \cdot \mathrm{Tr}_X(f_i^{2n-r} \cup e_i^r) = \sum_r (-1)^r \mathrm{trace}(\phi^* | H^r(X)).$$

□

4.2. Rationality and the functional equation via Weil cohomology

In this section we assume that we have a Weil cohomology theory for varieties over $k = \overline{\mathbf{F}_p}$, and show how to get the statements of Conjectures 2.15 and 2.16 for varieties over $\mathbf{F}_{p^e}$. We start with the rationality of the zeta function. As we have seen in § 2.2, given a variety X defined over $\mathbf{F}_q$, with $q = p^e$, we have the q-Frobenius morphism $\mathrm{Frob}_{X,q}\colon X \to X$ (a morphism over $\mathbf{F}_q$). Furthermore, if $\overline{X} = X \times_{\mathrm{Spec}\,\mathbf{F}_q} \mathrm{Spec}\,k$, then we have an endomorphism $F := \mathrm{Frob}_{\overline{X},q} = \mathrm{Frob}_{X,q} \times \mathrm{Id}$ of $\widetilde{X}$. Note that $\mathrm{Frob}_{\overline{X},q^m} = F^m$.

Theorem 4.11. *If X is a nonsingular, geometrically connected, n-dimensional projective variety over $\mathbf{F}_q$, then*

$$Z(X,t) = \frac{P_1(t) \cdot P_3(t) \cdots P_{2n-1}(t)}{P_0(t) \cdot P_2(t) \cdots P_{2n}(t)},$$

where for every i with $0 \le i \le 2n$ we have $P_i(t) = \det(\mathrm{Id} - tF^* | H^i(\overline{X}))$. In particular, $Z(X,t) \in \mathbf{Q}(t)$.

We will make use of the following general formula for the characteristic polynomial of a linear endomorphism.

Lemma 4.12. *For every endomorphism ϕ of a finite dimensional vector space V over a field K, we have*

$$\det(\mathrm{Id} - t\phi) = \exp\left(-\sum_{m\ge 1} \mathrm{trace}(\phi^m | V) \frac{t^m}{m}\right).$$

PROOF. After replacing K by its algebraic closure $\overline{K}$, V by $\overline{V} = V \otimes_K \overline{K}$, and ϕ by $\phi \otimes_K \overline{K} \colon \overline{V} \to \overline{V}$, we may assume that K is algebraically closed. After choosing a suitable basis for V, we may assume that ϕ is represented by an upper diagonal matrix. If the entries on the diagonal are $a_1, \ldots, a_d$, then $\det(\mathrm{Id} - t\phi) = (1 - a_1 t) \cdots (1 - a_d t)$. On the other hand,

$$\exp\left(-\sum_{m\geq 1} \mathrm{trace}(\phi^m | V)\frac{t^m}{m}\right) = \exp\left(-\sum_{m\geq 1}\sum_{i=1}^{d} \frac{a_i^m t^m}{m}\right) = \exp\left(\sum_{i=1}^{d} \log(1 - a_i t)\right)$$

$$= \prod_{i=1}^{d} (1 - a_i t).$$

□

PROOF OF THEOREM 4.11. Let $N_m = |X(\mathbf{F}_{q^m})|$. As we have seen in § 2.2, we have $N_m = |\{x \in \overline{X} \mid F^m(x) = x\}|$. Furthermore, the graph $\Gamma_m \subset \overline{X} \times \overline{X}$ of F^m is transverse to the diagonal, hence by Theorem 4.7 we have $N_m = \sum_{i=0}^{2n} (-1)^i \mathrm{trace}((F^m)^* | H^i(\overline{X}))$. Using Lemma 4.12, we get

$$Z(X, t) = \exp\left(\sum_{m\geq 1}\sum_{i=0}^{2n} (-1)^i \mathrm{trace}((F^*)^m | H^i(\overline{X}))\frac{t^m}{m}\right)$$

$$= \prod_{i=0}^{2n} \det(\mathrm{Id} - tF^* | H^i(\overline{X}))^{(-1)^{i+1}}.$$

This clearly shows that $Z(X, t)$ lies in $K(t)$. On the other hand, since $Z(X, t) \in \mathbf{Q}[\![t]\!]$, the proposition below shows that $Z(X, t)$ lies in $\mathbf{Q}(t)$. □

PROPOSITION 4.13. *Let L be an arbitrary field, and $f = \sum_{m\geq 0} a_m t^m \in L[\![t]\!]$. We have $f \in L(t)$ if and only if there are nonnegative integers M and N such that the linear span of the vectors*

$$\{(a_i, a_{i+1}, \ldots, a_{i+N}) \in L^{\oplus(N+1)} \mid i \geq M\} \tag{4.2}$$

is a proper subspace of $L^{\oplus(N+1)}$. In particular, if L'/L is a field extension, then f lies in $L'(t)$ if and only if it lies in $L(t)$.

PROOF. We have $f \in L(t)$ if and only if there are nonnegative integers M and N, and $c_0, \ldots, c_N \in L$, not all zero, such that $f(t) \cdot \sum_{i=0}^{N} c_i t^i$ is a polynomial of degree $< M + N$. In other words, we need

$$c_N a_i + c_{N-1} a_{i+1} + \ldots + c_0 a_{i+N} = 0 \text{ for all } i \geq M. \tag{4.3}$$

This condition holds precisely when the linear function $\ell(x_0, \ldots, x_N) = \sum_{j=0}^{N} c_{N-j} x_j$ vanishes on the linear span of the vectors in (4.2), hence the first assertion in the proposition. The second assertion follows from the fact that if $v_1, \ldots, v_r$ are elements of a vector space V over L, then $v_1, \ldots, v_r$ are linearly independent if and only if $v_1 \otimes 1, \ldots, v_r \otimes 1$ are linearly independent over L' in $V \otimes_L L'$. □

We now turn to the functional equation. We keep the same assumption and notation as in Theorem 4.11.

THEOREM 4.14. *If X is a nonsingular, geometrically connected, n-dimensional projective algebraic variety over $\mathbf{F}_q$, and $E = (\Delta^2)$, where $\Delta \subset \overline{X} \times \overline{X}$ is the diagonal, we have*

$$Z(X, 1/q^n t) = \pm q^{nE/2} t^E Z(X, t).$$

The key ingredient is the following linear algebra lemma (see [**Har**, Lemma 4.3, App. C]).

LEMMA 4.15. *Let $\phi\colon V \times W \to K$ be a perfect pairing of vector spaces of dimension r over the field K. If $\lambda \in K \smallsetminus \{0\}$ and $f \in \mathrm{End}_K(V)$ and $g \in \mathrm{End}_K(W)$ are such that $\phi(f(v), g(w)) = \lambda\phi(v, w)$ for every $v \in V$, $w \in W$, then*

$$\det(\mathrm{Id} - tg|W) = \frac{(-1)^r \lambda^r t^r}{\det(f|V)} \det(\mathrm{Id} - \lambda^{-1} t^{-1} f|V) \tag{4.4}$$

and

$$\det(g|W) = \frac{\lambda^r}{\det(f|V)}. \tag{4.5}$$

PROOF. After replacing K by its algebraic closure $\overline{K}$, and extending the scalars to $\overline{K}$, we may assume that K is algebraically closed. In this case we can find a basis $e_1, \dots, e_r$ of V such that if we write $f(e_i) = \sum_{j=1}^r a_{i,j} e_j$, we have $a_{i,j} = 0$ for $i > j$. Let $e'_1, \dots, e'_r$ be the basis of W such that $\phi(e_i, e'_j) = \delta_{i,j}$ for every i and j.

Note that g is invertible: if $g(w) = 0$, then $0 = \phi(f(v), g(w)) = \lambda\phi(v, w)$ for every $v \in V$, hence $w = 0$. Since $\phi(f(e_i), e'_j) = 0$ for $j < i$, we deduce that $\phi(e_i, g^{-1}(e'_j)) = 0$. If we write $g^{-1}(e'_j) = \sum_{\ell=1}^r b_{j,\ell} e'_\ell$, we have $b_{j,i} = 0$ for $i > j$. Furthermore,

$$a_{j,j} = \phi(f(e_j), e'_j) = \lambda\phi(e_j, g^{-1}(e'_j)) = \lambda b_{j,j}.$$

Since $\det(f|V) = \prod_{i=1}^r a_{i,i}$ and $\det(g|W) = \prod_{j=1}^r b_{j,j}^{-1} = \lambda^r / \prod_{i=1}^r a_{i,i}$, we get (4.5). We also have

$$\det(\mathrm{Id} - tg|W) = \det(g|W) \cdot \det(g^{-1} - t\mathrm{Id}|W) = \frac{\lambda^r}{\det(f|V)} \cdot \prod_{j=1}^r (a_{j,j}\lambda^{-1} - t)$$

$$= \frac{(-1)^r \lambda^r t^r}{\det(f|V)} \cdot \prod_{j=1}^r (1 - a_{j,j}\lambda^{-1} t^{-1}) = \frac{(-1)^r \lambda^r t^r}{\det(f|V)} \det(\mathrm{Id} - \lambda^{-1} t^{-1} f|V).$$

□

PROOF OF THEOREM 4.14. We apply the lemma to the perfect pairing given by Poincaré duality:

$$\phi_i\colon H^i(\overline{X}) \otimes H^{2n-i}(\overline{X}) \to H^{2n}(\overline{X}) \to K, \ \phi_i(\alpha \otimes \beta) = \mathrm{Tr}(\alpha \cup \beta).$$

Note that $F\colon \overline{X} \to \overline{X}$ is a finite morphism of degree q^n: indeed, it is enough to show that $\mathrm{Frob}_{X,q}\colon X \to X$ has this property. Arguing as in the proof of Proposition 2.4, we reduce the assertion to the case $X = \mathbf{A}^n$, when it follows from the fact that $k[x_1, \dots, x_n]$ is free of rank q^n over $k[x_1^q, \dots, x_n^q]$.

Proposition 4.1 implies that F^* is given by multiplication by q^n on $H^{2n}(\overline{X})$. Therefore

$$\phi_i(F^*(\alpha), F^*(\beta)) = \mathrm{Tr}_{\overline{X}}(F^*(\alpha \cup \beta)) = \mathrm{Tr}_{\overline{X}}(q^d \alpha \cup \beta) = q^d \phi_i(\alpha, \beta),$$

for every $\alpha \in H^i(\overline{X})$ and $\beta \in H^{2n-i}(\overline{X})$. Lemma 4.15 implies that if we put $B_i = \dim_K H^i(\overline{X})$ and $P_i(t) = \det(\mathrm{Id} - tF^*|H^i(\overline{X}))$, then

$$\det(F^*|H^{2n-i}(\overline{X})) = q^{nB_i}/\det(F^*|H^i(\overline{X})) \text{ and} \tag{4.6}$$

$$P_{2n-i}(t) = \frac{(-1)^{B_i} q^{nB_i} t^{B_i}}{\det(F^*|H^i(\overline{X}))} P_i(1/q^n t). \tag{4.7}$$

Using (4.6), (4.7) and Theorem 4.11, as well as the fact that $E = \sum_{i=0}^{2n} (-1)^i B_i$ by Proposition 4.8, we deduce

$$Z(1/q^n t) = \prod_{i=0}^{2n} P_i(1/q^n t)^{(-1)^{i+1}} = \prod_{i=0}^{2n} P_{2n-i}(t)^{(-1)^{i+1}} \cdot \frac{(-1)^E q^{nE} t^E}{\prod_{i=0}^{2n} \det(F^*|H^i(\overline{X}))^{(-1)^i}}$$

$$= \pm Z(X,t) \cdot \frac{q^{nE} t^E}{q^{nE/2}} = \pm q^{nE} t^E Z(X,t).$$

□

Remark 4.16. It follows from the above proof that the sign in the functional equation is $(-1)^{E+a}$, where $a = 0$ if $\det(F^* \mid H^i(\overline{X})) = q^{nB_n/2}$, and $a = 1$ if $\det(F^* \mid H^i(\overline{X})) = -q^{nB_n/2}$. If we write $P_n(t) = \prod_{i=1}^{B_n}(1 - \alpha_i t)$, an easy computation using the identity (4.7) for $i = n$ implies that the multiset $\{\alpha_1, \ldots, \alpha_{B_n}\}$ is invariant under $\alpha \to q^{B_n}/\alpha$, and $\prod_{i=1}^{B_n} \alpha_i = (-1)^a q^{nB_n/2}$. Therefore a has the same parity as the number of α_i equal to $-q^{n/2}$.

4.3. A brief introduction to ℓ-adic cohomology

In this section we give a brief overview of étale cohomology, in general, and of ℓ-adic cohomology, in particular. Needless to say, we will only describe the basic notions and results. For details and for proofs, the reader is referred to [Del1] or [Mil].

The basic idea behind étale topology is to replace the Zariski topology on an algebraic variety by a different topology. In fact, this is not a topology in the usual sense, but a *Grothendieck topology*. Sheaf theory, and in particular sheaf cohomology still make sense in this setting, and this allows the definition of ℓ-adic cohomology.

As a motivation, note that in the case of a smooth, projective, complex algebraic variety we would like to recover the singular cohomology, with suitable coefficients There are two ways of doing this algebraically. The first one consists in taking the hypercohomology of the de Rham complex. This approach, however, is known to produce pathologies in positive characteristic. The second approach consists in "refining" the Zariski topology, which as it stands, does not reflect the classical topology. The key is the notion of étale morphism. It is worth recalling that a morphism of complex algebraic varieties is étale if and only if it is a local analytic isomorphism *in the classical topology*.

Let X be a fixed Noetherian scheme. The role of the open subsets of X will be played by the category $\acute{\mathrm{E}}\mathrm{t}(X)$ of étale schemes $Y \to X$ over X. Instead of considering inclusions between open subsets, we consider morphisms in $\acute{\mathrm{E}}\mathrm{t}(X)$ (note that if Y_1 and Y_2 are étale schemes over X, any morphism $Y_1 \to Y_2$ of schemes over X is étale). The category $\acute{\mathrm{E}}\mathrm{t}(X)$ has fiber products. The role of open covers is

played by *étale covers*: these are families $(U_i \xrightarrow{f_i} U)_i$ of étale schemes over X such that $U = \bigcup_i f_i(U_i)$. The set of étale covers of U is denoted by $\mathrm{Cov}(U)$.

What makes this data into a Grothendieck topology is the fact that it satisfies the following conditions:

(C1) If $\phi\colon U \to V$ is an isomorphism in $\text{Ét}(X)$, then $(\phi) \in \mathrm{Cov}(V)$.
(C2) If $(U_i \to U)_i \in \mathrm{Cov}(U)$ and for every i we have $(U_{i,j} \to U_i)_j \in \mathrm{Cov}(U_i)$, then $(U_{i,j} \to U)_{i,j} \in \mathrm{Cov}(U)$.
(C3) If $(U_i \to U)_i \in \mathrm{Cov}(U)$, and $V \to U$ is a morphism in $\text{Ét}(X)$, then we have $(U_i \times_U V \to V)_i \in \mathrm{Cov}(V)$.

This Grothendieck topology is the *étale topology* on X.

It follows from definition that if $U \in \text{Ét}(X)$, and if $(U_i)_i$ is an open cover of U, then $(U_i \to U)_i$ is in $\mathrm{Cov}(U)$. Another important type of cover is the following. A finite étale morphism $V \to U$ is a *Galois cover* with group G if G acts (on the right) on V over U, and if the natural morphism

$$\bigsqcup_{g \in G} V_g \to V \times_U V,\ y \in V_g \to (y, yg)$$

is an isomorphism, where $V_g = V$ for every $g \in G$. Note that this is a G-equivariant isomorphism if we let G act on the left-hand side so that $h \in G$ takes V_g to V_{gh} via the identity map. It is a general fact that every finite étale morphism $V \to U$ can be dominated by a Galois cover $W \to U$.

Once we have a Grothendieck topology on X, we can extend the notions of presheaves and sheaves. An étale presheaf on X (say, of abelian groups) is a contravariant functor from $\text{Ét}(X)$ to the category of abelian groups. An étale presheaf $\mathcal{F}$ is a sheaf if for every $U \in \text{Ét}(X)$ and every étale cover $(U_i \to U)_i$, the following complex

$$0 \to \mathcal{F}(U) \to \prod_i \mathcal{F}(U_i) \to \prod_{i,j} \mathcal{F}(U_i \times_U U_j)$$

is exact. In particular, $\mathcal{F}$ defines a sheaf $\mathcal{F}_U$ on U, in the usual sense, for every U in $\text{Ét}(X)$. On the other hand, if $V \to U$ is a Galois cover in $\text{Ét}(X)$ with group G, then the corresponding condition on $\mathcal{F}$ is that $\mathcal{F}(U) \simeq \mathcal{F}(V)^G$ (note that G has a natural action on $\mathcal{F}$ since $\mathcal{F}$ is a presheaf). Let us consider some examples of étale sheaves.

Example 4.17. If $\mathcal{M}$ is a quasi-coherent sheaf of $\mathcal{O}_X$-modules on X (in the usual sense), then we put for $U \xrightarrow{f} X$ in $\text{Ét}(X)$

$$W(\mathcal{M})(U) = \Gamma(U, f^*(\mathcal{M})).$$

It is a consequence of faithfully flat descent that $W(\mathcal{M})$ is an étale sheaf on X. Abusing notation, we usually denote $W(\mathcal{M})$ simply by $\mathcal{M}$.

Example 4.18. If A is any abelian group, then we get an étale *constant sheaf* on X that takes every $U \to X$ in $\text{Ét}(X)$ to $A^{\pi_0(U)}$, where $\pi_0(U)$ is the set of connected components of U. This is denoted by A_X, but whenever the scheme X is understood, we drop the subscript.

Example 4.19. Suppose that $\mathbf{G}$ is an abelian group scheme over X. We may consider $\mathbf{G}$ as an étale presheaf on X by defining for $U \to X$ in $\text{Ét}(X)$, $\mathbf{G}(U) = \mathrm{Hom}_X(U, \mathbf{G})$. It is another consequence of faithfully flat descent that $\mathbf{G}$

is an étale sheaf on X. For example, if $\mathbf{G} = \mathbf{G}_m = X \times_{\operatorname{Spec} \mathbf{Z}} \operatorname{Spec} \mathbf{Z}[t, t^{-1}]$, then $\mathbf{G}_m(U)$ is the set $\mathcal{O}(U)^*$ of invertible elements in $\mathcal{O}(U)$. Another example is given by the closed subscheme

$$\mu_n = X \times_{\operatorname{Spec} \mathbf{Z}} \operatorname{Spec} \mathbf{Z}[t]/(t^n - 1) \hookrightarrow \mathbf{G}_m.$$

In this case we have $\mu_n(U) = \{u \in \mathcal{O}_X(U) \mid u^n = 1\}$.

Example 4.20. As a last example, consider the case when $X = \operatorname{Spec} k$, where k is a field. Note that in this case an object in $\text{Ét}(X)$ is just a disjoint union of finitely many $\operatorname{Spec} K_i$, where the K_i are finite, separable extensions of k. It is clear that every étale sheaf $\mathcal{F}$ over X is determined by its values $M_K := \mathcal{F}(\operatorname{Spec} K)$, for K/k as above. Furthermore, $G(K/k)$ has an induced action on M_K, and for every Galois extension L/K of finite, separable extensions of k, we have a functorial isomorphism $M_K \simeq (M_L)^{G(L/K)}$. Let $M := \varinjlim_{K/k} M_K$. This carries a continuous action of $G = G(k^{\text{sep}}/k)$, where k^{sep} is a separable closure of k (the action being continuous means that the stabilizer of every element in M is an open subgroup of G). One can show that this defines an equivalence of categories between the category of étale sheaves on $\operatorname{Spec} k$ and the category of abelian groups with a continuous G-action.

Suppose now that X is an arbitrary Noetherian scheme. It is easy to see that the category $\mathbf{Psh}_{\text{ét}}(X)$ of étale presheaves on X is an abelian category. If $\mathbf{Sh}_{\text{ét}}(X)$ is the category of étale sheaves on X, then one can show that the natural inclusion $\mathbf{Psh}_{\text{ét}}(X) \hookrightarrow \mathbf{Sh}_{\text{ét}}(X)$ has a left adjoint, that takes an étale presheaf $\mathcal{F}$ to the associated étale sheaf. Using this, one can show that also $\mathbf{Sh}_{\text{ét}}(X)$ is an abelian category. We note that a complex of étale sheaves on X

$$\mathcal{F}' \xrightarrow{u} \mathcal{F} \xrightarrow{v} \mathcal{F}''$$

is exact if and only if for every $U \to X$ in $\text{Ét}(X)$, every $a \in \mathcal{F}(U)$ such that $v(a) = 0$, and every $x \in U$, there is $f\colon V \to U$ in $\text{Ét}(X)$ with $x \in f(V)$, such that the image of a in $\mathcal{F}(V)$ lies in $\operatorname{Im}(\mathcal{F}'(V) \to \mathcal{F}(V))$.

Example 4.21. Suppose that X is a scheme over $\mathbf{F}_p$, and let us assume, for simplicity, that X is integral. There is an important exact sequence of étale sheaves on X, the *Artin-Schreier sequence*, given by

$$0 \longrightarrow (\mathbf{F}_p)_X \longrightarrow \mathcal{O}_X \xrightarrow{\text{Frob}_p - \text{Id}} \mathcal{O}_X \longrightarrow 0, \tag{4.8}$$

where for every $U \to X$ in $\text{Ét}(X)$, we recall that $\text{Frob}_p\colon \mathcal{O}_X(U) \to \mathcal{O}_X(U)$ is given by $u \to u^p$. It is clear that $(\mathbf{F}_p)_X$ is the kernel of $\text{Frob}_p - \text{Id}$: this follows from the fact that for every domain A over $\mathbf{F}_p$, we have $\mathbf{F}_p = \{a \in A \mid a^p = a\}$. Note that $\text{Frob}_p - \text{Id}$ is surjective on $\mathcal{O}_X$ (for the étale topology). Indeed, given any Noetherian ring A and $a \in A$, the morphism $\phi\colon A \to B = A[t]/(t^p - t - a)$ is étale and surjective, and there is $b = t \in B$ such that $\phi(a) = b^p - b$.

Example 4.22. Suppose now that X is a scheme over a field k, and n is a positive integer, not divisible by $\operatorname{char}(k)$. In this case we have an exact sequence of étale sheaves, the *Kummer sequence*

$$0 \to \mu_\ell \to \mathbf{G}_m \xrightarrow{n} \mathbf{G}_m \to 0.$$

In order to see that the morphism $\mathbf{G}_m \to \mathbf{G}_m$ that takes $u \to u^n$ is surjective, it is enough to note that for every k-algebra A, and every $a \in A$, the natural morphism $\phi\colon A \to B = A[t]/(t^n - a)$ is étale and surjective, and there is $b = t \in B$, such that $\phi(a) = t^n$.

Note that if k is separably closed, then it is clear that for every k-algebra that is an integral domain, we have $\{u \in A \mid u^n = 1\} \subseteq k$. Suppose, for simplicity, that X is an integral scheme. In this case, the choice of a primitive n^{th} root of 1 gives an isomorphism $\mu_n \simeq (\mathbf{Z}/n\mathbf{Z})_X$.

If $f\colon X \to Y$ is a morphism of Noetherian schemes, for every $U \to Y$ in $\text{Ét}(Y)$, we have $X \times_Y U \to X$ in $\text{Ét}(X)$. Furthermore, if $(U_i \to U)_i$ is an étale cover of U, then $(X \times_Y U_i \to X \times_Y U)_i$ is an étale cover of $X \times_Y U$. Using this, it is easy to see that we have a functor $f_*\colon \mathbf{Sh}_{\text{ét}}(X) \to \mathbf{Sh}_{\text{ét}}(Y)$, such that $f_*(\mathcal{F})(U) = \mathcal{F}(X \times_Y U)$. This is a left exact functor, and one can show that it has a left adjoint, denoted by f^*. For example, we have $f^*(A_Y) \simeq A_X$.

One can show that the category $\mathbf{S}h_{\text{ét}}(X)$ has enough injectives. In particular, for every $U \to X$ in $\text{Ét}(X)$ we can consider the right derived functors of the left exact functor $\mathcal{F} \to \mathcal{F}(U)$. These are written as $H^i_{\text{ét}}(U, \mathcal{F})$, for $i \geq 0$.

EXAMPLE 4.23. If $\mathcal{M}$ is a quasi-coherent sheaf on X, and $W(\mathcal{M})$ is the corresponding étale sheaf associated to $\mathcal{M}$ as in Example 4.17, then one can show that there are canonical isomorphisms $H^i(X, \mathcal{M}) \simeq H^i_{\text{ét}}(X, W(\mathcal{M}))$.

EXAMPLE 4.24. Let $X = \operatorname{Spec} k$, where k is a field. If we identify an étale sheaf on X with an abelian group M with a continuous G-action, where $G = G(k^{\text{sep}}/k)$, then the functor of taking global sections for the sheaf gets identified to the functor $M \to M^G$. Therefore its derived functors are given precisely by the Galois cohomology functors.

EXAMPLE 4.25. One can show that as in the case of the Zariski topology, there is an isomorphism $H^1_{\text{ét}}(X, \mathbf{G}_m) \simeq \operatorname{Pic}(X)$. Suppose now that X is an integral scheme over a separably closed field k, and n is a positive integer that is not divisible by $\operatorname{char}(k)$. It follows from Example 4.22 that we have an exact sequence

$$\Gamma(X, \mathcal{O}_X)^* \xrightarrow{\alpha} \Gamma(X, \mathcal{O}_X)^* \to H^1_{\text{ét}}(X, \mathbf{Z}/n\mathbf{Z}) \to \operatorname{Pic}(X) \xrightarrow{\beta} \operatorname{Pic}(X),$$

where both α and β are given by taking the n^{th}-power.

EXAMPLE 4.26. Suppose that X is an integral scheme over $\mathbf{F}_p$. The Artin-Schreier exact sequence from Example 4.21, together with the assertion in Example 4.23 implies that we have a long exact sequence of cohomology

(4.9)

$$\ldots \longrightarrow H^i_{\text{ét}}(X, \mathbf{F}_p) \longrightarrow H^i(X, \mathcal{O}_X) \xrightarrow{\text{Id} - \text{Frob}_p} H^i(X, \mathcal{O}_X) \longrightarrow H^{i+1}_{\text{ét}}(X, \mathbf{F}_p) \ldots.$$

Suppose now that X is complete over a field k, so each $H^i(X, \mathcal{O}_X)$ is finite-dimensional over k. Since $\text{Frob}_p\colon H^i(X, \mathcal{O}_X) \to H^i(X, \mathcal{O}_X)$ has the property that $\text{Frob}_p(au) = a^p \text{Frob}_p(u)$, it is a general fact that if k is algebraically closed, the morphism $\text{Id} - \text{Frob}_p$ is always surjective. It follows that under this assumption, the above long exact sequence breaks into short exact sequences

$$0 \longrightarrow H^i_{\text{ét}}(X, \mathbf{F}_p) \longrightarrow H^i(X, \mathcal{O}_X) \xrightarrow{\text{Id} - \text{Frob}_p} H^i(X, \mathcal{O}_X) \longrightarrow 0. \tag{4.10}$$

It turns out that it is particularly interesting to compute the étale cohomology of schemes with coefficients in finite abelian groups. The basic computation is that of the étale cohomology groups of a curve. In fact, the proofs of the fundamental results about étale cohomology are reduced to the case of curves via involved *dévissage* arguments.

THEOREM 4.27. *Let X be a smooth, connected, projective curve, over an algebraically closed field k. If n is a positive integer that is not divisible by* $\mathrm{char}(k)$*, then there are canonical isomorphisms*

$$H^0_{\acute{e}t}(X, \mu_n) \simeq \mu_n(\operatorname{Spec} k),$$
$$H^1_{\acute{e}t}(X, \mu_n) \simeq \{L \in \operatorname{Pic}(X) \mid L^n \simeq \mathcal{O}_X\},$$
$$H^2_{\acute{e}t}(X, \mu_n) \simeq \mathbf{Z}/n\mathbf{Z},$$

while $H^i_{\acute{e}t}(X, \mu_n) = 0$ for $i > 2$.

The key point is to show that $H^i_{\text{ét}}(X, \mathbf{G}_m) = 0$ for $i \geq 2$. This is deduced from a theorem of Tsen, saying that every nonconstant homogeneous polynomial $f \in k[x_1, \ldots, x_n]$ of degree $< n$ has a nontrivial zero. The assertions in the above theorem then follow from the long exact sequence in cohomology corresponding to the Kummer exact sequence. Note that $\mu_n(\operatorname{Spec} k)$ is non-canonically isomorphic to $\mathbf{Z}/n\mathbf{Z}$. Furthermore, every $L \in \operatorname{Pic}(X)$ such that $L^n \simeq \mathcal{O}_X$ lies in $\operatorname{Pic}^0(X)$. Since $\operatorname{Pic}^0(X)$ consists of the k-rational points of a g-dimensional abelian variety over k (where g is the genus of X), it follows that

$$\{L \in \operatorname{Pic}(X) \mid L^n \simeq \mathcal{O}_X\} \simeq (\mathbf{Z}/n\mathbf{Z})^{2g}$$

(see [**Mum1**, p. 60]). Furthermore, multiplication by n is surjective on $\operatorname{Pic}^0(X)$ (see [**Mum1**, p. 40]), which gives the isomorphism $H^2_{\text{ét}}(X, \mu_n) \simeq \mathbf{Z}/n\mathbf{Z}$ in the theorem.

REMARK 4.28. When the characteristic of k divides n, the ranks of the cohomology groups $H^i_{\text{ét}}(X, \mathbf{Z}/n\mathbf{Z})$ do not behave as expected. Suppose, for example, that X is an elliptic curve defined over an algebraically closed field of characteristic $p > 0$. It follows from the exact sequence (4.10) that $\dim_{\mathbf{F}_p} H^1_{\text{ét}}(X, \mathbf{Z}/p\mathbf{Z}) \leq 1$ (compare with the fact that for a prime $\ell \neq p$, we have $\dim_{\mathbf{F}_\ell} H^1_{\text{ét}}(X, \mathbf{Z}/p\mathbf{Z}) = 2$). On the other hand, this étale cohomology group detects interesting information about the elliptic curve: it follows from the exact sequence (4.10) that $\dim_{\mathbf{F}_p} H^1_{\text{ét}}(X, \mathbf{Z}/p\mathbf{Z}) = 1$ if and only if the Frobenius action on $H^1(X, \mathcal{O}_X)$ is nonzero (in this case one says that X is *ordinary*; otherwise, it is *supersingular*).

The ℓ-adic cohomology groups are defined as follows. Let k be an algebraically closed field, and let ℓ be a prime different from $\mathrm{char}(k)$ (in case this is positive). For every $i \geq 0$, and every $m \geq 1$, consider the $\mathbf{Z}/\ell^m\mathbf{Z}$-module $H^i_{\text{ét}}(X, \mathbf{Z}/\ell^m\mathbf{Z})$. We have obvious maps

$$H^i_{\text{ét}}(X, \mathbf{Z}/\ell^{m+1}\mathbf{Z}) \to H^i_{\text{ét}}(X, \mathbf{Z}/\ell^m\mathbf{Z})$$

and one puts

$$H^i_{\text{ét}}(X, \mathbf{Z}_\ell) := \varprojlim_m H^i_{\text{ét}}(X, \mathbf{Z}/\ell^m\mathbf{Z}).$$

This has a natural structure of $\mathbf{Z}_\ell$-module, where $\mathbf{Z}_\ell$ is the ring of ℓ-adic integers, and one defines

$$H^i_{\text{ét}}(X, \mathbf{Q}_\ell) := H^i_{\text{ét}}(X, \mathbf{Z}_\ell) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell.$$

It is worth pointing out that taking cohomology does *not* commute with projective limits, hence $H^i_{\text{ét}}(X, \mathbf{Z}_\ell)$ is *not* the étale cohomology group of X with coefficients in the constant sheaf $\mathbf{Z}_\ell$. It follows from the fundamental theorems on étale cohomology that when restricting to smooth, connected, projective varieties over k, one gets in this way a Weil cohomology theory with coefficients in $\mathbf{Q}_\ell$ (see [Mil, Chapter VI]).

In particular, if X is a smooth, geometrically connected, n-dimensional projective variety over $\mathbf{F}_q$, with $q = p^e$, let ℓ be a prime different from p. Theorem 4.11 gives the following expression for the zeta function of X:

$$Z(X,t) = \frac{P_1(t)\cdot P_3(t)\cdots P_{2n-1}(t)}{P_0(t)\cdot P_2(t)\cdots P_{2n}(t)}, \tag{4.11}$$

where $P_i(t) = \det\left(\mathrm{Id} - tF^* | H^i_{\text{ét}}(X \times_k \overline{k}, \mathbf{Q}_\ell)\right)$.

Furthermore, general results about étale cohomology give a proof for the Weil conjecture relating the zeta function $Z(X,t)$ with the Betti numbers for singular cohomology (see Conjecture 2.18). Note first that we have already seen the first assertion in this conjecture: with the above notation, Proposition 4.8 gives $\sum_{i\geq 0}(-1)^i \deg(P_i) = (\Delta^2)$, where $\Delta \subseteq X \times X$ is the diagonal. Suppose now that $\widetilde{X}$ is a smooth projective scheme over a finitely generated $\mathbf{Z}$-subalgebra R of $\mathbf{C}$, and $P \in \mathrm{Spec}(R)$ is such that $R/P = \mathbf{F}_q$, and $\widetilde{X} \times_{\mathrm{Spec}\, R} \mathrm{Spec}\, \mathbf{F}_q = X$. It is a consequence of the smooth base change theorem (see [Mil, Corollary VI.4.2]) that there are isomorphisms

$$H^i_{\text{ét}}(X, \mathbf{Z}/\ell^m\mathbf{Z}) \simeq H^i_{\text{ét}}(\widetilde{X} \times_{\mathrm{Spec}\, R} \mathrm{Spec}\, \mathbf{C}, \mathbf{Z}/\ell^m\mathbf{Z}).$$

Furthermore, a comparison theorem between singular and étale cohomology (see [Mil, Theorem III.3.12]) implies that the étale and singular cohomology groups of smooth complex varieties, with coefficients in finite abelian groups are isomorphic. In particular,

$$H^i_{\text{ét}}(\widetilde{X} \times_{\mathrm{Spec}\, R} \mathrm{Spec}\, \mathbf{C}, \mathbf{Z}/\ell^m\mathbf{Z}) \simeq H^i(\widetilde{X}(\mathbf{C})^{\mathrm{an}}, \mathbf{Z}/\ell^m\mathbf{Z}).$$

After taking the projective limit over $m \geq 1$, and tensoring with $\mathbf{Q}_\ell$, we get

$$H^i_{\text{ét}}(X, \mathbf{Q}_\ell) \simeq H^i(\widetilde{X}(\mathbf{C})^{\mathrm{an}}, \mathbf{Q}_\ell).$$

Therefore we have $\deg(P_i) = \dim_{\mathbf{Q}} H^i(\widetilde{X}(\mathbf{C})^{\mathrm{an}}, \mathbf{Q})$, proving the fourth of the Weil conjectures.

The fundamental result of Deligne [Del1], settling the hardest of the Weil conjectures, the analogue of the Riemann Hypothesis, is the following.

THEOREM 4.29. *If X is a smooth, geometrically connected, projective variety over $\mathbf{F}_q$, and $F = \mathrm{Frob}_{\overline{X},q}$ is the induced Frobenius morphism on $\overline{X} = X \times_k \overline{k}$, then*

$$\det\left(\mathrm{Id} - tF^* | H^i_{\acute{e}t}(\overline{X}, \mathbf{Q}_\ell)\right) = \prod_i (1 - \alpha_i t) \in \mathbf{Z}[t],$$

and for every choice of an isomorphism $\mathbf{Q}_\ell \simeq \mathbf{C}$, we have $|\alpha_i| = q^{i/2}$ for all i.

We mention that one can give a proof for the rationality of the zeta function for arbitrary varieties in the setting of ℓ-adic cohomology. The point is that if k is an algebraically closed field of characteristic p, and ℓ is a prime different from p, then for every separated variety over k one can define ℓ-adic cohomology groups

with compact supports $H^i_c(Y, \mathbf{Q}_\ell)$. These are always finite-dimensional $\mathbf{Q}_\ell$-vector spaces, and they are zero unless $0 \leq i \leq 2\dim(Y)$.

If X is a separated variety over a finite field $\mathbf{F}_q$, and if $F = \mathrm{Frob}_{\overline{X},q}$ is the Frobenius endomorphism of $\overline{X} = X \times_k \overline{k}$, then one has the following formula for the zeta function of X (see [Mil, Theorem VI.13.1]):

$$Z(X,t) = \prod_{i \geq 0} \det(F^* \mid H^i_c(\overline{X}, \mathbf{Q}_\ell)^{(-1)^{i+1}}.$$

In particular, it follows that $Z(X,t)$ is a rational function, and this implies the rationality of the zeta function for every variety over $\mathbf{F}_q$.

CHAPTER 5

Fulton's trace formula for coherent sheaf cohomology

Our goal in this chapter is to give a proof, following [Ful3], of a trace formula for the Frobenius action on the cohomology of the structure sheaf.

5.1. The statement of the main theorem

Suppose that X is a scheme over the finite field $k = \mathbf{F}_q$. Recall that we have the q-Frobenius morphism $F = \mathrm{Frob}_{X,q} \colon X \to X$, whose corresponding morphism of sheaves $\mathcal{O}_X \to F_*(\mathcal{O}_X) = \mathcal{O}_X$ is given by $u \to u^q$. This is an $\mathbf{F}_q$-linear morphism, and therefore we get induced $\mathbf{F}_q$-linear actions $F \colon H^i(X, \mathcal{O}_X) \to H^i(X, \mathcal{O}_X)$.

THEOREM 5.1. *If X is a projective scheme over a finite field $\mathbf{F}_q$, then*

$$|X(\mathbf{F}_q)| \bmod p = \sum_{i=0}^{\dim(X)} (-1)^i \mathrm{trace}(F | H^i(X, \mathcal{O}_X)). \tag{5.1}$$

REMARK 5.2. Note that we have $|X(\mathbf{F}_q)| = |X_{\mathrm{red}}(\mathbf{F}_q)|$. However, it is not a priori clear that the term on the right-hand side of (5.1) only depends on the reduced scheme structure of X.

REMARK 5.3. Given X as in the above theorem, let $X_m = X \times_{\mathrm{Spec}\,\mathbf{F}_q} \mathrm{Spec}\,\mathbf{F}_{q^m}$. Note that $\mathrm{Frob}_{X_m, q^m} = \mathrm{Frob}_{X,q}^m \times \mathrm{Id}$, and we have a canonical isomorphism

$$H^i(X_m, \mathcal{O}_{X_m}) \simeq H^i(X, \mathcal{O}_X) \otimes_{\mathbf{F}_q} \mathbf{F}_{q^m}.$$

By applying the theorem for X_m, we get

$$|X(\mathbf{F}_{q^m})| \bmod p = \sum_{i=0}^{\dim(X)} (-1)^i \mathrm{trace}(F^m | H^i(X, \mathcal{O}_X)).$$

Recall from § 2.2 that we may identify $X(\mathbf{F}_q)$ with the closed points $x \in X$ with $k(x) = \mathbf{F}_q$. In what follows we will often make this identification without any further comment.

A stronger congruence formula was proved be Deligne [Del2] and Katz [Katz]. In fact, we will also prove a strengthening of the above statement, but in a different direction. The first extension is to sheaves with a Frobenius action.

A coherent F-module on X is a coherent sheaf $\mathcal{M}$ on X, together with a *Frobenius action* on $\mathcal{M}$, that is, a morphism of sheaves of $\mathcal{O}_X$-modules $F_{\mathcal{M}} \colon \mathcal{M} \to F_*(\mathcal{M})$. In other words, $F_{\mathcal{M}}$ is a morphism of sheaves of $\mathbf{F}_q$-vector spaces $\mathcal{O}_X \to \mathcal{O}_X$ such that $F_{\mathcal{M}}(am) = a^q F_{\mathcal{M}}(m)$ for every $a \in \mathcal{O}_X(U)$ and $m \in \mathcal{M}(U)$, where U is any open subset of X. As above, since $F_{\mathcal{M}}$ is $\mathbf{F}_q$-linear, it follows that it induces $\mathbf{F}_q$-linear maps on cohomology that, abusing notation, we write $F_{\mathcal{M}} \colon H^i(X, \mathcal{M}) \to$

$H^i(X, \mathcal{M})$. Despite the fact that $F_{\mathcal{M}}$ is not $\mathcal{O}_X$-linear, for every $x \in X(\mathbf{F}_q)$ we get an $\mathbf{F}_q$-linear endomorphism of $\mathcal{M}(x) := \mathcal{M}_x \otimes k(x)$, that we denote by $F_{\mathcal{M}}(x)$.

THEOREM 5.4. *If X is a projective scheme over $\mathbf{F}_q$, and $(\mathcal{M}, F_{\mathcal{M}})$ is a coherent F-module on X, we have*

$$\sum_{x \in X(\mathbf{F}_q)} \operatorname{trace}(F_{\mathcal{M}}(x)) = \sum_{i=0}^{\dim(X)} (-1)^i \operatorname{trace}(F_{\mathcal{M}} | H^i(X, \mathcal{M})). \tag{5.2}$$

An obvious example of a coherent F-module on X is given by $(\mathcal{O}_X, F)$. Note that if $x \in X(\mathbf{F}_q)$, then $F(x)$ is the identity on $\mathcal{O}_X(x) = \mathbf{F}_q$. Therefore the result in Theorem 5.1 is a special case of the one in Theorem 5.4.

In fact, Theorem 5.4 will follow from a result describing the Grothendieck group of coherent F-modues. Given a scheme X of finite type over $\mathbf{F}_q$, consider the category $\mathcal{C}oh_F(X)$ consisting of coherent F-modules. A morphism $(\mathcal{M}, F_{\mathcal{M}}) \to (\mathcal{M}', F_{\mathcal{M}'})$ in this category is a morphism $f\colon \mathcal{M} \to \mathcal{M}'$ of coherent sheaves, such that $f \circ F_{\mathcal{M}} = F_{\mathcal{M}'} \circ f$. It is easy to see that if f is a morphism of coherent F-modules, then $\operatorname{Ker}(f)$ and $\operatorname{Coker}(f)$ have induced Frobenius actions that makes them coherent F-modules. We thus see that $\mathcal{C}oh_F(X)$ is an abelian category. Whenever the Frobenius action is understood, we simply write $\mathcal{M}$ instead of $(\mathcal{M}, F_{\mathcal{M}})$.

The Grothendieck group $K_\bullet^F(X)$ of coherent F-modules is the quotient of the free abelian group on isomorphism classes of coherent F-modules $(\mathcal{M}, F_{\mathcal{M}})$ as above, by the following type of relations:

(A) $(\mathcal{M}, F_{\mathcal{M}}) = (\mathcal{M}', F_{\mathcal{M}}) + (\mathcal{M}'', F_{\mathcal{M}''})$, for every exact sequence
$$0 \to (\mathcal{M}', F_{\mathcal{M}'}) \to (\mathcal{M}, F_{\mathcal{M}'}) \to (\mathcal{M}'', F_{\mathcal{M}''}) \to 0.$$

(B) $(\mathcal{M}, F_1 + F_2) = (\mathcal{M}, F_1) + (\mathcal{M}, F_2)$ for every morphisms of $\mathcal{O}_X$-modules $F_1, F_2\colon \mathcal{M} \to F_*(\mathcal{M})$, where $\mathcal{M}$ is a coherent sheaf on X.

Given a coherent F-module $(\mathcal{M}, F_{\mathcal{M}})$, we denote by $[\mathcal{M}, F_{\mathcal{M}}]$ its class in the Grothendieck group. Note that $K_\bullet^F(X)$ is, in fact, an $\mathbf{F}_q$-vector space, with $\lambda \cdot [\mathcal{M}, F_{\mathcal{M}}] = [\mathcal{M}, \lambda F_{\mathcal{M}}]$.

LEMMA 5.5. *We have an isomorphism $K_\bullet^F(\operatorname{Spec} \mathbf{F}_q) \simeq \mathbf{F}_q$ of $\mathbf{F}_q$-vector spaces, given by*
$$[\mathcal{M}, F_{\mathcal{M}}] \to \operatorname{trace}(F_{\mathcal{M}}(x)),$$
where x is the unique point of $\operatorname{Spec} \mathbf{F}_q$.

PROOF. Note that $\mathcal{C}oh_F(\operatorname{Spec} \mathbf{F}_q)$ is the category of pairs (V, ϕ), where V is a finite-dimensional vector space over $\mathbf{F}_q$, and ϕ is a linear endomorphism. Since $\operatorname{trace}(\phi_1 + \phi_2) = \operatorname{trace}(\phi_1) + \operatorname{trace}(\phi_2)$, and given an exact sequence $0 \to (V', \phi') \to (V, \phi) \to (V'', \phi'') \to 0$ we have $\operatorname{trace}(\phi) = \operatorname{trace}(\phi') + \operatorname{trace}(\phi'')$, taking (V, ϕ) to $\operatorname{trace}(\phi)$ gives a morphism of $\mathbf{F}_q$-vector spaces $u\colon K_\bullet^F(\operatorname{Spec} \mathbf{F}_q) \to \mathbf{F}_q$. We have a map w in the opposite direction that takes $a \in \mathbf{F}_q$ to $[\mathbf{F}_q, a \cdot \mathrm{Id}]$. It is clear that $u \circ w$ is the identity. In order to show that u and w are inverse isomorphisms, it is enough to show that w is surjective. The fact that $[V, \phi]$ lies in the image of w follows easily by induction on $\dim(V)$, since whenever $\dim(V) \geq 2$, ϕ can be written as a sum of maps, each of which has an invariant proper nonzero subspace. □

If $f\colon X \to Y$ is a proper morphism, note that the higher direct images induce functors $R^i f_*\colon \mathcal{C}oh_F(X) \to \mathcal{C}oh_F(Y)$. Indeed, if $U \subseteq Y$ is an affine open subset of Y, and $(\mathcal{M}, F_{\mathcal{M}}) \in \mathcal{C}oh_F(X)$, then $H^i(f^{-1}(U), \mathcal{M})$ has an endomorphism induced

by $F_{\mathcal{M}}$, and these endomorphisms glue together to give the Frobenius action on $R^i f_*(\mathcal{M})$. As a consequence, we get a morphism of $\mathbf{F}_q$-vector spaces $f_*\colon K_\bullet^F(X) \to K_\bullet^F(Y)$ given by $f_*([\mathcal{M}]) = \sum_{i\geq 0}(-1)^i[R^i f_*(\mathcal{M})]$. Note that this is well-defined: if

$$0 \to (\mathcal{M}', F_{\mathcal{M}'}) \to (\mathcal{M}, F_{\mathcal{M}}) \to (\mathcal{M}'', F_{\mathcal{M}''}) \to 0$$

is an exact sequence of coherent F-modules, then the long exact sequence in cohomology

$$\ldots \to R^i f_*(\mathcal{M}') \to R^i f_*(\mathcal{M}) \to R^i f_*(\mathcal{M}'') \to R^{i+1} f_*(\mathcal{M}') \to \ldots$$

is compatible with the Frobenius actions, and therefore we get

$$\sum_{i\geq 0}(-1)^i[R^i f_*(\mathcal{M})] = \sum_{i\geq 0}(-1)^i[R^i f_*(\mathcal{M}')] + \sum_{i\geq 0}(-1)^i[R^i f_*(\mathcal{M}'')] \text{ in } K_\bullet^F(Y).$$

The compatibility with the type (B) relations is straightforward, hence $f_*\colon K_\bullet^F(X) \to K_\bullet^F(Y)$ is well-defined.

EXERCISE 5.6. Use the Leray spectral sequence to show that if $g\colon Y \to Z$ is another proper morphism, then we have $(g\circ f)_* = g_* \circ f_*\colon K_\bullet^F(X) \to K_\bullet^F(Z)$.

In fact, we will only use the assertion in the above exercise when f is a closed immersion, in which case everything is clear since $R^i g_* \circ f_* = R^i(g\circ f)_*$ for all $i \geq 0$, and $R^j f_* = 0$ for all $j \geq 1$. The proof of the next lemma is straightforward.

LEMMA 5.7. *If X is the disjoint union of the subschemes $X_1, \ldots, X_r$, then the inclusions $X_i \hookrightarrow X$ induce an isomorphism*

$$\bigoplus_{i=1}^{r} K_\bullet^F(X_i) \simeq K_\bullet^F(X).$$

The following is the main result of this chapter. For a scheme X, we consider $X(\mathbf{F}_q)$ as a closed subscheme of X, with the reduced scheme structure. Note that by Lemmas 5.5 and 5.7, we have an isomorphism $K_\bullet^F(X(\mathbf{F}_q)) \simeq \oplus_{x\in X(\mathbf{F}_q)}\mathbf{F}_q(x)$, and we denote by $\langle x\rangle \in K_\bullet^F(X(\mathbf{F}_q))$ the element corresponding to $1 \in \mathbf{F}_q(x)$.

THEOREM 5.8. (*Localization Theorem*) *For every projective scheme X over $\mathbf{F}_q$, the inclusion $\iota\colon X(\mathbf{F}_q) \hookrightarrow X$ induces an isomorphism $K_\bullet^F(X(\mathbf{F}_q)) \simeq K_\bullet^F(X)$. Its inverse is given by $t\colon K_\bullet^F(X) \to K_\bullet^F(X(\mathbf{F}_q))$,*

$$t([\mathcal{M}, F_{\mathcal{M}}]) = \sum_{x\in X(\mathbf{F}_q)} \operatorname{trace}(F_{\mathcal{M}}(x))\langle x\rangle.$$

Let us see that this gives Theorem 5.4.

PROOF OF THEOREM 5.4. Consider the structure morphism $f\colon X \to \operatorname{Spec}\mathbf{F}_q$. Let $\langle \mathrm{pt}\rangle$ denote the element of $K_\bullet^F(\operatorname{Spec}\mathbf{F}_q)$ that corresponds to $1 \in \mathbf{F}_q$ via the isomorphism given by Lemma 5.5. By definition, for every $[\mathcal{M}, F_{\mathcal{M}}] \in K_\bullet^F(X)$, we have

$$f_*([\mathcal{M}, F_{\mathcal{M}}]) = \left(\sum_{i=0}^{\dim(X)} (-1)^i \operatorname{trace}(F_{\mathcal{M}}|H^i(X,\mathcal{M}))\right)\langle \mathrm{pt}\rangle.$$

On the other hand, if we apply the isomorphism t in Theorem 5.8, we have

$$u := t([\mathcal{M}, F_{\mathcal{M}}]) = \sum_{x\in X(\mathbf{F}_q)} \operatorname{trace}(F_{\mathcal{M}}(x))\langle x\rangle.$$

If $\iota\colon X(\mathbf{F}_q) \to X$ is the inclusion, then it is clear that

$$f_*\left(\iota_*\left(\sum_{x\in X(\mathbf{F}_q)} m_x\langle x\rangle\right)\right) = \left(\sum_{x\in X(\mathbf{F}_q)} m_x\right)\langle \mathrm{pt}\rangle.$$

In particular, we have $f_*\circ\iota_*(u) = \left(\sum_{x\in X(\mathbf{F}_q)} \mathrm{trace}(F_{\mathcal{M}}(x))\right)\langle \mathrm{pt}\rangle$. Since t and ι are inverse to each other, the assertion in Theorem 5.4 follows. □

REMARK 5.9. In fact, Theorem 5.8 is proved in [Ful3] also for arbitrary schemes of finite type over $\mathbf{F}_q$. In particular, Theorems 5.1 and 5.4 also hold if X is only assumed to be complete.

5.2. The proof of the Localization Theorem

We start with a few lemmas.

LEMMA 5.10. *For every scheme X, and every coherent sheaf on X with Frobenius action $(\mathcal{M}, F_{\mathcal{M}})$ such that $F_{\mathcal{M}}$ is nilpotent, we have $[\mathcal{M}, F_{\mathcal{M}}] = 0$ in $K_\bullet^F(X)$.*

PROOF. We prove the assertion by induction on m such that $\phi^m = 0$. If $m = 1$, it is enough to use relation (B) in the definition of $K_\bullet^F(X)$, that gives $[\mathcal{M}, 0] = [\mathcal{M}, 0] + [\mathcal{M}, 0]$. If $m \geq 2$, and $\mathcal{M}' = \mathrm{Ker}(F_{\mathcal{M}})$, then $\mathcal{M}'$ is a coherent $\mathcal{O}_X$-submodule of $\mathcal{M}$, and we have an exact sequence of coherent sheaves with Frobenius action

$$0 \to (\mathcal{M}', F_{\mathcal{M}'}) \to (\mathcal{M}, F_{\mathcal{M}}) \to (\mathcal{M}'', F_{\mathcal{M}''}) \to 0.$$

This gives $[\mathcal{M}, F_{\mathcal{M}}] = [\mathcal{M}', F_{\mathcal{M}'}] + [\mathcal{M}'', F_{\mathcal{M}''}]$. Since $F_{\mathcal{M}'} = 0$ and $F_{\mathcal{M}''}^{m-1} = 0$, it follows by the induction hypothesis that $[\mathcal{M}', F_{\mathcal{M}'}] = 0 = [\mathcal{M}'', F_{\mathcal{M}''}]$. Therefore $[\mathcal{M}, F_{\mathcal{M}}] = 0$. □

LEMMA 5.11. *If $j\colon X \hookrightarrow Y$ is a closed embedding, then we have a morphism of $\mathbf{F}_q$-vector spaces $j^*\colon K_\bullet^F(Y) \to K_\bullet^F(X)$ given by $j^*([\mathcal{M}, F_{\mathcal{M}}]) = [\mathcal{M}\otimes_{\mathcal{O}_Y}\mathcal{O}_X, \overline{F_{\mathcal{M}}}]$, where $\overline{F_{\mathcal{M}}}$ is the Frobenius action induced by $F_{\mathcal{M}}$ on $\mathcal{M}\otimes_{\mathcal{O}_Y}\mathcal{O}_X$. In particular, the composition $j^*\circ j_*$ is the identity on $K_\bullet^F(X)$.*

PROOF. Let $\mathcal{I}$ be the ideal defining X in Y. Since $F_{\mathcal{M}}(\mathcal{I}\mathcal{M}) \subseteq \mathcal{I}^q\mathcal{M}$, it follows that $F_{\mathcal{M}}$ indeed induces a Frobenius action $\overline{F_{\mathcal{M}}}$ on $\mathcal{M}/\mathcal{I}\mathcal{M}$. We have $\overline{F_1 + F_2} = \overline{F_1} + \overline{F_2}$, hence in order to show that we have an induced morphism $K_\bullet^F(Y) \to K_\bullet^F(X)$, we only need to show that if

$$0 \to (\mathcal{M}', F_{\mathcal{M}'}) \to (\mathcal{M}, F_{\mathcal{M}}) \to (\mathcal{M}'', F_{\mathcal{M}''}) \to 0$$

is an exact sequence of coherent F-modules on Y, then

$$[\mathcal{M}/\mathcal{I}\mathcal{M}] = [\mathcal{M}'/\mathcal{I}\mathcal{M}'] + [\mathcal{M}''/\mathcal{I}\mathcal{M}'']$$

in $K_\bullet^F(X)$. Note that we have an exact sequence of coherent F-modules on X

$$0 \to \mathcal{M}'/\mathcal{M}'\cap\mathcal{I}\mathcal{M} \to \mathcal{M}/\mathcal{I}\mathcal{M} \to \mathcal{M}''/\mathcal{I}\mathcal{M}'' \to 0,$$

and a surjection $\mathcal{M}'/\mathcal{I}\mathcal{M}' \to \mathcal{M}'/\mathcal{M}'\cap\mathcal{I}\mathcal{M}$, with kernel $\mathcal{M}'\cap\mathcal{I}\mathcal{M}/\mathcal{I}\mathcal{M}'$. In light of Lemma 5.10, it is enough to show that the Frobenius action on $\mathcal{M}'\cap\mathcal{I}\mathcal{M}/\mathcal{I}\mathcal{M}'$ is nilpotent. Since $F_{\mathcal{M}}^m(\mathcal{I}\mathcal{M}) \subseteq \mathcal{I}^{q^m}(\mathcal{M})$, we see that $\mathcal{M}'\cap F_{\mathcal{M}}^m(\mathcal{I}\mathcal{M}) \subseteq \mathcal{I}\mathcal{M}'$ for $m \gg 0$ by Artin-Rees. This shows that j^* is well-defined, and the fact that $j^*\circ j_*$ is the identity follows from definition. □

Note that if X is any scheme, and we consider $j\colon X(\mathbf{F}_q) \hookrightarrow X$, then j^* is the morphism t in Theorem 5.8. Since $j^* \circ j_*$ is the identity, in order to prove Theorem 5.8 for a projective scheme X, it is enough to show that $j_* \circ j^*$ is the identity on $K_\bullet^F(X)$. In fact, it is enough to show that j_* is surjective.

LEMMA 5.12. *If $(\mathcal{M}, \phi)$ is a coherent $\mathcal{O}_X$-module with a Frobenius action, and $\mathcal{M}$ decomposes as $\mathcal{M} = \mathcal{M}_1 \oplus \ldots \oplus \mathcal{M}_r$, and if $\phi_{i,j}$ is the composition $\mathcal{M}_i \to \mathcal{M} \xrightarrow{\phi} \mathcal{M} \to \mathcal{M}_j$, then $[\mathcal{M}, \phi] = \sum_{i=1}^r [\mathcal{M}_i, \phi_{i,i}]$ in $K_\bullet^F(X)$.*

PROOF. Let $\widetilde{\phi}_{i,j}\colon \mathcal{M} \to \mathcal{M}$ be the map induced by $\phi_{i,j}$, so that $\phi = \sum_{i,j} \widetilde{\phi}_{i,j}$. By condition (B) we have $[\mathcal{M}, \phi] = \sum_{i,j} [\mathcal{M}, \widetilde{\phi}_{i,j}]$. For every $i \neq j$ we have $\widetilde{\phi}_{i,j}^2 = 0$, hence $[\mathcal{M}, \widetilde{\phi}_{i,j}] = 0$ by Lemma 5.10. Therefore

$$[\mathcal{M}, \phi] = \sum_{i=1}^r [\mathcal{M}, \widetilde{\phi}_{i,i}] = \sum_{i=1}^r [\mathcal{M}_i, \phi_{i,i}],$$

by condition (A). □

The key ingredient in the proof of Theorem 5.8 is provided by the case $X = \mathbf{P}^n_{\mathbf{F}_q}$. We now turn to the description of $K_\bullet^F(\mathbf{P}^n_{\mathbf{F}_q})$. We will use the Serre correspondence between coherent sheaves on $\mathbf{P}^n_{\mathbf{F}_q}$ and finitely generated graded modules over $S = \mathbf{F}_q[x_0, \ldots, x_n]$.

Suppose that $\mathcal{M}$ is a coherent sheaf on $\mathbf{P}^n_{\mathbf{F}_q}$ with a Frobenius action $F_{\mathcal{M}}\colon \mathcal{M} \to F_*(\mathcal{M})$. This induces for every i a morphism

$$\mathcal{M}(i) \to F_*(\mathcal{M}) \otimes \mathcal{O}(i) \to F_*(\mathcal{M}(qi)),$$

where we used the projection formula, and the fact that for every line bundle L we have $F^*(L) \simeq L^q$. It follows that if $M = \Gamma_*(\mathcal{M}) := \oplus_{i \geq 0} \Gamma(\mathbf{P}^n_{\mathbf{F}_q}, \mathcal{M}(i))$, then we get a *graded Frobenius action* on M: this is an $\mathbf{F}_q$-linear map $F_M\colon M \to M$ such that $F_M(M_i) \subseteq M_{qi}$ and $F_M(au) = a^q F_M(u)$ for $a \in S$ and $u \in M$.

Conversely, given a finitely generated graded S-module M with a graded Frobenius action F_M, we get an induced coherent F-module structure on $\widetilde{M}$, as follows. If $U_i \subset \mathbf{P}^n_{\mathbf{F}_q}$ is the open subset defined by $x_i \neq 0$, then $\Gamma(U_i, \widetilde{M}) = (M_{x_i})_0$, and $F_{\widetilde{M}}\left(\frac{u}{x_i^N}\right) = \frac{F_M(u)}{x_i^{qN}}$ for every $u \in M_N$. It is straightforward to check that this gives a Frobenius action on $\widetilde{M}$. If $(\mathcal{M}, F_{\mathcal{M}})$ is a coherent F-module and $M = \Gamma_*(\mathcal{M})$, with the graded Frobenius action described above, then we have an isomorphism of graded F-modules $\mathcal{F} \simeq \widetilde{M}$.

If $M = S(-i)$, then giving a graded Frobenius action F_M on M, is equivalent to giving $f = F_M(1) \in S_{(q-1)i}$. In particular, if $i < 0$, then the only graded Frobenius action on $S(-i)$ is the zero one. For an arbitrary finitely generated graded S-module M, we consider a graded free resolution of M

$$0 \to F_n \to \ldots \to F_1 \to F_0 \to M \to 0,$$

where each F_j is a direct sum of of S-modules of the form $S(-b_{i,j})$, with $b_{i,j} \in \mathbf{Z}$. If we have a graded Frobenius action on M, then we can put graded Frobenius actions on each F_i, such that the above exact sequence is compatible with the graded Frobenius actions. In particular, we get $[\widetilde{M}] = \sum_{i=0}^n (-1)^i [\widetilde{F}_i]$ in $K_\bullet^F(\mathbf{P}^n_{\mathbf{F}_q})$. It follows from the above discussion and Lemma 5.12 that $K_\bullet^F(\mathbf{P}^n_{\mathbf{F}_q})$ is generated (as an $\mathbf{F}_q$-vector space) by $[\mathcal{O}(-i), x_0^{a_0} \cdots x_n^{a_n}]$, where $a_\ell \geq 0$ and $\sum_{\ell=0}^n a_\ell = i(q-1)$.

PROPOSITION 5.13. *The $\mathbf{F}_q$-vector space $K_\bullet^F(\mathbf{P}^n_{\mathbf{F}_q})$ is generated by $[\mathcal{O}(-i), x_0^{a_0}\cdots x_n^{a_n}]$, with $0 \le a_\ell \le q-1$ for all ℓ, with some $a_\ell < q-1$, and where $\sum_{\ell=0}^n a_\ell = i(q-1)$.*

PROOF. Let us show first that $K_\bullet^F(\mathbf{P}^n_{\mathbf{F}_q})$ is generated by $[\mathcal{O}(-i), x_0^{a_0}\cdots x_n^{a_n}]$, with $0 \le a_\ell \le q-1$ for all ℓ, and with $\sum_{\ell=0}^n a_\ell = i(q-1)$. In light of the discussion preceding the proposition, it is enough to show the following: if u is a monomial such that $u = x_i^q w$, then $[\mathcal{O}(-i), u] = [\mathcal{O}(-i+1), x_i w]$ in $K_\bullet^F(\mathbf{P}^n_{\mathbf{F}_q})$. If H is the hyperplane in $\mathbf{P}^n_{\mathbf{F}_q}$ defined by $(x_i = 0)$, we have an exact sequence of coherent sheaves with Frobenius action

$$0 \to \mathcal{O}(-i) \xrightarrow{\cdot x_i} \mathcal{O}(-i+1) \to \mathcal{O}_H(-i+1) \to 0,$$

where the Frobenius actions on $\mathcal{O}(-i)$ and $\mathcal{O}(-i+1)$ are defined by u and $x_i w$, respectively. Since $x_i w$ restricts to zero on H, it follows that the Frobenius action on $\mathcal{O}_H(-i+1)$ is zero, and we conclude from the above exact sequence that $[\mathcal{O}(-i), u] = [\mathcal{O}(-i+1), x_i w]$.

In order to complete the proof of the proposition, it is enough to show that we can write $[\mathcal{O}(-(n+1)), (x_0\cdots x_n)^{q-1}]$ in terms of the remaining elements of the above system of generators. In order to do this, let us consider the Koszul complex on $\mathbf{P}^n_{\mathbf{F}_q}$ corresponding to the global sections $x_0, \ldots, x_n$ of $\mathcal{O}(1)$:

$$0 \to \mathcal{E}_{n+1} \to \ldots \to \mathcal{E}_1 = \mathcal{O}(-1)^{\oplus(n+1)} \xrightarrow{h} \mathcal{E}_0 = \mathcal{O}_{\mathbf{P}^n_{\mathbf{F}_q}} \to 0,$$

where $h = (x_0, \ldots, x_n)$. Using the above decomposition $\mathcal{E}_1 = L_0 \oplus \ldots \oplus L_n$, then

$$\mathcal{E}_r = \bigoplus_{0 \le i_1 < \ldots < i_r \le n} (L_{i_1} \otimes \ldots \otimes L_{i_r}) \simeq \mathcal{O}(-r)^{\binom{n+1}{r}}.$$

If on the factor $L_{i_1} \otimes \ldots \otimes L_{i_r}$ of $\mathcal{E}_r$ we consider the F-module structure given by the monomial $x_{i_1}^{q-1}\cdots x_{i_r}^{q-1}$, then the above complex becomes a complex of F-modules. We deduce that in $K^F(\mathbf{P}^n_{\mathbf{F}_q})$ we have the following relation:

$$\sum_{r=0}^{n+1} (-1)^r \sum_{0 \le i_1 < \ldots < i_r \le n} [\mathcal{O}(-r), x_{i_1}^{q-1}\cdots x_{i_r}^{q-1}] = 0,$$

which completes the proof of the proposition. □

COROLLARY 5.14. *The assertion in Theorem 5.8 holds when $X = \mathbf{P}^n_{\mathbf{F}_q}$.*

PROOF. As we have seen, if $j\colon \mathbf{P}^n(\mathbf{F}_q) \hookrightarrow \mathbf{P}^n_{\mathbf{F}_q}$ is the inclusion, then j_* is injective, and it is enough to show that it is surjective. Proposition 5.13 implies that $\dim_{\mathbf{F}_q} K_\bullet^F(\mathbf{P}^n_{\mathbf{F}_q}) \le \alpha_n - 1$, where

$$\alpha_n := |\{(a_0, \ldots, a_n) \mid 0 \le a_i \le q-1,\ (q-1) \text{ divides } \sum_{i=0}^n a_i\}|.$$

Suppose we have $(a_0, \ldots, a_{n-1})$ with $0 \le a_\ell \le q-1$ for $0 \le \ell \le n-1$, and we want to choose a_n with $0 \le a_n \le q-1$ such that $\sum_{\ell=0}^n a_\ell$ is divisible by $(q-1)$. If $\sum_{\ell=0}^{n-1} a_\ell$ is divisible by $(q-1)$, then we may take $a_n = 0$ or $a_n = q-1$; if $\sum_{\ell=0}^{n-1} a_\ell$ is not divisible by $(q-1)$, then we have precisely one choice for a_n. Therefore $\alpha_n = 2\alpha_{n-1} + (q^n - \alpha_{n-1}) = q^n + \alpha_{n-1}$. Since $\alpha_0 = 2$, we conclude that $\alpha_n = (1 + q + \ldots + q^n) + 1$.

Therefore $\dim_{\mathbf{F}_q} K_\bullet^F(\mathbf{P}^n_{\mathbf{F}_q}) \leq |\mathbf{P}^n(\mathbf{F}_q)| = \dim_{\mathbf{F}_q} K_\bullet^F(\mathbf{P}^n(\mathbf{F}_q))$. Since j_* is injective, it follows that j_* is also surjective, completing the proof. □

Proof of Theorem 5.8. Let us fix a closed immersion $j\colon X \hookrightarrow Y = \mathbf{P}^n_{\mathbf{F}_q}$. By Corollary 5.14, it is enough to show that if Theorem 5.8 holds for Y, then it also holds for X.

Consider the following commutative diagram:

$$\begin{array}{ccc} X(\mathbf{F}_q) & \xrightarrow{j'} & Y(\mathbf{F}_q) \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota'} \\ X & \xrightarrow{j} & Y \end{array} \tag{5.3}$$

in which all maps are closed immersions. As we have already mentioned, in order to prove Theorem 5.8 for X, it is enough to show that $\iota_* \circ \iota^*$ is the identity on $K_\bullet^F(X)$. Since the theorem holds for Y, we know that $\iota'_* \circ (\iota')^*$ is the identity on $K_\bullet^F(Y)$.

Note that $j'_* \circ \iota^* = (\iota')^* \circ j_*$: this is an immediate consequence of the definitions. Therefore

$$j_* \circ \iota_* \circ \iota^* = (\iota')_* \circ j'_* \circ \iota^* = \iota'_* \circ (\iota')^* \circ j_* = j_*. \tag{5.4}$$

On the other hand, Lemma 5.11 implies that $j^* \circ j_*$ is the identity on $K_\bullet^F(X)$. In particular, j_* is injective. We conclude from (5.4) that $\iota_* \circ \iota^*$ is the identity on $K_\bullet^F(X)$, and this completes the proof of the theorem. □

5.3. Supersingular Calabi-Yau hypersurfaces

As an application of Theorem 5.1, we discuss a characterization of supersingular Calabi-Yau hypersurfaces. More generally, we prove the following

Proposition 5.15. *Let $f \in \mathbf{F}_q[x_0, \ldots, x_n]$ be a homogeneous polynomial of degree $n+1$, with $n \geq 2$, defining the hypersurface $Z \subset \mathbf{P}^n$. The following are equivalent:*

i) *The action induced by the Frobenius morphism on $H^{n-1}(Z, \mathcal{O}_Z)$ is bijective (equivalently, it is nonzero).*
ii) *$|Z(\mathbf{F}_q)| \not\equiv 1 \pmod p$.*
iii) *The coefficient of $(x_0 \cdots x_n)^{q-1}$ in f^{q-1} is nonzero.*
iv) *The coefficient of $(x_0 \cdots x_n)^{p-1}$ in f^{p-1} is nonzero.*

If Z as above is a smooth hypersurface, then it is *ordinary* if it satisfies the above equivalent conditions. Otherwise, it is *supersingular*.

Proof. Since Z is a hypersurface of degree $(n+1)$ in $\mathbf{P}^n$, we have an exact sequence

$$0 \to \mathcal{O}_{\mathbf{P}^n}(-n-1) \xrightarrow{\cdot f} \mathcal{O}_{\mathbf{P}^n} \to \mathcal{O}_Z \to 0. \tag{5.5}$$

This gives $H^i(Z, \mathcal{O}_Z) = 0$ for $1 \leq i \leq n-2$, and $H^0(Z, \mathcal{O}_Z) \simeq \mathbf{F}_q \simeq H^{n-1}(Z, \mathcal{O}_Z)$. Frobenius acts on $H^0(Z, \mathcal{O}_Z)$ as the identity, and if it acts as multiplication by $\lambda \in \mathbf{F}_q$ on $H^{n-1}(Z, \mathcal{O}_Z)$, then Theorem 5.1 gives

$$|Z(\mathbf{F}_q)| \bmod p = 1 + (-1)^{n-1}\lambda.$$

Therefore $\lambda = 0$ if and only if $|Z(\mathbf{F}_q)| \equiv 1 \pmod p$. This proves i)⇔ii).

In order to prove that iii) and iv) are equivalent, note first that for every $r \geq 1$, we may uniquely write

$$f^{p^r-1} = c_r(x_0 \cdots x_n)^{p^r-1} + u_r, \tag{5.6}$$

where $u_r \in (x_0^{p^r}, \ldots, x_n^{p^r})$. If we raise to the p^{th}-power in (5.6), we get

$$f^{p^{r+1}-p} = c_r^p(x_0 \cdots x_n)^{p^{r+1}-p} + u_r^p.$$

Since $u_r^p \in (x_0^{p^{r+1}}, \ldots, x_n^{p^{r+1}})$ and

$$(x_0 \cdots x_n)^{p^{r+1}-p} \cdot (x_0^p, \ldots, x_n^p) \subseteq (x_0^{p^{r+1}}, \ldots, x_n^{p^{r+1}}),$$

we deduce that

$$f^{p^{r+1}} - c_r^p c_1 (x_0 \cdots x_n)^{p^{r+1}-1} \in (x_0^{p^{r+1}}, \ldots, x_n^{p^{r+1}}).$$

Therefore $c_{r+1} = c_r^p c_1$, which immediately gives that $c_r = c_1^{1+p+\ldots p^{r-1}}$ for every $r \geq 1$. In particular, if $q = p^e$, we see that $c_1 \neq 0$ if and only if $c_e \neq 0$, hence iii)$\Leftrightarrow$iv).

In order to prove the equivalence of i) and iii), we consider the explicit description of the Frobenius action F on $H^{n-1}(Z, \mathcal{O}_Z)$ via the isomorphism

$$\delta \colon H^{n-1}(Z, \mathcal{O}_Z) \to H^n(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(-n-1))$$

induced by (5.5). We compute the cohomology of $\mathcal{O}_{\mathbf{P}^n}(-n-1)$ and of $\mathcal{O}_Z$ as Cech cohomology with respect to the affine cover of $\mathbf{P}^n$ by the open subsets $(x_i \neq 0)$. Recall that

$$H^n(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}(-n-1)) \simeq (S_{x_0 \cdots x_n})_{-n-1} / \sum_{i=0}^n (S_{x_0 \cdots \widehat{x_i} \cdots x_n})_{-n-1} = \mathbf{F}_q \cdot \frac{1}{x_0 \cdots x_n}.$$

Suppose that $u \in H^{n-1}(Z, \mathcal{O}_Z)$ is represented by the Cech cocyle $h = (\overline{h_0}, \ldots, \overline{h_n}) \in \oplus_{i=0}^n ((S/f)_{x_0 \cdots \widehat{x_i} \cdots x_n})_0$. If $h_i \in (S_{x_0 \cdots \widehat{x_i} \cdots x_n})_0$ is a lift of $\overline{h_i}$, then $\delta(u)$ is represented by the unique $w \in (S_{x_0 \ldots x_n})_{-n-1}$ such that $fw = \sum_{i=0}^n (-1)^i h_i$.

On the other hand, $F(u)$ is represented by $(\overline{h_0}^q, \ldots, \overline{h_n}^q)$. Since we have $f(f^{q-1}w^q) = \sum_{i=0}^n (-1)^i h_i^q$, it follows that via the isomorphism δ, we can describe F as the linear map on $(S_{x_0 \cdots x_n})_{-n-1} / \sum_{i=0}^n (S_{x_0 \cdots \widehat{x_i} \cdots x_n})_{-n-1}$ induced by $w \to f^{q-1}w^q$. This map multiplies the class of $\frac{1}{x_0 \cdots x_n}$ in this quotient by the coefficient of $(x_0 \cdots x_n)^{q-1}$ in f^{q-1}. This completes the proof of ii)$\Leftrightarrow$iii), hence the proof of the proposition. □

Remark 5.16. In the context of Proposition 5.15, note that if

$$\operatorname{trace}(F \mid H^{n-1}(Z, \mathcal{O}_Z)) = 1 + (-1)^{n-1}a,$$

then for every $r \geq 1$ we have $1 + (-1)^{n-1}a^r = |Z(\mathbf{F}_{q^r})| \bmod p$. This is a consequence of Theorem 5.1 (see also Remark 5.3).

Exercise 5.17. Give a direct proof for the implication ii) $\Leftrightarrow$ iii) in Proposition 5.15 by computing $\sum_{a \in \mathbf{F}_q^{n+1}} f(a)^{q-1}$ (see [Knu]).

Exercise 5.18. Show that if X is an elliptic curve (that is, X is a smooth, geometrically connected, projective curve of genus 1) over $\mathbf{F}_p$, with $p \neq 2, 3$, then X is supersingular if and only if $|X(\mathbf{F}_p)| = p + 1$.

EXERCISE 5.19. Let $Z \subset \mathbf{P}^n_{\mathbf{F}_q}$ be a complete intersection subscheme of codimension r, defined by $(F_1, \ldots, F_r)$. Let $d_i = \deg(F_i)$, and assume that $\sum_i d_i = n + 1$. Show that the following are equivalent:

i) The action induced by the Frobenius morphism on the cohomology group $H^{n-r}(Z, \mathcal{O}_Z)$ is bijective (equivalently, it is nonzero).
ii) $|Z(\mathbf{F}_q)| \not\equiv 1 \pmod{p}$.
iii) The polynomial $F_1 \cdots F_r$ satisfies the equivalent conditions in Proposition 5.15.

CHAPTER 6

The Lang-Weil estimate and the zeta function of an arithmetic scheme

Our main goal in this chapter is to introduce the zeta function of an arithmetic scheme. In order to compute the abscissa of convergence of this function, we will use the Lang-Weil estimate. The proof of this estimate will make use of the Chow variety, which we review in the first section.

6.1. The Chow variety

We review in this section some basic facts concerning the Chow variety. For proofs and further properties, see [Kol, Chapter I].

Suppose first that K is an algebraically closed field, and $V \subseteq \mathbf{P} = \mathbf{P}^n_K$ is a closed subvariety of dimension r and degree d. Let $\mathbf{P}^* \simeq \mathbf{P}^n_K$ denote the dual projective space parametrizing the hyperplanes in $\mathbf{P}$. Consider the following incidence variety:

$$\Lambda := \{x, H_1, \ldots, H_{r+1}) \in V \times (\mathbf{P}^*)^{r+1} \mid x \in H_i \text{ for all } i\}.$$

Let $f\colon \Lambda \to V$ and $g\colon \Lambda \to (\mathbf{P}^*)^{r+1}$ denote the morphisms induced by projections. It is clear that every $f^{-1}(x)$ is isomorphic to $(\mathbf{P}^{n-1}_K)^{r+1}$. Therefore Λ is irreducible, of dimension $r+(n-1)(r+1)$. On the other hand, since we can find $(H_1, \ldots, H_{r+1}) \in (\mathbf{P}^*)^{r+1}$ such that $V \cap H_1 \ldots \cap H_{r+1}$ is a nonempty finite set, it follows that g is generically finite onto its image W. Therefore W is an irreducible subvariety of $(\mathbf{P}^*)^{r+1}$ of codimension equal to $(r+1)n - (r + (r+1)(n-1)) = 1$, hence a divisor. One can show that $\mathcal{O}(W) = \mathcal{O}(d, d, \ldots, d)$. The *Caylay form* of V is an equation defining W. This is given by a polynomial R_V in $(r+1)$ sets of $(n+1)$ variables (unique up to a nonzero scalar), homogeneous of degree d in each set of variables. Note that W determines V: $x \in \mathbf{P}$ lies in V if and only if W contains all $(H_1, \ldots, H_{r+1}) \in (\mathbf{P}^*)^{r+1}$ such that $x \in H_i$ for all i. We thus have an injective map from the set of irreducible subvarieties of $\mathbf{P}$ of dimension r and degree d to $|\mathcal{O}(1, \ldots, 1)|$. The image $\mathrm{Chow}^\circ_K(n, d, r)$ is a quasiprojective variety, whose closure is the Chow variety $\mathrm{Chow}_K(n, d, r)$. In particular, the complement $\mathrm{Chow}_K(n, d, r) \smallsetminus \mathrm{Chow}^\circ_K(n, d, r)$ is a closed subset of $|\mathcal{O}(1, \ldots, 1)|$.

In fact, $\mathrm{Chow}_K(n, d, r)$ parametrizes effective r-cycles of degree d in $\mathbf{P}^n$, as follows. Consider an effective r-cycle $Z = \sum_i m_i V_i$ of degree d (that is, $\sum_i m_i \deg(V_i) = d$). Note that $R_Z := \prod_i R_{V_i}^{m_i}$ defines a divisor in $|\mathcal{O}(d, \ldots, d)|$. One can show that this gives a bijection between the set of cycles as above and $\mathrm{Chow}_K(n, d, r)$.

If k is an arbitrary field, let K be an algebraic closure of k. Every subscheme $Y \hookrightarrow \mathbf{P}^n_k$ of pure dimension r and degree d determines an r-cycle $[Y \times_k K]$ of degree d, hence a point $\Phi(Y) \in \mathrm{Chow}_K(n, d, r)$. Note that $\Phi(Y) \in \mathrm{Chow}^\circ_K(n, d, r)$ if and only if Y is generically reduced and geometrically irreducible (recall that Y is geometrically irreducible if $Y \times_k K$ is irreducible).

We will need two facts about Chow varieties. The first is that if $X \subseteq \mathbf{P}^n_K$ is an irreducible variety and $H \subset \mathbf{P}^n_K$ is a hyperplane that does not contain X, then $R_{[X\cap H]}(u_1, \ldots, u_r) = R_X(u_1, \ldots, u_r, h)$, where h is an equation of H (in the special case when $X \cap H$ is integral, this is an immediate consequence of the above definitions).

The second fact that we need is that one can do the above construction over $\operatorname{Spec} \mathbf{Z}$. More precisely, we have schemes $\operatorname{Chow}^\circ_{\mathbf{Z}}(n, d, r) \subset \operatorname{Chow}_{\mathbf{Z}}(n, d, r)$ such that for every algebraically closed field K, after taking the product with $\operatorname{Spec} K$ we obtain $\operatorname{Chow}^\circ_K(n, d, r) \subset \operatorname{Chow}_K(n, d, r)$. The upshot is that we can find e such that the subvariety

$$\operatorname{Chow}_K(n, d, r) \smallsetminus \operatorname{Chow}^\circ_K(n, d, r) \subset \mathbf{P}(\Gamma((\mathbf{P}^n_K)^* \times \ldots \times (\mathbf{P}^n_K)^*, \mathcal{O}(d, \ldots, d))^*)$$

is defined (set-theoretically) by finitely many equations of degree e with coefficients in the prime field of K (the key point is that e is independent of the field K).

6.2. The Lang-Weil estimate

In this section we work with a geometrically irreducible variety X defined over a finite field k. We show that if we assume that X is embedded in a projective space of fixed dimension, then we have universal estimates for $|X(k')|$, where k'/k is finite, in terms of $\dim(X)$, $\deg(X)$, and $|k'|$. More precisely, we show the following

THEOREM 6.1. ([LaWe]) *Given nonnegative integers n, d, and r, with $d > 0$, there is a positive constant $A(n, d, r)$ such that for every finite field $k = \mathbf{F}_q$, and every geometrically irreducible subvariety $X \subseteq \mathbf{P}^n_k$ of dimension r and degree d, we have*

$$|\#X(k) - q^r| \leq (d-1)(d-2)q^{r-\frac{1}{2}} + A(n, d, r)q^{r-1}. \tag{6.1}$$

The proof we give follows [LaWe], arguing by induction on r. The case of curves is a consequence of the Riemann hypothesis part of the Weil conjectures, that we have proved in Chapter 3. For the induction argument, we will need two lemmas. The first one gives a weaker bound than the assertion in the theorem.

LEMMA 6.2. *Given n, d, and r as in Theorem 6.1, there is a positive constant $A_1(n, d, r)$ such that for every finite field $k = \mathbf{F}_q$, and every irreducible subvariety $X \subseteq \mathbf{P}^n_k$ of dimension r and degree $\leq d$, we have*

$$\#X(k) \leq A_1(n, d, r)q^r. \tag{6.2}$$

PROOF. We argue by induction on n. If $n = 0$, then $X = \operatorname{Spec} k$, hence $r = 0$ and $d = 1$, and we may take $A_1(0, 1, 0) = 1$.

Suppose now that we have $A_1(n', d, r)$ for $n' \leq n$ that satisfy the condition in the lemma. Let $X \subseteq \mathbf{P}^{n+1}_k$ be an irreducible subvariety of dimension r and degree d. For every $\lambda \in k$, let $H_\lambda \subset \mathbf{P}^{n+1}_k$ be the hyperplane defined by $(x_1 - \lambda x_0 = 0)$, and let H_∞ be the hyerplane $(x_0 = 0)$. If X is degenerate, then it lies in some $\mathbf{P}^n_k$, and we get (6.2) if $A_1(n + 1, d, r) \geq A_1(n, d, r)$. On the other hand, if X is nondegenerate, then each $X_\lambda := (X \cap H_\lambda)_{\mathrm{red}}$ is a subvariety of $\mathbf{P}^n_k$ of degree $\leq d$, and of pure dimension $(r - 1)$. In particular, if its irreducible components are $X^1_\lambda, \ldots, X^{m_\lambda}_\lambda$, then $m_\lambda \leq d$. Therefore

$$|X(k)| \leq \sum_{\lambda \in k \cup \{\infty\}} |X_\lambda(k)| \leq dA_1(n, d, r)(q + 1)q^r \leq 2dA_1(n, d, r)q^{r+1}.$$

Therefore it is enough to take $A_1(n+1,d,r) = 2dA_1(n,d,r)$. □

REMARK 6.3. Suppose that X is as in Lemma 6.2, but instead of being irreducible, we only assume that it has pure dimension r. In this case the number of irreducible components of X is bounded above by d. Therefore we deduce from the lemma that $\#X(k) \leq dA_1(n,d,r)q^r$.

If X is allowed to have components of smaller dimension, then the number of such components is not controlled by the degree. However, we still get

COROLLARY 6.4. *If X is an r-dimensional variety over $\mathbf{F}_q$, then there is $c_X > 0$ such that $\#X(\mathbf{F}_{q^e}) \leq c_X q^{re}$ for every $e \geq 1$.*

PROOF. Arguing by induction on r, we see that it is enough to show that if $U \subseteq X$ is a dense affine open subset, then we have a similar bound for $\#U(\mathbf{F}_{q^e})$ (this follows since $\dim(X \smallsetminus U) < r$). It is of course enough to give such a bound for the closure $\overline{U}$ of U in some projective space. This in turn follows by applying Lemma 6.2 to each irreducible component of $\overline{U}$. □

Recall that we denote by $(\mathbf{P}^n_k)^*$ the dual projective space of $\mathbf{P}^n_k$. Note that a k-rational point of $(\mathbf{P}^n_k)^*$ corresponds to a k-hyperplane in $\mathbf{P}^n_k$, that is, to a hyperplane given by an equation $\sum_{i=0}^n a_i x_i = 0$, with all $a_i \in k$.

LEMMA 6.5. *Given n, d, and r as in Theorem 6.1, with $r \geq 2$, there is a positive constant $A_2(n,d,r)$ such that for every nondegenerate geometrically irreducible subvariety $X \subseteq \mathbf{P}^n_k$ of dimension r and degree d, the number of k-hyperplanes H in $\mathbf{P}^n_k$ such that $H \cap X$ is either not geometrically irreducible, or not generically reduced, is $\leq A_2(n,d,r)q^{n-1}$.*

PROOF. We make use of the definitions and notation introduced in §1. Let $K = \overline{k}$, and consider $V = \mathrm{Chow}_K(n-1,d,r-1) \smallsetminus \mathrm{Chow}^\circ_K(n-1,d,r-1)$. As we have mentioned, $V = W \times_k K$ for a closed subvariety $W \hookrightarrow \mathbf{P}^N_k$ that is the set-theoretic intersection of finitely many hypersurfaces Z_j of degree e (where N and e only depend on n, d, and r).

By construction, if $X \cap H$ is not geometrically irreducible or not generically reduced, then $\Phi(X \cap H) \in V$. Consider the morphism $(\mathbf{P}^n_K)^* \to \mathbf{P}^N_K$ defined over k that takes H to $R_X(\cdot,\ldots,\cdot,h)$, where h is an equation of H. Note that there is j such that $Z_j \times_k K$ does not contain the image of $(\mathbf{P}^n_K)^*$: indeed, since X is geometrically irreducible and $r \geq 2$, we know by Bertini's theorem that there is a hyperplane in $\mathbf{P}^n_K$ whose intersection with $X \times_k K$ is integral. The pull-back of this hypersurface $Z_j \times_k K$ to $(\mathbf{P}^n_K)^*$ is a hypersurface of degree e' defined over k, where e' only depends on n, d, and r. It follows from Lemma 6.2 (see also Remark 6.3) that if we take $A_2(n,d,r) = e'A_1(n,e',n-1)$, this satisfies the requirement in the lemma. □

We can now give the proof of the main result of this section.

PROOF OF THEOREM 6.1. For every variety X, we denote by X_K the variety $X \times_{\operatorname{Spec} k} \operatorname{Spec} K$, where K is a fixed algebraic closure of k, and for a morphism $\pi\colon Y \to X$, we denote by π_K the corresponding morphism $Y_K \to X_K$. It will be convenient to think of $X(k)$ as the points of X_K fixed under the suitable Frobenius morphism. We will use the fact that $\gamma_n := |\mathbf{P}^n(\mathbf{F}_q)| = \frac{q^{n+1}-1}{q-1}$ (see Corollary 2.23).

The proof is by induction on r. The case $r = 0$ is trivial, since in this case $|X(k)| = 1 = q^r$. Suppose that $r = 1$, and let $\pi\colon Y \to X$ be the normalization of X. The curve Y is nonsingular, projective, and geometrically connected (for the last assertion, note that we have a dense open subset U of Y such that U_K is irreducible). Therefore we may apply to Y the results in Chapter 3, and in particular the estimate for the number of rational points on Y given by the analogue of the Riemann hypothesis (see Lemma 3.8 and Theorem 3.6). We deduce that if g is the genus of Y, then

$$|\#Y(\mathbf{F}_q) - (q+1)| \leq 2gq^{1/2}. \tag{6.3}$$

Note that

$$|\#X(\mathbf{F}_q) - q| \leq |\#Y(\mathbf{F}_q) - (q+1)| + 1 + \sum_{x \in (X_K)_{\mathrm{sing}}} \deg(\pi_K^{-1}(x)). \tag{6.4}$$

In order to estimate the sum in (6.4), as well as the genus of Y, let us consider a general projection of X_K to $\mathbf{P}^2_K$, which gives a birational morphism $\phi\colon X_K \to C$, where C is an ireducible plane curve of degree d. Let $\psi = \phi \circ \pi_K$. Note that if $x \in C$ is a smooth point, then ψ is an isomorphism around x, hence $\phi^{-1}(x)$ is contained in the smooth locus of X_K. Therefore

$$\sum_{x \in (X_K)_{\mathrm{sing}}} \deg(\pi_K^{-1}(x)) \leq \sum_{x \in C_{\mathrm{sing}}} \deg(\psi^{-1}(x)). \tag{6.5}$$

For every $x \in C_{\mathrm{sing}}$ we have $\deg(\psi^{-1}(x)) \leq d$: if L is a hyperplane in $\mathbf{P}^2_K$ passing through x and not containing C, then $\deg(\psi^{-1}(x)) \leq \deg(\psi^{-1}(C \cap H)) = d$.

The arithmetic genus of C is $h^1(C, \mathcal{O}_C) = \frac{(d-1)(d-2)}{2}$. We have a short exact sequence of sheaves

$$0 \to \mathcal{O}_C \to \psi_*(\mathcal{O}_{Y_K}) \to \oplus_{x \in C_{\mathrm{sing}}} \widetilde{\mathcal{O}_{C,x}}/\mathcal{O}_{C,x} \to 0,$$

where $\widetilde{\mathcal{O}_{C,x}}$ is the integral closure of $\mathcal{O}_{C,x}$. If $\delta_x = \mathrm{length}(\widetilde{\mathcal{O}_{C,x}}/\mathcal{O}_{C,x})$, then we get from the long exact sequence in cohomology that $g = p_a(C) - \sum_{x \in C_{\mathrm{sing}}} \delta_x$. This gives $g \leq p_a(C) = \frac{(d-1)(d-2)}{2}$. We also obtain $\sum_{x \in C_{\mathrm{sing}}} \delta_x \leq \frac{(d-1)(d-2)}{2}$. Since $\delta_x \geq 1$ for every singular point $x \in C$, we deduce that $\#C_{\mathrm{sing}} \leq \frac{(d-1)(d-2)}{2}$. We deduce using (6.3), (6.4) and (6.5) that

$$|\#X(\mathbf{F}_q) - q| \leq (d-1)(d-2)q^{1/2} + \frac{d(d-1)(d-2)}{2} + 1,$$

hence we are done in the case $r = 1$ by taking $A(n, d, 1) = \frac{d(d-1)(d-2)}{2} + 1$.

Suppose now that we can find $A(n, d, r)$ as in the theorem for $r \geq 1$, and let us find $A(n, d, r+1)$. Arguing also by induction on n, we may assume that we can find $A(n-1, d, r+1)$ as required (note that the cases $n = 0$ and $n = 1$ are clear). Let X be a geometrically irreducible subvariety of $\mathbf{P}^n_k$, of degree d and dimension $(r+1)$. If X is degenerate, then X lies in some $\mathbf{P}^{n-1}_k$, in which case we get the bound in the theorem if we take $A(n, d, r+1) \geq A(n-1, d, r+1)$. Assume henceforth that X is nondegenerate.

In order to avoid messy computations, we introduce the following notation: given two real numbers a and b, we write $a \leq b + o(q^r)$ if there is an inequality $a \leq b + C \cdot q^r$, where C is a positive constant that is only allowed to depend on n, d, and r. Note that we have $a \leq b + o(q^r)$ if and only if $\gamma_{n-1}a \leq \gamma_{n-1}b + o(q^{r+n-1})$.

Let $W \subseteq X \times (\mathbf{P}^n_k)^*$ be the subvariety consisting of the pairs (x, H) such that $x \in H$. The projections onto the two components give the maps $W \to X$ and $W \to (\mathbf{P}^n_k)^*$. The key idea is to compute in two ways $\#W(\mathbf{F}_q)$, using these two morphisms. Note that for every $x \in X(\mathbf{F}_q)$, the number of $\mathbf{F}_q$-hyperplanes containing x is $\#\mathbf{P}^{n-1}(\mathbf{F}_q) = \gamma_{n-1}$. Therefore

$$|W(\mathbf{F}_q)| = \gamma_{n-1} \cdot |X(\mathbf{F}_q)|. \tag{6.6}$$

On the other hand, using the morphism $W \to (\mathbf{P}^n_k)^*$, we see that

$$|W(\mathbf{F}_q)| = \sum_{H \in (\mathbf{P}^n)^*(k)} |(X \cap H)(\mathbf{F}_q)|. \tag{6.7}$$

We break the sum in (6.7) into two sums, in the first one S_1 collecting all H such that $H \cap X$ is either not geometrically irreducible, or not generically reduced, and in the second one S_2, collecting the remaining terms. Note that for every H that contributes to S_1, the subvariety $(H \cap X)_{\mathrm{red}} \subseteq H \simeq \mathbf{P}^{n-1}_k$ has degree $\leq d$, and pure dimension r. In particular, the number of irreducible components of $(H \cap X)_{\mathrm{red}}$ is $\leq d$, and each has degree $\leq d$. It follows from Lemma 6.2 that $|(X \cap H)(\mathbf{F}_q)| \leq o(q^r)$. On the other hand, we can use Lemma 6.5 to bound the number of such hyperplanes by $A_2(n, d, r+1)q^{n-1}$, hence $S_1 \leq o(q^{r+n-1})$, and therefore

$$\frac{1}{\gamma_{n-1}} S_1 \leq o(q^r). \tag{6.8}$$

Note, in particular, that this sum can be absorbed in the error term.

On the other hand, if $H \cap X$ is geometrically irreducible and generically reduced, then $(H \cap X)_{\mathrm{red}}$ is a variety of dimension r and degree d, and we can estimate the number of points in $(X \cap H)(\mathbf{F}_q)$ by induction: we have

$$|\#(X \cap H)(\mathbf{F}_q) - q^r| \leq (d-1)(d-2)q^{r-\frac{1}{2}} + o(q^{r-1}). \tag{6.9}$$

Let δ be the number of hyperplanes that contribute to S_2. Note that

$$\left| \frac{1}{\gamma_{n-1}} S_2 - q^{r+1} \right| \leq \left| \frac{1}{\gamma_{n-1}} (S_2 - \delta q^r) \right| + \left| \frac{\delta q^r}{\gamma_{n-1}} - q^{r+1} \right|. \tag{6.10}$$

By Lemma 6.5 we have $|\delta - \gamma_n| \leq o(q^{n-1})$. This implies $\frac{\delta}{\gamma_{n-1}} \leq o(q)$ and

$$\left| \frac{\delta q^r}{\gamma_{n-1}} - q^{r+1} \right| \leq \frac{|\delta - \gamma_n| \cdot q^r}{\gamma_{n-1}} + \left| \frac{\gamma_n q^r}{\gamma_{n-1}} - q^{r+1} \right| \leq o(q^r).$$

On the other hand, it follows from (6.9) that

$$\left| \frac{1}{\gamma_{n-1}} (S_2 - \delta q^r) | \right| \leq (d-1)(d-2)q^{r+\frac{1}{2}} + o(q^r), \tag{6.11}$$

hence

$$\left| \frac{1}{\gamma_{n-1}} S_2 - q^{r+1} \right| \leq (d-1)(d-2)q^{r+\frac{1}{2}} + o(q^r).$$

By combining this with (6.8), we get the existence of $A(n, d, r+1)$, which completes the proof of the theorem. □

6.3. Estimating the number of points on arbitrary varieties

We explain in this section how to estimate the number of k-rational points on X when X is not assumed to be geometrically irreducible. In this section, however, the constant in the estimate will be allowed to depend on X.

Let us first introduce some notation. Suppose that $k = \mathbf{F}_q$ is a finite field, and $X \hookrightarrow \mathbf{P}^n_k$ is an irreducible closed subvariety of degree d and dimension r. We denote by $\Gamma = \{W_1, \ldots, W_m\}$ the set of irreducible components of $X_{\overline{k}} = X \times_k \overline{k}$. It follows from Proposition **??** that $G = G(\overline{k}/k)$ acts transitively on Γ. Let $G' \subseteq G$ be the stabilizer of any of the elements of Γ with respect to this action. Note that $G' = G(\overline{k}/\mathbf{F}_{q^\ell})$, where $\mathbf{F}_{q^\ell}$ is the smallest extension of $\mathbf{F}_q$ over which one (hence all) of the W_i is defined (see Proposition A.16 and its proof). Since G/G' has ℓ elements, it follows that $\ell = m$.

PROPOSITION 6.6. *Let n, d, r be nonnegative integers, with $d > 0$. Given any $k = \mathbf{F}_q$ and X as above, there are positive constants c_X and c'_X such that if m is as above, then for every $e \geq 1$ we have*

$$|\#X(\mathbf{F}_{q^e}) - mq^{er}| \leq \frac{(d-m)(d-2m)}{m} q^{e(r-\frac{1}{2})} + c_X q^{e(r-1)} \text{ if } m|e, \text{ and}$$

$$\#X(\mathbf{F}_{q^e}) \leq c'_X q^{e(r-1)}, \text{ if } m \not| e.$$

Furthermore, if X is smooth over $\mathbf{F}_q$, then we may take $c'_X = 0$ and c_X only to depend on n, d, and r (but not on X or on k).

PROOF. For every $e \geq 1$, let $X_e := X \times_{\mathbf{F}_q} \mathbf{F}_{q^e}$. If $m|e$, then X_e has m irreducible components $V_1, \ldots, V_m$, and each of them is geometrically irreducible. Furthermore, we have $\dim(V_i) = r$ and $\deg(V_i) = \frac{d}{m}$ for every i. Note that each $V_i \cap V_j$ is the extension to $\mathbf{F}_{q^e}$ of the corresponding intersection of irreducible components defined over $\mathbf{F}_{q^m}$, and has dimension $< r$ when $i \neq j$. Moreover, if X is smooth, then $V_i \cap V_j = \emptyset$ for $i \neq j$. Since

$$|\#X(\mathbf{F}_{q^e}) - mq^{er}| \leq \sum_{i=1}^{m} |\#V_i(\mathbf{F}_{q^e}) - q^{er}| + \sum_{i<j} \#(V_i \cap V_j)(\mathbf{F}_{q^e}),$$

we deduce the first estimate in the proposition from Theorem 6.1 and Corollary 6.4. Moreover, when X is smooth, it is enough to take $c_X = d \cdot \max_{1 \leq d' \leq d} A(n, d', r)$, where we use the notation in Theorem 6.1.

Suppose now that m does not divide e. Recall that if $F = \mathrm{Frob}_{X,q} \times \mathrm{Id}$, then $X(\mathbf{F}_{q^e})$ can be identified with the fixed points of F^e on $X_{\overline{k}}$. By assumption, none of $W_1, \ldots, W_m$ is fixed by $G(\overline{k}/\mathbf{F}_{q^e}) \subseteq G$. Note also that an irreducible subset $Z \subset X_{\overline{k}}$ is fixed by $G(\overline{k}/\mathbf{F}_{q^e})$ if and only if $F^e(Z) \subseteq Z$ (see the proof of Proposition A.16). It follows that if $u \in W_i$ is fixed by F^e, then $u \in \bigcap_j F^{ej}(W_i)$, which is a proper closed subvariety of W_i, defined over $\mathbf{F}_{q^e}$ (empty when X is smooth). Since its dimension is $\leq r - 1$, we conclude by Remark 6.3 that we can find c'_X as required (note that the varieties $\bigcap_j F^{ej}(W_i)$ only depend on the congruence class of e mod ℓ, hence we only get finitely many such varieties). This completes the proof of the proposition. □

It is now straightforward to estimate the number of $\mathbf{F}_{q^e}$-rational points on an arbitrary variety X over $\mathbf{F}_q$. Let $X_1, \ldots, X_\ell$ be the irreducible components of X

of maximal dimension r, and let m_i be the number of irreducible components of $X_i \times_k \overline{k}$.

PROPOSITION 6.7. *For every X as above, there are positive constants α_X, α'_X such that for every $e \geq 1$, if we put $a_e = \sum_{m_i|e} m_i$, then*

$$|\#X(\mathbf{F}_{q^e}) - a_e q^{er}| \leq \alpha_X q^{e(r-\frac{1}{2})} \text{ if } a_e > 0, \text{ and}$$
$$\#X(\mathbf{F}_{q^e}) \leq \alpha'_X q^{e(r-1)}, \text{ otherwise.}$$

PROOF. Let $U_i \subseteq X_i$ be affine open subsets that do not intersect the other irreducible components of X, and let $U = \bigcup_{i=1}^{\ell} U_i$. Since $\dim(X \smallsetminus U) < r$, it follows from Corollary 6.4 that it is enough to prove the assertion in the proposition for U. If $\overline{U_i}$ is the closure of U_i in some projective space, and $\overline{U} = \bigsqcup_{i=1}^{\ell} \overline{U_i}$, it follows as before that it is enough to prove the estimate for $\overline{U}$. This follows by applying Proposition 6.6 to each of the $\overline{U_i}$. □

6.4. Review of Dirichlet series

In this section we collect some basic facts about Dirichlet series. In the first part we follow [Se1, Chapter VI, §2]. A *Dirichlet series* is a series of functions of the form

$$\sum_{n\geq 1} \frac{a_n}{n^s}, \tag{6.12}$$

where $a_n \in \mathbf{C}$, and s varies over $\mathbf{C}$. The following proposition is the basic result that controls the convergence of Dirichlet series.

PROPOSITION 6.8. *If the series $\sum_{n\geq 1} \frac{a_n}{n^s}$ converges for $s = s_0$, then it converges uniformly in every domain of the form: $\mathrm{Re}(s - s_0) \geq 0$, $\mathrm{Arg}(s - s_0) \leq \alpha$, where $0 < \alpha < \pi/2$.*

PROOF. Let us write $s - s_0 = z = x + yi$, with $x, y \in \mathbf{R}$. It is enough to show that the sequence of functions $\left(\sum_{n=1}^{m} \frac{a_n}{n^s}\right)_m$ is uniformly Cauchy in any domain with $x \geq 0$, and $|z| \leq Mx$. Suppose that $\epsilon > 0$ is given. By hypothesis, we can find m such that $|A_p| \leq \epsilon$ for every p, where $A_p = \sum_{n=m+1}^{m+p} \frac{a_n}{n^{s_0}}$.

We may of course assume that $x > 0$, and we write

$$\sum_{n=m+1}^{m+p} \frac{a_n}{n^s} = \sum_{n=m+1}^{m+p} \frac{a_n}{n^{s_0}} \cdot \frac{1}{n^z} = \frac{A_p}{(m+p)^z} + \sum_{\ell=1}^{p-1} A_\ell \left(\frac{1}{(m+\ell)^z} - \frac{1}{(m+\ell+1)^z} \right) \tag{6.13}$$

We now bound

$$\left| \frac{1}{(m+\ell)^z} - \frac{1}{(m+\ell+1)^z} \right| = \left| z \cdot \int_{\log(m+\ell)}^{\log(m+\ell+1)} e^{-tz} dt \right| \leq |z| \cdot \int_{\log(m+\ell)}^{\log(m+\ell+1)} e^{-tx} dt$$
$$= \frac{|z|}{x} \left(\frac{1}{(m+\ell)^x} - \frac{1}{(m+\ell+1)^x} \right).$$

Using this bound and the condition on $|A_\ell|$, we conclude that that

$$\left| \sum_{n=m+1}^{m+p} \frac{a_n}{n^s} \right| \leq \frac{\epsilon}{(m+p)^x} + \epsilon \frac{|z|}{x} \cdot \sum_{\ell=1}^{p-1} \left(\frac{1}{(m+\ell)^x} - \frac{1}{(m+\ell+1)^x} \right) \leq \epsilon(1+M).$$

This completes the proof of the proposition. □

The *abscissa of convergence* of the series $\sum_{n\geq 1}\frac{a_n}{n^s}$ is

$$\rho = \inf\{\mathrm{Re}(s) \mid \sum_{n\geq 1}\frac{a_n}{n^s} \text{ is convergent at } s\}.$$

It follows from Proposition 6.8 that $\sum_{n\geq 1}\frac{a_n}{n^s}$ converges uniformly on every compact subset contained in $\{s \mid \mathrm{Re}(s) > \rho\}$ (this is called the half-plane of convergence of the series). In particular, it defines a holomorphic function on this half-plane. It follows from definition that the series is divergent at every s with $\mathrm{Re}(s) < \rho$. Note that $\rho = \infty$ if and only if the series diverges everywhere, and $\rho = -\infty$ if and only if the series is everywhere convergent.

EXAMPLE 6.9. Suppose that $\alpha \in \mathbf{R}$ is such that the sequence $|a_n|/n^\alpha$ is bounded above. In this case the abscissa of convergence ρ of $\sum_{n\geq 1}\frac{a_n}{n^s}$ satisfies $\rho \leq 1+\alpha$. Furthermore, suppose that $a_n \in \mathbf{R}_{\geq 0}$ and $\liminf_{n\to\infty}\frac{a_n}{n^\alpha} > 0$; in this case $\rho = \alpha + 1$. Both assertions follow from the fact that for $p \in \mathbf{R}$, the series $\sum_{n\geq 1}\frac{1}{n^p}$ is convergent if and only if $p > 1$.

EXAMPLE 6.10. If we consider the Dirichlet series $\sum_{n\geq 1}\frac{1}{n^s}$ defining the Riemann zeta function $\zeta(s)$, then the abscissa of convergence is $\rho = 1$.

PROPOSITION 6.11. *Suppose that* $f(s) = \sum_{n\geq 1}\frac{a_n}{n^s}$ *and* $g(s) = \sum_{n\geq 1}\frac{b_n}{n^s}$ *are both convergent for every* s *with* $\mathrm{Re}(s) > \alpha$. *If* $f(s) = g(s)$ *for every such* s, *then* $a_n = b_n$ *for every* $n \geq 1$.

PROOF. By considering $h = \sum_{n\geq 1}\frac{a_n - b_n}{n^s}$, we see that it is enough to prove the assertion when all b_n are zero. In this case, we prove by induction on n that $a_n = 0$. Suppose that $a_1 = \ldots = a_{n-1} = 0$, and that $f(s) = 0$ for all s with $\mathrm{Re}(s) > \alpha$. It follows from Proposition 6.8 that the series of functions $\sum_{m\geq n}\frac{a_m n^s}{m^s}$ is uniformly convergent (to 0, by our assumption) for $s \in \mathbf{R}$, with $s > \rho$. For every $m > n$ we have $\lim_{s\to\infty}\frac{a_m n^s}{m^s} = 0$, hence $a_n = \lim_{s\to\infty}\sum_{m\geq n}\frac{a_m n^s}{m^s} = 0$. This completes the induction step.

□

As we have seen in Example 6.9, if $|a_m| \leq Cm^\alpha$ for all m, then the abscissa of convergence of the Dirichlet series $\sum_{n\geq 1}\frac{a_n}{n^s}$ is $\leq 1+\alpha$. The following proposition improves this upper bound when $\alpha \geq 0$ and when we have the similar bound for all sums $a_1 + \ldots + a_m$.

PROPOSITION 6.12. *If* $\alpha \in \mathbf{R}_{\geq 0}$ *is such that* $|\sum_{n=1}^m a_n| \leq Cm^\alpha$ *for all* m, *then the Dirichlet series* $\sum_{n\geq 1}\frac{a_n}{n^s}$ *is convergent in the half-plane* $\{s \mid \mathrm{Re}(s) > \alpha\}$.

PROOF. We follow a similar argument to that used in the proof of Proposition 6.8. Note that we have $|\sum_{n=m+1}^{m+\ell} a_n| \leq C((m+\ell)^\alpha + m^\alpha) \leq 2C(m+\ell)^\alpha$ for all m and ℓ. Consider $s \in \mathbf{C}$ with $\mathrm{Re}(s) > \alpha$, and let us write $s = x + yi$, with $x, y \in \mathbf{R}$. If we put $A_p = \sum_{n=m+1}^{m+p} a_n$ for all p, then we have

$$\left|\sum_{n=m+1}^{m+p}\frac{a_n}{n^s}\right| = \left|\frac{A_p}{(m+p)^s} + \sum_{\ell=1}^{p-1} A_\ell\left(\frac{1}{(m+\ell)^s} - \frac{1}{(m+\ell+1)^s}\right)\right|$$

$$\leq \frac{|A_p|}{(m+p)^x} + \sum_{\ell=1}^{p-1}|A_\ell s|\cdot\left|\int_{\log(m+\ell)}^{\log(m+\ell+1)} e^{-ts}dt\right|$$

$$\leq \frac{2C}{(m+p)^{x-\alpha}} + \sum_{\ell=1}^{p-1} |s| \int_{\log(m+\ell)}^{\log(m+\ell+1)} |A_\ell| e^{-tx} dt.$$

Since $|A_\ell| \leq 2C(m+\ell)^\alpha$, it follows that $|A_\ell| \leq 2Ce^{\alpha t}$ for $t \geq \log(m+\ell)$. Therefore

$$\sum_{\ell=1}^{p-1} \int_{\log(m+\ell)}^{\log(m+\ell+1)} |A_\ell| e^{-tx} dt \leq 2C \cdot \sum_{\ell=1}^{p-1} \int_{\log(m+\ell)}^{\log(m+\ell+1)} e^{t(\alpha-x)} dt = 2C \cdot \int_{\log(m+1)}^{\log(m+p)} e^{t(\alpha-x)} dt$$

$$= \frac{2C}{x-\alpha} \left(\frac{1}{(m+1)^{x-\alpha}} - \frac{1}{(m+p)^{x-\alpha}} \right).$$

We thus conclude that

$$\left| \sum_{n=m+1}^{m+p} \frac{a_n}{n^s} \right| \leq \frac{2C}{(m+p)^{x-\alpha}} + \frac{2C|s|}{x-\alpha} \left(\frac{1}{(m+1)^{x-\alpha}} - \frac{1}{(m+p)^{x-\alpha}} \right),$$

and for fixed s this can be made arbitrarily small by taking m large enough. This shows that $\sum_{n\geq 1} \frac{a_n}{n^s}$ is convergent. □

PROPOSITION 6.13. *The Riemann zeta function has a meromorphic continuation to the half-space* $\{s \mid \mathrm{Re}(s) > 0\}$*, with a unique pole at* $s = 1$*, which is simple, and with residue* 1*.*

PROOF. The trick is to consider the following auxiliary Dirichlet series

$$\zeta_r(s) = \sum_{n\geq 1} \frac{a_{n,r}}{n^s} = \sum_{r \not| m} \frac{1}{m^s} - \sum_{r|m} \frac{r-1}{m^s},$$

for every $r \geq 2$. It is clear that $\sum_{n=1}^{m} a_{n,r} \in \{0, 1, \ldots, r-1\}$, hence Proposition 6.12 applies to give that $\zeta_r(s)$ is a holomorphic function on $\{s \mid \mathrm{Re}(s) > 0\}$. It is clear that for $\mathrm{Re}(s) > 1$ we have $\zeta_r(s) + r^{1-s}\zeta(s) = \zeta(s)$, hence

$$\zeta(s) = \frac{\zeta_r(s)}{1 - r^{1-s}}.$$

This shows that ζ has a meromorphic continuation to the half-plane $\{s \mid \mathrm{Re}(s) > 0\}$. Furthermore, every pole in this region is simple, and it is of the form $1 + \frac{2m\pi i}{\log(r)}$, for some $m \in \mathbf{Z}$. By considering $r = 2$ and $r = 3$, we see that in fact, the only possible pole of ζ in this region is at $s = 1$.

Note that the residue at 1 is $\frac{\zeta_2(1)}{\log(2)}$. Recall that we have $\log(1+x) = \sum_{n\geq 1} (-1)^{n-1} \frac{x^n}{n}$ for $|x| < 1$. The series is convergent at $x = 1$, hence by Abel's theorem the sum for $x = 1$ is equal to $\lim_{x\in\mathbf{R}, x\to 1} \log(x) = \log(2)$. Therefore $\log(2) = \sum_{n\geq 1} \frac{(-1)^{n-1}}{n} = \zeta_2(1)$, and we see that the residue of ζ at $s = 1$ is 1. □

In fact, ζ can be meromorphically extended to $\mathbf{C}$, and the only pole is $s = 1$. Furthermore, after multiplication by a suitable factor involving the Γ-function, ζ satisfies a functional equation. We refer to [**Lang**, Chapter XIII] for the statement of the functional equation, for proofs and generalizations.

In the case of Dirichlet series with nonnegative coefficients, the sum has a singularity at the real point on the boundary of the half-plane of convergence. More precisely, we have the following.

PROPOSITION 6.14. *Consider a Dirichlet series $\sum_{n\geq 1}\frac{a_n}{n^s}$, with $a_n \in \mathbf{R}_{\geq 0}$ for all n. If the abscissa of convergence ρ is finite, then the sum $f(s)$ of this series can not be analytically extended to a holomorphic function in the neighborhood of $s=\rho$.*

PROOF. Let us denote $f(s)=\sum_{n\geq 1}\frac{a_n}{n^s}$ for $\mathrm{Re}(s)>\rho$, and suppose that f has an analytic continuation to a neighborhood of ρ. In this case there is $\epsilon>0$ such that f is holomorphic inside the disc $\{s \mid |s-(\rho+1)|<1+2\epsilon\}$. Therefore in the interior of this disc we have the Taylor expansion

$$f(s)=\sum_{i\geq 0}\frac{f^{(i)}(\rho+1)}{i!}(s-\rho-1)^i. \tag{6.14}$$

On the other hand, since the series converges uniformly in the half-space $\{s \mid \mathrm{Re}(s)>\rho\}$, we can differentiate term-by-term in this region to get

$$f^{(i)}(s)=\sum_{n\geq 1}\frac{a_n}{n^s}(-\log n)^i. \tag{6.15}$$

By taking $s=\rho+1$, we get

$$f^{(i)}(\rho+1)=\sum_{n\geq 1}\frac{a_n}{n^{\rho+1}}(-\log n)^i. \tag{6.16}$$

Computing $f(\rho-\epsilon)$ via (6.14), and using also (6.16), we deduce that

$$f(\rho-\epsilon)=\sum_{i\geq 0}\frac{f^{(i)}(\rho+1)}{i!}(-1-\epsilon)^i=\sum_{i\geq 0}\sum_{n\geq 1}\frac{a_n}{n^{\rho+1}}\frac{((1+\epsilon)\log n)^i}{i!}.$$

Since this is a convergent double series with nonnegative terms, we may change the order of summation, and deduce that

$$\sum_{n\geq 1}\frac{a_n}{n^{\rho+1}}\sum_{i\geq 0}\frac{((1+\epsilon)\log n)^i}{i!}=\sum_{n\geq 1}\frac{a_n}{n^{\rho-\epsilon}}$$

is convergent. Hence our Dirichlet series is convergent for $s=\rho-\epsilon$, a contradiction. □

Suppose now that $\sum_{n\geq 1}\frac{a_n}{n^s}$ is an arbitrary Dirichlet series. The *abscissa of absolute convergence* ρ^+ of this series is the abscissa of convergence of $\sum_{n\geq 1}\frac{|a_n|}{n^s}$. It is clear that if ρ is the abscissa of convergence of the given Dirichlet series, then $\rho\leq\rho^+$. One can show that $\rho^+\leq\rho+1$, hence in particular $\rho<\infty$ if and only if $\rho^+<\infty$. We will not use this result, so we simply refer to [**MoVa**, Theorem 1.4] for a proof.

We now want to show that in the half-plane of absolute convergence, under suitable multiplicative properties, we can decompose the sum of the Dirichlet series as an Euler product. Before doing this, let us recall a basic lemma concerning infinite products. Recall that if $(a_n)_{n\geq 1}$ is a sequence of complex numbers, then the product $\prod_{n\geq 1}(1+a_n)$ is *absolutely convergent* if the series $\sum_{n\geq 1}a_n$ is absolutely convergent.

LEMMA 6.15. *If the product $\prod_{n\geq 1}(1+a_n)$ is absolutely convergent, then it is convergent. Furthermore, the product is independent of the order of the factors, and it is zero if and only if one of the factors is zero.*

It is clear that if $(a_i)_{i\in I}$ is any set of complex numbers indexed by a countable set, then it makes sense to say that the product $\prod_{i\in I}(1+a_i)$ is absolutely convergent. The lemma implies that in this case the product $\prod_{i\in I}(1+a_i)$ is well-defined.

PROOF. The hypothesis implies in particular that $\lim_{n\to\infty} a_n = 0$. Therefore there is n_0 such that $|a_n| < 1$ for all $n \geq n_0$. For all statements in the lemma we may ignore finitely many of the factors, hence we may assume that $n_0 = 1$. Since

$$\log\left(\prod_{i=1}^{n}(1+a_i)\right) = \sum_{i=1}^{n}\log(1+a_i),$$

the first two assertions in the lemma follow if we show that the series $\sum_{i\geq 1}|\log(1+a_i)|$ is convergent. For every u with $|u| < 1$, we have

$$|\log(1+u)| = \left|\sum_{n\geq 1}(-1)^{n-1}\frac{u^n}{n}\right| \leq \sum_{n\geq 1}\frac{|u|^n}{n} = -\log(1-|u|) = \log(1+w) \leq w,$$

where $1+w = (1-|u|)^{-1}$. Note that $w = \frac{|u|}{1-|u|} \leq \frac{1}{2}|u|$ if $|u| \leq \frac{1}{2}$, hence $|\log(1+u)| \leq \frac{1}{2}|u|$ when $|u| \leq \frac{1}{2}$. Since $|a_i| \leq \frac{1}{2}$ for $i \gg 0$, the hypothesis that $\sum_{i\geq 1}|a_i|$ is convergent implies that $\sum_{i\geq 1}|\log(1+a_i)|$ is convergent.

For the last assertion in the lemma, note that if $\sum_{n\geq 1}\log(1+a_n) = u$, then the product $\prod_{n\geq 1}(1+a_n)$ is equal to $\exp(u)$, hence it is nonzero. □

REMARK 6.16. Note that the infinite product $\prod_{n\geq 1}(1+|a_n|)$ is convergent if and only if it is absolutely convergent. Indeed, the "if" part follows from the above lemma, while the "only if" part is a consequence of the fact that for every n

$$\sum_{i=1}^{n}|a_i| \leq \prod_{i=1}^{n}(1+|a_i|) \leq \prod_{i=1}^{\infty}(1+|a_i|).$$

This implies that the infinite product $\prod_{n\geq 1}(1+a_n)$ is absolutely convergent if and only if the product $\prod_{n\geq 1}(1+|a_n|)$ is convergent, which is the case if and only if the series with nonnegative terms $\sum_{n\geq 0}\log(1+|a_n|)$ is convergent.

EXERCISE 6.17. Consider $(a_{m,n})_{m,n\geq 1}$, with $a_{m,n} \in \mathbf{C}$. Show that if each infinite product $\prod_{n\geq 1} a_{m,n}$ is absolutely convergent and $b_m = \prod_{n\geq 1} a_{m,n}$, then the following are equivalent

i) The product $\prod_{m\geq 1} b_m$ is absolutely convergent.
ii) The product $\prod_{m,n\geq 1} a_{m,n}$ is absolutely convergent.

Furthermore, show that in this case $\prod_{m,n\geq 1} a_{m,n} = \prod_{m\geq 1} b_m$.

We say that a sequence $(a_n)_{n\geq 1}$ is *multiplicative* if $a_{mn} = a_m a_n$ whenever m and n are relatively prime. In this case we have $a_1 \cdot a_m = a_m$ for every m. In particular, we either have $a_m = 0$ for all m, or $a_1 = 1$. In order to avoid trivial cases, we always assume that $a_1 = 1$.

PROPOSITION 6.18. *Let $(a_n)_{n\geq 1}$ be a multiplicative sequence, and consider the Dirichlet series $f = \sum_{n\geq 1}\frac{a_n}{n^s}$. If the abscissa of absolute convergence ρ^+ is not $+\infty$, then for every s with $\mathrm{Re}(s) > \rho^+$ the following product over all positive prime*

integers

$$\prod_p \left(\sum_{m \geq 0} \frac{a_{p^m}}{p^{ms}} \right) \tag{6.17}$$

is absolutely convergent, and it is equal to $f(s)$. Furthermore, if we assume that all $a_n \geq 0$ and we know that the product (6.17) is convergent for every $s_0 \in \mathbf{R}$ with $s_0 > \alpha$, then $\rho = \rho^+ \leq \alpha$.

PROOF. Let $s \in \mathbf{C}$ be such that $\mathrm{Re}(s) > \rho^+$. By assumption, the series $\sum_{n \geq 1} \frac{a_n}{n^s}$ is absolutely convergent. In particular, we see that $\sum_p \sum_{m \geq 1} \frac{|a_{p^m}|}{p^{ms}}$ is absolutely convergent, hence the product (6.17) is absolutely convergent.

Let $f_p(s)$ be the factor in (6.17) corresponding to the prime p. If $p_1, \ldots, p_r$ are the first r prime integers, then the series

$$S_r := \sum_{n = p_1^{j1} \cdots p_r^{jr}} \frac{a_n}{n^s}$$

is absolutely convergent, where n varies over the positive integers whose prime factors are among $p_1, \ldots, p_r$. The sum of this series is equal to $\prod_{i=1}^r f_{p_i}(s)$. By assumption, S_r converges to $f(s)$, hence we get the assertion in the proposition.

Suppose now that all $a_m \geq 0$, and that $\prod_p \left(\sum_{m \geq 0} \frac{a_{p^m}}{p^{ms_0}} \right)$ is convergent whenever $s_0 \in \mathbf{R}$ with $s_0 > \alpha$. Let us fix such s_0. With the above notation, we see that S_r is finite, and $S_r \leq \prod_p \left(\sum_{m \geq 0} \frac{a_{p^m}}{p^{ms_0}} \right)$. Therefore the sequence $(S_r)_{r \geq 1}$ is convergent, and its limit is clearly equal to $\sum_{n \geq 1} \frac{a_n}{n^{s_0}}$. This implies that $\rho = \rho^+ \leq \alpha$. □

COROLLARY 6.19. *Under the assumptions in the above proposition, suppose that the sequence $(a_n)_{n \geq 1}$ is* strongly multiplicative, *in the sense that $a_{mn} = a_m a_n$ for all positive integers m and n, and $a_0 = 1$. In this case we have the decomposition*

$$\sum_{n \geq 1} \frac{a_n}{n^s} = \prod_p \frac{1}{1 - a_p p^{-s}}$$

for every $s \in \mathbf{C}$ with $\mathrm{Re}(s) > \rho^+$.

PROOF. The assertion follows from the formula in Proposition 6.18, noting that for every prime p we have

$$\sum_{m \geq 0} \frac{a_{p^m}}{p^{ms}} = \sum_{m \geq 0} \frac{a_p^m}{p^{ms}} = \frac{1}{1 - a_p p^{-s}}.$$

□

EXAMPLE 6.20. In the case of the Riemann zeta function we have $\rho^+ = \rho = 1$, and we get the product decomposition

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

for every $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$. Note also that since the product is absolutely convergent, it follows from Lemma 6.15 that $\zeta(s) \neq 0$ for every s with $\mathrm{Re}(s) > 0$.

Let us recall the notion of product of Dirichlet series. Given ℓ Dirichlet series $f_i = \sum_{n\geq 1} \frac{a_{n,i}}{n^s}$ for $1 \leq i \leq \ell$, let us consider the *product* of the f_i defined by $g = \sum_{n\geq 1} \frac{b_n}{n^s}$, where $b_n = \sum_{d_1\cdots d_\ell = n} a_{d_1,1}\cdots a_{d_\ell,\ell}$, the sum being over all tuples of positive integers $(d_1,\ldots,d_\ell)$ such that $d_1\cdots d_\ell = n$.

PROPOSITION 6.21. *With the above notation, the following hold:*

i) *We have the following relation between the abscissas of absolute convergence*
$$\rho^+(g) \leq \max_i \rho^+(f_i),$$
and for every $s \in \mathbf{C}$ with $\mathrm{Re}(s) > \max_i \rho^+(f_i)$, we have $g(s) = \prod_{i=1}^\ell f_i(s)$.

ii) *If each sequence $(a_{n,i})_{n\geq 1}$ is multiplicative, and if we consider the Euler product decompositions $f_i = \prod_p f_i^{(p)}$, then the sequence $(b_n)_{n\geq 1}$is multiplicative, and the Euler product decomposition of g is given by $g = \prod_p g^{(p)}$, where $g^{(p)} = \prod_{i=1}^\ell f_i^{(p)}$.*

iii) *If $h = \sum_{n\geq 1} \frac{c_n}{n^s}$ is a Dirichlet series such that $h(s) = \prod_{i=1}^\ell f_i(s)$ for $\mathrm{Re}(s) \gg 0$, then $b_n = c_n$ for every n. In particular, we have $\rho^+(h) \leq \max_i \rho^+(f_i)$.*

PROOF. All the assertions are straightforward to prove, so we leave them as an exercise. We only note that iii) is a consequence of i) and of Proposition 6.11. □

In what follows we make some considerations that will be useful in the next section, when dealing with zeta functions of arithmetic schemes. Suppose that f is a formal power series $f = \sum_{m\geq 0} a_m t^m \in \mathbf{C}[\![t]\!]$. Given a prime p, we may associate to f the Dirichlet series $\widetilde{f} = \sum_{m\geq 0} \frac{a_m}{p^{ms}}$. If $r(f)$ is the radius of convergence of f, then $\widetilde{f}(s)$ is absolutely convergent for $\mathrm{Re}(s) > -\frac{\log(r(f))}{\log p}$, and it is divergent for $\mathrm{Re}(s) < -\frac{\log(r(f))}{\log p}$. Therefore $\rho(\widetilde{f}) = \rho^+(\widetilde{f}) = -\frac{\log(r(f))}{\log p}$.

If $f(0) = 0$, then we may consider $g = \exp(f)$. It is clear that $r(g) \geq r(f)$, and it follows from the above formulas that $\rho(\widetilde{g}) \leq \rho(\widetilde{f})$.

Suppose now that for every prime p we have a formal power series $f_p = \sum_{m\geq 1} a_m^{(p)} t^m$ with $a_m \in \mathbf{R}_{\geq 0}$ for all m, and consider as above the corresponding Dirichlet series $\widetilde{f}_p = f_p(1/p^s) = \sum_{m\geq 0} \frac{a_m^{(p)}}{p^{ms}}$. Let $g_p = \exp(f_p)$, and $\widetilde{g}_p = g_p(1/p^s)$.

PROPOSITION 6.22. *With the above notation, suppose that the $C > 0$ and $\alpha \in \mathbf{R}$, and $p_0 \in \mathbf{Z}_{>0}$ are such that*
$$a_m^{(p)} \leq \begin{cases} Cp^{m\alpha}, & \text{if } p \geq p_0, m \geq 1; \\ Cp^{m(\alpha+1)}, & \text{if } p < p_0, m \geq 1. \end{cases}$$
In this case $\prod_p \widetilde{g}_p(s)$ is the Euler product decomposition of a Dirichlet series with nonnegative coefficients, which is absolutely convergent in the half-plane $\{s \mid \mathrm{Re}(s) > \alpha + 1\}$.

PROOF. Let us write $g_p = \sum_{m\geq 0} b_m^{(p)} t^m$, so that $\widetilde{g}_p(s) = \sum_{m\geq 0} \frac{b_m^{(p)}}{p^{ms}}$. Note that $b_0^{(p)} = 1$, and since $a_m^{(p)} \geq 0$ for all m and p, we have $b_m^{(p)} \geq 0$ for all m and p. For a positive integer n having the prime decomposition $n = p_1^{m_1}\cdots p_r^{m_r}$, we put $b_n = b_{m_1}^{(p_1)}\cdots b_{m_r}^{(p_r)}$. Let us consider the Dirichlet series $g(s) = \sum_{n\geq 1} \frac{b_n}{n^s}$.

It is enough to show that the product $\prod_p \widetilde{g}_p(s)$ is convergent for every $s \in \mathbf{R}$ with $s > \alpha + 1$. Indeed, we can then apply Proposition 6.18 to deduce that this is the Euler product decomposition of $g(s)$, whose abscissa of convergence is $\leq \alpha + 1$.

Let us fix $s \in \mathbf{R}$ with $s > \alpha + 1$. Using the definition of the $\widetilde{g}_p$, we see that it is enough to show that $\sum_p \widetilde{f}_p(s)$ is convergent. Note that this is a series with nonnegative terms, and by assumption we have

$$\sum_{p<p_0} \sum_{m\geq 1} \frac{a_m^{(p)}}{p^{ms}} \leq C \cdot \sum_{p<p_0} \sum_{m\geq 1} p^{m(\alpha-s+1)} = C \cdot \sum_{p<p_0} \frac{1}{p^{s-\alpha-1}-1} < \infty, \text{ and}$$

$$\sum_{p\geq p_0} \sum_{m\geq 1} \frac{a_m^{(p)}}{p^{ms}} \leq C \cdot \sum_{p\geq p_0} \sum_{m\geq 1} p^{m(\alpha-s)} = C \cdot \sum_{p\geq p_0} \frac{1}{p^{s-\alpha}-1} \leq 2C \cdot \sum_{p\geq p_0} \frac{1}{p^{s-\alpha}} < \infty.$$

Since the above series are convergent, this completes the proof. □

6.5. The zeta function of an arithmetic scheme

In this section we consider arithmetic schemes, that is, schemes of finite type over $\mathbf{Z}$. For every such scheme X, we denote by X_p the fiber of X over the point $p\mathbf{Z}$ in $\operatorname{Spec} \mathbf{Z}$. This is a scheme of finite type over $\mathbf{F}_p$. The following lemma describes the set X_{cl} of closed points of an arithmetic scheme X.

LEMMA 6.23. *If X is a scheme of finite type over $\mathbf{Z}$, and $x \in X$ is a point, then x is a closed point if and only if its residue field $k(x)$ is a finite field. In this case, the image of x in $\operatorname{Spec} \mathbf{Z}$ is a closed point.*

PROOF. Let $\pi\colon X \to \operatorname{Spec} \mathbf{Z}$ denote the canonical morphism. If $k(x)$ is a finite field, then $k(\pi(x))$ is finite too, being a subfield of $k(x)$, hence $\pi(x)$ is a closed point $p\mathbf{Z}$. In this case we know that x is a closed point in the fiber X_p, hence it is closed in X.

Conversely, suppose that x is closed in X. If $U = \operatorname{Spec} A$ is an affine open neighborhood of x, then x is closed in U, hence it corresponds to a maximal ideal $\mathfrak{m} \subset A$. If $\pi(x)$ is a closed point, then we are done: since x is a closed point on a scheme of finite type over $\mathbf{F}_p$, the residue field $k(x)$ is finite. Suppose that $\pi(x)$ is the generic point of $\operatorname{Spec} \mathbf{Z}$. The field $K = A/\mathfrak{m}$ is a finitely generated $\mathbf{Z}$-algebra. In particular, it is a finitely generated $\mathbf{Q}$-algebra, hence it is finite over $\mathbf{Q}$ by Nullstellensatz. If B is the integral closure of $\mathbf{Z}$ in K, then B is a Dedekind domain with field of fractions K. Since K is a finitely generated $\mathbf{Z}$-algebra, it is also finitely generated over B, hence it is equal to $B[1/b]$ for some nonzero $b \in B$. However, b is only contained in finitely many prime ideals, while B has infinitely many such ideals. Therefore $B[1/b]$ can not be a field. This contradiction shows that $\pi(x)$ is a closed point. □

Let X be an arithmetic scheme. For every closed point $x \in X$, we put $N(x) = |k(x)|$. Note that given any M, there are only finitely many closed points $x \in X$ with $N(x) \leq M$. Indeed, this condition bounds the characteristic of $k(x)$, and we have seen in Proposition 2.1 that on every X_p there are only finitely many closed points with $\deg(k(x)/\mathbf{F}_p)$ bounded.

A 0-cycle on X is an element of the free abelian group on the set of closed points of X. We say that a 0-cycle $\alpha = \sum_{i=1}^{\ell} m_i x_i$ is *effective* if all m_i are non-negative.

In this case, we put $N(\alpha) := \prod_i N(x_i)^{m_i}$. Note that if α is an effective cycle on X_p, then $N(\alpha) = p^{\deg(\alpha)}$.

The zeta function L_X of X is defined by $L_X(s) = \sum_{n\geq 1} \frac{a_n}{n^s}$, where a_n is the number of effective 0-cycles α on X with $N(\alpha) = n$ (with the convention $a_1 = 1$). Note that the sequence $(a_n)_{n\geq 1}$ is multiplicative: this is an easy consequence of the fact that for every closed point $x \in X$, $N(x)$ is a prime power, hence $N(x)$ divides a product mn, with m and n relatively prime if and only if it divides precisely one of m and n. Therefore we have an Euler product decomposition of L_X as $L_X(s) = \prod_p L_{X,p}(s)$, where

$$L_{X,p}(s) = \sum_{n\geq 0} \frac{b_n^{(p)}}{p^{ns}},$$

where $b_n^{(p)}$ is the number of effective 0-cycles on X_p of degree n. It follows from Remark 2.9 that $L_{X,p}(s) = Z(X_p, p^{-s}) = L_{X_p}(s)$ (for a possibly non-reduced scheme W of finite type over $\mathbf{F}_p$, we put $Z(W,t) = Z(W_{\mathrm{red}}, t)$).

Up to this point, the above Euler product only holds at a formal level, since we have not proved yet that the above Dirichlet series converges in a nonempty half-plane. Our main goal in this section is to prove this fact, to compute the abscissa of convergence, and to show that the zeta function has a meromorphic continuation to a half-space containing the half-plane of convergence. Note that the above Dirichlet series has nonnegative coefficients, so in this case the abscissa of absolute convergence is equal to the abscissa of convergence.

As a warm-up, we start with the case of a scheme that lies over a closed point in $\operatorname{Spec}\mathbf{Z}$. Suppose that Y is a scheme of finite type over $\mathbf{F}_p$. Recall that in this case we have $L_Y(s) = Z(Y, p^{-s})$. The following is the main result in this setting.

THEOREM 6.24. *If Y is a scheme of finite type over $\mathbf{F}_p$, then the Dirichlet series with nonnegative coefficients $L_Y(s)$ is convergent for $\mathrm{Re}(s) > r := \dim(Y)$, and it has no zeros in this half-plane. Furthermore, if the r-dimensional irreducible components of Y are $Y_1, \ldots, Y_\ell$, and each $Y_j \times_{\mathbf{F}_p} \overline{\mathbf{F}_p}$ has m_j irreducible components, then*

$$L_Y(s) = \widetilde{L}(s) \cdot \prod_{j=1}^{\ell} \frac{1}{1 - p^{m_j(r-s)}},$$

where $\widetilde{L}$ is the sum of a Dirichlet series with abscissa of absolute convergence $\leq r - \frac{1}{2}$. In particular, the abscissa of convergence of L_Y is r, and L_Y admits a meromorphic continuation to the half-plane $\{s \mid \mathrm{Re}(s) > r - \frac{1}{2}\}$, such that the set of poles is given by

$$\left\{ r + \frac{2\pi i m}{m_j \log(p)} \mid m \in \mathbf{Z}, 1 \leq j \leq \ell \right\}.$$

PROOF. Let $f = \sum_{e\geq 1} \frac{N_e}{e} t^e$, where $N_e = |Y(\mathbf{F}_{p^e})|$, and $g = \exp(f)$, so that $L_Y(s) = g(p^{-s})$. We thus are in the setting discussed at the end of §4. It follows from Corollary 6.4 that there is a constant $\alpha_Y > 0$ such that $N_e \leq \alpha_Y p^{er}$ for every $e \geq 1$. This implies $N_e^{1/e} \leq \alpha_Y^{1/e} p^r$, so that the radius of convergence R of f is $\geq p^{-r}$, and we thus obtain

$$\rho(L_Y) = \rho^+(L_Y) = -\frac{\log(R)}{\log p} \leq r.$$

Note also that if $\mathrm{Re}(s) > r$, then $L_Y(s) = \exp(f(p^{-s}))$, hence it is nonzero. This proves the first assertion in the theorem.

The second assertion is the deeper one, and for this we will make use the Lang-Weil estimate. Let $f_1 = \sum_{i=1}^{\ell} \sum_{m_i | e} \frac{m_i p^{er}}{e} t^e$ and $f_2 = f - f_1$. Note that

$$f_1 = \sum_{i=1}^{\ell} \sum_{j \geq 1} \frac{p^{jm_i r} t^{jm_i}}{j} = -\sum_{i=1}^{\ell} \log(1 - p^{m_i r} t^{m_i}),$$

hence $\exp(f_1) = \prod_{i=1}^{\ell} \frac{1}{1-p^{rm_i} t^{m_i}}$. On the other hand, if we write $f_2 = \sum_{m \geq 1} \frac{b_m}{m} t^m$, it follows from Proposition 6.7 that there is a constant $C > 0$ such that $|b_m| \leq C p^{(r-\frac{1}{2})m}$ for all m. Arguing as above, we see that the radius of convergence of f_2 is $\geq p^{-r+\frac{1}{2}}$. Therefore the abscissa of convergence of $\widetilde{L}(s) = \exp(f_2)(p^{-s})$ is $\leq r - \frac{1}{2}$, and we have

$$L_Y(s) = \exp(f_1)(p^{-s}) \cdot \exp(f_2)(p^{-s}) = \widetilde{L}(s) \cdot \prod_{i=1}^{\ell} \frac{1}{1 - p^{m_i(r-s)}}.$$

Note also that if $\mathrm{Re}(s) > r - \frac{1}{2}$, then $\widetilde{L}(s) = \exp(f_2(p^{-s})) \neq 0$. The last assertions in the theorem are now easy consequences. □

EXERCISE 6.25. Let $(m_i)_{i \in I}$ be positive integers, where I is a countable set, such that for every M there are only finitely many i with $m_i \leq M$. Show that if the power series $f(t) = \prod_{i \in I} (1 - t^{m_i})^{-1} \in \mathbf{Z}[\![t]\!]$ has radius of convergence R, then for every $u \in \mathbf{C}$ with $|u| < \min\{1, R\}$ the product $\prod_{i \in I} (1 - u^{m_i})^{-1}$ is absolutely convergent and $f(u) = \prod_{i \in I} (1 - u^{m_i})^{-1}$.

EXERCISE 6.26. Show that if Y is a scheme of finite type over $\mathbf{F}_p$, then for every $s \in \mathbf{C}$ with $\mathrm{Re}(s) > \dim(Y)$ the product $\prod_{x \in Y_{\mathrm{cl}}} (1 - N(x)^{-s})^{-1}$ is absolutely convergent, and $L_Y(s) = \prod_{x \in X_{\mathrm{cl}}} (1 - N(x)^{-s})^{-1}$.

The case of an arithmetic scheme X whose irreducible components dominate $\operatorname{Spec} \mathbf{Z}$ is more involved. We begin by giving an upper-bound for the abscissa of convergence of an arbitrary arithmetic scheme. This will be a consequence of the following complement to Corollary 6.4.

PROPOSITION 6.27. *For every arithmetic scheme X of dimension r, there is a constant $c_X > 0$ and p_0 such that for every prime $p \geq p_0$ and every $e \geq 1$, we have*

$$\#X(\mathbf{F}_{p^m}) \leq \begin{cases} c_X p^{m(r-1)}, & \text{if } p \geq p_0, m \geq 1; \\ c_X p^{mr}, & \text{if } p < p_0, m \geq 1. \end{cases}$$

PROOF. It is enough to show that there is c_X and p_0 such that $\#X(\mathbf{F}_{p^m}) \leq c_X p^{m(r-1)}$ for all $p \geq p_0$ and $m \geq 1$. Indeed, applying Proposition 6.7 to each X_p with $p < p_0$, we see that after possibly enlarging c_X we have $\#X(\mathbf{F}_{p^m}) \leq p^{mr}$ for all $p < p_0$ and $m \geq 1$.

We first prove this assertion in the case when X is irreducible, and it is smooth and projective over $\operatorname{Spec} \mathbf{Z}[1/N]$ for some positive integer N. Consider an embedding $X \hookrightarrow \mathbf{P}^n_{\mathbf{Z}[1/N]}$, and let d denote the degree of the fibers. In particular, for every prime p that does not divide N, $X_p \hookrightarrow \mathbf{P}^n_{\mathbf{F}_p}$ is a smooth closed subvariety of dimension $r-1$ and degree d. In particular, $X_p \times_{\mathbf{F}_p} \overline{\mathbf{F}_p}$ has $\leq d$ irreducible components. Applying Proposition 6.6 to each connected component of X, we see

that there is a positive constant c_X such that $\#X(\mathbf{F}_{p^e}) \leq c_X p^{(r-1)e}$ for every p that does not divide N, and every $e \geq 1$.

We now consider the general case, that we prove by induction on r. If $r = 0$, then X_p is empty for $p \gg 0$, and the assertion to prove is trivial. Suppose that $r \geq 1$. Note first that we may assume that X is irreducible: if $X_1, \ldots, X_\ell$ are the irreducible components of X, and if we can find c_{X_i} for every i, then it is enough to take $c_X = \sum_{i=1}^{\ell} c_{X_i}$.

Suppose from now on that X is irreducible, and after replacing X by X_{red} we may also assume that X is reduced. If X does not dominate $\operatorname{Spec} \mathbf{Z}$, then X_p is empty for $p \gg 0$, hence the assertion to prove is trivial. We henceforth assume that X dominates $\operatorname{Spec} \mathbf{Z}$.

Note that if X is birational to Y, for an integral scheme Y of finite type over $\operatorname{Spec} \mathbf{Z}$, and if we can find c_Y as required, then we can also find c_X. Indeed, if V is an open subset of X isomorphic to an open subset of Y, then we can find $c_{X \smallsetminus V}$ by induction, and it is enough to take $c_X = \max\{c_Y, c_{X \smallsetminus V}\}$.

In particular, we may assume that X is projective over $\operatorname{Spec} \mathbf{Z}$. We apply Hironaka's theorem on resolution of singularities to find a projective birational morphism $\phi_{\mathbf{Q}} \colon \widetilde{X}_{\mathbf{Q}} \to X \times_{\mathbf{Z}} \mathbf{Q}$, with $\widetilde{X}_{\mathbf{Q}}$ nonsingular, hence smooth over $\mathbf{Q}$. We can find a positive integer N such that $\phi_{\mathbf{Q}}$ is obtained by base-change from a projective birational morphism $\phi \colon \widetilde{X} \to X \times_{\mathbf{Z}} \mathbf{Z}[1/N]$, such that $\widetilde{X}$ is smooth and projective over $\operatorname{Spec} \mathbf{Z}[1/N]$. We have already seen that the assertion in the proposition holds for $\widetilde{X}$, and since X is birational to $\widetilde{X}$, it follows that we can find c_X as required. This completes the proof of the proposition. □

Corollary 6.28. *If X is an arithmetic scheme of dimension r, then the Dirichlet series with nonnegative coefficients L_X is convergent in $\{s \mid \mathrm{Re}(s) > r\}$, and it has no zeros in this region.*

Proof. Let $f_p = \sum_{e \geq 1} \frac{N_e(p)}{e} t^e$, where $N_e(p) = \#X(\mathbf{F}_{p^e})$. It follows from Proposition 6.27 that there is a constant $c_X > 0$ and p_0 such that the series f_p satisfy the conditions in Proposition 6.22, with $\alpha = r - 1$. Since $\prod_p \exp(f_p(p^{-s}))$ is the Euler product corresponding to L_X, we deduce that $L_X(s)$ is (absolutely) convergent for $\mathrm{Re}(s) > r$. Furthermore, each of the factors of the Euler product is nonzero, hence $L_X(s)$ is nonzero in this half-plane. □

Remark 6.29. It follows from Corollary 6.28 and Proposition 6.18 that if X is an arithmetic scheme of dimension r, then $L_X(s) = \prod_p L_{X_p}(s)$ whenever $\mathrm{Re}(s) > r$. Furthermore, it follows from Exercise 6.26 that for every prime p, we have $L_{X_p}(s) = \prod_{x \in (X_p)_{\mathrm{cl}}} (1 - N(x)^{-s})^{-1}$, and the product is absolutely convergent. We conclude using Exercise B.22 that

$$L_X(s) = \prod_{x \in X_{\mathrm{cl}}} \left(1 - N(x)^{-s}\right)^{-1},$$

and the product is absolutely convergent.

Example 6.30. Let K be a number field and $\mathcal{O}_K$ the ring of integers of K (that is, the ring of elements of K that are integral over $\mathbf{Z}$). The zeta function of K (also called the Dedekind zeta function of K) is $\zeta_K := L_{\operatorname{Spec} \mathcal{O}_K}$. Corollary 6.28 implies that ζ_K is (absolutely) convergent in the half-plane $\{s \mid \mathrm{Re}(s) > 1\}$. We

deduce from the previous remark that we have a product description in this region

$$\zeta_K(s) = \prod_{P \in \mathrm{Spec}(\mathcal{O}_K)} \left(1 - \frac{1}{N(P)^s}\right)^{-1}.$$

The description of ζ_K as a Dirichlet series can also be written as

$$\zeta_K(s) = \sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s},$$

where the sum is over all proper nonzero ideals $\mathfrak{a}$ of $\mathcal{O}_K$, and where $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$ (by the unique factorization of an ideal in $\mathcal{O}_K$ as a product of prime ideals, we can identify nonzero ideals in $\mathcal{O}_K$ with effective cycles on $\operatorname{Spec} \mathcal{O}_K$, such that the two definitions of $N(\mathfrak{a})$ are compatible). Of course, if $K = \mathbf{Q}$, then ζ_K is the Riemann zeta function.

EXAMPLE 6.31. Recall that by Corollary 2.23 we have

$$Z(\mathbf{P}^n_{\mathbf{F}_p}, t) = \frac{1}{(1-t)(1-pt)\cdots(1-p^n t)}.$$

Therefore the zeta function of $\mathbf{P}^n_{\mathbf{Z}}$ is given by

$$L_{\mathbf{P}^n_{\mathbf{Z}}}(s) = \prod_p Z(\mathbf{P}^n_{\mathbf{F}_p}, p^{-s}) = \prod_{i=0}^n \prod_p \frac{1}{(1-p^{i-s})} = \prod_{i=0}^n \zeta(s-i).$$

REMARK 6.32. If X is an arithmetic scheme, Y is a closed subscheme of X, and $U = X \smallsetminus Y$, then $L_X(s) = L_Y(s)L_U(s)$ for all $s > \dim(X)$. Indeed, this is a consequence of the Euler product description of the zeta function, and of the fact that $Z(X_p, t) = Z(Y_p, t) \cdot Z(U_p, t)$ for all primes p. In particular, we see that L_X is the product of L_Y and L_U in the sense of Proposition 6.21, and therefore $\rho(L_X) \leq \max\{\rho(L_Y), \rho(L_U)\}$.

Our last result in this section describes, in particular, the abscissa of convergence of zeta functions of arithmetic schemes.

THEOREM 6.33. *If X is an arithmetic scheme of dimension r, then the following hold:*

i) *The abscissa of convergence of L_X is $\rho = r$.*
ii) *L_X admits a meromorphic continuation to the half-plane $\{s \mid \mathrm{Re}(s) > r - \epsilon\}$, for some $\epsilon > 0$, and $s = r$ is a pole.*
iii) *If X is irreducible and dominates $\operatorname{Spec} \mathbf{Z}$, then the only pole of L_X in the half-plane $\{s \mid \mathrm{Re}(s) > r - \epsilon\}$, with ϵ as in ii), is at $s = r$, and this occurs with order one.*

In fact, as we will explain below, one can show that one can take $\epsilon = \frac{1}{2}$ in the theorem. The key ingredient that we will need, in addition to the Lang-Weil estimate, is given by the special case of the ring of integers in a number field. This is the content of the following proposition.

PROPOSITION 6.34. *If K is a number field with $\deg(K/\mathbf{Q}) = \ell$, then ζ_K admits a meromorphic continuation to the half-plane $\{s \mid \mathrm{Re}(s) > 1 - \frac{1}{\ell}\}$. In this region the only pole is $s = 1$, and this occurs with order one. In particular, the abscissa of convergence of ζ_K is $\rho = 1$.*

PROOF. We will use the following result from algebraic number theory: there is a positive number α_K such that if $i(m)$ denotes the number of proper nonzero ideals I in $\mathcal{O}_K$ with $N(I) \leq m$, then

$$\frac{i(m) - \alpha_K m}{m^{1-\frac{1}{\ell}}}$$

is bounded see [Mar, Theorem 39]. This implies that if we write $\zeta_K - \alpha_K \zeta(s)$ as a Dirichlet series $\sum_{m\geq 1} \frac{b_m}{m^s}$, then there is a positive constant C such that $|b_1 + \ldots + b_m| \leq C m^{1-\frac{1}{\ell}}$ for all m. Proposition 6.12 implies that $\zeta_K - \alpha_K \zeta$ is analytic in the half-plane $\{s \mid \mathrm{Re}(s) > 1 - \frac{1}{\ell}\}$. On the other hand, by Proposition 6.13 we know that ζ is meromorphic in the half-plane $\{s \mid \mathrm{Re}(s) > 0\}$, with a unique (simple) pole at $s = 1$. This gives the assertions in the proposition concerning ζ_K. □

One can show that, in fact, ζ_K admits a meromorphic continuation to $\mathbf{C}$, such that the only pole is at $s = 1$. However, the proof is quite involved, so we refer to [Lang, Chapter XIII] for this result.

PROOF OF THEOREM 6.33. Note first that if U is an open subset of X such that $\dim(W) < \dim(X)$, where $W = X \smallsetminus U$, then the theorem holds for X if and only if it holds for U. Indeed, $L_X(s) = L_W(s) L_U(s)$ by Remark 6.32. Since $\dim(W) \leq r-1$, the function L_W is analytic in $\{s \mid \mathrm{Re}(s) > r-1\}$ by Corollary 6.28, and it has no zeros in this half-plane. Therefore the assertions in the theorem hold for X if and only if they hold for U. This implies, in particular, that if X and Y are birational integral schemes, then the theorem holds for X if and only if it holds for Y.

Given any X, let us consider an affine open subset U of X with $\dim(X \smallsetminus U) < r$, such that U is isomorphic to the disjoint union of some U_i, with each U_i irreducible of dimension r. Since $L(U, s) = \prod_i L_{U_i}(s)$, it is clear that if each U_i satisfies properties i) and ii), then so does U, and therefore so does X. This shows that we may assume that X is affine and irreducible, and after replacing X by X_{red}, we may assume that X is integral.

If X does not dominate $\mathrm{Spec}\, \mathbf{Z}$, then $X = X_p$ for some p. In this case, Theorem 6.24 shows that properties i) and ii) are satisfied with $\epsilon = \frac{1}{2}$. Hence from now on we may assume that X dominates $\mathrm{Spec}\, \mathbf{Z}$. Arguing as in the proof of Proposition 6.27, we find an integral scheme Y that is smooth and projective over some $\mathrm{Spec}\, \mathbf{Z}[1/N]$, connected, and that is birational to X. As we have seen, it is enough to show that Y satisfies the assertions in the theorem.

Let $\pi \colon Y \to \mathrm{Spec}\, \mathbf{Z}[1/N]$ be the structure morphism. After possibly replacing N by a multiple, we may assume that $\pi_*(\mathcal{O}_Y)$ is free (say, of rank m) and $\pi_*(\mathcal{O}_{Y_p}) \simeq \pi_*(\mathcal{O}_Y) \otimes \mathbf{Z}/p\mathbf{Z}$ for all primes p that do not divide N. Therefore $A = \Gamma(Y, \mathcal{O}_Y)$ is an integral domain, free of rank m over $\mathbf{Z}[1/N]$. If $K = A \otimes_{\mathbf{Z}} \mathbf{Q}$, then K is a domain that is a finite extension of $\mathbf{Q}$, hence it is a number field, equal to the fraction field of A. If $\mathcal{O}_K$ is the ring of integers in K, then we have an inclusion $A \subseteq \mathcal{O}_K[1/N]$. After possibly replacing N by a multiple, we may assume that $A = \mathcal{O}_K[1/N]$ and that $O_K[1/N]$ is smooth over $\mathbf{Z}[1/N]$.

Suppose that p is a prime that does not divide N, and let us consider its prime decomposition in $\mathcal{O}_K$:

$$pO_K = P_1 \cdot \ldots \cdot P_\ell,$$

and let $m_i = [\mathcal{O}_K/P_i : \mathbf{F}_p]$. Note that the fiber Y_p is a smooth, $(r-1)$-dimensional projective variety, with ℓ irreducible components $Y_p^{(1)}, \ldots, Y_p^{(\ell)}$, with $Y_p^{(i)} \times_{\operatorname{Spec} \mathbf{F}_p} \operatorname{Spec} \overline{\mathbf{F}_p}$ having m_i irreducible components.

For every prime p that does not divide N, let $f_p = \sum_{e \geq 1} \frac{|X(\mathbf{F}_{p^e})|}{e} t^e$ and

$$f_p^{(1)} = \sum_{e \geq 1} \frac{|\operatorname{Spec} \mathcal{O}_K(\mathbf{F}_{p^e})|}{e} t^e = \sum_{i=1}^{\ell} \sum_{m_i | e} \frac{m_i}{e} t^e.$$

If we write $f_p^{(2)}(t) = f_p(t) - f_p^{(1)}(p^{r-1}t) = \sum_{e \geq 1} \frac{b_e^{(p)}}{e} t^e$, then we apply Proposition 6.6 to every connected component of Y_p to deduce that we have a positive constant C such that $|b_e^{(p)}| \leq C p^{(r-\frac{1}{2})e}$ for all e and all primes p that do not divide N. We deduce from Proposition 6.22 that $\prod_{p \not| N} \exp(f_p^{(2)})(p^{-s})$ is the Euler product of a Dirichlet series $\widetilde{L_Y}$ that is absolutely convergent in the half-plane $\{s \mid \operatorname{Re}(s) > r - \frac{1}{2}\}$, and which has no zeros in this region. On the other hand, if we put $Y' = \operatorname{Spec} \mathcal{O}_K[1/N]$, then $L_Y(s) = L_{Y'}(s - r + 1)\widetilde{L_Y}(s)$. Note that $\zeta_K(s) = L_{Y'}(s) \prod_j \left(1 - \frac{1}{N(P_j)^s}\right)^{-1}$, where the P_j are the (finitely many) prime ideals of $\mathcal{O}_K$ that lie over primes in $\mathbf{Z}$ dividing N. It follows from Proposition 6.34 that $L_{Y'}(s)$ is a meromorphic function in the half-plane $\{s \mid \operatorname{Re}(s) > 1 - \frac{1}{d}\}$, where $d = \deg(K/\mathbf{Q})$, and its only pole in this region is at $s = 1$, and this has order one. We deduce that properties i), ii), and iii) are satisfied by L_Y, where we may take $\epsilon = 1/d$. This completes the proof of the theorem. □

Remark 6.35. If one assumes the fact that ζ_K has a meromorphic continuation to the half-plane $\{s \mid \operatorname{Re}(s) > \frac{1}{2}\}$, we see that the argument in the proof of Theorem 6.33 shows that for every arithmetic scheme of dimension r, the zeta function L_X can be extended as a meromorphic function to $\{s \mid \operatorname{Re}(s) > r - \frac{1}{2}\}$.

Remark 6.36. If X is any arithmetic scheme of dimension r, then the order of $s = r$ as a pole of L_X is equal to the number of r-dimensional irreducible components of X. Indeed, if $X_1, \ldots, X_\ell$ are the r-dimensional irreducible components of X, then the order of $s = r$ as a pole of L_X is the sum of the corresponding orders of $s = r$ as a pole of each L_{X_j}. These orders in turn can be computed using Theorem 6.24 (for those X_j that lie in a fiber over $\operatorname{Spec} \mathbf{Z}$) and Theorem 6.33 (for those X_j that dominate $\operatorname{Spec} \mathbf{Z}$).

It is conjectured that for *every* arithmetic scheme X, the zeta function L_X admits a meromorphic continuation to $\mathbf{C}$. This seems, however, to be completely out of reach at the moment. One important case is when $X \times_{\mathbf{Z}} \mathbf{Q}$ is an elliptic curve, in which case the assertion is known to follow from the famous Taniyama-Shimura conjecture, proved in [Wil], [TW], and [BCDT].

CHAPTER 7

The Grothendieck ring of varieties and Kapranov's motivic zeta function

In this chapter we give an introduction to the Grothendieck ring of algebraic varieties, and discuss Kapranov's lifting of the Hasse-Weil zeta function to this Grothendieck ring. One interesting feature is that this makes sense over an arbitrary field. We will prove the rationality of Kapranov's zeta function for curves by a variant of the argument used Chapter 3 for the Hasse-Weil zeta function. We will end by discussing the results of Larsen and Lunts on Kapranov zeta functions of algebraic surfaces.

7.1. The Grothendieck ring of algebraic varieties

In this section we recall the definition and the basic properties of the Grothendieck ring of algebraic varieties. Let k be an arbitrary field. The *Grothendieck group* $K_0(\mathrm{Var}/k)$ *of varieties over* k is the quotient of the free abelian group on the set of isomorphism clases of varieties over k, by relations of the form

$$[X] = [Y] + [X \setminus Y],$$

where Y is a closed subvariety of the variety X (here $[X]$ denotes the image of the variety X in $K_0(\mathrm{Var}/k)$). Note that the above relation implies $[\emptyset] = 0$.

In fact, $K_0(\mathrm{Var}/k)$ is a commutative ring, with the product given by

$$[X] \cdot [Y] = [(X \times Y)_{\mathrm{red}}],$$

where the product on the right is understood to be over $\operatorname{Spec} k$. It is clear that this induces a bilinear map $K_0(\mathrm{Var}/k) \times K_0(\mathrm{Var}/k) \to K_0(\mathrm{Var}/k)$ that is commutative and associative, and has unit $\operatorname{Spec} k$.

The class of $\mathbf{A}^1_k$ in $K_0(\mathrm{Var}/k)$ is denoted by $\mathbf{L}$. Therefore $[\mathbf{A}^n_k] = \mathbf{L}^n$. The usual decomposition $\mathbf{P}^n_k = \mathbf{P}^{n-1}_k \sqcup \mathbf{A}^n_k$ implies by induction on n that $[\mathbf{P}^n_k] = 1 + \mathbf{L} + \ldots + \mathbf{L}^n$.

PROPOSITION 7.1. *Suppose that X is a variety over k, and we have a decomposition $X = Y_1 \sqcup \ldots \sqcup Y_r$, where all Y_i are locally closed subvarieties of X. In this case $[X] = [Y_1] + \ldots + [Y_r]$.*

PROOF. We argue by induction on $\dim(X)$ (the case $\dim(X) = 0$ being trivial), and then by induction on the number of irreducible components of X of maximal dimension. Let Z be an irreducible component of X of maximal dimension, and η_Z its generic point. If i is such that $\eta_Z \in Y_i$, then $Z \subseteq \overline{Y_i}$, and since Y_i is open in $\overline{Y_i}$, it follows that there is an open subset U of X contained in $Y_i \cap Z$ (for example, we may take to be the complement in $Y_i \cap Z$ of all irreducible components of X different from Z). By definition, we have

$$[Y_i] = [U] + [Y_i \setminus U] \text{ and } [X] = [U] + [X \setminus U]. \tag{7.1}$$

On the other hand, either $\dim(X \smallsetminus U) < \dim(X)$, or $\dim(X \smallsetminus U) = \dim(X)$ and $X \smallsetminus U$ has fewer irreducible components of maximal dimension than X does. Applying the induction hypothesis to the decomposition $X \smallsetminus U = (Y_i \smallsetminus U) \sqcup \bigsqcup_{j \neq i} Y_j$, we have

$$[X \smallsetminus U] = [Y_i \smallsetminus U] + \sum_{j \neq i} [Y_j]. \tag{7.2}$$

By combining (7.1) and (7.2), we get the formula in the proposition. □

Given a variety X over k, we want to define the class in $K_0(\mathrm{Var}/k)$ of a constructible subset of X. This is achieved using the following easy lemma.

LEMMA 7.2. *Any constructible subset W of a variety X over k can be written as a finite disjoint union of locally closed subsets.*

PROOF. We prove this by induction on $d = \dim(\overline{W})$, the case $d = 0$ being trivial. Let us write $W = W_1 \cup \ldots \cup W_r$, with all W_i locally closed, hence $\overline{W} = \overline{W_1} \cup \ldots \cup \overline{W_r}$. After replacing each W_i by its irreducible decomposition, we may assume that all W_i are irreducible. After renumbering, we may assume that $\overline{W_1}, \ldots, \overline{W_s}$ are the irreducible components of $\overline{W}$. Since each W_i is open in $\overline{W_i}$, the set $U = \bigcup_{i=1}^{s} \left(W_i \smallsetminus \bigcup_{j \neq i} \overline{W_j} \right)$ is open and dense in $\overline{W}$, and it is contained in W. If $V = W \smallsetminus U$, then V is constructible, and $\dim(\overline{V}) < \dim(\overline{W})$, hence by induction we have a decomposition $V = V_1 \sqcup \ldots \sqcup V_s$, with each V_i locally closed in X. Therefore we have a decomposition $W = U \sqcup V_1 \sqcup \ldots \sqcup V_s$, as required. □

Suppose now that X is a variety over k, and W is a constructible subset of X. By the above lemma, there is a disjoint decomposition $W = W_1 \sqcup \ldots \sqcup W_r$, with each W_i locally closed in X. We put $[W] := \sum_{i=1}^{r} [W_i]$.

PROPOSITION 7.3. *With the above notation, the following hold:*

i) *The definition of $[W]$, for W constructible in X, is independent of the disjoint decomposition.*
ii) *If $W_1, \ldots, W_s$ are disjoint constructible subsets of X, and $W = \bigcup_i W_i$, then $[W] = \sum_{i=1}^{s} [W_i]$.*

PROOF. Suppose that we have two decompositions into locally closed subsets

$$W = W_1 \sqcup \ldots \sqcup W_r \text{ and } W = W' \sqcup \ldots \sqcup W'_s.$$

Let us also consider the decomposition $W = \bigsqcup_{i,j} (W_i \cap W'_j)$. It follows from Proposition 7.1 that $[W_i] = \sum_{j=1}^{s} [W_i \cap W'_j]$ for every i, and $[W'_j] = \sum_{i=1}^{r} [W_i \cap W'_j]$ for every j. Therefore

$$\sum_{i=1}^{r} [W_i] = \sum_{i=1}^{r} \sum_{j=1}^{s} [W_i \cap W'_j] = \sum_{j=1}^{s} \sum_{i=1}^{r} [W_i \cap W'_j] = \sum_{j=1}^{s} [W'_j].$$

This proves i). The assertion in ii) follows from i): if we consider disjoint unions $W_i = W_{i,1} \sqcup \ldots \sqcup W_{i,m_i}$ for every i, with each $W_{i,j}$ locally closed in X, then $W = \bigsqcup_{i,j} W_{i,j}$, and

$$[W] = \sum_{i,j} [W_{i,j}] = \sum_{i} [W_i].$$

□

A morphism $f\colon X \to Y$ is *piecewise trivial*, with fiber F, if there is a decomposition $Y = Y_1 \sqcup \ldots \sqcup Y_r$, with all Y_i locally closed in Y, such that $f^{-1}(Y_i) \simeq Y_i \times F$ for all i.

PROPOSITION 7.4. *If $f\colon X \to Y$ is piecewise trivial with fiber F, then $[X] = [Y] \cdot [F]$ in $K_0(\mathrm{Var}/k)$.*

PROOF. By assumption, there is a decomposition $Y = Y_1 \sqcup \ldots \sqcup Y_r$ into locally closed subsets such that $[f^{-1}(Y_i)] = [F] \cdot [Y_i]$. By Proposition 7.1 we have $[X] = \sum_i [f^{-1}(Y_i)]$ and $[Y] = \sum_i [Y_i]$, hence we get the assertion in the proposition. □

EXAMPLE 7.5. It is clear that if E is a vector bundle on Y of rank n, then $E \to Y$ is piecewise trivial with fiber $\mathbf{A}^n_k$ and $\mathbf{P}(E) \to Y$ is piecewise trivial with fiber $\mathbf{P}^{n-1}_k$. Therefore $[E] = [Y] \cdot \mathbf{L}^n$ and $[\mathbf{P}(E)] = [Y](1 + \mathbf{L} + \ldots + \mathbf{L}^{n-1})$.

The following lemma is an immediate consequence of the definitions.

LEMMA 7.6. *If k'/k is a field extension, then we have a ring homomorphism $K_0(\mathrm{Var}/k) \to K_0(\mathrm{Var}/k')$, that takes $[X]$ to $[(X \times_k k')_{\mathrm{red}}]$ for every variety X over k.*

An Euler-Poincaré characteristic for varieties over k is a map χ that associates to a variety X over k an element $\chi(X)$ in a group A, such that if Y is a closed subvariety of X, we have $\chi(X) = \chi(Y) + \chi(X \setminus Y)$. Note that the map taking X to $[X] \in K_0(\mathrm{Var}/k)$ is the *universal Euler-Poincaré characteristic*: every Euler-Poincaré characteristic as above is induced by a unique group homomorphism $\chi\colon K_0(\mathrm{Var}/k) \to A$. If A is a ring, then the Euler-Poincaré characteristic is called *multiplicative* if χ is a ring homomorphism.

EXAMPLE 7.7. If k is a finite field, then for every finite extension K/k we have a multiplicative Euler-Poicaré characteristic with values in $\mathbf{Z}$, that takes X to $|X(K)|$. One can put all these together in a group homomorphism

$$K_0(\mathrm{Var}/k) \to (1 + t\mathbf{Z}[\![t]\!], \cdot), \ [X] \to Z(X, t).$$

EXAMPLE 7.8. If $k = \mathbf{C}$, then we have a multiplicative Euler-Poincaré characteristic that associates to X the usual Euler-Poincaré characteristic for singular cohomology $\chi_{\mathrm{top}}(X) = \sum_{i \geq 0} (-1)^i \dim_{\mathbf{Q}} H^i(X^{\mathrm{an}}, \mathbf{Q})$ (compare with the more refined invariant in Example 7.13 below). The fact that $\chi_{\mathrm{top}}(X)$ gives an Euler-Poincaré characteristic is a consequence of the fact that $\chi_{\mathrm{top}}(X)$ is also equal to the Euler-Poincaré characteristic for compactly supported cohomology $\chi^c_{\mathrm{top}}(X) := \sum_{i \geq 0} (-1)^i \dim_{\mathbf{Q}} H^i_c(X^{\mathrm{an}}, \mathbf{Q})$ (see [**Ful2**, p. 141-142]). Indeed, if Y is a closed subvariety of the complex variety X, and $U = X \setminus Y$, then there is a long exact sequence for cohomology with compact supports

$$\ldots \to H^i_c(U^{\mathrm{an}}, \mathbf{Q}) \to H^i_c(X^{\mathrm{an}}, \mathbf{Q}) \to H^i_c(Y^{\mathrm{an}}, \mathbf{Q}) \to H^{i+1}_c(U^{\mathrm{an}}, \mathbf{Q}) \to \ldots,$$

which implies $\chi^c_{\mathrm{top}}(X) = \chi^c_{\mathrm{top}}(U) + \chi^c_{\mathrm{top}}(Y)$.

The most convenient way of constructing Euler-Poincaré characteristics when the ground field is algebraically closed of characteristic zero involves a presentation of $K_0(\mathrm{Var}/k)$ due to Bittner [**Bit**]. The following lemma is elementary (and we have seen some of its avatars before).

LEMMA 7.9. *If* $\mathrm{char}(k) = 0$*, then* $K_0(\mathrm{Var}/k)$ *is generated by classes of nonsingular, connected, projective varieties over* k*. More precisely, given any irreducible variety* X *of dimension* n*, there is a nonsingular, irreducible, projective variety* Y *that is birational to* X *such that* $[X] - [Y] = \sum_{i=1}^{N} m_i[W_i]$*, for some smooth, projective, irreducible varieties* W_i *of dimension* $< n$*, and some* $m_i \in \mathbf{Z}$*.*

PROOF. Note first that the second assertion implies the first. Indeed, it is enough to show by induction on n that for every n-dimensional variety W over k, we have $[W] \in K_0'$, where K_0' is the subgroup of $K_0(\mathrm{Var}/k)$ generated by classes of nonsingular, connected, projective varieties. The assertion is clear if $n = 0$. For the induction step, given W with irreducible components $W_1, \ldots, W_r$, let $U_i = W_i \smallsetminus \bigcup_{j \neq i} W_j$, and $U = \bigcup_{i=1}^{r} U_i$. Since $\dim(W \smallsetminus U) < n$, it follows by induction that $[W \smallsetminus U] \in K_0'$, and since $[U] = \sum_{i=1}^{r} [U_i]$ we see that it is enough to show that every $[U_i]$ lies in K_0'. This is a consequence of the second assertion in the lemma.

We now prove the second assertion in the lemma by induction on $n = \dim(X)$. Let X' be an irreducible projective variety that is birational to X. By Hironaka's theorem on resolution of singularities, there is a birational morphism $f\colon Y \to X'$, with Y nonsingular, connected, and projective. Since X and Y are birational, we can find isomorphic open subsets $U \subseteq X$ and $V \subseteq Y$, so that we have

$$[X] - [Y] = [X \smallsetminus U] - [Y \smallsetminus V], \tag{7.3}$$

and $\dim(X \smallsetminus V)$, $\dim(Y \smallsetminus U) < n$. Arguing as above, we see that the induction hypothesis implies that both $[X \smallsetminus U]$ and $[Y \smallsetminus V]$ can be written as linear combinations of classes of nonsingular, irreducible, projective varieties of dimension $< n$, with integer coefficients. Using (7.3), we obtain the assertion in the lemma about X. □

Bittner's theorem shows that with respect to the system of generators described in the lemma, the relations are generated by the ones coming from blow-ups with smooth centers.

THEOREM 7.10. ([Bit]) *Let* k *be an algebraically closed field of characteristic zero. The kernel of the natural morphism from the free abelian group on isomorphism classes of smooth, connected, projective varieties over* k *to* $K_0(\mathrm{Var}/k)$ *is generated by the following elements:*

i) $[\emptyset]$
ii) $([\mathrm{Bl}_Y X] - [E]) - ([X] - [Y])$,

with X *and* Y *are smooth, connected, projective varieties, with* Y *a subvariety of* X*, and where* $\mathrm{Bl}_Y X$ *is the blow-up of* X *along* Y*, with exceptional divisor* E*.*

We do not give the proof here, but only mention that the main ingredient is the following Weak Factorization Theorem of Abramovich, Karu, Matsuki, and Włodarczyk.

THEOREM 7.11. ([AKMW]) *If* k *is an algebraically closed field of characteristic zero, then every birational map between two smooth projective varieties over* k *can be realized as a composition of blow-ups and blow-downs of smooth irreducible centers on smooth projective varieties.*

EXAMPLE 7.12. Let us show that if k is algebraically closed, of characteristic zero, then there is a (unique) Euler-Poincaré characteristic Q with values in $\mathbf{Z}[t]$

such that for every smooth projective variety X, we have

$$Q(X,t) = \sum_{i=0}^{\dim(X)} (-1)^i h^i(X, \mathcal{O}_X) t^i.$$

By Theorem 7.10, it is enough to show that if X and Y are smooth, connected, projective varieties, with Y a closed subvariety of X, and if W is the blow-up of X along Y, with exceptional divisor E, then $Q(W,t) - Q(E,t) = Q(X,t) - Q(Y,t)$. If $p\colon W \to X$ and $q\colon E \to Y$ are the natural projections, then $R^i p_*(\mathcal{O}_W) = 0$, and $R^i q_*(\mathcal{O}_E) = 0$ for all $i > 0$, while $p_*(\mathcal{O}_W) = \mathcal{O}_X$ and $q_*(\mathcal{O}_E) = \mathcal{O}_Y$. We thus have isomorphisms

$$H^j(X, \mathcal{O}_X) \simeq H^j(W, \mathcal{O}_W),\ H^j(Y, \mathcal{O}_Y) \simeq H^j(E, \mathcal{O}_E)$$

for all $j \geq 0$, which imply $Q(W,t) = Q(X,t)$ and $Q(E,t) = Q(Y,t)$.

Example 7.13. A more refined example of an Euler-Poincaré characteristic is given by the Hodge-Deligne polynomial of algebraic varieties. This is an Euler-Poincaré characteristic of varieties over an algebraically closed field k of characteristic zero that takes values in $\mathbf{Z}[u,v]$, such that for a smooth projective variety X, $E(X,u,v)$ is the Hodge polynomial

$$\sum_{p,q=0}^{\dim(X)} (-1)^{p+q} h^{p,q}(X) u^p v^q,$$

where $h^{p,q}(X) = h^q(X, \Omega_X^p)$. Note that with the notation in the previous example, we have $Q(X,t) = E(X,0,t)$. The original definition of the Hodge-Deligne polynomial (over $\mathbf{C}$) uses the mixed Hodge structure on the singular cohomology with compact supports of complex algebraic varieties. It would be nice to give an elementary argument using Theorem 7.10, as in the previous example.

The polynomial $P_{\mathrm{vir}}(X,t) := E(X,t,t)$ is the *virtual Poincaré polynomial* of X. Note that if $k = \mathbf{C}$, then this polynomial is characterized by the fact that it induces a group homomorphism $K_0(\mathrm{Var}/\mathbf{C}) \to \mathbf{Z}[t]$, and if X is a smooth projective variety, then $P_{\mathrm{vir}}(X,t)$ is the usual Poincaré polynomial of X, given by $\sum_{i\geq 0}(-1)^i \dim_{\mathbf{Q}} H^i(X, \mathbf{Q}) t^i$ (this is a consequence of the Hodge decomposition for smooth projective varieties). In particular, we see that $P_X(1) = \chi_{\mathrm{top}}(X)$.

Exercise 7.14. Use the Künneth formula to show that the Hodge-Deligne polynomial is a multiplicative Euler-Poincaré characteristic.

Example 7.15. If $X = \mathbf{P}^1$, then $h^{0,0}(X) = h^{1,1}(X) = 1$ and $h^{1,0}(X) = h^{0,1}(X) = 0$, hence $E(\mathbf{P}^1, u, v) = 1 + uv$, and therefore

$$E(\mathbf{A}^1, u, v) = E(\mathbf{P}^1, u, v) - E(\mathrm{Spec}\, k, u, v) = uv.$$

It follows from the previous exercise that $E(\mathbf{A}^n, u, v) = (uv)^n$.

Remark 7.16. Recall that if X is a smooth projective complex variety, then we have the following symmetry of the Hodge numbers: $h^{p,q}(X) = h^{q,p}(X)$. This implies that $E(Y,u,v) = E(Y,v,u)$ for every variety over an algebraically closed field of characteristic zero.

Exercise 7.17. Let k be an algebraically closed field of characteristic zero. Show that if X is a variety iver k, then $E(X,u,v)$ is a polynomial of degree

$2\dim(X)$, and the term of maximal degree is $m(uv)^{\dim(X)}$, where m is the number of irreducible components of X of maximal dimension.

EXERCISE 7.18. Show that if X and Y are varieties over a field k such that $[X] = [Y]$ in $K_0(\mathrm{Var}/k)$, then $\dim(X) = \dim(Y)$. Hint: in characteristic zero, one can use the previous exercise; in positive characteristic, reduce to the case $k = \overline{\mathbf{F}_p}$, and then use the Lang-Weil estimates (in fact, the characteristic zero case can also be reduced to positive characteristic).

As an application of Bittner's result, we give a proof of a result of Larsen and Lunts [LL2] (see also [Sa]), relating the Grothendieck group of varieties with stable birational geometry.

We keep the assumption that k is an algebraically closed field of characteristic zero. Recall that two irreducible varieties X and Y are *stably birational* if $X \times \mathbf{P}^m$ and $Y \times \mathbf{P}^n$ are birational for some $m, n \geq 0$.

Let SB/k denote the set of stably birational equivalence classes of irreducible algebraic varieties over k. We denote the class of X in SB/k by $\langle X \rangle$. Note that SB/k is a commutative semigroup, with multiplication induced by $\langle X \rangle \cdot \langle Y \rangle = \langle X \times Y \rangle$. Of course, the identity element is $\mathrm{Spec}\, k$.

Let us consider the semigroup algebra $\mathbf{Z}[\mathrm{SB}/k]$ associated to the semigroup SB/k.

PROPOSITION 7.19. *There is a unique ring homomorphism* $\Phi\colon K_0(\mathrm{Var}/k) \to \mathbf{Z}[\mathrm{SB}/k]$ *such that* $\Phi([X]) = \langle X \rangle$ *for every smooth, connected, projective variety* X *over* k.

PROOF. Uniqueness is a consequence of Lemma 7.9. In order to prove the existence of a group homomorphism Φ as in the proposition, we apply Theorem 7.10. This shows that it is enough to check that whenever X and Y are smooth, connected, projective varieties, with Y a closed subvariety of X, we have

$$\langle \mathrm{Bl}_Y(X) \rangle - \langle E \rangle = \langle X \rangle - \langle Y \rangle,$$

where $\mathrm{Bl}_Y X$ is the blow-up of X along Y, and E is the exceptional divisor. In fact, we have $\langle X \rangle = \langle \mathrm{Bl}_Y(X) \rangle$ since X and $\mathrm{Bl}_Y(X)$ are birational, and $\langle Y \rangle = \langle E \rangle$, since E is birational to $Y \times \mathbf{P}_k^{r-1}$, where $r = \mathrm{codim}_X(Y)$.

In order to check that Φ is a ring homomorphism, it is enough to show that $\Phi(uv) = \Phi(u)\Phi(v)$, where u and v vary over a system of group generators of $K_0(\mathrm{Var}/k)$. By Lemma 7.9, we may take this system to consist of classes of smooth, connected, projective varieties, in which case the assertion is clear. □

Since $\langle \mathbf{P}_k^1 \rangle = \langle \mathrm{Spec}\, k \rangle$, it follows that $\Phi(\mathbf{L}) = 0$, hence Φ induces a ring homomorphism

$$\overline{\Phi}\colon K_0(\mathrm{Var}/k)/(\mathbf{L}) \to \mathbf{Z}[\mathrm{SB}].$$

THEOREM 7.20. ([LL2]) *The above ring homomorphism* $\overline{\Phi}$ *is an isomorphism.*

PROOF. The key point is to show that we can define a map

$$\mathrm{SB}/k \to K_0(\mathrm{Var}/k)/(\mathbf{L})$$

such that whenever X is a smooth, connected, projective variety, $\langle X \rangle$ is mapped to $[X] \bmod (\mathbf{L})$. Note first that by Hironaka's theorem on resolution of singularities, for every irreducible variety Y over k, there is a nonsingular, irreducible, projective variety X that is isomorphic to Y. In particular $\langle X \rangle = \langle Y \rangle$. We claim that if

X_1 and X_2 are stably birational nonsingular, irreducible, projective varieties, then $[X] - [Y] \in (\mathbf{L})$.

Suppose that $X_1 \times \mathbf{P}^m$ and $X_2 \times \mathbf{P}^n$ are birational. It follows from Theorem 7.11 that $X_1 \times \mathbf{P}^m$ and $X_2 \times \mathbf{P}^n$ are connected by a chain of blow-ups and blow-downs with smooth centers. Note that

$$[X_1] - [X_1 \times \mathbf{P}^m] = -[X_1] \cdot \mathbf{L}(1 + \mathbf{L} + \ldots + \mathbf{L}^{m-1}) \in (\mathbf{L}).$$

Similarly, we have $[X_2] - [X_2 \times \mathbf{P}^n] \in (\mathbf{L})$. Therefore in order to prove our claim, it is enough to show the following: if Z and W are smooth, connected, projective varieties, with Z a closed subvariety of W, then $[\mathrm{Bl}_Z W] - [W] \in (\mathbf{L})$, where $\mathrm{Bl}_Z(W)$ is the blow-up of W along Z. Let $r = \mathrm{codim}_W(Z)$, and let E be the exceptional divisor, so $E \simeq \mathbf{P}(N)$, where N is the normal bundle of Z in W. Our assertion now follows from

$$[\mathrm{Bl}_Z(W)] - [W] = [E] - [Z] = [E \cdot \mathbf{P}^{r-1}] - [E] = [E] \cdot \mathbf{L}(1 + \mathbf{L} + \ldots + \mathbf{L}^{r-2}).$$

We thus get a group homomorphism $\Psi \colon \mathbf{Z}[\mathrm{SB}/k] \to K_0(\mathrm{Var}/k)/(\mathbf{L})$ such that $\Psi(\langle X \rangle) = [X] \bmod (\mathbf{L})$ for every smooth, connected, projective variety X. It is clear that $\overline{\Phi}$ and Ψ are inverse maps, which proves the theorem. □

We end this section by mentioning the following result of Poonen [Po]:

THEOREM 7.21. *If k is a field of characteristic zero, then $K_0(\mathrm{Var}/k)$ is not a domain.*

SKETCH OF PROOF. Let $\overline{k}$ denote an algebraic closure of k. We denote by $\mathrm{AV}/\overline{k}$ the semigroup of isomorphism classes of abelian varieties over $\overline{k}$ (with the product given again by Cartezian product). Note that we have a morphism of semigroups $\mathrm{SB}/\overline{k} \to \mathrm{AB}/\overline{k}$, that takes $\langle X \rangle$ to $\mathrm{Alb}(X)$ for every smooth, connected, projective variety X over $\overline{k}$, where $\mathrm{Alb}(X)$ is the Albanese variety of X. Indeed, arguing as in the proof of Theorem 7.20, we see that it is enough to show that $\mathrm{Alb}(X) = \mathrm{Alb}(X \times \mathbf{P}^n)$ and $\mathrm{Alb}(X') = \mathrm{Alb}(X)$ if $X' \to X$ is the blow-up of the smooth, connected, projective variety X along a smooth closed subvariety. Both assertions follow from the fact that any rational map $\mathbf{P}^m \dashrightarrow A$, where A is an abelian variety, is constant. Therefore we have ring homomorphisms

$$K_0(\mathrm{Var}/k) \to K_0(\mathrm{Var}/\overline{k}) \to \mathbf{Z}[\mathrm{SB}/\overline{k}] \to \mathbf{Z}[\mathrm{AV}/\overline{k}].$$

The technical result in [Po] says that there are abelian varieties A and B over k such that $A \times A \simeq B \times B$, but $A_{\overline{k}} \not\simeq B_{\overline{k}}$. In this case $([A] - [B])([A] + [B]) = 0$ in $K_0(\mathrm{Var}/k)$. However, both $[A] - [B]$ and $[A] + [B]$ are nonzero in $K_0(\mathrm{Var}/k)$, since their images in $\mathbf{Z}[\mathrm{AV}/\overline{k}]$ are nonzero. Hence $K_0(\mathrm{Var}/k)$ is not a domain. □

REMARK 7.22. Note that the zero-divisors constructed in the proof of the above theorem are nonzero in $K_0(\mathrm{Var}/\overline{k})/(\mathbf{L})$. This suggests that the localized Grothendieck ring $K_0(\mathrm{Var}/k)[\mathbf{L}^{-1}]$ might still be a domain, but this is an open question.

7.2. Symmetric product and Kapranov's motivic zeta function

We begin by recalling the definition of the symmetric products of an algebraic variety. For simplicity we work over a perfect field k. Let X be a quasiprojective variety over k. For every $n \geq 1$, we have a natural action of the symmetric group S_n on the product X^n. Since X^n is again quasiprojective, by the results in A.1,

we may construct the quotient by the action of S_n. This is the *symmetric product* $\mathrm{Sym}^n(X)$. We make the convention that $\mathrm{Sym}^0(X)$ is $\operatorname{Spec} k$. Note that since k is perfect, X^n is reduced, hence $\mathrm{Sym}^n(X)$ is reduced too.

EXAMPLE 7.23. For every $n \geq 1$, there is an isomorphism $\mathrm{Sym}^n(\mathbf{A}^1_k) \simeq \mathbf{A}^n_k$. Indeed, the ring of symmetric polynomials $k[x_1, \ldots, x_n]^{S_n} \subseteq k[x_1, \ldots, x_n]$ is generated as a k-algebra by the elementary symmetric functions $e_1, \ldots, e_n$. Note that since $\dim(k[x_1, \ldots, x_n]^{S_n}) = n$, the polynomials $e_1, \ldots, e_n$ are algebraically independent over k, hence $\mathrm{Sym}^n(\mathbf{A}^1_k) \simeq \mathbf{A}^n_k$.

REMARK 7.24. Note that by Remark 1.5, for every field extension K/k (say, with K perfect), we have $\mathrm{Sym}^n(X) \times_k K \simeq \mathrm{Sym}^n(X \times_k K)$. In particular, if K is algebraically closed, then $\mathrm{Sym}^n(X)(K)$ is in bijection with the set of effective zero-cycles on $X \times_k K$ of degree n.

In order to define Kapranov's motivic zeta function [**Kap**], we need some preparations. We will work with the quotient $\widetilde{K}_0(\mathrm{Var}/k)$ of $K_0(\mathrm{Var}/k)$ by the subgroup generated by the relations $[X] - [Y]$, where we have a radicial surjective morphism $X \to Y$ of varieties over k. See A.3 for a review of radicial morphisms. Note that in fact $\widetilde{K}_0(\mathrm{Var}/k)$ is a quotient ring of $K_0(\mathrm{Var}/k)$: this follows from the fact that if $f\colon X \to Y$ is surjective and radicial, then for every variety Z, the morphism $f \times \mathrm{Id}_Z\colon X \times Z \to Y \times Z$ is surjective and radicial (since $f \times \mathrm{Id}_Z$ is the base-change of f with respect to the projection $Y \times Z \to Y$).

PROPOSITION 7.25. *If* $\mathrm{char}(k) = 0$*, then the canonical morphism* $K_0(\mathrm{Var}/k) \to \widetilde{K}_0(\mathrm{Var}/k)$ *is an isomorphism.*

PROOF. This is a consequence of the fact that if $\mathrm{char}(k) = 0$ and $f\colon X \to Y$ is radicial and surjective, then f is a piecewise isomorphism (see Proposition A.24), hence $[X] = [Y]$ in $K_0(\mathrm{Var}/k)$. □

PROPOSITION 7.26. *If* $k = \mathbf{F}_q$ *is a finite field, then the ring homomorphism* $K_0(\mathrm{Var}/k) \to \mathbf{Z}$ *given by* $[X] \to |X(\mathbf{F}_{q^e})|$ *factors through* $\widetilde{K}_0(\mathrm{Var}/k)$.

PROOF. We need to show that if $f\colon X \to Y$ is a radicial, surjective morphism of varieties over $\mathbf{F}_q$, then $|X(\mathbf{F}_{q^e})| = |Y(\mathbf{F}_{q^e})|$. This is a consequence of the fact that f gives a bijection between the closed points of X and Y, such that for every $x \in X_{\mathrm{cl}}$ we have $k(f(x)) = k(x)$ (for this it is enough to note that $k(f(x))$ is a finite field, hence perfect, and therefore it has no nontrivial purely inseparable extensions). □

The next proposition shows that the Grothendieck group of varieties over k can be described in terms of quasiprojective varieties. Let $K_0^{\mathrm{qpr}}(\mathrm{Var}/k)$ be the quotient of the free abelian group on the set of isomorphism classes of quasiprojective varieties over k, modulo the relations

$$[X] = [Y] + [X \smallsetminus Y],$$

where X is a quasiprojective variety and Y is a closed subvariety of X. It is clear that we have a group homomorphism $\Phi\colon K_0^{\mathrm{qpr}}(\mathrm{Var}/k) \to K_0(\mathrm{Var}/k)$, such that $\Phi([X]) = [X]$. We similarly define $\widetilde{K}^{\mathrm{qpr}}(\mathrm{Var}/k)$ as the quotient of $K_0^{\mathrm{qpr}}(\mathrm{Var}/k)$ by the relations $[X] - [Y]$, where we have a surjective, radicial morphism of quasiprojective varieties $f\colon X \to Y$. We have a corresponding group homomorphism $\widetilde{\Phi}\colon \widetilde{K}_0^{\mathrm{qpr}}(\mathrm{Var}/k) \to \widetilde{K}_0(\mathrm{Var}/k)$.

PROPOSITION 7.27. *Both Φ and $\widetilde{\Phi}$ are isomorphisms.*

PROOF. Let us define an inverse homomorphism $\Psi\colon K_0(\mathrm{Var}/k) \to K_0^{\mathrm{qpr}}(\mathrm{Var}/k)$. Given a variety X over k, we consider a disjoint decomposition $X = V_1 \sqcup \ldots \sqcup V_r$, where each V_i is quasiprojective and locally closed in X (for example, we may even take the V_i to be affine). In this case, we define $\Psi([X]) = \sum_{i=1}^r [V_i] \in K_0^{\mathrm{qpr}}(\mathrm{Var}/k)$.

We need to show that the definition is independent of the decomposition we choose. Suppose that $X = W_1 \sqcup \ldots \sqcup W_s$ is another such decomposition. We get a corresponding decomposition $X = \bigsqcup_{i,j}(V_i \sqcup W_j)$. We have an obvious analogue of Proposition 7.1 for $K_0^{\mathrm{qpr}}(\mathrm{Var}/k)$, hence

$$[V_i] = \sum_{j=1}^{s} [V_i \cap W_j] \text{ and } [W_j] = \sum_{i=1}^{r} [V_i \cap W_j] \text{ in } K_0^{\mathrm{qpr}}(\mathrm{Var}/k).$$

This gives the following equalities in $K_0^{\mathrm{qpr}}(\mathrm{Var}/k)$:

$$\sum_{i=1}^{r} [V_i] = \sum_{i=1}^{r}\sum_{j=1}^{s} [V_i \cap W_j] = \sum_{j=1}^{s}\sum_{i=1}^{r} [V_i \cap W_j] = \sum_{j=1}^{s} [W_j].$$

Therefore $\Psi([X])$ is well-defined.

Suppose now that Y is a closed subvariety of X, and consider a decomposition $X = V_1 \sqcup \ldots \sqcup V_r$ for X as above. If $U = X \smallsetminus Y$, we get corresponding decompositions

$$Y = \bigsqcup_{i=1}^{r} (V_i \cap Y), \quad U = \bigsqcup_{i=1}^{r} (V_i \cap U),$$

from which we get that $\Psi([X]) = \Psi([Y]) + \Psi([U])$. Therefore Ψ gives a group homomorphism $K_0(\mathrm{Var}/k) \to K_0^{\mathrm{qpr}}(\mathrm{Var}/k)$, and it is clear that Φ and Ψ are inverse to each other.

In order to show that Ψ induces an inverse to $\widetilde{\Phi}$, it is enough to show that if $f\colon X \to Y$ is a surjective, radicial morphism, then there is a disjoint decomposition $Y = V_1 \sqcup \ldots \sqcup V_r$ such that all V_i and $f^{-1}(V_i)$ are quasiprojective (note that each $f^{-1}(V_i) \to V_i$ is automatically radicial and surjective). Arguing by Noetherian induction, it is enough to show that there is an affine open subset $V \subseteq Y$ such that $f^{-1}(V)$ is affine. If $Y_1, \ldots, Y_m$ are the irreducible components of Y, we may replace Y by $Y_1 \smallsetminus \bigcup_{i \geq 2} Y_i$, and therefore assume that Y is irreducible. Since f is bijective, there is only one irreducible component of X that dominates Y, hence after restricting to a suitable open subset of Y, we may assume that both X and Y are irreducible. In this case there is an open subset V of Y such that $f^{-1}(V)_{\mathrm{red}} \to V_{\mathrm{red}}$ is a finite morphism (see [**Har**, Exercise II.3.7]). We may assume that V is affine, in which case $f^{-1}(V)_{\mathrm{red}}$ is affine, hence $f^{-1}(V)$ is affine by [**Har**, Exercise III.3.1]. This completes the proof of the proposition. □

For every quasiprojective variety over X, the *Kapranov zeta function* of X is

$$Z_{\mathrm{mot}}(X,t) = \sum_{n \geq 0} [\mathrm{Sym}^n(X)] t^n \in 1 + t \cdot \widetilde{K}_0(\mathrm{Var}/k)[t].$$

PROPOSITION 7.28. *The map $[X] \to Z_{\mathrm{mot}}(X,t)$, for X quasiprojective, defines a group homomorphism*

$$K_0(\mathrm{Var}/k) \to (1 + t\widetilde{K}_0(\mathrm{Var}/k)[\![t]\!], \cdot),$$

which factors through $\widetilde{K}_0(\mathrm{Var}/k)$.

The key ingredient is provided by the following lemma.

LEMMA 7.29. *If X is a quasiprojective variety, and $Y \hookrightarrow X$ is a closed subvariety with complement U, then*

$$[\mathrm{Sym}^n(X)] = \sum_{i+j=n} [\mathrm{Sym}^i(Y)] \cdot [\mathrm{Sym}^j(U)] \text{ in } \widetilde{K}_0(\mathrm{Var}/k).$$

PROOF. For nonnegative i and j with $i+j=n$, we denote by $W^{i,j}$ the locally closed subset of X^n given by $\bigcup_{g\in S_n}(Y^i \times U^j)g$. The $W^{i,j}$ give a disjoint decomposition of X^n by locally closed subvarieties preserved by the S_n-action (in order to show that these sets are disjoint and cover X^n, it is enough to consider the $\overline{k}$-rational points, where $\overline{k}$ is an algebraic closure of k). If $\pi\colon X^n \to \mathrm{Sym}^n(X)$ is the quotient morphism, it follows that the locally closed subvarieties $\pi(W^{i,j})$ give a disjoint decomposition of $\mathrm{Sym}^n(X)$ in locally closed subsets, hence

$$[\mathrm{Sym}^n(X)] = \sum_{i+j=n} [\pi(W^{i,j})] \text{ in } K_0(\mathrm{Var}/k). \tag{7.4}$$

For every pair (i,j) as above, consider the open subset $Y^i \times U^j$ of $W^{i,j}$. For every $g, h \in S_n$, the subsets $(Y^i \times U^j)g$ and $(Y^i \times U^j)h$ of $W^{i,j}$ are either equal, or disjoint. Note also that the subgroup H consisting of all $g \in G$ such that $(Y^i \times U^j)g = Y^i \times U^j$ is equal to $S_i \times S_j \subseteq S_n$. We may therefore apply Propositions A.8 and A.7 to conclude that we have an isomorphism

$$W^{i,j}/S_n \simeq \mathrm{Sym}^i(Y) \times \mathrm{Sym}^j(U).$$

On the other hand, Proposition A.25 implies that the induced morphism $W^{i,j}/S_n \to \pi(W^{i,j})$ is radicial and surjective, hence

$$[\pi(W^{i,j})] = [(W^{i,j}/S_n)] = [\mathrm{Sym}^i(Y)] \cdot [\mathrm{Sym}^j(U)] \text{ in } \widetilde{K}_0(\mathrm{Var}/k).$$

Using this and (7.4), we obtain the statement in the lemma. □

PROOF OF PROPOSITION 7.28. It follows from the lemma that if X is a quasiprojective variety, Y is a closed subvariety of X, and $U = X \smallsetminus Y$, then

$$Z_{\mathrm{mot}}(X,t) = \sum_{n\geq 0} [\mathrm{Sym}^n(X)]t^n = \sum_{n\geq 0} \sum_{i+j=n} [\mathrm{Sym}^i(Y)] \cdot [\mathrm{Sym}^j(U)]t^{i+j}$$

$$= Z_{\mathrm{mot}}(Y,t) \cdot Z_{\mathrm{mot}}(U,t).$$

In light of Proposition 7.27, this proves the first assertion in the proposition. For the second assertion, it is enough to show that if $f\colon X \to Y$ is a surjective, radicial morphism of varieties over k, then the induced morphism $\mathrm{Sym}^n(f)\colon \mathrm{Sym}^n(X) \to \mathrm{Sym}^n(Y)$ is radicial and surjective for every $n \geq 1$. It is easy to see that the surjectivity of f implies that $X^n \to Y^n$ is surjective, and since $Y^n \to \mathrm{Sym}^n(Y)$ is surjective, we deduce that $\mathrm{Sym}^n(f)$ is surjective. In order to show that $\mathrm{Sym}^n(f)$ is radicial, it is enough to prove the injectivity of

$$\mathrm{Hom}(\mathrm{Spec}\, K, \mathrm{Sym}^n(X)) \to \mathrm{Hom}(\mathrm{Spec}\, K, \mathrm{Sym}^n(Y)) \tag{7.5}$$

for every algebraically closed extension K of k. Using Remark 7.24, we may identify $\mathrm{Hom}(\mathrm{Spec}\, K, \mathrm{Sym}^n(X))$ with the quotient of $X(K)^n$ by the action of S_n. A similar description holds for $\mathrm{Hom}(\mathrm{Spec}\, K, \mathrm{Sym}^n(Y))$, and the injectivity of $X(K) \to Y(K)$ implies the injectivity of (7.5). This completes the proof of the proposition. □

REMARK 7.30. If X is not necessarily perfect, then we may still define the motivic zeta function of a quasiprojective variety X by considering the reduced scheme corresponding to X^n/S_n. All results in this section carry through in that setting. We preferred to make the assumption that k is perfect in order to simplify the exposition, since we are mostly interested in the case when k is either a finite field, or it has characteristic zero.

As a consequence of Proposition 7.28, we can define $Z_{\mathrm{mot}}(X,t)$ for a variety over k that is not necessarily quasiprojective. Indeed, we just apply the morphism in that proposition to $[X] \in \widetilde{K}_0(\mathrm{Var}/k)$.

As we have seen in Proposition 7.26, when $k = \mathbf{F}_q$ is a finite field, we have a specialization map $\widetilde{K}_0(\mathrm{Var}/k) \to \mathbf{Z}$ given by counting the number of $\mathbf{F}_q$-rational points. The following proposition shows that if we apply this specialization to Kapranov's motivic zeta function, we recover the Hasse-Weil zeta function.

PROPOSITION 7.31. *If k is a finite field, and X is a variety over k, then the image of $Z_{\mathrm{mot}}(X,t)$ in $1+t\mathbf{Z}[\![t]\!]$ is equal to $Z(X,t)$.*

PROOF. We may clearly assume that X is quasiprojective. By Remark 2.9, it is enough to show that for every $n \geq 1$, the number of effective 0-cycles on X of degree n is equal to $|\mathrm{Sym}^n(X)(k)|$. We have $\mathrm{Sym}^n(X)_{\overline{k}} \simeq \mathrm{Sym}^n(X_{\overline{k}})$by Remark 7.24. Note that if $g \in G = G(\overline{k}/k)$ acts on $X_{\overline{k}}$ by σ, then g acts on $\mathrm{Sym}^n(X)_{\overline{k}}$ by $\mathrm{Sym}^n(\sigma)$. We can identify $\mathrm{Sym}^n(X)(k)$ with the points of $\mathrm{Sym}^n(X)(\overline{k}) = X(\overline{k})^n/S_n$ that are fixed by all $g \in G$. An element of $X(\overline{k})^n/S_n$ corresponds to an effective 0-cycle of degree n on $X_{\overline{k}}$, and this is fixed by every $g \in G$ if and only if it corresponds to an effective cycle of degree n on X (see Proposition A.15). This completes the proof of the proposition. □

PROPOSITION 7.32. *If X is a variety over k, then $Z_{\mathrm{mot}}(X \times \mathbf{A}^n_k, t) = Z_{\mathrm{mot}}(X, \mathbf{L}^n t)$, where $\mathbf{L} = [\mathbf{A}^1_k]$.*

PROOF. We only sketch the argument, which is due to Totaro [Göt1, Lemma 4.4]. It is enough to prove the assertion when X is quasiprojective. Arguing by induction on n, it follows that it is enough to prove the case $n = 1$. We need to show that for every $n \geq 1$, we have $[\mathrm{Sym}^n(X \times \mathbf{A}^1_k)] = [\mathrm{Sym}^n(X)] \cdot \mathbf{L}^n$ in $\widetilde{K}_0(\mathrm{Var}/k)$.

We start by describing a general decomposition into locally closed subsets of $\mathrm{Sym}^n(X)$. For every $r \geq 1$, we denote by $(X^r)^\circ$ the complement in X^r of the union of the (big) diagonals (when $r = 1$, this is simply X). Given positive integers $d_1, \ldots, d_r$ with $d_1 \leq \ldots \leq d_r$ and $\sum_{i=1}^r d_i = n$, consider the locally closed embedding $(X^r)^\circ \hookrightarrow X^n$ given by $\Delta_{d_1} \times \ldots \times \Delta_{d_r}$, where $\Delta_i \colon X \to X^i$ is the diagonal embedding. We denote the image of $(X^r)^\circ$ by $X_{d_1,\ldots,d_r}$. It is clear that for every $\sigma, \tau \in S_n$, the subsets $X_{d_1,\ldots,d_r}\sigma$ and $X_{d_1,\ldots,d_r}\tau$ are either disjoint, or equal. We may thus apply Propositions A.8 and A.25 to deduce that if $H = \{g \in G \mid X_{d_1,\ldots,d_r} g = X_{d_1,\ldots,d_r}\}$, then $X_{d_1,\ldots,d_r}/H$ has a radicial morphism onto its image in $\mathrm{Sym}^n(X)$, that we denote by $\widetilde{X}_{d_1,\ldots,d_r}$. It is clear that when we consider all tuples $(d_1, \ldots, d_r)$ as above, the $\widetilde{X}_{d_1,\ldots,d_r}$ give a partition of $\mathrm{Sym}^n(X)$ into locally closed subsets (consider, for example, the $\overline{k}$-valued points, where $\overline{k}$ is an algebraic closure of k).

Suppose that $m_1 < m_2 < \ldots < m_s$ are such that the first ℓ_1 of the d_i are equal to m_1, the next ℓ_2 of the d_i are equal to m_2, and so on. In this case $H = H_1 \rtimes H_2$,

where $H_1 = \prod_{i=1}^r S_{d_i}$ and $H_2 = \prod_{j=1}^s S_{\ell_j}$. Each S_{d_i} acts by permuting the entries of X^n in the slots $d_1+\ldots+d_{i-1}+1, \ldots, d_1+\ldots+d_i$, while S_{ℓ_j} permutes the ℓ_j sets of m_j entries of X^n. Note that H_1 acts trivially on $X_{d_1,\ldots,d_r}$, hence $X_{d_1,\ldots,d_r}/H = X_{d_1,\ldots,d_r}/H_2$.

We now consider the inverse image $W_{d_1,\ldots,d_r} = X_{d_1,\ldots,d_r} \times \mathbf{A}_k^n$ of $X_{d_1,\ldots,d_r}$ in $(X \times \mathbf{A}_k^1)^n$, as well as its image $\widetilde{W}_{d_1,\ldots,d_r}$ in $\mathrm{Sym}^n(X \times \mathbf{A}_k^1)$. As above, we have a surjective, radicial morphism $W_{d_1,\ldots,d_r}/H \to \widetilde{W}_{d_1,\ldots,d_r}$. In order to complete the proof of the proposition, it is enough to show that $[W_{d_1,\ldots,d_r}/H] = [(X_{d_1,\ldots,d_r}/H) \times \mathbf{A}_k^n]$ in $\widetilde{K}_0(\mathrm{Var}/k)$.

It follows from Proposition A.10 that $W_{d_1,\ldots,d_r}/H \simeq (W_{d_1,\ldots,d_r}/H_1)/H_2$. On the other hand, Proposition A.7 and Example 7.23 give an isomorphism $W_{d_1,\ldots,d_r}/H_1 \simeq X_{d_1,\ldots,d_r} \times \prod_{i=1}^r \mathbf{A}_k^{d_i} = X_{d_1,\ldots,d_r} \times \prod_{j=1}^s (\mathbf{A}_k^{m_j})^{\ell_j} = X_{d_1,\ldots,d_r} \times \mathbf{A}_k^n$. One can show that since H_2 acts without fixed points on $X_{d_1,\ldots,d_r}$, the projection $\pi\colon X_{d_1,\ldots,d_r} \to X_{d_1,\ldots,d_r}/H_2$ is étale, and we have a Cartezian diagram

$$\begin{array}{ccc} X_{d_1,\ldots,d_r} \times \mathbf{A}_k^n & \longrightarrow & (W_{d_1,\ldots,d_r}/H_1)/H_2 \\ \downarrow & & \downarrow \phi \\ X_{d_1,\ldots,d_r} & \longrightarrow & X_{d_1,\ldots,d_r}/H_2. \end{array}$$

One can show using this that ϕ has a structure of rank n vector bundle locally trivial in the étale topology, and by Hilbert's Theorem 90 [Se2, p. 1.24], this is locally trivial also in the Zariski topology. This gives $[W_{d_1,\ldots,d_r}/H] = [X_{d_1,\ldots,d_r}/H_2] \cdot \mathbf{L}^n$ in $K_0(\mathrm{Var}/k)$. □

7.3. Rationality of the Kapranov zeta function for curves

Our goal in this section is to prove a result of Kapranov [Kap], extending the rationality of the Hasse-Weil zeta function for smooth, geometrically connected, projective curves defined over finite fields to motivic zeta functions.

Since the Kapranov zeta function does not have coefficients in a field, there are (at least) two possible notions of rationality that can be considered. If R is a commutative ring and $f \in R[\![t]\!]$, we say that f is *rational* if there are polynomials $u, v \in R[t]$, with v invertible in $R[\![t]\!]$ such that $f(t) = \frac{u(t)}{v(t)}$. We say that f is *pointwise rational* if for every morphism $R \to K$, where K is a field, the image of f in $K[\![t]\!]$ is rational. It is clear that a rational formal power series is also pointwise rational. The formal power series we will consider satisfy $f(0) = 1$, hence the image in every $K[\![t]\!]$ as above is nonzero. Of course, when R is a field, then the two notions of rationality coincide.

THEOREM 7.33. *Let k be a perfect field. If X is a smooth, geometrically connected, projective curve of genus g over k which has a k-rational point, then $Z_{\mathrm{mot}}(X,t)$ is a rational function. Moreover, we have*

$$Z_{\mathrm{mot}}(X,t) = \frac{f(t)}{(1-t)(1-\mathbf{L}t)},$$

for a polynomial f of degree $\leq 2g$ with coefficients in $\widetilde{K}_0(\mathrm{Var}/k)$.

PROOF. The existence of a k-rational point on X implies that the Picard variety of X represents the Picard functor, suitably rigidified. More precisely, if $x_0 \in X(k)$,

then $\mathrm{Pic}^d(X)$ represents the contravariant functor that associates to a scheme S over k the set of line bundles $\mathcal{L} \in \mathrm{Pic}(S \times X)$ which have degree d on the fibers over S and such that $\mathcal{L}|_{S\times\{x_0\}}$ is trivial. This representability implies that the usual properties of the Picard variety, familiar over an algebraically closed field, extend to our setting.

In particular, recall that for every $d \geq 0$ we have a morphism $\mathrm{Sym}^d(X) \to \mathrm{Pic}^d(X)$. This can be defined using the universal property of $\mathrm{Pic}^d(X)$, but let us describe it at the level of $\overline{k}$-valued points, where $\overline{k}$ is an algebraic closure of k. A $\overline{k}$-valued point of $\mathrm{Sym}^d(X)$ corresponds to an effective divisor D on $X_{\overline{k}}$ of degree d. On the other hand, a $\overline{k}$-valued point of $\mathrm{Pic}^d(X)$ corresponds to a line bundle on $X_{\overline{k}}$ of degree d, and the above map takes D to $\mathcal{O}_X(D)$. If $d \geq 2g-1$, then the fiber of $\mathrm{Sym}^d(X)_{\overline{k}} \to \mathrm{Pic}^d(X)_{\overline{k}}$ over L is naturally isomorphic to the linear system $|L| \simeq \mathbf{P}^{d-g}_{\overline{k}}$. In fact, there is an isomorphism[1] $\mathrm{Sym}^d(X) \simeq \mathbf{P}(E)$, where E is a vector bundle on $\mathrm{Pic}^d(X)$ of rank $d-g+1$.

Since we assume that $X(k) \neq \emptyset$, it follows that there are line bundles of degree 1 on X. Therefore we have an isomorphism $\mathrm{Pic}^d(X) \simeq \mathrm{Pic}^0(X)$ for every d. It follows from definition and the above discussion that

$$Z_{\mathrm{mot}}(X,t) = \sum_{d\geq 0}[\mathrm{Sym}^d(X)]t^d = \sum_{0\leq d\leq 2g-2}[\mathrm{Sym}^d(X)]t^d + \sum_{d\geq \min\{2g-1,0\}}[\mathrm{Pic}^0(X)]\cdot[\mathbf{P}^{d-g}_k]t^d.$$

We write the rest of the argument for $g \geq 1$ and leave it for the reader to treat the (trivial) case $g = 0$. It follows from the above formula and an easy computation that

$$Z_{\mathrm{mot}}(X,t) = \sum_{0\leq d\leq 2g-2}[\mathrm{Sym}^d(X)]t^d + [\mathrm{Pic}^0(X)]\cdot\sum_{d\geq 2g-1}\frac{\mathbf{L}^{d-g+1}-1}{\mathbf{L}-1}t^d$$

$$= \sum_{0\leq d\leq 2g-2}[\mathrm{Sym}^d(X)]t^d + \frac{1}{(1-t)(1-\mathbf{L}t)}\cdot\left(t^{2g-1}\frac{\mathbf{L}^g-1}{\mathbf{L}-1} - t^{2g}\frac{\mathbf{L}^{g-1}-\mathbf{L}}{\mathbf{L}-1}\right),$$

which implies the statement in the theorem. □

7.4. Kapranov zeta function of complex surfaces

In this section we assume that k is an algebraically closed field, and consider the rationality of $Z_{\mathrm{mot}}(X,t)$ when $\dim(X) = 2$, following [LL1] and [LL2].

PROPOSITION 7.34. *If X is a variety over k with $\dim(X) \leq 1$, then $Z_{\mathrm{mot}}(X,t)$ is rational.*

PROOF. The assertion is clearly true when X is a point, since

$$Z(\mathrm{Spec}\, k, t) = \sum_{n\geq 0} t^n = \frac{1}{1-t},$$

and for a smooth, connected, projective curve it follows from Theorem 7.33. It is easy to deduce the general case in the proposition by taking closures of affine

[1] The existence of this isomorphism is crucial for the rest of the argument. In a previous version of these notes, one did not assume that X has a rational point. I am indebted to Daniel Litt who pointed out that without this assumption, it might not be the case that $\mathrm{Sym}^d(X)$ is a projective bundle over $\mathrm{Pic}^d(X)$. It is an interesting question whether the rationality assumption in the theorem also holds when $X(k) = \emptyset$.

curves in suitable projective spaces, and normalizations of irreducible projective curves. Since we have already given several such arguments, we leave the details as an exercise for the reader. □

Given a variety X of dimension 2, we consider a decomposition of $X = X_1 \sqcup \ldots \sqcup X_r$, with each X_i irreducible and quasiprojective. Since $Z_{\mathrm{mot}}(X,t) = \prod_{i=1}^{r} Z_{\mathrm{mot}}(X_i,t)$, we reduce studying the rationality or pointwise rationality of $Z_{\mathrm{mot}}(X,t)$ to that of all $Z_{\mathrm{mot}}(X_i,t)$.

PROPOSITION 7.35. *If X and Y are birational irreducible varieties over k of dimension two, then $Z_{\mathrm{mot}}(X,t)$ is rational (pointwise rational) if and only if $Z_{\mathrm{mot}}(Y,t)$ has the same property.*

PROOF. By assumption, there are isomorphic open subsets $U \subseteq X$ and $V \subseteq Y$. We thus have

$$Z_{\mathrm{mot}}(X,t) = Z_{\mathrm{mot}}(Y,t)\frac{Z_{\mathrm{mot}}(X \smallsetminus U,t)}{Z_{\mathrm{mot}}(Y \smallsetminus V)},$$

and both $Z_{\mathrm{mot}}(X \smallsetminus U,t)$ and $Z_{\mathrm{mot}}(Y \smallsetminus V,t)$ are rational by Proposition 7.34. Therefore $Z_{\mathrm{mot}}(X,t)$ is rational (pointwise rational) if and only if $Z_{\mathrm{mot}}(Y,t)$ is. □

If X is an arbitrary irreducible surface, there is a smooth, connected, projective surface Y such that X is birational to Y. Indeed, resolution of singularities for surfaces holds over fields of arbitrary characteristic.

Therefore from now on we concentrate on smooth, connected, projective surfaces. Let X be such a surface. We start by recalling a fundamental result from classification of surfaces. We refer to [**Beau**] for the case of complex surfaces, and to [**Bad**] for the general case. Recall that the Kodaira dimension of X is said to be negative if $H^0(X, \mathcal{O}(mK_X)) = 0$ for al $m \geq 1$. This is a birational property of X. Given any X, there is a morphism $\pi\colon X \to Y$ that is a composition of blow-ups of points on smooth surfaces such that Y is *minimal*, that is, it admits no birational morphism $Y \to Z$, where Z is a smooth surface. By Castelnuovo's criterion for contractibility, this is the case if and only if Y contains no smooth curve $C \simeq \mathbf{P}^1$ with $(C^2) = -1$. A fundamental result in the classification of surfaces says that if X (hence also Y) has negative Kodaira dimension, then Y is birational to $C \times \mathbf{P}^1$, for some smooth curve C.

PROPOSITION 7.36. *If X is a smooth, connected, projective surface of negative Kodaira dimension, then $Z_{\mathrm{mot}}(X,t)$ is a rational power series.*

PROOF. It follows from the above discussion that X is birational to $C \times \mathbf{P}^1$ for a smooth curve C, hence by Proposition 7.35 it is enough to show that $Z_{\mathrm{mot}}(C \times \mathbf{A}^1, t)$ is rational. This follows from Proposition 7.34, since $Z_{\mathrm{mot}}(C \times \mathbf{A}^1, t) = Z_{\mathrm{mot}}(C, \mathbf{L}t)$ by Proposition 7.32. □

The following theorem, the main result of [**LL1**], gives the converse in the case of complex surfaces.

THEOREM 7.37. *If X is a smooth, connected, projective complex surface such that $Z_{\mathrm{mot}}(X,t)$ is pointwise rational, then X has negative Kodaira dimension.*

We will not discuss the proof of this result, but in what follows we will sketch the proof of the following earlier, more special result of Larsen and Lunts [**LL2**]. Recall that if X is a smooth projective variety, its geometric genus is $p_g(X) = h^0(X, \omega_X)$.

PROPOSITION 7.38. *If X is a smooth, connected, projective surface with $p_g(X) \geq 2$, then $Z_{\mathrm{mot}}(X,t)$ is not pointwise rational.*

We start by describing the group homomorphism $K_0(\mathrm{Var}/\mathbf{C}) \to K$ that is used in the proof of Proposition 7.38. Let S denote the multiplicative semigroup of polynomials $h \in \mathbf{Z}[t]$ with $h(0) = 1$. Since the only invertible element in S is 1, and $\mathbf{Z}[t]$ is a factorial ring, every element in S can be written uniquely as $h_1^{n_1} \cdots h_r^{n_r}$, where the h_i are elements in S that generate prime ideals in $\mathbf{Z}[t]$. It follows that the semigroup algebra $\mathbf{Z}[S]$ is a polynomial ring in infinitely many variables. In particular, it is a domain, and we take K to be the fraction field of $\mathbf{Z}[S]$. In order to avoid confusion, we denote by $\phi(h)$ the element in $\mathbf{Z}[S]$ corresponding to $h \in S$, hence $\phi(g)\phi(h) = \phi(gh)$.

We now define a group homomorphism $\mathrm{SB}/\mathbf{C} \to S$ by taking $\langle X \rangle$, for X smooth, connected, and projective, to $R(X,t) := E(X,t,0) = \sum_{i=0}^{\dim(X)} (-1)^i h^0(X, \Omega_X^i) t^i \in S$. It is an easy consequence of the Künneth theorem (see Exercise 7.14) that $R(X \times Y, t) = R(X,t) \cdot R(Y,t)$. Note that $R(\mathbf{P}^n, t) = 1$ for all $n \geq 0$. Indeed, using the Hodge symmetry we have $h^0(\mathbf{P}^n, \Omega^i_{\mathbf{P}^n}) = h^i(\mathbf{P}^n, \mathcal{O}_{\mathbf{P}^n}) = 0$ (exercise: give a direct proof using the description of $\Omega_{\mathbf{P}^n}$ provided by the Euler exact sequence). We deduce that $R(X \times \mathbf{P}^n, t) = R(X,t)$. Furthermore, if X and Y are smooth, projective birational varieties, then $h^0(X, \Omega_X^i) = h^0(Y, \Omega_Y^i)$ for all i (see [**Har**, Theorem II.8.19], whose proof extends to the case $i < \dim(X)$). We conclude that we have a well-defined semigroup homomorphism $\mathrm{SB}/\mathbf{C} \to S$ that takes $\langle X \rangle$ to $R(X,t)$ for every X smooth, connected, and projective. This induces a ring homomorphism $\mathbf{Z}[\mathrm{SB}/\mathbf{C}] \to \mathbf{Z}[S]$.

By Theorem 7.20, we have an isomorphism $K_0(\mathrm{Var}/\mathbf{C})/(\mathbf{L}) \to \mathbf{Z}[\mathrm{SB}/\mathbf{C}]$. We thus have a ring homomorphism $K_0(\mathrm{Var}/\mathbf{C}) \to \mathbf{Z}[S] \hookrightarrow K$, that we denote by μ, which takes $[X]$ to $\phi(R(X,t))$ for every smooth, connected, projective variety X. Therefore if $X_1, \ldots, X_r$ are such varieties, then

$$\mu(\sum_{i=1}^{r} n_i [X_i]) = \sum_{i=1}^{r} n_i \phi(E(X_i, t, 0)).$$

We emphasize that μ is different from the Euler-Poincaré characteristic that takes X to $E(X,t,0)$, which takes values in $\mathbf{Z}[t]$. We will see in Lemma 7.39 below that μ recovers more information than this latter Euler-Poincaré characteristic.

Note that if X is a smooth, connected, n-dimensional projective variety, then the degree of $R(X,t)$ is $\leq n$, and the coefficient of t^n is $(-1)^n p_g(X)$. When X is an arbitrary irreducible variety, we will denote by $p_g(X)$ the geometric genus of every smooth, irreducible, projective variety Y that is birational to X. As we have mentioned, this is independent of the choice of Y.

LEMMA 7.39. *Suppose that $Y, X_1, \ldots, X_r$ are irreducible varieties of the same dimension, and $n_1, \ldots, n_r$ are integers such that $\mu(Y) = \sum_{i=1}^r n_i \mu(X_i)$. If $p_g(Y) \neq 0$, then there is i such that $p_g(X) = p_g(Y_i)$.*

PROOF. It follows from Lemma 7.9 that we can find a smooth, connected, projective variety Y' that is birational to Y, such that $[Y] - [Y']$ is a linear combination, with integer coefficients, of classes of smooth, irreducible, projective varieties of dimension smaller than $n = \dim(Y)$. Applying this also to the X_i, we conclude that we may assume that Y and all X_i are smooth, connected, and projective, and that we have smooth, connected, projective varieties $X_1', \ldots, X_s'$ of dimension less than

n, and $n'_1, \ldots, n'_s \in \mathbf{Z}$ such that

$$\mu(Y) = \sum_{i=1}^{r} n_i \mu(X_i) + \sum_{j=1}^{s} n'_j \mu(X'_j).$$

By assumption, $\mu(Y)$ has degree n, while each $\mu(X'_j)$ has degree $< n$, hence $\mu(Y) \neq \mu(X'_j)$ for every j. This implies that there is i such that $\mu(Y) = \mu(X_i)$, and we get, in particular, $p_g(Y) = p_g(X_i)$. □

The key technical ingredient in the proof of Proposition 7.38 is the computation of the geometric genera for the symmetric powers of a smooth, connected, projective complex surface X. It is shown in [LL2] that if $p_g(X) = r$, then

$$p_g(\mathrm{Sym}^n(X)) = \binom{n+r-1}{r-1}. \tag{7.6}$$

Note that $\mathrm{Sym}^n(X)$ has a resolution of singularities given by the Hilbert scheme of n points on X. This is a projective scheme $X^{[n]}$ that parametrizes 0-dimensional subschemes of X of length n. It is a result of Fogarty that for a smooth, connected surface X, the Hilbert scheme $X^{[n]}$ is smooth and connected. Furthermore, there is a morphism $X^{[n]} \to \mathrm{Sym}^n(X)$ that takes a scheme Z supported at the points $x_1, \ldots, x_m$ to $\sum_{i=1}^m \ell(\mathcal{O}_{Z,x_i}) x_i$. This gives an isomorphism onto the image on the open subset parametrizing reduced subschemes. Therefore $X^{[n]}$ gives a resolution of singularities of $\mathrm{Sym}^n(X)$, hence $p_g(\mathrm{Sym}^n(X)) = p_g(X^{[n]})$. The above formula for $p_g(\mathrm{Sym}^n(X))$ is then deduced from results of Göttsche and Soergel [GS] on the Hodge structure on the cohomology of $X^{[n]}$.

Proof of Proposition 7.38. Suppose by way of contradiction that $h = \sum_{n \geq 0} \mu_n t^n \in K[\![t]\!]$ is a rational function, where $\mu_n = \mu(\mathrm{Sym}^n(X))$. Therefore we may write

$$h = \frac{a_0 + a_1 t + \ldots + a_e t^e}{b_0 + b_1 t + \ldots + b_m t^m},$$

for some $a_i, b_j \in K$, with not all b_j zero. This implies that $\mu_d b_m + \mu_{d+1} b_{m-1} + \ldots + \mu_{d+m} b_0 = 0$ for all $d \geq \min\{0, e-m+1\}$. Since some b_j is nonzero, by considering these relations for $d, d+1, \ldots, d+m$, we conclude that $D := \det(\mu_{d+i+j})_{0 \leq i \leq m} = 0$. By expanding this determinant, we obtain a relation

$$\mu\left(\prod_{i=0}^{m} \mathrm{Sym}^{d+2i}(X)\right) = \sum_{\sigma \in S_{m+1} \smallsetminus \{1\}} -\mathrm{sign}(\sigma)\, \mu\left(\prod_{i=0}^{m} \mathrm{Sym}^{d+\sigma(i)+i}(X)\right), \tag{7.7}$$

where we consider S_{m+1} to be the group of permutations of $\{0, 1, \ldots, m\}$.

Note that for every $\sigma \in S_{m+1}$, the variety $\prod_{i=0}^m \mathrm{Sym}^{d+\sigma(i)+i}(X)$ has dimension equal to $2(m+1)(d+m)$, and geometric genus $\prod_{i=0}^m \binom{d+\sigma(i)+i+r-1}{r-1}$ (see formula (7.6)). We deduce from (7.7) and Lemma 7.39 that there is a permutation $\sigma \in S_{m+1}$ different from the identity such that

$$\prod_{i=0}^{m} \binom{d+\sigma(i)+i+r-1}{r-1} = \prod_{i=0}^{m} \binom{d+2i+r-1}{r-1}. \tag{7.8}$$

Since $r \geq 2$, for every $\sigma \in S_{m+1}$ different from the identity, the following polynomial in d

$$P_\sigma(d) = \prod_{i=0}^{m} \binom{d+\sigma(i)+i+r-1}{r-1} - \prod_{i=0}^{m} \binom{d+2i+r-1}{r-1}$$

is not zero, hence it does not vanish for $d \gg 0$. Indeed, if i_0 is the largest i such that $\sigma(i) \neq i$, then we can write

$$P_\sigma(d) = \prod_{i=i_0+1}^{m} \binom{d+2i+r-1}{r-1} \cdot (Q_1(d) - Q_2(d)),$$

and the linear polynomial $d+2i_0+r-1$ divides $Q_2(d)$, but it does not divide $Q_1(d)$. Since we have only finitely many permutations to consider (note that m is fixed), we conclude that by taking $d \gg 0$, we obtain a contradiction. □

REMARK 7.40. The Euler-Poincaré characteristic constructed above, that makes $Z_{\mathrm{mot}}(X,t)$ not pointwise rational, vanishes on $\mathbf{L}$. It would be interesting to find such an Euler-Poincaré characteristic that is nonzero on $\mathbf{L}$ (hence factors through $K_0(\mathrm{Var}/\mathbf{C})[\mathbf{L}^{-1}]$).

REMARK 7.41. It is interesting to compare Theorem 7.37 on the rationality of $Z_{\mathrm{mot}}(X,t)$ with Mumford's theorem on the finiteness of the Chow group $A^2(X)_0$ of rational equivalence classes of 0-cycles on X of degree zero. It is shown in [**Mum2**] that if X is a smooth, connected, projective complex surface with $p_g(X) \neq 0$, then $A^2(X)_0$ is infinitely dimensional in a suitable sense (in particular, it can not be parametrized by the points of an algebraic variety). This can also be interpreted as a statement about the growth of the symmetric products $\mathrm{Sym}^n(X)$, when n goes to infinity. On the other hand, it was conjectured by Bloch that the converse is also true, namely that if $p_g(X) = 0$, then $A^2(X)_0$ is finite-dimensional. While this is still a conjecture, it is known to hold for surfaces of Kodaira dimension ≤ 1. In particular, we see that for any surface X of Kodaira dimension 0 or 1 with $p_g(X) = 0$, we have $A^0(X)_0$ finite dimensional, but $Z_{\mathrm{mot}}(X,t)$ is not rational.

CHAPTER 8

Dwork's proof of rationality of zeta functions

In this chapter we present Dwork's proof [Dwo] for the first of the Weil conjectures, asserting the rationality of the Hasse-Weil zeta function for a variety over a finite field. We follow, with small modifications, the presentation in [Kob]. We freely make use of the basic facts about p-adic fields as covered in § B.

8.1. A formula for the number of $\mathbf{F}_q$-points on a hypersurface

Recall that our goal is to prove the rationality of the zeta function of an algebraic variety X over $\mathbf{F}_q$. As we have seen in Chapter 2, in order to prove this in general, it is enough to prove it in the case when X is a hypersurface in $\mathbf{A}^d_{\mathbf{F}_q}$, defined by some $f \in \mathbf{F}_q[x_1, \ldots, x_d]$. Furthermore, an easy argument based an induction and on the inclusion-exclusion principle, will allow us to reduce ourselves to proving the rationality of

$$\widetilde{Z}(X,t) := \exp\left(\sum_{n\geq 0} \frac{N'_n}{n} t^n\right),$$

where

$$N'_n = |\{u = (u_1, \ldots, u_d) \in \mathbf{F}^d_{q^n} \mid f(u) = 0, u_i \neq 0 \,\text{for all}\, i\}|.$$

Hence from now on we will focus on $\widetilde{Z}(X,t)$.

The starting point consists in a formula for N'_n in terms of an additive character of $\mathbf{F}_{q^n}$. By this we mean a group homomorphism $\chi\colon \mathbf{F}_{q^n} \to \overline{\mathbf{Q}_p}$. We say that such a character is trivial if $\chi(u) = 1$ for every $u \in \mathbf{F}_q$. The main example that we will need is the following,

LEMMA 8.1. *If $\epsilon \in \overline{\mathbf{Q}_p}$ is a primitive root of 1, then $\chi\colon \mathbf{F}_{q^n} \to \mathbf{Q}_p(\epsilon)$ given by $\chi(u) = \epsilon^{\mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p}(u)}$ is a nontrivial additive character of $\mathbf{F}_{q^n}$.*

PROOF. It is clear that $\psi\colon \mathbf{F}_p \to \mathbf{Q}_p(\epsilon)$ given by $\psi(m \bmod p) = \epsilon^m$ is an injective homomorphism. Since $\mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_q}$ is additive, we deduce that χ is an additive character. If χ is trivial, then $\mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p}(u) = 0$ for every $u \in \mathbf{F}_q$. This contradicts the fact that the bilinear pairing $(u,v) \to \mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p}(u,v)$ is nondegenerate (recall that $\mathbf{F}_{q^n}$ is separable over $\mathbf{F}_p$). □

REMARK 8.2. Since $\mathbf{F}_{q^n}/\mathbf{F}_p$ is Galois, with Galois group cyclic and generated by the Frobenius morphism, it follows that for every $a \in \mathbf{F}_{q^n}$, we have $\mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p}(a) = a + a^p + \ldots + a^{p^{ne-1}}$, where $q = p^e$.

LEMMA 8.3. *If χ is a nontrivial additive character of $\mathbf{F}_{q^n}$, then $\sum_{u\in\mathbf{F}_{q^n}} \chi(u) = 0$.*

PROOF. Let $v \in \mathbf{F}_{q^n}$ be such that $\chi(v) \neq 1$. We have

$$\sum_{u \in \mathbf{F}_{q^n}} \chi(u) = \sum_{u \in \mathbf{F}_{q^n}} \chi(u+v) = \chi(v) \cdot \sum_{u \in \mathbf{F}_{q^n}} \chi(u),$$

which implies the assertion in the lemma since $\chi(v) \neq 1$. □

Suppose now that $f \in \mathbf{F}_q[x_1, \ldots, x_n]$ is as above, and ψ_n is a nontrivial additive character of $\mathbf{F}_{q^n}$. It follows from Lemma 8.3 that for every $a \in \mathbf{F}_{q^n}$, we have $\sum_{v \in \mathbf{F}_{q^n}} \psi_n(va) = 0$, unless $a = 0$, in which case the sum is clearly equal to q^n. Therefore we have

$$\sum_{u \in (\mathbf{F}_{q^n}^*)^d} \sum_{v \in \mathbf{F}_{q^n}} \psi_n(vf(u)) = N'_n q^n.$$

Since the sum of the terms corresponding to $v = 0$ is $(q^n - 1)^d$, we conclude that

$$\sum_{u \in (\mathbf{F}_{q^n}^*)^d} \sum_{v \in \mathbf{F}_{q^n}^*} \psi_n(vf(u)) = N'_n q^n - (q^n - 1)^d. \tag{8.1}$$

The main result of this section will be a formula for the left-hand side of (8.1) by applying a suitable analytic function to the Teichmüller lifts of $u_1, \ldots, u_n, v$. Furthermore, the analytic functions corresponding to the various n will turn out to be related in a convenient way. Let us fix a primitive root ϵ of 1 of order p in $\overline{\mathbf{Q}_p}$. For every $a \in \mathbf{F}_{p^m}$, we denote by $\widetilde{a} \in \mathbf{Z}_p^{(m)}$ the Teichmüller lift of a (see § B.2). The key ingredient is provided by a formal power series $\Theta \in \mathbf{Q}_p(\epsilon)[\![t]\!]$, that satisfies the following two properties:

P1) The radius of convergence of Θ is > 1.
P2) For every $n \geq 1$ and every $a \in \mathbf{F}_{q^n}$, we have

$$\epsilon^{\mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p}(a)} = \Theta(\widetilde{a})\Theta(\widetilde{a}^q) \cdots \Theta(\widetilde{a}^{q^{n-1}}). \tag{8.2}$$

Note that by Lemma 8.1, the left-hand side of (8.2) is a nontrivial character of $\mathbf{F}_{q^n}$. Furthermore, note that if $a \in \mathbf{F}_{q^n}$, then $|\widetilde{a}|_p = 1$, hence $\Theta(\widetilde{a}^{q^i})$ is well-defined by P1).

Let us assume for the moment the existence of such Θ, and let us see how we can rewrite the left-hand side of (8.1). Suppose that $f = \sum_{m \in \mathbf{Z}_{\geq 0}^d} c_m x^m \in \mathbf{F}_q[x_1, \ldots, x_d]$, where for $m = (m_1, \ldots, m_d)$ we put $x^m = x_1^{m_1} \cdots x_d^{m_d}$. Note that only finitely many of the c_m are nonzero. It is clear that for $u = (u_1, \ldots, u_d) \in (\mathbf{F}_{q^n}^*)^d$ and $v \in \mathbf{F}_{q^n}^*$, we have

$$\psi_n(vf(u)) = \prod_{m \in \mathbf{Z}_{\geq 0}^d} \psi_n(c_m\, v u_1^{m_1} \cdots u_d^{m_d}). \tag{8.3}$$

We take $\psi_n(a) = \epsilon^{\mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_p}(a)}$, and let

$$G(y, x) = \prod_{m \in \mathbf{Z}_{\geq 0}^d} \Theta(\widetilde{c_m}\, y x^m) \in \overline{\mathbf{Q}_p}[\![x_1, \ldots, x_d, y]\!]. \tag{8.4}$$

hence (8.2) and (8.3) imply

$$\sum_{u \in (\mathbf{F}_{q^n}^*)^d} \sum_{v \in \mathbf{F}_{q^n}^*} \psi_n(vf(u)) = \sum_{v, u_1, \ldots, u_d \in \mathbf{F}_{q^n}^*} \left(\prod_{i=0}^{n-1} G(\widetilde{v}^{q^i}, \widetilde{u_1}^{q^i}, \ldots, \widetilde{u_d}^{q^i}) \right). \tag{8.5}$$

We will use this formula in §3 to prove that $\widetilde{Z}(X,t)$ can be written as the quotient of two formal power series in $\mathbf{C}_p[\![t]\!]$, both having infinite radius of convergence.

8.2. The construction of Θ

We now explain how to construct the formal power series Θ whose existence was assumed in the previous section. Note first that it is enough to do the construction when $q = p$: indeed, if $\Theta_1 \in \mathbf{Q}_p(\epsilon)[\![t]\!]$ satisfies P1) and P2) for $q = p$, and for $q = p^e$ we take $\Theta(t) = \Theta_1(t)\Theta_1(t^p)\cdots\Theta_1(t^{p^{e-1}})$, then Θ satisfies P1) and P2) for q. Indeed, if $R > 1$ is the radius of convergence of Θ_1, then the radius of convergence of Θ is at least $R^{1/p^{e-1}} > 1$. Furthermore,

$$\epsilon^{\mathrm{Tr}_{\mathbf{F}_{p^{ne}}/\mathbf{F}_p}(a)} = \prod_{i=0}^{ne-1} \Theta_1(\widetilde{a}^{p^i}) = \prod_{j=0}^{e-1} \Theta(\widetilde{a}^{q^j}).$$

Therefore, in the rest of this section we assume $q = p$.

We begin by considering the formal power series in two variables given by the following infinite product

$$F(x,y) = (1+y)^x (1+y^p)^{\frac{x^p - x}{p}} \cdots (1+y^{p^n})^{\frac{x^{p^n} - x^{p^{n-1}}}{p^n}} \cdots \in \mathbf{Q}[\![x,y]\!].$$

Note that if $1 + h_i$ is the i^{th} factor in the above product, then $h_i \in (y^{p^{i-1}})$, hence the above product gives, indeed, a formal power series[1].

Proposition 8.4. *We have $F(x,y) \in \mathbf{Z}_p[\![x,y]\!]$*[2].

The following lemma gives a general criterion for proving an assertion as in the proposition.

Lemma 8.5. *If $f \in \mathbf{Q}_p[\![x,y]\!]$ is such that $f(0,0) = 1$, then $f \in \mathbf{Z}_p[\![x,y]\!]$ if and only if*

$$\frac{f(x^p, y^p)}{f(x,y)^p} \in 1 + p(x,y)\mathbf{Z}_p[\![x,y]\!]. \tag{8.6}$$

Proof. Suppose first that $f \in \mathbf{Z}_p[\![x,y]\!]$. Since $f(0,0) = 1$, it follows that f is invertible and $\frac{1}{f} \in 1 + (x,y)\mathbf{Z}_p[\![x,y]\!]$. We deduce that $\frac{1}{f^p}$, hence also $\frac{f(x^p,y^p)}{f(x,y)^p}$ lies in $1 + (x,y)\mathbf{Z}_p[\![x,y]\!]$. If $\overline{f} \in \mathbf{F}_p[\![x,y]\!]$ is the reduction of f mod $p\mathbf{Z}_p[\![x,y]\!]$, we clearly have $\overline{f}(x^p,y^p) = \overline{f}(x,y)^p$. This implies that $\frac{f(x^p,y^p)}{f(x,y)^p}$ lies in $1 + p(x,y)\mathbf{Z}_p[\![x,y]\!]$, as required.

Conversely, suppose that (8.6) holds, and let us write $f = \sum_{i,j\geq 0} a_{i,j} x^i y^j$, with $a_{i,j} \in \mathbf{Q}_p$ and $a_{0,0} = 1$. By hypothesis, we may write

$$\sum_{i,j\geq 0} a_{i,j} x^{pi} y^{pj} = \left(\sum_{i,j\geq 0} a_{i,j} x^i y^j\right)^p \cdot \sum_{i,j\geq 0} b_{i,j} x^i y^j, \tag{8.7}$$

where $b_{0,0} = 1$, and all other $b_{i,j}$ lie in $p\mathbf{Z}_p$. Arguing by induction, we see that it is enough to show the following: if $\alpha, \beta \in \mathbf{Z}_{\geq 0}$, not both zero, are such that

[1] The general assertion is that if $h_i \in (x,y)^{N_i}$ are such that $\lim_{i\to\infty} N_i = \infty$, then $\prod_i (1+h_i)$ is a formal power series, as the coefficient of each monomial $x^m y^n$ comes from only finitely many factors in the product.

[2] Of course, since F has coefficients in $\mathbf{Q}$, this is equivalent to saying that F has coefficients in $\mathbf{Z}_{(p\mathbf{Z})}$.

$a_{k,\ell} \in \mathbf{Z}_p$ for all (k,ℓ) with $k \leq \alpha$ and $\ell \leq \beta$ such that one of the inequalities is strict, then $a_{\alpha,\beta} \in \mathbf{Z}_p$. Let us consider the coefficient $c_{\alpha,\beta}$ of $x^\alpha y^\beta$ in the power series in (8.7). By considering the left-hand side of (8.7), we see that $c_{\alpha,\beta} = 0$ unless p divides both α and β, in which case it is equal to $a_{\alpha/p,\beta/p}$. By considering the right-hand side of (8.7), we see that $c_{\alpha,\beta} = pa_{\alpha,\beta} + Q_1 + \ldots + Q_r$, where each Q_j is a product of the form $Nb_{k,\ell}a_{k_1,\ell_1}\cdots a_{k_s,\ell_s}$, for some multinomial coefficient $N \in \mathbf{Z}$, and with all (k_i,ℓ_i) having the property that $k_i \leq \alpha$ and $\ell_i \leq \beta$, with one of the inequalities being strict. It follows that every Q_j lies in $\mathbf{Z}_p$, and if Q_j is not in $p\mathbf{Z}_p$, then $k = \ell = 0$, and $c_{\alpha,\beta}x^\alpha y^\beta = (a_{k,\ell}x^k y^\ell)^p$ for some k and ℓ. This can happen only when both α and β are divisible by p, and in this case Q_j is equal to $a^p_{\alpha/p,\beta/p}$. Furthermore, since in this case we have $a^p_{\alpha/p,\beta/p} \equiv a_{\alpha/p,\beta/p} \pmod p$, we deduce that $a_{\alpha,\beta} \in \mathbf{Z}_p$, and this completes the proof of the proposition. □

REMARK 8.6. It should be clear from the proof of the lemma that a similar statement holds for formal power series in any number of variables. We restricted to the case of two variables, which is the one we will need, in order to avoid complicating too much the notation.

PROOF OF PROPOSITION 8.4. Since we clearly have $F(0,0) = 1$, we may apply Lemma 8.5, so it is enough to show that $\frac{F(x^p,y^p)}{F(x,y)^p}$ lies in $1+p(x,y)\mathbf{Z}_p$. By definition, we have

$$\frac{F(x^p,y^p)}{F(x,y)^p} = \frac{(1+y^p)^{x^p}\cdot(1+y^{p^2})^{\frac{x^{p^2}-x^p}{p}}\cdot(1+y^{p^3})^{\frac{x^{p^3}-x^{p^2}}{p^2}}\cdots}{(1+y)^{px}\cdot(1+y^p)^{x^p-x}\cdot(1+y^{p^2})^{\frac{x^{p^2}-x^p}{p}}\cdots} = \frac{(1+y^p)^x}{(1+y)^{px}}$$

$$= \left(\frac{(1+y^p)}{(1+y)^p}\right)^x.$$

In order to see that this lies in $1+p(x,y)\mathbf{Z}_p[\![x,y]\!]$, we apply Lemma 8.5 in the other direction: since $g = 1+y \in \mathbf{Z}_p[\![y]\!]$, and $g(0) = 1$, we deduce that $\frac{1+y^p}{(1+y)^p} = 1+pw$, for some $w \in y\mathbf{Z}_p[\![y]\!]$. It follows from definition that

$$(1+pw)^x = 1 + \sum_{m\geq 1} \frac{x(x-1)\ldots(x-m+1)}{m!}p^m w^m,$$

and $\frac{p^m}{m!} \in p\mathbf{Z}_p$ for every $m \geq 1$. Indeed, we have

$$\mathrm{ord}_p(m!) = \sum_{i\geq 1}\lfloor m/p^i\rfloor < \frac{m}{p}\sum_{i\geq 0}\frac{1}{p^i} = \frac{m}{p-1} \leq m.$$

We conclude that $\left(\frac{(1+y^p)}{(1+y)^p}\right)^x \in 1+p(x,y)\mathbf{Z}_p[\![x,y]\!]$, which completes the proof. □

Recall that $\epsilon \in \overline{\mathbf{Q}_p}$ is our fixed primitive root of order p of 1. Let $\lambda = \epsilon - 1$. The following estimate for $|\lambda|_p$ is well-known, but we include a proof for completeness.

LEMMA 8.7. *With the above notation, we have* $|\lambda|_p = \left(\frac{1}{p}\right)^{1/(p-1)}$.

PROOF. Since $(1+\lambda)^p = 1$, it follows that λ is a root of the polynomial $h(x) = x^{p-1} + \sum_{i=1}^{p-1}\binom{p}{i}x^{p-1-i}$. Since all coefficients of f but the leading one are divisible by p, and $h(0)$ is not divisible by p^2, it follows from Eisenstein's criterion

that $h \in \mathbf{Q}_p[x]$ is an irreducible polynomial. This shows that $\mathbf{Q}_p(\epsilon) = \mathbf{Q}_p(\lambda)$ has degree $(p-1)$ over $\mathbf{Q}_p$.

Every $\sigma\colon \mathbf{Q}_p(\epsilon) \to \overline{\mathbf{Q}_p}$ must satisfy $\sigma(\epsilon) = \epsilon^i$ for some $1 \leq i \leq p-1$, and σ is uniquely determined by i. This shows that $\mathbf{Q}_p(\epsilon)$ is a Galois extension of $\mathbf{Q}_p$, and since $[\mathbf{Q}_p(\epsilon) : \mathbf{Q}_p] = n-1$, we conclude that the Galois conjugates of ϵ are precisely the ϵ^i, with $1 \leq i \leq p-1$. In particular, we have $|1-\epsilon|_p = |1-\epsilon^i|_p$ for every $1 \leq i \leq p$. On the other hand, we have

$$1 + x + \ldots + x^{p-1} = \prod_{i=1}^{p-1}(x - \epsilon^i),$$

hence $\prod_{i=1}^{p-1}(1-\epsilon^i) = p$. We thus deduce

$$|\epsilon - 1|_p = |p|_p^{1/(p-1)} = \left(\frac{1}{p}\right)^{1/(p-1)}.$$

□

We put $\Theta(t) = F(t, \lambda)$. We first show that this is well-defined and has radius of convergence > 1.

LEMMA 8.8. *We have $\Theta \in \mathbf{Q}_p(\epsilon)[\![t]\!]$, and its radius of convergence is at least $p^{1/(p-1)} > 1$.*

PROOF. Let us write $F(x,y) = \sum_{m\geq 0}\left(\sum_{n\geq 0} a_{m,n}y^n\right)x^m$. By Proposition 8.4, we have $a_{m,n} \in \mathbf{Z}_p$ for every m and n. We claim that $a_{m,n} = 0$ whenever $m > n$. Indeed, note that in

$$(1+y)^x = \sum_{n\geq 0} \frac{x(x-1)\ldots(x-n+1)}{n!}y^n,$$

every monomial x^iy^j that appears with nonzero coefficient, has $i \leq j$. The same then holds for each $(1+y^{p^i})^{\frac{x^{p^i}-x^{p^{i-1}}}{p^i}}$, for $i \geq 1$. Since this property holds for each of the factors in the definition of $F(x,y)$, it also holds for F, as claimed.

Since $|a_{m,n}|_p \leq 1$ for every m and n, each series $\sum_{n\geq 0} a_{m,n}y^n$ has radius of convergence at least $1 > |\lambda|_p$, hence $F(t,\lambda)$ is a well-defined series in $\mathbf{Q}_p(\epsilon)[\![t]\!]$. Furthermore, for every m we have

$$|\sum_{n\geq 0} a_{m,n}\lambda^n|_p = |\sum_{n\geq m} a_{m,n}\lambda^n|_p \leq |\lambda|_p^m.$$

This implies that the radius of convergence of $F(t,\lambda)$ is at least $|\lambda|_p^{-1} = p^{1/(p-1)} > 1$. □

We now show that Θ also satisfies the property P2) from §1 and thus complete the proof of the existence of Θ with the required properties.

LEMMA 8.9. *For every $n \geq 1$, and every $a \in \mathbf{F}_{p^n}$, we have*

$$\epsilon^{\mathrm{Tr}_{\mathbf{F}_{p^n}/\mathbf{F}_p}(a)} = \Theta(\widetilde{a})\Theta(\widetilde{a}^p)\cdots\Theta(\widetilde{a}^{p^{n-1}}).$$

PROOF. Note first that since Θ has radius of convergence larger than 1, and $|\widetilde{a}^{p^i}|_p$ is either 1 or 0, we may apply Θ to the $\widetilde{a}^{p^i}$. Let us compute, more generally,

$$\prod_{i=0}^{n-1} F(\widetilde{a}^{p^i}, y) = \prod_{i=0}^{n-1}(1+y)^{\widetilde{a}^{p^i}} \cdot \prod_{m\geq 1}(1+y^{p^m})^{\sum_{i\geq 0}^{n-1} \frac{\widetilde{a}^{p^{m+i}} - \widetilde{a}^{p^{m+i-1}}}{p^m}}$$

$$= (1+y)^{\widetilde{a}+\widetilde{a}^p+\ldots+\widetilde{a}^{p^{n-1}}} \cdot \prod_{m\geq 1}(1+y^{p^m})^{\frac{\widetilde{a}^{p^{m+n-1}} - \widetilde{a}^{p^{m-1}}}{p^m}} = (1+y)^{\widetilde{a}+\widetilde{a}^p+\ldots+\widetilde{a}^{p^{n-1}}},$$

where the last equality follows from the fact that $\widetilde{a}^{p^n} = \widetilde{a}$. Since $\lambda = \epsilon - 1$, in order to complete the proof of the lemma it is enough to show that

$$\epsilon^{\widetilde{a}+\widetilde{a}^p+\ldots+\widetilde{a}^{p^{n-1}}} = \epsilon^{\mathrm{Tr}_{\mathbf{F}_{p^n}/\mathbf{F}_p}(a)}. \tag{8.8}$$

Recall that $\mathbf{F}_{p^n}$ is a Galois extension of $\mathbf{F}_p$ with Galois group isomorphic to $\mathbf{Z}/n\mathbf{Z}$, and generated by σ, where $\sigma(u) = u^p$. By Theorem B.6 we have an isomorphism $G(\mathbf{Q}_p^{(n)}/\mathbf{Q}_p) \simeq G(\mathbf{F}_{p^n}/\mathbf{F}_p)$, and let $\widetilde{\sigma}$ be the automorphism of $\mathbf{Q}_p^{(n)}$ corresponding to σ. Since $\widetilde{\sigma}(\widetilde{a})^{p^n} = \widetilde{\sigma}(\widetilde{a})$, it follows that $\widetilde{\sigma}(\widetilde{a})$ is the Teichmüller lift of its residue class, which is $\sigma(a) = a^p$. Therefore $\widetilde{\sigma}(\widetilde{a}) = \widetilde{a}^p$. We conclude that $\sum_{i=0}^{n-1} \widetilde{a}^{p^i} \in \mathbf{Z}_p$, and it clearly lies over $\sum_{i=0}^{n-1} a^{p^i} = \mathrm{Tr}_{\mathbf{F}_{p^n}/\mathbf{F}_p}(a)$. Therefore in order to show (8.8), we see that it suffices to show that if $w \in \mathbf{Z}_p$ lies over $b \in \mathbf{F}_p$, then $\epsilon^w = \epsilon^b$, where the left-hand side is defined as $(1+\lambda)^w$. We may write $w = pw_0 + \ell$ for some $\ell \in \mathbf{Z}$, and using Proposition B.25, we obtain

$$(1+\lambda)^w = ((1+\lambda)^p)^{w_0} \cdot (1+\lambda)^\ell = 1 \cdot \epsilon^\ell = \epsilon^b.$$

This completes the proof of the lemma. □

8.3. Traces of certain linear maps on rings of formal power series

Our goal in this section is to establish the following intermediary step towards the proof of the rationality of the zeta function.

PROPOSITION 8.10. *With the notation introduced in §1, for every $X = V(f)$, where $f \in \mathbf{F}_q[x_1, \ldots, x_n]$, the formal power series $\widetilde{Z}(X,t)$ can be written as a quotient $\frac{g(t)}{h(t)}$, where $g, h \in \mathbf{C}_p[\![t]\!]$ have infinite radii of convergence.*

The proof of the proposition will rely on the formula for the numbers N'_n coming out of (8.1) and (8.5) in §1, and on a formalism for treating certain linear maps on a formal power series ring, that we develop in this section.

For $N \geq 1$, we consider the formal power series ring $R = \mathbf{C}_p[\![x_1, \ldots, x_N]\!]$, and we denote by $\mathfrak{m}$ the maximal ideal in R. We will apply this with $N = d+1$, where d is as in the previous sections. As usual, for $\alpha = (\alpha_1, \ldots, \alpha_N) \in \mathbf{Z}_{\geq 0}^N$, we put $x^\alpha = x_1^{\alpha_1} \cdots x_N^{\alpha_N}$ and $|\alpha| = \sum_{i=1}^N \alpha_i$. The order $\mathrm{ord}(h)$ of $h \in R$ is the largest $r \geq 0$ such that $h \in \mathfrak{m}^r$ (we make the convention that $\mathrm{ord}(0) = \infty$). On R we consider the $\mathfrak{m}$-adic topology. Recall that this is invariant under translations, and a basis of open neighborhoods of the origin is given by $\{\mathfrak{m}^r \mid r \geq 0\}$. Therefore we have $h_m \to h$ when m goes to infinity if and only if $\lim_{m\to\infty} \mathrm{ord}(f_m - f) = \infty$. As in the case of a DVR, one shows that one can put a metric on R that induces the $\mathfrak{m}$-adic topology.

We will consider $\mathbf{C}_p$-linear maps $A\colon R \to R$ that are continuous with respect to the $\mathfrak{m}$-adic topology. Such a map is determined by its values on the monomials in R. More precisely, such a map must satisfy

$$\lim A(x^\alpha) = 0 \text{ when } |\alpha| \to \infty, \tag{8.9}$$

and for $f = \sum_\alpha c_\alpha x^\alpha$, we have $A(f) = \sum_\alpha c_\alpha A(x^\alpha)$. Conversely, given a set of elements $(A(x^\alpha))_{\alpha \in \mathbf{Z}^N_{\geq 0}}$ that satisfies (8.9), we obtain a continuous linear map A given by the above formula. If we write $A(x^\beta) = \sum_\alpha a_{\alpha\beta} x^\alpha$, with $a_{\alpha\beta} \in \mathbf{C}_p$, then we can represent A by the "matrix" $(a_{\alpha\beta})_{\alpha,\beta \in \mathbf{Z}^N_{\geq 0}}$. Note that condition (8.9) translates as follows: for every α, we have $a_{\alpha\beta} = 0$ for $|\beta| \gg 0$.

We say that A has finite support if the corresponding "matrix" $(a_{\alpha\beta})$ has only finitely many nonzero entries. In this case A can be identified to an endomorphism of a finite-dimensional subspace of $\mathbf{C}_p[x_1, \ldots, x_N] \subseteq \mathbf{C}_p[\![x_1, \ldots, x_n]\!]$, and $(a_{\alpha\beta})$ can be identified to the corresponding matrix.

The usual rules for dealing with matrices apply in this setting. If A is described by the "matrix" $(a_{\alpha\beta})$, then

$$A(\sum_\beta c_\beta x^\beta) = \sum_\alpha \left(\sum_\beta a_{\alpha\beta} c_\beta \right) x^\alpha$$

(note that by hypothesis, the sum $\sum_\beta a_{\alpha\beta} c_\beta$ has only finitely many nonzero terms). If A and B are linear, continuous maps as above, described by the "matrices" $(a_{\alpha\beta})$ and $(b_{\alpha\beta})$, then the composition $A \circ B$ is again linear and continuous, and it is represented by the product $(c_{\alpha\beta})$ of the two "matrices": $c_{\alpha\beta} = \sum_\gamma a_{\alpha\gamma} b_{\gamma\beta}$.

We now introduce the two main examples of such maps that we will consider. Given $H \in R$, we define $\Psi_H\colon R \to R$ to be given by multiplication by H: $\Psi_H(f) = fH$. This is clearly $\mathbf{C}_p$-linear and continuous. If $H = \sum_\alpha h_\alpha x^\alpha$, then Ψ_H is represented by the "matrix" $(h_{\alpha-\beta})_{\alpha,\beta}$, where we put $h_{\alpha-\beta} = 0$ if $\alpha - \beta \notin \mathbf{Z}^N_{\geq 0}$. Note that $\Psi_{H_1} \circ \Psi_{H_2} = \Psi_{H_1 H_2}$.

For another example, if q is any positive integer, let $T_q\colon R \to R$ be given by $T_q(\sum_{\alpha \in \mathbf{Z}^N_{\geq 0}} a_\alpha x^\alpha) = \sum_{\alpha \in \mathbf{Z}^N_{\geq 0}} a_{q\alpha} x^\alpha$. It is clear that T_q is $\mathbf{C}_p$-linear and continuous. If $H = \sum_\alpha h_\alpha x^\alpha \in R$, let $\Psi_{q,H} = T_q \circ \Psi_H$. We have

$$\Psi_{q,H}(x^\beta) = T_q(\sum_\alpha h_\alpha x^{\alpha+\beta}) = T_q(\sum_\alpha h_{\alpha-\beta} x^\alpha) = \sum_\alpha h_{q\alpha-\beta} x^\beta.$$

Therefore $\Psi_{q,H}$ is represented by the "matrix" $(h_{q\alpha-\beta})_{\alpha,\beta}$.

LEMMA 8.11. *We have* $\Psi_H \circ T_q = \Psi_{q,H_q}$, *where* $H_q(x_1, \ldots, x_N) = H(x_1^q, \ldots, x_N^q)$.

PROOF. Let $H = \sum_{\alpha \in \mathbf{Z}^d_{\geq 0}} h_\alpha x^\alpha$, and we put $h_\alpha = 0$ if $\alpha \notin \mathbf{Z}^N_{\geq 0}$. We have

$$\Psi_H \circ T_q(\sum_\beta b_\beta x^\beta) = H \cdot \sum_\beta b_{q\beta} x^\beta = \sum_\gamma \left(\sum_{\alpha+\beta=\gamma} h_\alpha b_{q\beta} \right) x^\gamma. \tag{8.10}$$

On the other hand,

$$T_q \circ H_q \left(\sum_\beta b_\beta x^\beta \right) = T_q \left(\sum_\gamma \left(\sum_{q\alpha+\beta=\gamma} h_\alpha b_\beta \right) x^\gamma \right) = \sum_\gamma \left(\sum_{q\alpha+\beta=q\gamma} h_\alpha b_\beta \right) x^\gamma \tag{8.11}$$

In the last sum in (8.11) we see that β has to be divisible by q, and we deduce that the two expressions in (8.10) and (8.11) are equal. □

We now discuss the trace of a continuous linear map as above. Given such a map $A\colon R \to R$ described by the "matrix" $(a_{\alpha\beta})$, we consider the series $\sum_{\alpha\in\mathbf{Z}^N_{\geq 0}} a_{\alpha\alpha}$. If this is convergent in $\mathbf{C}_p$, we denote its sum by $\mathrm{Trace}(A)$. Note that if A has finite support, then $\mathrm{Trace}(A)$ is equal to the trace of any corresponding endomorphism of a finite-dimensional vector space of polynomials.

Let R_0 be the set of those $H = \sum_\alpha h_\alpha x^\alpha \in R$ with the property that there is $M > 0$ such that $|h_\alpha|_p \leq \left(\frac{1}{p}\right)^{M|\alpha|}$ for every $\alpha \in \mathbf{Z}^N_{\geq 0}$.

Remark 8.12. If $H \in R_0$, then there is $\rho > 1$ such that $H(u_1, \ldots, u_N)$ is convergent whenever $u_i \in \mathbf{C}_p$ are such that $|u_i| \leq \rho$ for all i. Indeed, with M as above, if $\rho = p^a$, where $0 < a < M$, then

$$|h_\alpha u_1^{\alpha_1} \ldots u_N^{\alpha_N}|_p \leq |h_\alpha|_p \cdot \rho^{|\alpha|} \leq \left(\frac{1}{p}\right)^{(M-a)|\alpha|},$$

which converges to zero when $|\alpha|$ goes to infinity.

Lemma 8.13. *R_0 is a subring of R. Furthermore, if $j_1, \ldots, j_N$ are positive integers, and if $H \in R_0$, then $H(x_1^{j_1}, \ldots, x_N^{j_N}) \in R_0$.*

Proof. The first assertion follows from the fact that if $M > 0$ works for both H_1 and H_2, then it also works for $H_1 - H_2$ and $H_1 H_2$. The second assertion follows from the fact that if M works for H, and if $j = \max\{j_1, \ldots, j_N\}$, then M/j works for $H(x_1^{j_1}, \ldots, x_N^{j_N})$. □

Proposition 8.14. *Let $H \in R_0$ and $\Psi = \Psi_{q,H}$ for some integer $q \geq 2$. For every $s \geq 1$ the trace of Ψ^s is well-defined, and*

$$(q^s - 1)^N \mathrm{Trace}(\Psi^s) = \sum_u H(u) H(u^q) \ldots H(u^{q^{s-1}}),$$

where the sum is over all $u = (u_1, \ldots, u_N) \in \mathbf{C}_p^N$ such that $u_i^{q^s - 1} = 1$ for all i.

Proof. Let us first consider the case $s = 1$. Recall that if $H = \sum_\alpha h_\alpha x^\alpha$, then Ψ is described by the matrix $(h_{q\alpha-\beta})_{\alpha,\beta}$. Therefore $\mathrm{Trace}(\Psi) = \sum_{\alpha\in\mathbf{Z}^N_{\geq 0}} h_{(q-1)\alpha}$. By assumption, there is $M > 0$ such that $|h_\alpha|_p \leq \left(\frac{1}{p}\right)^{M|\alpha|}$ for every α. In particular, $\lim_{|\alpha|\to\infty} h_{(q-1)\alpha} = 0$.

Furthermore, we have seen in Remark 8.12 that $H(u_1, \ldots, u_N)$ is well-defined when $|u_i| \leq 1$ for all i. The subset $U = \{\lambda \in \mathbf{C}_p \mid \lambda^{q-1} = 1\}$ is a cyclic subgroup of $\mathbf{C}_p$. If $\lambda_0 \in U$ is a generator, then

$$\sum_{\lambda\in U} \lambda^i = \sum_{j=0}^{q-2} \lambda_0^{ij} = \begin{cases} q-1, & \text{if } (q-1)|i; \\ 0, & \text{otherwise.} \end{cases}$$

Therefore

$$\sum_{u\in U^N} H(u) = \sum_{u\in U^N} \sum_{\alpha\in\mathbf{Z}^N_{\geq 0}} h_\alpha u^\alpha = \sum_{\alpha\in\mathbf{Z}^N_{\geq 0}} h_\alpha \cdot \prod_{i=1}^N \left(\sum_{u_i\in U} u_i^{\alpha_i}\right)$$

$$= (q-1)^N \sum_{\alpha \in (q-1)\mathbf{Z}^N_{\geq 0}} h_\alpha = (q-1)^N \mathrm{Trace}(\Psi).$$

This completes the proof when $s = 1$. Suppose now that $s \geq 2$. Using repeatedly Lemma 8.11, we obtain

$$\Psi^s = (T_q \circ \Psi_H)^s = (T_q^2 \circ \Psi_{H_q} \circ \Psi_H) \circ (T_q \circ \Psi_H)^{s-2} = (T_q^2 \circ \Psi_{H_q H}) \circ (T_q \circ \Psi_H)^{s-2} = \dots$$
$$= T_q^s \circ \Psi_{H_{q^{s-1}} \dots H_q H} = \Psi_{q^s, H_{q^{s-1}} \dots H_q H}.$$

It follows from Lemma 8.13 that since H lies in R_0, we also have $H_{q^{s-1}} \dots H_q H \in R_0$. Therefore we may apply the case $s = 1$ to deduce that $\mathrm{Trace}(\Psi^s)$ is well-defined, and that

$$(q^s - 1)^N \mathrm{Trace}(\Psi^s) = \sum_{u \in U^N} H(u) H(u^q) \dots H(u^{q^{s-1}}).$$

□

Suppose now that $A \colon R \to R$ is a $\mathbf{C}_p$-linear continuous map, described by the "matrix" $(a_{\alpha\beta})_{\alpha,\beta}$. We define the characteristic power series of A by

$$\det(\mathrm{Id} - tA) := \sum_{m \geq 0} (-1)^m \left(\sum_\sigma \epsilon(\sigma) a_{\alpha_1 \sigma(\alpha_1)} \cdots a_{\alpha_m \sigma(\alpha_m)} \right) t^m, \tag{8.12}$$

where the second sum is over all subsets with m elements $\{\alpha_1, \dots, \alpha_m\}$ of $\mathbf{Z}^N_{\geq 0}$, and over all permutations σ of such a set. Of course, the definition makes sense if the series that appears as the coefficient of t^m is convergent in $\mathbf{C}_p$ for every m. It is clear that if A has finite support, then $\det(\mathrm{Id} - tA)$ is equal to the characteristic polynomial of a corresponding endomorphism of a finite-dimensional vector space of polynomials.

LEMMA 8.15. *If $H \in R_0$, then for every integer $q \geq 2$ the characteristic power series of $\Psi = \Psi_{q,H}$ is well-defined, and it has infinite radius of convergence.*

PROOF. Let us write $H = \sum_\alpha h_\alpha x^\alpha$, and let $M > 0$ be such that $|h_\alpha|_p \leq \left(\frac{1}{p}\right)^{M|\alpha|}$ for every α. We have seen that Ψ is described by the "matrix" $(a_{\alpha\beta})$, where $a_{\alpha\beta} = h_{q\alpha-\beta}$. Given $\{u_1, \dots, u_m\} \subseteq \mathbf{Z}^N_{\geq 0}$, and a permutation σ of this set, we have

$$|a_{\alpha_1 \sigma(\alpha_1)} \cdots a_{\alpha_m \sigma(\alpha_m)}|_p \leq \left(\frac{1}{p}\right)^{M \sum_{i=1}^m |q\alpha_i - \sigma(\alpha_i)|}.$$

Note that $|q\alpha_i - \sigma(\alpha_i)| = q|\alpha_i| - |\sigma(\alpha_i)|$ if $q\alpha_i - \sigma(\alpha_i)$ is in $\mathbf{Z}^N_{\geq 0}$, and $|q\alpha_i - \sigma(\alpha_i)| = 0$, otherwise. Furthermore, in the latter case we also have $a_{\alpha_i \sigma(\alpha_i)} = 0$. We thus conclude that

$$|a_{\alpha_1 \sigma(\alpha_1)} \cdots a_{\alpha_m \sigma(\alpha_m)}|_p \leq \left(\frac{1}{p}\right)^{M(q-1)(|\alpha_1| + \dots + |\alpha_m|)}.$$

Since the right-hand side tends to zero when $\max\{|\alpha_i|\}$ goes to infinity, it follows that $\det(\mathrm{Id} - tA)$ is well-defined.

Furthermore, the above computation shows that if we write $\det(\mathrm{Id} - tA) = \sum_{m \geq 0} b_m t^m$, then

$$|b_m|_p^{1/m} \leq \max_{\alpha_1, \dots, \alpha_m} \left(\frac{1}{p}\right)^{\frac{M(q-1)(|\alpha_1| + \dots + |\alpha_m|)}{m}},$$

where the maximum is over *distinct* $\alpha_1, \ldots, \alpha_m \in \mathbf{Z}_{\geq 0}^N$. When m goes to infinity, we have

$$\min_{\alpha_1,\ldots,\alpha_m} \frac{M(q-1)(|\alpha_1| + \ldots + |\alpha_m|)}{m} \to \infty.$$

The above estimate therefore implies that $\lim_{m\to\infty} |b_m|_p^{1/m} = 0$, hence $\det(\mathrm{Id} - tA)$ has infinite radius of convergence. □

PROPOSITION 8.16. *If $A\colon R \to R$ is a continuous $\mathbf{C}_p$-linear map such that $\det(\mathrm{Id} - tA)$ and $\mathrm{Trace}(A^s)$ are well-defined for all $s \geq 1$, then*

$$\det(\mathrm{Id} - tA) = \exp\left(-\sum_{s\geq 1} \frac{\mathrm{Trace}(A^s)}{s} t^s\right).$$

PROOF. If A has finite support, then the assertion follows from Lemma 4.12. Our goal is to use this special case to deduce the general one.

Let us consider a sequence $(A^{(m)})_{m\geq 1}$ of maps with finite support, each described by the matrix $(a_{\alpha\beta}^{(m)})_{\alpha,\beta\in\mathbf{Z}_{\geq 0}^N}$, that satisfies the following condition. For every α and β, we have $a_{\alpha\beta}^{(m)} = a_{\alpha\beta}$ or $a_{\alpha\beta}^{(m)} = 0$, and the former condition holds for all $m \gg 0$. It is clear that we can find a sequence $(A^{(m)})_{m\geq 1}$ with this property.

It is convenient to consider on $\mathbf{C}_p[\![t]\!]$ (identified to a countable product of copies of $\mathbf{C}_p$) the product topology, where each $\mathbf{C}_p$ has the usual p-adic topology. Explicitly, a sequence of formal power series $(f_m)_{m\geq 1}$, with $f_m = \sum_{i\geq 0} b_{m,i} t^i$, converges to $f = \sum_{i\geq 0} b_i t^i$ if and only if $\lim_{m\to\infty} b_{m,i} = b_i$ for every i. Note that if this is the case, and all $f_m(0)$ are zero, then $\exp(f_m)$ converges to $\exp(f)$ when m goes to infinity (this is the case if we replace exp by any other element of $\mathbf{C}_p[\![t]\!]$). Since each $A^{(m)}$ satisfies the conclusion of the proposition, in order to complete the proof it is enough to show that

i) $\lim_{m\to\infty} \det(\mathrm{Id} - tA^{(m)}) = \det(\mathrm{Id} - tA)$.
ii) $\lim_{m\to\infty} \mathrm{Trace}((A^{(m)})^s) = \mathrm{Trace}(A^s)$ for every $s \geq 1$.

Let us first check i). We consider the coefficients $b_\ell^{(m)}$ and b_ℓ of t^ℓ in $\det(\mathrm{Id} - tA^{(m)})$ and $\det(\mathrm{Id} - tA)$, respectively. By definition, we have

$$b_\ell^{(m)} = (-1)^\ell \sum_\sigma \epsilon(\sigma) a_{\alpha_1\sigma(\alpha_1)}^{(m)} \cdots a_{\alpha_\ell\sigma(\alpha_\ell)}^{(m)}. \tag{8.13}$$

By our choice of $A^{(m)}$, every product in the sum above is either zero, or it shows up in the corresponding expression for b_ℓ. Furthermore, given any $\{\alpha_1, \ldots, \alpha_\ell\}$ and any permutation σ of this set, the product $\epsilon(\sigma) a_{\alpha_1\sigma(\alpha_1)} \cdots a_{\alpha_\ell\sigma(\alpha_\ell)}$ appears in (8.13) for $m \gg 0$. Since we know that $\det(\mathrm{Id} - tA)$ exists, the assertion in i) follows.

The proof of ii) is similar. By definition, we have

$$\mathrm{Trace}((A^{(m)})^s) = \sum_{\alpha_1,\ldots,\alpha_s} a_{\alpha_1\alpha_2}^{(m)} \cdots a_{\alpha_{s-1}\alpha_s}^{(m)} a_{\alpha_s\alpha_1}^{(m)}. \tag{8.14}$$

By hypothesis, each product $a_{\alpha_1\alpha_2}^{(m)} \cdots a_{\alpha_s\alpha_1}^{(m)}$ is either equal to $a_{\alpha_1\alpha_2} \cdots a_{\alpha_s\alpha_s}$, or i is zero. Moreover, by hypothesis every product $a_{\alpha_1\alpha_2} \cdots a_{\alpha_s\alpha_{s+1}}$ appears in (8.14) if $m \gg 0$. Since $\mathrm{Trace}(A^s)$ exists, we deduce the assertion in ii). This completes the proof of the proposition. □

By Lemmas 8.14 and 8.15, we may apply the above proposition, to get the following

COROLLARY 8.17. *If $H \in R_0$ and $\Psi = \Psi_{q,H}$ for an integer $q \geq 2$, then*

$$\det(\mathrm{Id} - t\Psi) = \exp\left(-\sum_{s\geq 1} \frac{\mathrm{Trace}(\Psi^s)}{s} t^s\right).$$

We now apply the above framework to give a proof of Proposition 8.10. Given $f \in \mathbf{F}_q[x_1, \ldots, x_d]$, we let $N = d + 1$. We begin with the following lemma.

LEMMA 8.18. *For every $n \geq 1$, the formal power series $G \in R = \mathbf{C}_p[\![y, x_1, \ldots, x_d]\!]$ defined in (8.4) lies in R_0.*

PROOF. Since G is a product of factors of the form $\Theta(\widetilde{c}yx_1^{m_1} \cdots x_d^{m_d})$, it follows from Lemma 8.13 that it is enough to see that $\Theta(ayx_1^{m_1} \cdots y_d^{m_d})$ lies in R_0 whenever $|a|_p = 1$ and $m_1, \ldots, m_d \in \mathbf{Z}_{\geq 0}$. Furthermore, if $q = p^e$, then we have taken $\Theta(t) = \prod_{i=0}^{e-1} \Theta_0(t^{p^i})$, where Θ_0 is constructed for $q = p$. A second application of Lemma 8.13 allows us to reduce to the case when $q = p$.

Recall that we have seen in the proof of Lemma 8.8 that if $\Theta = \sum_{i\geq 0} b_i t^i$, then $|b_i|_p \leq |\lambda|_p^i = \left(\frac{1}{p}\right)^{i/(p-1)}$. If a and $m_1, \ldots, m_d$ are as above, then

$$\Theta(ayx_1^{m_1} \cdots x_d^{m_d}) = \sum_i b_i a^i y^i x_1^{im_1} \cdot x_d^{im_d}.$$

Note that

$$|b_i a^i|_p = |b_i|_p \leq \left(\frac{1}{p}\right)^{i/(p-1)} = \left(\frac{1}{p}\right)^{M|(i,im_1,\ldots,im_d)|},$$

where $M = \frac{1}{(p-1)(1+m_1+\ldots+m_d)}$. Therefore $\Theta(ayx_1^{m_1} \cdots x_d^{m_d})$ lies in R_0. □

We can now prove the result stated at the beginning of this section.

PROOF OF PROPOSITION 8.10. Since $G \in R_0$, we may apply Proposition 8.14 in order to compute $\mathrm{Trace}(\Psi_{q,G})$. Note that $\{w \in \mathbf{C}_p \mid w^{q^n-1} = 1\} = \{\widetilde{u} \mid u \in \mathbf{F}_{q^n}^*\}$. We deduce using (8.1) and (8.5) that

(8.15)
$$N_n' q^n - (q^n-1)^d = \sum_{v,u_1,\ldots,u_d \in \mathbf{F}_{q^n}^*} \left(\prod_{i=0}^{n-1} G(\widetilde{v}^{q^i}, \widetilde{u_1}^{q^i}, \ldots, \widetilde{u_d}^{q^i})\right) = (q^n-1)^{d+1}\mathrm{Trace}(\Psi_{q,G}^n).$$

Let us compute

(8.16)
$$\exp\left(\sum_{n\geq 1} \frac{N_n' q^n - (q^n-1)^d}{n} t^n\right) = \widetilde{Z}(X, qt) \cdot \exp\left(-\sum_{i=0}^{d} (-1)^{d-i}\binom{d}{i}\frac{q^{ni}}{n} t^n\right)$$

$$= \widetilde{Z}(X, qt) \cdot \prod_{i=0}^{d} \exp\left((-1)^{d-i}\binom{d}{i}\log(1-q^i t)\right) = \widetilde{Z}(X, qt) \cdot \prod_{i=0}^{d} (1-q^i t)^{(-1)^{d-i}\binom{d}{i}}.$$

On the other hand, using Corollary 8.17 and Lemma 8.18 we get

(8.17)
$$\exp\left(\sum_{n\geq 1}(q^n-1)^{d+1}\mathrm{Trace}(\Psi_{q,G}^n)\frac{t^n}{n}\right)=\exp\left(\sum_{i=0}^{d+1}(-1)^{d+1-i}\binom{d+1}{i}\mathrm{Trace}(\Psi_{q,G}^n)\frac{q^{ni}t^n}{n}\right)$$
$$=\prod_{i=0}^{d+1}\det(\mathrm{Id}-q^it\Psi_{q,G})^{(-1)^{d-i}\binom{d+1}{i}}.$$

It follows from Lemma 8.15 that each $\det(\mathrm{Id}-q^it\Psi_{q,G})$ has infinite radius of convergence. Since the expressions in (8.16) and (8.17) are equal, we conclude that $\widetilde{Z}(X,qt)$ is the quotient of two formal power series in $\mathbf{C}_p[\![t]\!]$ with infinite radius of convergence, hence $\widetilde{Z}(X,t)$ has the same property. □

8.4. The rationality of the zeta function

The last ingredient in Dwork's proof for the rationality of the zeta function is the following proposition. In order to avoid confusion, we denote by $|m|_\infty$ the usual (Archimedean) absolute value of an integer m.

PROPOSITION 8.19. *Let $Z(t)=\sum_{n\geq 0}a_nt^n$ be a formal power series in $\mathbf{Z}[\![t]\!]$, that satisfies the following two properties:*

1) *There are $C,s>0$ such that $|a_n|_\infty\leq Cs^n$ for all $n\geq 0$.*
2) *The image of Z in $\mathbf{C}_p[\![t]\!]$ can be written as a quotient $\frac{g(t)}{h(t)}$, where $g,h\in\mathbf{C}_p[\![t]\!]$ have infinite radii of convergence.*

Then $Z(t)$ lies in $\mathbf{Q}(t)$.

We first need a lemma that gives a sharper version of the rationality criterion in Proposition 4.13. We will consider a formal power series $f=\sum_{n\geq 0}a_nt^n$ with coefficients in a field K. For every $i,N\geq 0$, we consider the matrix $A_{i,N}=(a_{i+\alpha+\beta})_{0\leq\alpha,\beta\leq N}$.

LEMMA 8.20. *With the above notation, the power series f is rational if and only if there is N such that $\det(A_{i,N})=0$ for all $i\gg 0$.*

PROOF. We have $f\in K(t)$ if and only if there is a nonzero polynomial $Q(t)$ such that Qf is a polynomial. If we write $Q=b_0+b_1t+\ldots+b_Nt^N$, then the condition we need is that

$$b_Na_i+b_{N-1}a_{i+1}+\ldots+b_0a_N=0 \tag{8.18}$$

for all $i\gg 0$. The existence of $b_0,\ldots,b_N$, not all zero, that satisfy these conditions clearly implies that $\det(A_{i,N})=0$ for $i\gg 0$.

Conversely, suppose that we have N such that $\det(A_{i,N})=0$ for $i\gg 0$ (say, for $i\geq i_0$), and that N is minimal with this property. For every i, we put

$$L_i=(a_i,\ldots,a_{i+N})\in K^{N+1}\text{ and }L_i'=(a_i,\ldots,a_{i+N-1})\in K^N.$$

Claim. We have $\det(A_{i,N-1})\neq 0$ for every $i\geq i_0$. If this is the case, since $\det(A_{i,N})=0$, it follows that for every $i\geq i_0+N$, we have $L_i\in\sum_{j=1}^N L_{i-j}$, so that $\sum_{i\geq i_0}K\cdot L_i$ is spanned by $L_{i_0},\ldots,L_{i_0+N-1}$. In this case, it is clear that we can find $b_0,\ldots,b_N$ not all zero such that (8.18) holds for all $i\geq i_0$. Therefore, in order to complete the proof it is enough to show the claim.

By the minimality assumption in the definition of N, it is enough to show that if $i \geq i_0$ and $\det(A_{i,N-1}) = 0$, then $\det(A_{i+1,N-1}) = 0$. Since $\det(A_{i,N-1}) = 0$, we have $L'_i, \ldots, L'_{i+N-1}$ linearly dependent. We have two cases to consider. If $L'_{i+1}, \ldots, L'_{i+N-1}$ are linearly dependent, then it is clear that $\det(A_{i+1,N-1}) = 0$. On the other hand, if this is not the case, then we can write $L'_i = \sum_{j=1}^{N-1} c_j L'_{i+j}$. Let us replace in the first row of $A_{i,N}$ each $a_{i+\ell}$ by $a_{i+\ell} - \sum_{j=1}^{N-1} c_j a_{i+\ell+j}$. We thus obtain $0 = \det(A_{i,N}) = \det(A_{i+1,N-1}) \cdot \delta$, where $\delta = a_{i+N} - \sum_{j=1}^{N-1} c_\ell a_{i+N+j}$. If $\delta \neq 0$, we clearly get $\det(A_{i+1,N-1}) = 0$. On the other hand, if $\delta = 0$, then it follows that L_i lies in the linear span of $L_{i+1}, \ldots, L_{i+N-1}$. Hence the top-right N-minor of $A_{i,N}$ vanishes, but this is precisely $\det(A_{i+1,N-1})$. This completes the proof of the claim, hence that of the proposition. □

Proof of Proposition 8.19. We begin by choosing $\alpha > 0$ such that $\alpha > \frac{\log(s)}{\log p}$. We then apply Proposition B.21 to h and $R > p^\alpha$, to write $h = Pu$, where $P \in \mathbf{C}_p[t]$ and $u \in \mathbf{C}_p[\![t]\!]$ is invertible, and u and u^{-1} have radius of convergence $> p^\alpha$. We may clearly assume that $P(0) = 1$. We thus can write $f = \frac{gu^{-1}}{P}$, and the radius of convergence of gu^{-1} is $> p^\alpha$. If we write $gu^{-1} = \sum_{n\geq 0} b_n t^n$, then by Proposition B.18 we have $\limsup_m |b_m|_p^{1/m} < p^{-\alpha}$. Therefore there is m_0 such that

$$|b_m|_p \leq p^{-m\alpha} \text{ for all } m \geq m_0. \tag{8.19}$$

Let us write $f = \sum_{n\geq 0} a_n t^n$. Using the notation in Lemma 8.20, we need to show that we can choose N such that $\det(A_{i,N})$ for all $i \gg 0$. The key is to compare $|\det(A_{i,N})|_p$ and $|\det(A_{i,N})|_\infty$. Using condition 1) is the proposition, we get

$$|\det(A_{i,n})|_\infty \leq \sum_{\sigma\in S_{n+1}} |\prod_{\alpha=0}^{N} |a_{i+\alpha+\sigma(\alpha)}|_\infty \leq C^{N+1}(N+1)! \cdot s^{2\sum_{j=0}^{N}(i+j)}$$
$$= C^{N+1}(N+1)! \cdot s^{(N+1)(2i+N)}.$$

On the other hand, let us write $P = 1 + \lambda_1 t + \ldots + \lambda_r t^r$, so that $b_i = a_i + c_1 a_{i-1} + \ldots + c_r a_{i-r}$ for every $i \geq r$. Suppose that $N+1 = r+\ell$, and let $T_0, \ldots, T_N$ denote the columns of the matrix $A_{i,N}$. Starting with $j = N$ and going down up to $j = r$, we may replace T_j by $T_j + \lambda_1 T_{j-1} + \ldots + \lambda_r T_{j-r}$, without changing $\det(A_{i,N})$. In this way, we have replaced in the last ℓ columns each a_j by b_j. Since all a_m are in $\mathbf{Z}$, we have $|a_m|_p \leq 1$, and is we assume $i \geq m_0$, we deduce using (8.19) that

$$|\det(A_{i,N})|_p \leq p^{-2\alpha\sum_{j=0}^{\ell-1}(i+r+j)} = p^{-\alpha\ell(2i+2r+\ell-1)}.$$

It follows from definition that if m is any nonzero integer, then $|m|_\infty \geq |m|_p^{-1}$. We conclude from the above that if $\det(A_{i,N})$ is nonzero, then

$$p^{\alpha\ell(2i+2r+\ell-1)} \leq |\det(A_{i,N})|_p^{-1} \leq |\det(A_{i,N})|_\infty \leq C^{N+1}(N+1)! s^{(N+1)(2i+N)}.$$

By taking log, we get

$$\alpha\ell(2i+2r+\ell-1)\log(p) \leq (r+\ell)(i+r+\ell)\log(s) + \log(C^{\ell+r}(\ell+r)!).$$

If ℓ is fixed and $i \gg 0$, this can only happen if $\alpha\ell \cdot \log(p) \leq (r+\ell)\log(s)$. However, by assumption we have $\alpha \cdot \log(p) > \log(s)$, hence if $\ell \gg 0$ we have $\alpha\ell \cdot \log(p) > (r+\ell)\log(s)$, and therefore $\det(A_{i,N}) = 0$ for all $i \gg 0$. This completes the proof of the proposition. □

We can now complete Dwork's proof of the rationality of the zeta function.

THEOREM 8.21. *If X is a variety defined over a finite field $\mathbf{F}_q$, then the zeta function $Z(X,t)$ is rational.*

PROOF. We have seen in Remark 2.21 that, arguing by induction on $\dim(X)$, it is enough to show that $Z(X,t)$ is a rational function when X is a hypersurface in $\mathbf{A}^d_{\mathbf{F}_q}$, defined by some nonzero $f \in \mathbf{F}_q[x_1,\ldots,x_d]$. We denote by H_i the hyperplane $(x_i = 0)$, where $1 \leq i \leq d$. For every $I \subseteq \{1,\ldots,d\}$ (including $I = \emptyset$), we put

$$X_I = X \cap \left(\bigcap_{i\in I} H_i\right) \text{ and } X_I^\circ = X_I \smallsetminus \left(\bigcup_{i\notin I} H_i\right).$$

We have a disjoint decomposition into locally closed subsets $X = \bigsqcup_I X_I^\circ$, hence Proposition 2.12 implies

$$Z(X,t) = \prod_{I\subseteq\{1,\ldots,d\}} Z(X_I^\circ). \tag{8.20}$$

Note that X_I is isomorphic to a hypersurface in $\mathbf{A}^{d-\#I}_{\mathbf{F}_q}$, and using the notation introduced in §1, we have $Z(X_I^\circ,t) = \widetilde{Z}(X_I,t)$. By Proposition 8.10, we can write $Z(X_I^\circ,t)$ as the quotient of two formal power series in $\mathbf{C}_p[\![t]\!]$, having infinite radii of convergence. Formula (8.20), implies that $Z(X,t)$ has the same property.

Recall that $Z(X,t)$ has nonnegative integer coefficients. Furthermore, if we write $Z(X,t) = \sum_{n\geq 0} a_n t^n$, then $a_n \leq q^{dn}$ for every n. Indeed, we have $|X(\mathbf{F}_{q^n})| \leq q^{dn}$ for every $n \geq 1$. Since the exponential function has non-negative coefficients, we deduce that $a_n \leq b_n$, where

$$\sum_{n\geq 0} b_n t^n = \exp\left(\sum_{n\geq 1} \frac{q^{dn}t^n}{n}\right) = \exp(-\log(1-q^d t)) = \frac{1}{1-q^d t} = \sum_{n\geq 0} q^{dn}t^n.$$

Therefore $a_n \leq q^{nd}$ for all $n \geq 0$, and we can apply Proposition 8.19 to conclude that $Z(X,t)$ is a rational function. □

Note the unlike the proof of the rationality of the zeta function described in Chapter 4 (using ℓ-adic cohomology), the above proof is much more elementary, as it only uses some basic facts about p-adic fields. At the same time, its meaning is rather mysterious. A lot of activity has been devoted to giving a cohomological version; in other words, to constructing a p-adic cohomology theory, and a corresponding trace formula, that would "explain" Dwork's proof. Such cohomology theories are the Monsky-Washnitzer cohomology (which behaves well for smooth affine varieties, see [**vdP**]) and the crystalline cohomology of Berthelot and Grothendieck (which behaves well for smooth projective varieties, see [**Ber**]). More recently, Berthelot introduced the *rigid cohomology* [**LeS**] that does not require smoothness, and which extends the Monsky-Washnitzer and the crystalline cohomolgy theories, when these are well-behaved.

APPENDIX A

Quotients by finite groups and ground field extensions

We recall in this appendix some basic facts about quotients of quasiprojective schemes by finite group actions, following [SGA1]. As an application, we discuss in the second section some generalities concerning ground field extensions for algebraic varieties.

A.1. The general construction

Let Y be a scheme of finite type over a field k, and let G be a finite group, acting (on the right) on Y by algebraic automorphisms over k. We denote by σ_g the automorphism corresponding to $g \in G$. A *quotient of Y by G* is a morphism $\pi\colon Y \to W$ with the following two properties:

i) π is G-invariant, that is $\pi \circ \sigma_g = \pi$ for every $g \in G$.
ii) π is universal with this property: for every scheme Z over k, and every G-invariant morphism $f\colon Y \to Z$, there is a unique morphism $h\colon W \to Z$ such that $h \circ \pi = f$.

It is clear from this universal property that if a quotient exists, then it is unique, up to a canonical isomorphism. In this case, we write $W = Y/G$.

We start by considering the case when $Y = \operatorname{Spec} A$ is an affine scheme. Note that G acts on A on the left. We show that the induced morphism $\pi\colon \operatorname{Spec} A \to W = \operatorname{Spec} A^G$ is the quotient of Y by G.

PROPOSITION A.1. *With the above notation, the following hold:*

i) *W is a scheme of finite type over k, and π is a finite, surjective morphism.*
ii) *The fibers of π are precisely the orbits of the G-action on Y.*
iii) *The topology on W is the quotient topology.*
iv) *We have a natural isomorphism $\mathcal{O}_W = \pi_*(\mathcal{O}_Y)^G$.*

PROOF. It is clear that $A^G \hookrightarrow A$ is integral: indeed, for every $u \in A$, we have $P(u) = 0$, where $P = \prod_{g\in G}(x - gu) \in A^G[x]$. Since A is finitely generated over k, it follows that there is a finitely generated k-algebra $B \subseteq A^G$ such that A is integral over B, hence finite over B. Since B is Noetherian, it follows that A^G is a finite over B. We conclude that A^G is a finitely generated k-algebra, and the morphism π is finite. Since $A^G \to A$ is injective, it follows that π is surjective.

It is clear that π is G-invariant, hence each orbit is contained in a fiber. Conversely, if P, Q are primes in A such that $P \cap A^G = Q \cap A^G$, then $P \subseteq \bigcup_{g\in G} gQ$. Indeed, if $u \in P$, then

$$\prod_{g\in G}(gu) \in P \cap A^G = Q \cap A^G,$$

hence there is $g \in G$ such that $gu \in Q$. The Prime Avoidance Lemma implies that $P \subseteq gQ$ for some $g \in G$. Similarly, we get $Q \subseteq hP$ for some $h \in G$. Since $P \subseteq ghP$, and gh is an automorphism, we must have $P = ghP$, hence $P = gQ$.

This proves ii), and the assertion in iii) is now clear since π is closed, being finite. It is easy to deduce iv) from the fact that if $f \in A^G$, then $(A_f)^G = (A_G)_f$. This completes the proof of the proposition. □

REMARK A.2. Suppose that Y is a scheme with an action of the finite group G. If $\pi\colon Y \to W$ is a surjective morphism of schemes that satisfies ii)-iv) in Proposition A.1, then π gives a quotient of Y by G. This is a consequence of the definition of morphisms of schemes. In particular, we see that the morphism $\pi\colon Y \to W$ in Proposition A.1 is such a quotient.

COROLLARY A.3. *If $\pi\colon Y \to W$ is as in the proposition, then for every open subset U of W, the induced morphism $\pi^{-1}(U) \to U$ is the quotient of $\pi^{-1}(U)$ by the action of G.*

PROOF. It is clear that since π is a surjective morphism that satisfies ii)-iv) in the above proposition, the morphism $\pi^{-1}(U) \to U$ satisfies the same properties. □

Suppose now that Y is a scheme over k, with an action of G. We assume that every $y \in Y$ has an affine open neighborhood that is preserved by the G-action. This happens, for example, if Y is quasiprojective. Indeed, in this case for every $y \in Y$, the finite set $\{\sigma_g(y) \mid g \in G\}$ is contained in some affine open subset U of Y[1]. After replacing U by $\cap_{g\in G}\sigma_g(U)$ (this is again affine, since Y is separated), we may assume that U is affine, and preserved by the action of G.

By assumption, we can thus cover Y by $U_1, \ldots, U_r$, where each U_i is affine, and preserved by the G-action. By what we have discussed so far, we may construct the quotient morphisms $\pi_i\colon U_i \to W_i = U_i/G$. Furthermore, it follows from Corollary A.3 that for every i and j we have canonical isomorphisms $\pi_i(U_i \cap U_j) \simeq \pi_j(U_i \cap U_j)$. We can thus glue these morphisms to get a quotient $\pi\colon Y \to Y/G$ of Y with respect to the G-action. Note that this is a finite surjective morphism that satisfies conditions ii)-iv) in Proposition A.1, hence gives a quotient of Y by the action of G.

REMARK A.4. It follows from the above construction that if Y is reduced, then Y/G is reduced too.

REMARK A.5. The above construction is compatible with field extensions in the following sense. Suppose that Y is a scheme over k with an action of the finite group G, such that every point on Y has an affine open neighborhood preserved by the G-action. Suppose that K/k is a field extension, and $Y_K = Y \times_{\operatorname{Spec} k} \operatorname{Spec} K$. Note that Y_K has an induced G-action, and every point on Y_K has an affine open neighborhood preserved by the G-action. We have an isomorphism of K-varieties $Y_K/G \simeq (Y/G) \times_{\operatorname{Spec} k} \operatorname{Spec} K$. Indeed, it is enough to consider the case when $Y = \operatorname{Spec} A$, and in this case the assertion follows from the lemma below.

[1] If Y is a locally closed subset of $\mathbf{P}^n_k$, and $x_1, \ldots, x_n \in Y$, then there is a hypersurface H in $\mathbf{P}^n_k$ that contains $\overline{Y} \smallsetminus Y$, but does not contain $x_1, \ldots, x_n$. Indeed, by the graded version of Prime Avoidance Lemma, there is a homogeneous element of positive degree in the ideal of $\overline{Y} \smallsetminus Y$ (if this set is empty, we take this ideal to be the "irrelevant" maximal ideal), but that does not lie in the ideal of any $\overline{\{x_i\}}$. The complement of H in Y is an affine open subset of Y that contains all the x_i.

LEMMA A.6. *Let V and W be k-vector spaces, and suppose that a group G acts on V on the left by k-linear automorphisms. If we consider on $V \otimes_k W$ the induced G-action, then we have a canonical isomorphism $(V \otimes_k W)^G \simeq V^G \otimes_k W$.*

PROOF. We clearly have an inclusion $V^G \otimes_k W \hookrightarrow (V \otimes_k W)^G$. Consider $u \in V \otimes_k W$. If $(b_i)_{i\in I}$ is a k-basis of W, we can write $u = \sum_i a_i \otimes b_i$ for a unique tuple $(a_i)_{i\in I}$. Since $gu = \sum_i (ga_i) \otimes b_i$, it follows that $gu = u$ if and only if $ga_i = a_i$ for every i. Therefore $u \in (V \otimes_k W)^G$ if and only if all a_i lie in V^G. □

PROPOSITION A.7. *Let G and H be finite groups, acting by algebraic automorphisms over k on the schemes X and Y, respectively, where X and Y are of finite type over k. If both X and Y can be covered by affine open subsets preserved by the action of the corresponding group, then $X \times Y$ satisfies the same property with respect to the product action of $G \times H$, and $X \times Y/G \times H \simeq X/G \times Y/H$.*

PROOF. Let $X = \bigcup_i U_i$ and $Y = \bigcup_j V_j$ be covers by affine open subsets, preserved by the respective group actions. It is clear that $X \times Y = \bigcup_{i,j} U_i \times V_j$ is a cover by affine open subsets preserved by the $G \times H$-action. Furthermore, using Lemma A.6 twice, we obtain

$$(\mathcal{O}(U_i) \otimes_k \mathcal{O}(V_j))^{G\times H} \simeq \mathcal{O}(U_i)^G \otimes_k \mathcal{O}(V_j)^H,$$

and these isomorphisms glue together to give the isomorphism in the proposition. □

PROPOSITION A.8. *Let G be a finite group acting by algebraic automorphisms on a scheme X of finite type over k, such that X has an affine open cover by subsets preserved by the G-action. Suppose that H is a subgroup of G, and Y is an open subset of X such that*

i) *Y is preserved by the action of H on X.*
ii) *If $Hg_1, \dots, Hg_r$ are the right equivalence classes of G mod H, then $X = \bigcup_{i=1}^r Yg_i$ is a disjoint cover.*

In this case the natural morphism $Y/H \to X/G$ is an isomorphism.

PROOF. Note that by ii), Y is also closed in X. Consider a cover $X = \bigcup_j U_j$ by affine open subsets preserved by the G-action. Each $V_j = Y \cap U_j$ is an affine open subset of Y preserved by the H-action (note that $U_j \cap Y$ is nonempty since U_j must intersect some Yg_i). Therefore we have the quotient Y/H, and since the natural morphism $Y \to X/G$ is H-invariant, we obtain a morphism $\phi\colon Y/H \to X/G$.

We claim that each $Y \cap U_j \hookrightarrow U_j$ still satisfies i) and ii). Indeed, it is clear that $Y \cap U_j$ is preserved by the H-action, and we have $U_j = \bigsqcup_{i=1}^r (Y \cap U_j)g_i$. Therefore we may assume that X and Y are affine.

It follows from ii) that $\mathcal{O}(X) = \prod_{i=1}^r \mathcal{O}(Yg_i)$, and it is clear that if $\phi \in \mathcal{O}(X)^G$, then $\phi = (\psi g_1^{-1}, \dots, \psi g_r^{-1})$ for some $\psi \in \mathcal{O}(Y)$, and in fact we must have $\psi \in \mathcal{O}(Y)^H$. This shows that the natural homomorphism $\mathcal{O}(X)^G \to \mathcal{O}(Y)^H$ is an isomorphism. □

REMARK A.9. Given X as in the above proposition, suppose that Y is an open subset of X such that for every $g, h \in G$, the sets Yg and Yh are either equal, or disjoint. In this case i) and ii) are satisfied if we take $H = \{g \in G \mid Yg = Y\}$ and if we replace X by $\bigcup_{g\in G} Yg$.

PROPOSITION A.10. *Let G be a finite group acting by algebraic automorphisms on a scheme X of finite type over k, such that X has an affine open cover by subsets preserved by the $G \times H$-action. If H is a normal subgroup of G, then X/H has an induced G/H-action, and the quotient by this action is isomorphic to X/G.*

PROOF. Let $X = \bigcup_i U_i$ be an affine open cover of X, with each U_i preserved by the G-action. In particular, each U_i is preserved by the G-action, hence the quotient X/G exists. The action of G on X induces an action of G/H on X/H by the universal property of the quotient. Note that the U_i/H give an affine open cover of X/H by subsets preserved by the G/H-action. Since we clearly have $\mathcal{O}(U_i)^G = (\mathcal{O}(U_i)^H)^{G/H}$, we get isomorphisms of the quotient of U_i/H by the G/H-action with U_i/G. These isomorphisms glue to give the required isomorphism. □

A.2. Ground field extension for algebraic varieties

Let X be a variety over a field k (recall that this means that X is a reduced scheme of finite type over k). Let K/k be a finite Galois extension, with group G, and put $X_K = X \times_{\operatorname{Spec} k} \operatorname{Spec} K$. Note that this is a variety over K, since the extension K/k is separable. Since K is flat over k, we see that the canonical projection $|pi\colon X_K \to X$ is flat.

The left action of G on K induces a right action of G on $\operatorname{Spec} K$, hence on X_K (note that the corresponding automorphisms of X_K are k-linear, but not K-linear). If $x \in X_K$ and V is an affine open neighborhood of $\pi(x)$, then $\pi^{-1}(U)$ is an affine open neighborhood of x, preserved by the G-action. Therefore we may apply to the G-action on X_K the considerations in the previous section. In fact, π is the quotient of X_K by the action of G. Indeed, it is enough to note that if $U \simeq \operatorname{Spec}(A)$ is an affine open subset of X, then Lemma A.6 gives

$$(A \otimes_k K)^G = A \otimes_k K^G = A.$$

By the discussion in the previous section, it follows that π identifies X with the set of G-orbits of X_K, with the quotient topology.

If $Y \hookrightarrow X$ is a closed subvariety, then $Y_K \hookrightarrow X_K$ is a closed subvariety preserved by the G-action. The following proposition gives a converse.

PROPOSITION A.11. *With the above notation, suppose that W is a closed subvariety of X_K preserved by the G-action. If $Y = \pi(W)$, then W is a closed subvariety of X, and $W = Y_K$.*

PROOF. Since π is finite, it follows that Y is closed in X. We clearly have an inclusion $W \subseteq Y_K$. This is an equality of sets since W is preserved by the G-action, and π identifies X with the set of G-orbits in X_K. Since both W and Y_K are reduced, it follows that $W = Y_K$. □

The above considerations can be easily extended to the case of infinite Galois extensions. In what follows, we assume that k is perfect, and consider an algebraic closure $\overline{k}$ of k. Note that $\overline{k}$ is the union of the finite Galois subextensions K of k, and we have $G(\overline{k}/k) \simeq \varprojlim_K G(K/k)$. As above, if X is a variety over k, we put $X_{\overline{k}} = X \times_{\operatorname{Spec} k} \operatorname{Spec} \overline{k}$, and let $\pi\colon X_{\overline{k}} \to X$ be the canonical projection. Note that since k is perfect, all fibers of π are reduced. We have a right action of $G(\overline{k}/k)$ on $X_{\overline{k}}$, induced by its left action on $\overline{k}$.

PROPOSITION A.12. *If W is a closed subvariety of $X_{\overline{k}}$ that is preserved by the G-action, and if $Y = \pi(W)$, then Y is a closed subvariety of X, and $W = Y_{\overline{k}}$ (in this case we say that W is defined over k).*

PROOF. The fact that Y is closed in X follows from the fact that π is an integral morphism. There is a finite Galois extension K of k such that for some closed subscheme V of X_K, we have $V_{\overline{k}} = W$. After replacing V by V_{red}, we may assume that V is reduced, in which case we see that it is the image of W via the canonical projection $X_{\overline{k}} \to X_K$. Since W is preserved by the $G(\overline{k}/k)$-action, it follows that V is preserved by the $G(K/k)$-action (recall that $G(K/k)$ is the quotient of $G(\overline{k}/k)$ by $G(\overline{k}/K)$). We may thus apply Proposition A.11 to conclude that $V = Y_K$, and therefore $W = Y_{\overline{k}}$. □

PROPOSITION A.13. *The fibers of the projection $\pi\colon X_{\overline{k}} \to X$ are the orbits of the $G(\overline{k}/k)$-action on $X_{\overline{k}}$.*

PROOF. It is clear from definition that $G(\overline{k}/k)$ acts on $X_{\overline{k}}$ by automorphisms over X. Suppose now that $x, y \in X_{\overline{k}}$ are such that $\pi(x) = \pi(y)$. There is a finite Galois extension K of k such that both $\overline{\{x\}}$ and $\overline{\{y\}}$ are defined over K, and let x_K and y_K denote the images of x and y, respectively, in X_K. Since x_K and y_K lie in the same fiber of $X_K \to X$, we can find $\sigma \in G(K/k)$ such that $x_K\sigma = y_K$. In this case, for every $\widetilde{\sigma} \in G(\overline{k}/k)$ that extends σ, we have $x\sigma = y$. □

PROPOSITION A.14. *If X is an irreducible variety over k, then $G = G(\overline{k}/k)$ acts transitively on the set of irreducible components of $X_{\overline{k}}$.*

PROOF. Note first that every automorphism of $X_{\overline{k}}$ maps an irreducible component to an irreducible component, hence G indeed has an induced action on the set of irreducible components of $X_{\overline{k}}$. Let V and W be irreducible components of $X_{\overline{k}}$. Since $X_{\overline{k}}$ is flat over X, and X is irreducible, it follows that both V and W dominate X. Therefore the generic points of V and W lie in the same fiber of π, and we conclude by applying the previous proposition. □

PROPOSITION A.15. *If X is a variety over k and $\pi\colon X_{\overline{k}} \to X$ is the canonical projection, then taking $x \in X$ to the sum of the elements in $\pi^{-1}(x)$ induces a bijection between the set of effective 0-cycles on X of degree n and the set of effective 0-cycles on $X_{\overline{k}}$ that have degree n and that are fixed by $G(\overline{k}/k)$.*

PROOF. By Proposition A.13, an effective cycle α on $X_{\overline{k}}$ is invariant by $G(\overline{k}/k)$ if and only if for every closed point $x \in X_{\overline{k}}$ that appears in α, all $y \in \pi^{-1}(\pi(x))$ appear in α with the same coefficient. In other words, α can be written as $\sum_{i=1}^{r} \sum_{y \in \pi^{-1}(u_i)} y$ for some $u_1, \ldots, u_r \in X$. In order to complete the proof, it is enough to note that for every $u \in X$, we have $\deg(k(u)/k) = |\pi^{-1}(u)|$ (recall that $\pi^{-1}(u)$ is reduced). □

Suppose now that $k = \mathbf{F}_q$ is a finite field. Recall that $G(\overline{k}/k) \simeq \widehat{\mathbf{Z}}$, and we may take as a topological generator either the arithmetic Frobenius element $x \to x^q$, or its inverse, the geometric Frobenius element. Let σ denote the automorphism of $X_{\overline{k}}$ corresponding to the action of the arithmetic Frobenius element. Recall that the endomorphism $\mathrm{Frob}_{X,q}$ on X induces by base extension the $\overline{k}$-linear endomorphism $F = \mathrm{Frob}_{X_{\overline{k}},q}$ of $X_{\overline{k}}$.

PROPOSITION A.16. *Let X be a variety over $k = \mathbf{F}_q$, and W a closed subvariety of $X_{\overline{k}}$. There is a closed subvariety Y of $X_{\mathbf{F}_{q^r}}$ such that $W = Y_{\overline{k}}$ (in which case Y is the image of W in $X_{\mathbf{F}_{q^r}}$) if and only if $F^r(W) \subseteq W$.*

PROOF. After replacing X by $X_{\mathbf{F}_{q^r}}$, we may assume that $r = 1$. We have seen in Exercise 2.5 that $\sigma \circ F = F \circ \sigma$, and this is the absolute q-Frobenius morphism of $X_{\overline{k}}$ (let's denote it by T). Since $T(W) = W$ for every closed subvariety W of $X_{\overline{k}}$, it is easy to see that $\sigma^{-1}(W) \subseteq W$ if and only if $F(W) \subseteq W$ (in which case $F(W) = W$).

Applying Proposition A.12, we are done if we show that if $\sigma^{-1}(W) \subseteq W$, then W is preserved by $G(\overline{k}/k)$. Since the geometric Frobenius element is a topological generator of $G(\overline{k}/k)$, this follows from the fact that the action of $G(\overline{k}/k)$ on $X_{\overline{k}}$ is continuous, where on $X_{\overline{k}}$ we consider the discrete topology. Continuity simply means that the stabilizer of every point in $X_{\overline{k}}$ contains a subgroup of the form $G(\overline{k}/K)$, for some finite Galois extension K of k. This is clear for $X_{\overline{k}}$, since it is clear for $\mathbf{A}^n_{\overline{k}}$: for the point $(u_1, \dots, u_n) \in \overline{k}^n$, we may simply take K to be the Galois closure of $k(u_1, \dots, u_n)$. □

A.3. Radicial morphisms

We will need the notion of radicial morphism in the next section, in order to discuss quotients of closed subschemes. In this section we recall the definition of this class of morphisms and prove some basic properties.

PROPOSITION A.17. *If $f\colon X \to Y$ is a morphism of schemes, then the following are equivalent:*

i) *For every field K (which may be assumed algebraically closed), the induced map*
$$\operatorname{Hom}(\operatorname{Spec} K, X) \to \operatorname{Hom}(\operatorname{Spec} K, Y)$$
is injective.

ii) *For every scheme morphism $Y' \to Y$, the morphism induced by base-change $X \times_Y Y' \to Y'$ is injective.*

iii) *f is injective, and for every $x \in X$, the extension of residue fields $k(f(x)) \hookrightarrow k(x)$ is purely inseparable.*

If f satisfies the above equivalent conditions, one says that f is *radicial*.

PROOF. We first prove i)⇒ii). Let $Y' \to Y$ be a morphism of schemes, and suppose that $x_1, x_2 \in X \times_Y Y'$ are two distinct points that map to the same point $y \in Y'$. Let K be a field extension of $k(y)$ containing both $k(x_1)$ and $k(x_2)$ (note that we may take K to be algebraically closed). The inclusions $k(x_1), k(x_2) \hookrightarrow K$ give two distinct morphisms $\operatorname{Spec} K \to X \times_Y Y'$ such that the induced morphisms to Y' are equal. In particular, the induced morphisms to Y are equal, hence by i) the induced morphisms to X are equal. The universal property of the fiber product shows that we have a contradiction.

We now prove ii)⇒i). Suppose that $\phi, \psi\colon \operatorname{Spec} K \to X$ induce the same morphism $\operatorname{Spec} K \to Y$, and let $X_K = X \times_Y \operatorname{Spec} K$. By the universal property of the fiber product, ϕ and ψ induce morphisms $\widetilde{\phi}, \widetilde{\psi}\colon \operatorname{Spec} K \to X_K$ over $\operatorname{Spec} K$. These correspond to two points $x_1, x_2 \in X_K$ and to isomorphisms $K \simeq k(x_i)$. By ii) we have $x_1 = x_2$, hence $\widetilde{\phi} = \widetilde{\psi}$ and $\phi = \psi$.

Suppose now that i) holds, and let us deduce iii). The fact that f is injective follows since we know i)⇒ii), so let us suppose that $x \in X$ and $y = f(x)$ are such that $k(y) \hookrightarrow k(x)$ is not purely inseparable. In this case there is a field K and two homomorphisms $\alpha, \beta\colon k(x) \to K$ such that α and β agree on $k(y)$. We thus get two scheme morphisms $\operatorname{Spec} K \to X$ taking the unique point to x, such that they induce the same morphism $\operatorname{Spec} K \to Y$. This contradicts i).

In order to complete the proof of the proposition, it is enough to show that iii)⇒i). Suppose that $u, v\colon \operatorname{Spec} K \to X$ are such that $f \circ u = f \circ v$. Since f is injective, it follows that both u and v take the unique point to the same $x \in X$. We thus have two homomorphisms $k(x) \to K$ whose restrictions to $k(f(x))$ are equal. This shows that $k(x)$ is not purely inseparable over $k(f(x))$, a contradiction. □

Example A.18. It is clear that every closed immersion is radicial. For a more interesting example, consider a scheme X over $\mathbf{F}_p$, and let $f\colon X \to X$ be the absolute Frobenius morphism. It is clear that f is a surjective, radicial morphism (use description iii) in the above proposition).

Remark A.19. It follows from either of the descriptions in Proposition A.17 that the class of radicial morphisms is closed under composition and base-change. Of course, the same holds for radicial surjective morphisms.

Remark A.20. If $f\colon X \to Y$ is a morphism of schemes, it is a consequence of the description iii) in Proposition A.17 that f is radicial of and only if $f_{\mathrm{red}}\colon X_{\mathrm{red}} \to Y_{\mathrm{red}}$ has this property.

Remark A.21. The notion of radicial morphism is local on the target: $f\colon X \to Y$ is radicial if and only if there is an open cover $Y = \bigcup_i V_i$ such that each $f^{-1}(V_i) \to V_i$ is radicial (one can use for this any of the descriptions in Proposition A.17).

Remark A.22. A morphism $f\colon X \to Y$ of schemes over a field k is radicial and surjective if and only if for every algebraically closed field K containing k, the induced map $f_K\colon X(K) \to Y(K)$ is bijective. Indeed, Proposition A.17 shows that f is radicial if and only if all f_K are injective. Assuming that this is true, it is easy to see that if all f_K are surjective, then f is surjective, and the converse follows from the fact that for every $x \in X$, the extension of residue fields $k(f(x)) \hookrightarrow k(x)$ is algebraic.

Example A.23. If $\phi\colon R \to S$ is a morphism of rings of characteristic p such that

i) The kernel of ϕ is contained in the nilradical of R.
ii) For every $b \in S$, there is m such that $b^{p^m} \in \operatorname{Im}(\phi)$,

then the induced morphism $\operatorname{Spec} S \to \operatorname{Spec} R$ is radicial and surjective. Indeed, if $\mathfrak{p}$ is a prime ideal of R, then there is a unique prime ideal $\mathfrak{q}$ of S such that $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$, namely

$$\mathfrak{q} = \{b \in S \mid b^{p^m} = \phi(a) \text{ for some } a \in \mathfrak{p} \text{ and } m \geq 1\}.$$

Furthermore, for every $u \in S/\mathfrak{q}$, there is $m \geq 1$ such that u^{p^m} lies in the image of $R/\mathfrak{p}$, hence $R/\mathfrak{p} \hookrightarrow S/\mathfrak{q}$ is purely inseparable.

Proposition A.24. *If $f\colon X \to Y$ is a morphism of schemes of finite type over a field k of characteristic zero, then the following are equivalent:*

i) *f is radicial and surjective.*

ii) $X(\overline{k}) \to Y(\overline{k})$ *is bijective, where* $\overline{k}$ *is an algebraic closure of* k.
iii) f *is a piecewise isomorphism, that is, there is a disjoint cover* $Y = Y_1 \sqcup \ldots \sqcup Y_m$ *by locally closed subsets, such that all induced morphisms* $f^{-1}(Y_i)_{\mathrm{red}} \to (Y_i)_{\mathrm{red}}$ *are isomorphisms.*

PROOF. The implication i)⇒ii) follows from Remark A.22. Suppose now that f is a piecewise isomorphism and $Y = \bigsqcup_i Y_i$ is a disjoint cover as in iii). Given a morphism $\phi\colon Y' \to Y$, let $g\colon X \times_Y Y' \to Y'$ be the morphism obtained by base-change from f. We get a locally closed disjoint cover $Y' = \bigsqcup_i Y_i'$, where $Y_i' = \phi^{-1}(Y_i)$, such that each $g^{-1}(Y_i')_{\mathrm{red}} \to (Y_i')_{\mathrm{red}}$ is an isomorphism. Therefore f is radicial, and it is clear that f is surjective. Therefore in order to finish the proof of the proposition it is enough to show that if f satisfies ii), then f is a piecewise isomorphism.

Arguing by Noetherian induction, we may assume that the property holds for $f^{-1}(Z) \to Z$, for every proper closed subset Z of Y. Therefore whenever it is convenient, we may replace f by $f^{-1}(U) \to U$, where U is a nonempty open subset of Y. We may put on both X and Y their reduced scheme structures, and therefore assume that they are reduced. If $Y_1, \ldots, Y_r$ are the irreducible components of Y, we may replace Y by $Y_1 \smallsetminus \cup_{i\neq 1} Y_i$, and therefore assume that Y is irreducible.

Since $X(\overline{k}) \to Y(\overline{k})$ is injective, we deduce that there is a unique irreducible component of X that dominates Y. Therefore there is an open subset U in Y such that $f^{-1}(U)$ does not meet the other irreducible components of X. After replacing Y by U, we may assume that both X and Y are irreducible. Let $d = \deg(K(X)/K(Y))$. It is enough to show that $d = 1$, since in this case f is birational, hence there is an open subset U of X such that $f^{-1}(U) \to U$ is an isomorphism.

Since we are in characteristic zero, f is generically smooth, that is, there are open subsets $V \subseteq X$ and $W \subseteq Y$ such that f induces a smooth morphism $g\colon V \to W$. It follows from [**Har**, Exercise II.3.7] that there is an open subset W' of W such that $g^{-1}(W') \to W'$ is finite. After restricting further to an open subset of W', we may assume that W' is affine, and $\mathcal{O}(g^{-1}(W'))$ is free of rank d over $\mathcal{O}(W')$. Since all fibers of $g^{-1}(W') \times_k \overline{k} \to W' \times_k \overline{k}$ are reduced, it follows that each such fiber has d elements, so by assumption $d = 1$. This completes the proof of the proposition. □

A.4. Quotients of locally closed subschemes

PROPOSITION A.25. *Let* X *be a scheme of finite type over* k*, and* G *a finite group acting on* X *by algebraic automorphisms over* k*. We assume that* X *is covered by affine open subsets preserved by the* G*-action, and let* $\pi\colon X \to X/G$ *be the quotient morphism. If* W *is a locally closed subscheme of* X *such that* G *induces an action on* W*, then the canonical morphism* $W/G \to \pi(W)$ *is radicial and surjective.*

PROOF. We first need to show that W/G exists, and that we have an induced morphism $W/G \to X/G$. If $\overline{W}$ is the closure of W (with the image scheme structure), then W is an open subscheme of $\overline{W}$, which is a closed subscheme of X. Furthermore, G has an induced action on $\overline{W}$. It follows that it is enough to consider separately the cases when W is an open or a closed subscheme of X. If W is an open subscheme, then the assertion is clear: $\pi(W)$ is open in X/G, and we have seen that $W = \pi^{-1}(\pi(W)) \to \pi(W)$ is the quotient of W by the G-action.

Suppose now that W is a closed subscheme of X, and consider $\pi(W)$ (with the image scheme structure). Note first that since $\pi(W)$ can be covered by affine open subsets, and π is finite, it follows that W is covered by affine open subsets that are preserved by the G-action. In particular, W/G exists, and the G-invariant morphism $W \to X \to X/G$ induces a morphism $\phi\colon W/G \to X/G$. It is clear that the image of this morphism is $\pi(W)$. In order to show that ϕ is radicial, we may assume that $X = \operatorname{Spec} A$ is affine (simply consider an affine cover of X by affine open subsets preserved by the G-action). Let I denote the ideal defining W. If B is the image of $A^G \to (A/I)^G$, then it is enough to prove that $\operatorname{Spec}(A/I)^G \to \operatorname{Spec} B$ is radicial. In light of Example A.23, this is a consequence of the more precise statement in the lemma below. □

LEMMA A.26. *Let A be a finitely generated k-algebra, and let G be a finite group acting on A by k-algebra automorphisms. Suppose that $I \subseteq A$ is an ideal preserved by the G-action. If p^n is the largest power of $p = \operatorname{char}(k)$ that divides $|G|$ (we make the convention that $p^n = 1$ if $\operatorname{char}(k) = 0$), then for every $b \in (A/I)^G$, we have $b^{p^n} \in \operatorname{Im}(A^G \to (A/I)^G)$.*

PROOF. The argument that follows is inspired from [KM, p.221]. We write it assuming $p > 0$, and leave for the reader to do the translation when $\operatorname{char}(k) = 0$.

Let $u \in A$ be such that $b = \overline{u} \in A/I$ is G-invariant. Since $gu - u \in I$ for every $g \in G$, we have the following congruence in the polynomial ring $A[x]$:

$$\prod_{g \in G} (1 + (gu)x) \equiv (1 + ux)^{|G|} \bmod IA[x].$$

The polynomial on the left-hand side has coefficients in A^G, hence by considering the coefficient of x^{p^n} on the right-hand side, we conclude that $\binom{|G|}{p^n} u^{p^n}$ is congruent mod I to an element in A^G. Since $\binom{|G|}{p^n}$ is invertible in k[2], it follows that $\overline{u}^{p^n}$ lies in the image of R^G. □

REMARK A.27. It follows from the proof of Proposition A.25 and Lemma A.26 that if $\operatorname{char}(k)$ does not divide $|G|$, then under the assumptions in Proposition A.25, the morphism $W/G \to \pi(W)$ is an isomorphism. In particular, this is the case for every G if $\operatorname{char}(k) = 0$.

[2]It is easy to show this by computing the exponent of p in this binomial coefficient. On the other hand, this is also a consequence of Lucas' theorem, see [Gra]: if $|G| = p^n m$, with m and p relatively prime, then $\binom{|G|}{p^n} \equiv m \pmod p$.

APPENDIX B

Basics of p-adic fields

We collect in this appendix some basic facts about p-adic fields that are used in Chapter 8. In the first section we review the main properties of p-adic fields, in the second section we describe the unramified extensions of $\mathbf{Q}_p$, while in the third section we construct the field $\mathbf{C}_p$, the smallest complete algebraically closed extension of $\mathbf{Q}_p$. In §4 section we discuss convergent power series over p-adic fields, and in the last section we give some examples. The presentation in §2-§4 follows [**Kob**].

B.1. Finite extensions of $\mathbf{Q}_p$

We assume that the reader has some familiarity with I-adic topologies and completions, for which we refer to [**Mat**]. Recall that if $(R, \mathfrak{m})$ is a DVR with fraction field K, then there is a unique topology on K that is invariant under translations, and such that a basis of open neighborhoods of 0 is given by $\{\mathfrak{m}^i \mid i \geq 1\}$. This can be described as the topology corresponding to a metric on K, as follows. Associated to R there is a discrete valuation v on K, such that for every nonzero $u \in R$, we have $v(u) = \max\{i \mid u \notin \mathfrak{m}^i\}$. If $0 < \alpha < 1$, then by putting $|u| = \alpha^{v(u)}$ for every nonzero $u \in K$, and $|0| = 0$, one gets a *non-Archimedean absolute value* on K. This means that $|\cdot|$ has the following properties:

i) $|u| \geq 0$, with equality if and only if $u = 0$.
ii) $|u + v| \leq \max\{|u|, |v|\}$ for every $u, v \in K$[1].
iii) $|uv| = |u| \cdot |v|$ for every $u, v \in K$.

In this case, by taking $d(x, y) = |x - y|$ we get a non-Archimedean[2] metric on K such that the corresponding topology is the unique topology mentioned above. Note that the topology is independent of the choice of α. It is clear that addition, multiplication, and taking the inverse of a nonzero element are all continuous.

The completion of R is defined algebraically as $\widehat{R} = \varprojlim_i R/\mathfrak{m}^i$. It is a general fact that R is local and Noetherian, and the canonical morphism $R \to \widehat{R}$ is injective. Furthermore, the maximal ideal in $\widehat{R}$ is $\mathfrak{m} \cdot R$, and for all $i \geq 1$ we have $R/\mathfrak{m}^i \simeq \widehat{R}/\mathfrak{m}^i\widehat{R}$. This implies that $\dim(\widehat{R}) = \dim(R) = 1$. Since the maximal ideal in $\widehat{R}$ is principal (being generated by a generator π of $\mathfrak{m}$), it is easy to see that $\widehat{R}$ is a DVR. Furthermore, we have $\widehat{K} := \mathrm{Frac}(\widehat{R}) = \widehat{R}[1/\pi] = K \otimes_R \widehat{R}$. In particular, we have a valuation and a non-Archimedean absolute value on $\widehat{K}$ that extend the corresponding ones on K. In fact, $\widehat{K}$ is the completion of K with respect to the

[1] A useful observation is that we automatically get that this is an equality if $|u| \neq |v|$.

[2] This means that we have the strong triangle inequality $d(x, y) \leq d(x, z) + d(y, z)$ for all x, y, and z.

topology defined by $|\cdot|$, and the absolute value on $\widehat{K}$ is the unique one extending the absolute value on K.

Suppose now that p is a fixed prime integer. We apply the above discussion to $K = \mathbf{Q}$, where $R = \mathbf{Z}_{(p\mathbf{Z})}$ is the localization of $\mathbf{Z}$ at the maximal ideal $p\mathbf{Z}$. The corresponding topology on $\mathbf{Q}$ is the *p-adic topology*, and the corresponding absolute value, with $\alpha = \frac{1}{p}$ is denoted by $|\cdot|_p$. The field $\widehat{K}$ is the *field of p-adic rational numbers* $\mathbf{Q}_p$, and $\widehat{R}$ is the *ring of p-adic integers* $\mathbf{Z}_p$. The corresponding valuation and absolute value on $\mathbf{Q}_p$ are denoted by ord_p, and respectively, $|\cdot|_p$.

We now recall Hensel's Lemma, one of the basic results about complete local rings. For a proof, see [Mat, Theorem 8.3]. Let $(A, \mathfrak{m}, k)$ be a complete local ring. For a polynomial $g \in A[x]$, we denote by $\overline{g}$ its image in $k[x]$.

PROPOSITION B.1. *With the above notation, suppose that $f \in A[x]$ is a monic polynomial. If $u, v \in k[x]$ are relatively prime monic polynomials such that $\overline{f} = uv$, then there are monic polynomials $g, h \in A[x]$ such that*

i) $f = gh$
ii) $\overline{g} = u$ *and* $\overline{h} = v$.

A consequence of the above proposition is that if (keeping the notation) B is a finite A-algebra such that $B/\mathfrak{m}B$ splits as the product of two (nonzero) rings, then the same holds for B. Indeed, the hypothesis gives the existence of an idempotent $u \in B$ such that $u \neq 0, 1$. Applying Hensel's Lemma for the decomposition $x^2 - x = (x-u)(x-(1-u))$ in $k[x]$, we get an idempotent in B different from 0 and 1. In particular, we see that if B is a domain, then the zero-dimensional ring $B/\mathfrak{m}_B$ is local, hence B is local, too.

A *p-adic field* is a finite field extension of $\mathbf{Q}_p$. If K is such a field, we denote by $\mathcal{O}_K$ the ring of integers in K (that is, the integral closure of $\mathbf{Z}_p$ in K). It is easy to see that since every element $u \in K$ is algebraic over $\mathbf{Q}_p$, there is $a \in \mathbf{Z}_p$ such that $au \in \mathcal{O}_K$. Therefore $\mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathcal{O}_K = K$ and K is the fraction field of $\mathcal{O}_K$.

Since $\mathbf{Z}_p$ is a DVR, it is well-known that $\mathcal{O}_K$ is a finite $\mathbf{Z}_p$-algebra (see [Lang, Precise]). Therefore the discussion after Proposition B.1 implies that $\mathcal{O}_K$ is a local ring (and the inclusion $\mathbf{Z}_p \hookrightarrow \mathcal{O}_K$ is local, since $\mathcal{O}_K$ is finite over $\mathbf{Z}_p$). Furthermore, since $\dim(\mathcal{O}_K) = \dim(\mathbf{Z}_p) = 1$, and $\mathcal{O}_K$ is clearly normal, we conclude that $\mathcal{O}_K$ is again a DVR.

If v_K is the discrete valuation of K corresponding to $\mathcal{O}_K$, then $e_K := v_K(p)$ is the *ramification index* of K over $\mathbf{Q}_p$. We say that K is unramified over $\mathbf{Q}_p$ if $e_K = 1$. It is clear that for every $u \in \mathbf{Q}_p$, we have $v_K(u) = e_K \cdot \mathrm{ord}_p(u)$. The p-adic absolute value on K is defined by $|u|_p = \left(\frac{1}{p}\right)^{v_K(u)/e_K}$. Note that for $u \in \mathbf{Q}_p$, this agrees with the definition we gave before. We have $\mathcal{O}_K = \{u \in K, |u|_p \leq 1\}$, and the maximal ideal in $\mathcal{O}_K$ is $\mathfrak{m}_K = \{u \in K, |u| < 1\}$.

Since every ideal in $\mathbf{Z}_p$ is generated by some p^m, and $\mathcal{O}_K$ is clearly torsion-free, it follows that $\mathcal{O}_K$ is flat over $\mathbf{Z}_p$. We deduce that $\mathcal{O}_K$ is a free module over $\mathbf{Z}_p$, and its rank is clearly equal to $n = [K : \mathbf{Q}_p]$. Let π_K denote a generator of the maximal ideal $\mathfrak{m}_K$. The quotient $\mathcal{O}_K/p\mathcal{O}_K$ is free of rank n over $\mathbf{F}_p$; on the other hand, it has a filtration

$$(0) \subset \mathfrak{m}_K^{e_K - 1}/\mathfrak{m}_K^{e_K} \subset \ldots \subset \mathfrak{m}_K/\mathfrak{m}_K^{e_K} \subset \mathcal{O}_K/\mathfrak{m}_K^{e_K},$$

with each successive quotient isomorphic to $\mathcal{O}_K/\mathfrak{m}_K$. We deduce that if $f = [\mathcal{O}_K/\mathfrak{m}_K : \mathbf{F}_p]$, then $n = ef$.

EXERCISE B.2. Let K be a p-adic field.

i) Show that a basis of open neighborhoods of 0 in $\mathcal{O}_K$ is given by $\{p^m\mathcal{O}_K \mid m \geq 1\}$.
ii) Deduce that if we choose an isomorphism of $\mathbf{Z}_p$-modules $\mathcal{O}_K \simeq \mathbf{Z}_p^n$, the topology on $\mathcal{O}_K$ corresponds to the product topology on $\mathbf{Z}_p^n$.
iii) Deduce that $\mathcal{O}_K$ is complete (and therefore so is K).

EXERCISE B.3. Let $K \hookrightarrow L$ be two finite extensions of $\mathbf{Q}_p$.

ii) Show that if $e_{L/K}$ is defined by $\pi_K\mathcal{O}_L = (\pi_L^{e_{L/K}})$, and $f_{L/K} = [\mathcal{O}_L/\mathfrak{m}_L : \mathcal{O}_K/\mathfrak{m}_K]$, then $e_L = e_K \cdot e_{L/K}$ and $f_L = f_K \cdot f_{L/K}$. Deduce that $[L\colon K] = e_{L/K}f_{L/K}$.
i) Show that the two definitions of $|\cdot|_p$ on K and L are compatible.

We say that L/K is unramified if $e_{L/K} = 1$, and that it is totally ramified if $e_{L/K} = [L\colon K]$.

EXERCISE B.4. Let K be a finite Galois extension of $\mathbf{Q}_p$. Show that if $\sigma \in G(K/\mathbf{Q}_p)$, then $|\sigma(u)|_p = |u|_p$ for every $u \in K$. Deduce that for every p-adic field K and every $u \in K$, we have $|u|_p = N_{K/\mathbf{Q}_p}(u)^{1/n}$, where $n = [K : \mathbf{Q}_p]$.

Suppose now that $(K, |\cdot|)$ is an arbitrary field endowed with a non-Archimedean absolute value, and we consider on K the corresponding metric space structure. The following exercise gives some special features of the non-Archimedean setting.

EXERCISE B.5. With K as above, suppose that $(a_n)_{n\geq 1}$ is a sequence of elements of K.

i) Show that (a_n) is Cauchy if and only if $\lim_{n\to\infty}(a_n - a_{n+1}) = 0$.
ii) Show that if K is complete, then the series $\sum_{n\geq 1} a_n$ is convergent if and only if $\lim_{n\to\infty} a_n = 0$.
iii) Show that if the series $\sum_{n\geq 1} a_n$ is convergent, then for every permutation σ of $\mathbf{Z}_{>0}$, we have $\sum_{n\geq 1} a_{\sigma(n)} = \sum_{n\geq 1} a_n$.

B.2. Unramified extensions of $\mathbf{Q}_p$ and Teichmüller lifts

Our main goal in this section is to describe the unramified extensions of $\mathbf{Q}_p$, and the morphisms between them. We will also take this opportunity to discuss Teichmüller lifts of elements in a finite field. In order to state the results, it is convenient to fix an algebraic closure $\overline{\mathbf{Q}_p}$ of $\mathbf{Q}_p$. The following is the main result of this section.

THEOREM B.6. *The unramified extensions of $\mathbf{Q}_p$ in $\overline{\mathbf{Q}_p}$ are described as follows.*

i) *For every n, there is a unique unramified extension of $\mathbf{Q}_p$ in $\overline{\mathbf{Q}_p}$ of degree n, denoted by $\mathbf{Q}_p^{(n)}$. This can be obtained by attaching to $\mathbf{Q}_p$ a primitive root of 1 of order $p^n - 1$.*
ii) *If $K \subseteq \overline{\mathbf{Q}_p}$ is a finite extension of $\mathbf{Q}_p$ and $f = f_K$, then $\mathbf{Q}_p^{(f)} \subseteq K$, and this extension is totally ramified.*
ii) *$\mathbf{Q}_p^{(n)}$ is a Galois extension of $\mathbf{Q}_p$, and we have an isomorphism of Galois groups $G(\mathbf{Q}_p^{(n)}/\mathbf{Q}_p) \to G(\mathbf{F}_{p^n}/\mathbf{F}_p)$, that associates to an automorphism of $\mathbf{Q}_p^{(n)}$ the induced automorphism of the residue field.*

PROOF. We begin by showing that for every $n \geq 1$, there is an unramified extension of $\mathbf{Q}_p$ of degree n. Let $u \in \mathbf{F}_{p^n}^*$ be a multiplicative generator. Since $\mathbf{F}_{p^n} = \mathbf{F}_p(u)$, it follows that the minimal polynomial $P \in \mathbf{F}_p[x]$ of u over $\mathbf{F}_p$ has degree $[\mathbf{F}_{p^n} : \mathbf{F}_p] = n$. Let $\widetilde{P} \in \mathbf{Z}_p[x]$ be a monic polynomial lifting P. Since P is irreducible, it follows that $\widetilde{P}$ is irreducible. Let $w \in \overline{\mathbf{Q}_p}$ be a root of $\widetilde{P}$, and put $L = \mathbf{Q}_p(w)$. We have $[L : \mathbf{Q}_p] = \deg(\widetilde{P}) = n$, and since $\widetilde{P}$ is monic, we see that $w \in \mathcal{O}_L$. Let $\mathfrak{m}_L$ denote the maximal ideal in $\mathcal{O}_L$. The image $\overline{w} \in \mathcal{O}_L/\mathfrak{m}_L$ of w satisfies $P(\overline{w}) = 0$, hence w is a conjugate of u, so that $f_L \geq n$. Since $e_L f_L = n$, we conclude that $f_L = n$, and the extension $L/\mathbf{Q}_p$ is unramified. We thus have unramified extensions of $\mathbf{Q}_p$ of arbitrary degree.

Let us consider an arbitrary extension K of $\mathbf{Q}_p$ of degree d, contained in $\overline{\mathbf{Q}_p}$. We put $e = e_K$ and $f = f_K$. Let α be a multiplicative generator of $(\mathcal{O}_K/\mathfrak{m}_K)^*$. We claim that there is a lifting $\widetilde{\alpha} \in \mathcal{O}_K$ of α such that $\widetilde{\alpha}^{p^f-1} = 1$. We can write $x^{p^f-1} - 1 = (x - \alpha)G(x)$ for a monic polynomial $G \in \mathbf{F}_{p^f}[x]$. Since $G(\alpha) \neq 0$, it follows from Proposition B.1 that we can write $x^{p^f-1} - 1 = (x - \widetilde{\alpha})\widetilde{G}(x)$ for some $\widetilde{G} \in \mathcal{O}_K[x]$, and some lift $\widetilde{\alpha} \in \mathcal{O}_K$ of α. This proves our claim. Note that $\widetilde{\alpha}$ is a primitive root of 1 of order $p^f - 1$: if $\widetilde{\alpha}^i = 1$ for some $0 < i < p^f - 1$, then $\alpha^i = 1$, a contradiction. It is clear that $f_{\mathbf{Q}_p(\widetilde{\alpha})} \geq [\mathbf{F}_p(\alpha) : \mathbf{F}_p] = f$, and since the reverse inequality follows from $\mathbf{Q}_p(\widetilde{\alpha}) \subseteq K$, we have $f_{\mathbf{Q}_p(\widetilde{\alpha})} = f$ and the extension $K/\mathbf{Q}_p(\widetilde{\alpha})$ is totally ramified.

Suppose now that K is unramified over $\mathbf{Q}_p$, hence $e = 1$. The above shows that $K = \mathbf{Q}_p(\alpha)$. Therefore every unramified degree n extension of $\mathbf{Q}_p$ is obtained by adjoining to $\mathbf{Q}_p$ a primitive root $\widetilde{\alpha}$ of 1 of order $p^n - 1$. Since such an extension is clearly independent of the choice of the primitive root, we get the assertion in i). We note that from the construction we also get that the image α of $\widetilde{\alpha}$ in the residue field of K is again a primitive root of 1 of order $p^n - 1$.

Returning to the case of an arbitrary K as above, we see that $\mathbf{Q}_p(\widetilde{\alpha}) = \mathbf{Q}_p^{(f)}$, hence the assertion in ii).

For every $\sigma \in G(\overline{\mathbf{Q}_p}/\mathbf{Q}_p)$, note that $\sigma(\mathbf{Q}_p^{(n)})$ is an unramified extension of $\mathbf{Q}_p$ of degree n, hence by the uniqueness statement in i), it is equal to $\mathbf{Q}_p^{(n)}$. This shows that the extension $\mathbf{Q}_p^{(n)}/\mathbf{Q}_p$ is Galois (it is separable since $\mathrm{char}(\mathbf{Q}_p) = 0$). It is clear that an automorphism σ of $L = \mathbf{Q}_p^{(n)}$ induces an automorphism of $\mathcal{O}_L$, hence an automorphism $\overline{\sigma}$ of the residue field $\mathcal{O}_L/\mathfrak{m}_L$. We thus get a group homomorphism $G := G(\mathbf{Q}_p^{(n)}/\mathbf{Q}_p) \to G(\mathbf{F}_{p^n}/\mathbf{F}_p)$. Since both groups have n elements, it is enough to show that this is an injective morphism. We have seen that $\mathbf{Q}_p^{(n)} = \mathbf{Q}_p(\widetilde{\alpha})$, where $\widetilde{\alpha} \in \overline{\mathbf{Q}_p}$ is a primitive root of 1 of order $p^n - 1$, and the image α of $\widetilde{\alpha}$ in the residue field is again a primitive root of 1 of order $p^n - 1$. Every σ in G satisfies $\sigma(\widetilde{\alpha}) = \widetilde{\alpha}^i$ for some i. If $\overline{\sigma} = \mathrm{id}$, then $\alpha = \overline{\sigma}(\alpha) = \alpha^i$, hence $\widetilde{\alpha} = \widetilde{\alpha}^i$, and we see that $\sigma = \mathrm{id}$. This completes the proof of iii), and thus the proof of the theorem. □

COROLLARY B.7. *We have $\mathbf{Q}_p^{(m)} \subseteq \mathbf{Q}_p^{(n)}$ if and only if m divides n.*

PROOF. If $\mathbf{Q}_p^{(m)} \subseteq \mathbf{Q}_p^{(n)}$, then $m = [\mathbf{Q}_p^{(m)} : \mathbf{Q}]$ divides $n = [\mathbf{Q}_p^{(n)} : \mathbf{Q}]$. Conversely, suppose that $m|n$, so that $r = \frac{p^n-1}{p^m-1}$ is an integer. If $\beta \in \overline{\mathbf{Q}_p}$ is a primitive root of 1 of order $p^n - 1$, then β^r is a primitive root of 1 of order $p^m - 1$, and $\mathbf{Q}_p^{(m)} = \mathbf{Q}_p(\beta^r) \subseteq \mathbf{Q}_p(\beta) = \mathbf{Q}_p^{(n)}$. □

We end this section by discussing the Teichmüller lift of an element in a finite field. For every $n \geq 1$, let $\mathbf{Z}_p^{(n)}$ denote the ring of integers of $\mathbf{Q}_p^{(n)}$.

PROPOSITION B.8. *For every $u \in \mathbf{F}_{p^n}$, there is a unique $\widetilde{u} \in \mathbf{Z}_p^{(n)}$ that is a lift of u, and such that $\widetilde{u}^{p^n} = u$.*

The element $\widetilde{u}$ in the above proposition is the *Teichmüller lift* of u. We start with a lemma.

LEMMA B.9. *If I is an ideal in a commutative ring A, and if $u, v \in A$ are such that $u \equiv v \pmod{pI}$, then $u^{p^i} \equiv v^{p^i} \pmod{p^{i+1}I}$ for every $i \geq 1$.*

PROOF. Arguing by induction on i, we see that it is enough to prove the case $i = 1$. Write $u = v + a$, where $a \in pI$, hence

$$u^p - v^p = \sum_{j=1}^{p} \binom{p}{j} v^{p-j} a^j.$$

Since $a^j \in p^2 I^2$ for every $j \geq 2$, and $pa \in p^2 I$, we get the assertion in the lemma. □

PROOF OF PROPOSITION B.8. For the existence part, it is clear that if $u = 0$, then we may take $\widetilde{u} = 0$. Suppose now that u is nonzero. We have seen in the proof of Theorem B.6 that $\mathbf{Q}_p^{(n)} = \mathbf{Q}_p(\widetilde{\alpha})$, where $\widetilde{\alpha} \in \overline{\mathbf{Q}_p}$ is a primitive root of 1 of order $p^n - 1$, and its image $\alpha \in \mathbf{F}_{p^n}$ is again a primitive root of 1 of order $p^n - 1$. Therefore α is a multiplicative generator of $\mathbf{F}_{p^n}^*$, hence there is m such that $u = \alpha^m$. Since $\widetilde{\alpha} \in \mathbf{Z}_p^{(n)}$, if we take $\widetilde{u} = \widetilde{\alpha}^m$, this has the required properties.

In order to prove uniqueness, suppose that $\widetilde{u}, \widetilde{v} \in \mathbf{Z}_p^{(n)}$ both satisfy the conditions in the proposition. In particular, we have $\widetilde{u} \equiv \widetilde{v} \pmod{p\mathbf{Z}_p^{(n)}}$, and the lemma implies $\widetilde{u}^{p^{ni}} \equiv \widetilde{v}^{p^{ni}} \pmod{p^{ni+1}\mathbf{Z}_p^{(n)}}$ for every $i \geq 1$. Since $\widetilde{u}^{p^{ni}} = \widetilde{u}$ and $\widetilde{v}^{p^{ni}} = \widetilde{v}$, we conclude that $\widetilde{u} - \widetilde{v} \in \bigcap_{i \geq 1} p^{ni}\mathbf{Z}_p^{(e)}$, hence $\widetilde{u} = \widetilde{v}$. □

COROLLARY B.10. *Every element in $\mathbf{Z}_p^{(n)}$ has a unique expression as the sum of a series $\sum_{i \geq 0} a_i p^i$, where $a_i^{p^n} = a_i$ for every i.*

PROOF. Given $u \in \mathbf{Z}_p^{(n)}$, let a_0 be the Teichmüller lift of the image of u in $\mathbf{F}_{p^n}$, so that $u - a_0 = pu_1$, for some $u_1 \in \mathbf{Z}_p^{(n)}$. Repeating this construction for u_1 etc., we see that we can write u as a sum as in the corollary. For uniqueness, note that if we have two expressions as in the statement

$$u = \sum_{i \geq 0} a_i p^i = \sum_{i \geq 0} b_i p^i,$$

then $a_0 = b_0$ by Proposition B.8, and then $\sum_{i \geq 1} a_i p^{i-1} = \sum_{i \geq 1} b_i p^{i-1}$, and we repeat. □

REMARK B.11. Note that if m divides n, then $\mathbf{F}_{p^m} \subseteq \mathbf{F}_{p^n}$ and $\mathbf{Q}_p^{(m)} \subseteq \mathbf{Q}_p^{(n)}$. It follows from the uniqueness part in Proposition B.8 that the Teichmüller lift $\widetilde{u}$ of an element $u \in \mathbf{F}_{p^m}$ is equal to the Techmüller lift of u when considered as an element in $\mathbf{F}_{p^n}$.

REMARK B.12. If $\widetilde{u}$ and $\widetilde{v}$ are the Teichmüller lifts of $u, v \in \mathbf{F}_{p^n}$, respectively, then $\widetilde{u}\widetilde{v}$ is the Teichmüller lift of uv. Indeed, it is clear that $\widetilde{u}\widetilde{v}$ satisfies both conditions in the definition of a Teichmüller lift.

B.3. The field $\mathbf{C}_p$

In this section we follow closely the presentation in [Kob, Chapter III.3]. Let $\overline{\mathbf{Q}_p}$ be an algebraic closure of $\mathbf{Q}_p$. We can write $\mathbf{Q}_p = \bigcup_K K$, where K varies over the finite extensions of $\mathbf{Q}_p$. By Exercise B.3 the absolute values on the various K are compatible, hence we get a non-Archimedean absolute value $|\cdot|_p$ on $\overline{\mathbf{Q}_p}$, that restricts on each K to the one we have defined. As in §1, this gives a non-Archimedean metric on $\overline{\mathbf{Q}_p}$, and each finite extension K of $\mathbf{Q}_p$ is a metric subspace of $\overline{\mathbf{Q}_p}$. The *ring of integers* $\mathcal{O}_{\overline{\mathbf{Q}_p}}$ of $\overline{\mathbf{Q}_p}$ is the union $\bigcup_K \mathcal{O}_K$, hence it is the set of elements of $\overline{\mathbf{Q}_p}$ that are integral over $\mathbf{Z}_p$. We may also describe this as $\{u \in \overline{\mathbf{Q}_p}, |u|_p \leq 1\}$.

Exercise B.13. Show that $\mathcal{O}_{\overline{\mathbf{Q}_p}}$ is a local ring, with maximal ideal $\mathfrak{m} = \{u \in \overline{\mathbf{Q}_p}, |u|_p < 1\}$. Prove that there is an isomorphism $\mathcal{O}_{\overline{\mathbf{Q}_p}}/\mathfrak{m} \simeq \overline{\mathbf{F}_p}$.

Proposition B.14. *The field $\overline{\mathbf{Q}_p}$, with the metric described above, is not complete.*

Proof. We need to construct a Cauchy non-convergent sequence in $\overline{\mathbf{Q}_p}$. We start by choosing for every $i \geq 0$ a primitive root $b_i \in \overline{\mathbf{Q}_p}$ of 1 of order $p^{2^i} - 1$. Let $K_i = \mathbf{Q}_p(b_i)$. It follows from Theorem B.6 that $[K_i : \mathbf{Q}_p] = 2^i$. If $i < j$, then $p^{2^i} - 1$ divides $p^{2^j} - 1$. This implies that b_i is a power of b_j, hence we have $K_i \subseteq K_j$.

We take $a_i = b_0 p^{N_0} + b_1 p^{N_1} + \ldots b_i p^{N_i}$, where $N_0 < N_1 < \ldots < N_i < \ldots$ will be chosen later. Note that since $|b_i|_p = 1$ for every i, we have $|a_i - a_{i+1}|_p = \frac{1}{p^{N_i}}$, hence the sequence $(a_i)_i$ is Cauchy by Exercise B.5.

Suppose that $N_0, \ldots, N_i$ have been constructed, and a_i is defined as above. It is clear that we have $\mathbf{Q}_p(a_i) \subseteq K_i$. We claim that in fact this is an equality. Indeed, otherwise there is $\sigma\colon K_i \to \overline{\mathbf{Q}_p}$ that fixes $\mathbf{Q}_p(a_i)$, but such that $\sigma(b_i) \neq b_i$. We have

$$\sum_{j=0}^{i} \sigma(b_j) p^{N_j} = \sigma(a_i) = a_i = \sum_{j=0}^{i} b_j p^{N_j},$$

and the uniqueness part in Corollary B.10 implies that $\sigma(b_i) = b_i$, a contradiction.

Assuming N_i chosen, we claim that there is $N_{i+1} > N_i$ such that a_i does not satisfy any congruence

$$\alpha_n a_i^n + \alpha_{n-1} a_i^{n-1} + \ldots + \alpha_0 \equiv 0 \pmod{p^{N_{i+1}}} \tag{B.1}$$

for any $n < d := [\mathbf{Q}_p(a_i) : \mathbf{Q}_p] = 2^i$, with $\alpha_j \in \mathbf{Z}_p$, not all of them divisible by p. Indeed, for every $N \geq N_i$, consider the set A_N of all $(\alpha_0, \ldots, \alpha_{d-1}) \in \mathbf{Z}/p^{N+1}\mathbf{Z}$ with the property that $\sum_{j=0}^{d-1} \alpha_j a_i^j = 0$ in $\mathbf{Z}/p^{N+1}\mathbf{Z}$, and some α_j does not lie in $p\mathbf{Z}/p^{N+1}\mathbf{Z}$. Note that the projection $\mathbf{Z}/p^{N+2}\mathbf{Z} \to \mathbf{Z}/p^{N+1}\mathbf{Z}$ induces a map $A_{N+1} \to A_N$. If all A_N are nonempty, then $\varprojlim_N A_N$ is nonempty. Indeed, we may choose an element $c_{N_i} \in \bigcap_N \mathrm{Im}(A_N \to A_{N_i})$, then an element $c_{N_i+1} \in \bigcap_N \mathrm{Im}(A_N \to A_{N_i+1})$ that lies over c_{N_i}, etc. Since an element in $\varprojlim_N A_N$ determines a nontrivial equation of degree $< d$ with coefficients in $\mathbf{Q}_p$, we get a contradiction.

We choose the N_i inductively, such that the above condition is satisfied, and we claim that in this case the sequence $(a_i)_i$ is not convergent to an element of $\overline{\mathbf{Q}_p}$. Indeed, if the sequence converges to $a \in \overline{\mathbf{Q}_p}$, then let us consider a polynomial

$f = \alpha_n x^n + \ldots + \alpha_0 \in \mathbf{Z}_p[x]$, with not all $\alpha_i \in p\mathbf{Z}_p$, such that $f(a) = 0$. Since $a \equiv a_\ell \pmod{p^{N_{i+1}}\mathbf{Z}_p}$ for $\ell \gg 0$, and $a_i \equiv a_\ell \pmod{p^{N_{i+1}}\mathbf{Z}_p}$ for $\ell \geq i$, it follows that $a \equiv a_i \pmod{p^{N_{i+1}}\mathbf{Z}_p}$. We get a contradiction if we take i such that $2^i > n$. This completes the proof of the proposition. □

Since $\overline{\mathbf{Q}_p}$ is a metric space, it is a general result that there is a *completion* of $\overline{\mathbf{Q}_p}$ that is denoted by $\mathbf{C}_p$. This means that we can embed $\overline{\mathbf{Q}_p}$ as a dense metric subspace in $\mathbf{C}_p$, which is complete. The field operations extend (uniquely) by continuity to $\mathbf{C}_p$, so this is a field. Furthermore, the absolute value on $\overline{\mathbf{Q}_p}$ extends uniquely to a non-Archimedean absolute value on $\mathbf{C}_p$, still denoted by $|\cdot|_p$, that induces the metric, hence the topology of $\mathbf{C}_p$. The miracle is that we do not have to repeat the process of taking algebraic closure and completion.

THEOREM B.15. *The field $\mathbf{C}_p$ is algebraically closed.*

PROOF. Let $f = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$ be a polynomial in $\mathbf{C}_p[x]$, with $a_0 \neq 0$. We need to show that f has a root in $\mathbf{C}_p$. Since $\overline{\mathbf{Q}_p}$ is dense in $\mathbf{C}_p$, we can find $a_{m,i} \in \overline{\mathbf{Q}_p}$ with $a_{m,0} \neq 0$ and $|a_{m,i} - a_i|_p < \epsilon_m < 1$, where (ϵ_m) is a strictly decreasing sequence, converging to 0. Let $f_m = \sum_{i=0}^n a_{m,i} x^{n-i} \in \overline{\mathbf{Q}_p}[x]$. Since $\overline{\mathbf{Q}_p}$ is algebraically closed, we can factor each f_m as

$$f_m = a_{m,0}(x - \alpha_{m,1}) \cdots (x - \alpha_{m,n}),$$

for suitable $\alpha_{m,i} \in \overline{\mathbf{Q}_p}$.

We first show that there is $C \geq 1$ such that $|\alpha_{m,i}|_p \leq C$ for all i and m. Indeed, let us fix m, and suppose after reordering the $(\alpha_{m,j})_j$ that

$$\alpha_{m,1} = \ldots = \alpha_{m,r} > \alpha_{m,j} \text{ for all } j > r.$$

If s_r is the r^{th} elementary symmetric function of the $\alpha_{m,j}$, then

$$|\alpha_{m,1}|^r = |s_r|_p = |a_{m,r}/a_{m,0}|_p.$$

We conclude that

$$\alpha_{m,i} \leq \max_{1 \leq j \leq n} \frac{|a_{m,j}|_p^{1/j}}{|a_{m,0}|_p^{1/j}},$$

and since each $a_{m,j}$ is close to a_j, we see that we can find C as desired.

We now show that we can reorder $(\alpha_{m,i})_i$ for all m, such that $|\alpha_{m,1} - \alpha_{m+1,1}| \leq C' \epsilon_m^{1/n}$ for all m, where C' is a constant independent of m. Note that this implies by Exercise B.5 that the sequence $(\alpha_{m,1})_m$ is Cauchy. Let us suppose that we did this up to m. We have

$$f_{m+1}(\alpha_{m,1}) = a_{m,0} \prod_{j=1}^n (\alpha_{m,1} - \alpha_{m+1,j}),$$

and on the other hand

$$f_{m+1}(\alpha_{m,1}) = f_{m+1}(\alpha_{m,1}) - f_m(\alpha_{m,1}) = \sum_{i=0}^n (a_{m+1,i} - a_{m,i}) \alpha_{m,1}^{n-i}.$$

Therefore we get

$$|a_{m,0}|_p \cdot \prod_{j=1}^n |\alpha_{m,1} - \alpha_{m+1,j}|_p \leq \epsilon_m C^{n-1},$$

and after reordering the $\alpha_{m+1,j}$ we may assume that

$$|\alpha_{m,1} - \alpha_{m+1,1}|_p \leq C' \epsilon_m^{1/n},$$

where C' is a constant that only depends on C, n, and $\min_m |a_{m,0}|_p > 0$.

Therefore we may assume that $(\alpha_{m,1})_m$ is a Cauchy sequence, hence is convergent to some $\alpha \in \mathbf{C}_p$. Since $f_m(\alpha_{m,1}) = 0$ for every m, and $\lim_{m\to\infty} a_{m,i} = a_i$ for every i, we have $f(\alpha) = 0$. This completes the proof. □

REMARK B.16. Note that $\mathbf{C}_p$ is obtained from $\mathbf{Q}$ in a similar way that with how $\mathbf{C}$ is obtained from $\mathbf{Q}$, with the respect to the usual Archimedean absolute value on $\mathbf{Q}$ (however, in the case of $\mathbf{C}_p$ we had to complete twice).

REMARK B.17. Note that the algebraic closure and the completion are unique up to a canonical isomorphism. Therefore the field $\mathbf{C}_p$ is unique up to a canonical isomorphism (of fields equipped with an absolute value).

The field $\mathbf{C}_p$ therefore is algebraically closed and complete with respect to the non-Archimedean absolute value $|\cdot|_p$. This provides the right setting for doing p-adic analysis.

B.4. Convergent power series over complete non-Archimedean fields

In this section we review some basic facts about convergent power series and analytic functions in the non-Archimedean setting. The principle is that the familiar results over $\mathbf{R}$ or $\mathbf{C}$ carry over to this framework, sometimes in a slightly improved version.

Let $(K, |\cdot|)$ be a field endowed with a nontrivial[3] non-Archimedean absolute value, which is complete with respect to the induced metric space structure. For applications we will be interested in the case when $K = \mathbf{C}_p$, or K is a p-adic field. For every point $a \in K$ and every $r > 0$, we put

$$D_r(a) = \{u \in K, |u - a| \leq r\}, \quad D_r^\circ(a) = \{u \in K, |u - a| < r\}.$$

It is clear that $D_r^\circ(a)$ is an open neighborhood of a. A special feature of the non-Archimedean setting is that $D_r(a)$ is both open and closed[4].

PROPOSITION B.18. *Given a formal power series $f = \sum_{n\geq 0} a_n t^n \in K[\![t]\!]$ be a over K, let $r(f) := 1/\limsup_n |a_n|^{1/n}$[5], and consider $u \in K$.*

i) *If $|u| < r(f)$, then $\sum_{n\geq 0} a_n u^n$ is convergent.*
ii) *If $|u| > r(f)$, then $\sum_{n\geq 0} a_n u^n$ is divergent.*
iii) *If $v \in K$ is such that $|u| = |v| = r(f)$, then $\sum_{n\geq 0} a_n u^n$ is convergent if and only if $\sum_{n\geq 0} a_n v^n$ is.*

The *radius of convergence* of f is $r(f)$.

---

[3] An absolute value is trivial if it only takes the values 0 and 1.

[4] This shows that K is *totally disconnected*, that is, every point has a basis of neighborhoods that are both open and closed. This is a fact of life in the non-Archimedean setting, and the need to correct this led to the theory of rigid analytic spaces, see [Con].

[5] We make the convention that if $\limsup_n |a_n|^{1/n}$ is zero or infinite, then $r(f) = \infty$ or $r(f) = 0$, respectively.

PROOF. If $|u| < r(f)$, then $\inf_m \sup_{n\geq m} |a_n|^{1/n} < \frac{1}{|u|}$, hence there is n_0 and $\rho < 1$ such that $|a_n|^{1/n} < \frac{\rho}{|u|}$ for all $n \geq n_0$. Therefore $|a_n u^n| < \rho^n$ for $n \geq n_0$, hence $\lim_{n\to\infty} a_n u^n = 0$, and we deduce from Exercise B.5 that $\sum_{n\geq 0} a_n u^n$ is convergent.

Suppose now that $|u| > r(f)$, hence $\inf_m \sup_{n\geq m} |a_n|^{1/n} > \frac{1}{|u|}$. It follows that we can find $\rho > \frac{1}{|u|}$ such that for every m, there is $n \geq m$ with $|a_n u^n| > (\rho|u|)^n$. Therefore $\sum_{n\geq 0} a_n u^n$ is divergent. The assertion in iii) follows from the fact that if $|u| = r(f)$, then $\sum_{n\geq 0} a_n u^n$ is convergent if and only if $\lim_{n\to\infty} |a_n| r(f)^n = 0$. □

If $U \subseteq K$ is open, a function $\phi\colon U \to K$ is *analytic* if for every $a \in U$, there is $r > 0$ with $D_r^\circ(a) \subseteq U$, and a formal power series $f \in K[\![t]\!]$ with radius of convergence $r(f) \geq r$ such that $\phi(u) = f(u-a)$ for every $u \in D_r^\circ(a)$.

LEMMA B.19. *If $f = \sum_{n\geq 0} a_n t^n \in K[\![t]\!]$ and $|b| < r(f)$, then there is $g \in K[\![t]\!]$ with $r(g) \geq r(f)$ such that $f(u) = g(u-b)$ for every $u \in K$ with $|u| < r(f)$.*

PROOF. For every $u \in K$ we have $|u-b| < r(f)$ if and only if $|u| < r(f)$, and in this case

$$f(u) = \sum_{n\geq 0} a_n((u-b)+b)^n = \sum_{n\geq 0} a_n \sum_{i=0}^{n} \binom{n}{i} (u-b)^i b^{n-i}$$

$$= \sum_{i\geq 0} \left(\sum_{j\geq 0} \binom{i+j}{i} a_{i+j} b^j \right) (u-b)^i.$$

In particular, $\beta_i := \sum_{j\geq 0} \binom{i+j}{i} a_{i+j} b^j$ is well-defined, the series $g = \sum_{i\geq 0} \beta_i t^i$ has radius of convergence $\geq r(f)$, and $f(u) = g(u-b)$ whenever $|u-b| < r(f)$. □

COROLLARY B.20. *If $f \in K[\![t]\!]$ has radius of convergence $r(f) > 0$, then the function*

$$\{u \in K, |u| < r(f)\} \ni u \to f(u) \in K$$

is an analytic function.

Analytic functions on open subsets of K satisfy properties entirely analogous to the ones of real or complex analytic functions. We list some of these properties, but leave as an exercise for the reader the task of checking that the familiar proofs also work in the non-Archimedean setting.

• Every analytic function is continuous. This is a consequence of the fact that for every $f = \sum_{n\geq 0} a_n t^n \in K[\![t]\!]$, if we put $f_m = \sum_{n=0}^{m} a_n t^n$, then the convergence of $f_m(u)$ to $f(u)$ is uniform on every subset $D_R(0)$, with $R < r(f)$. Indeed, we have

$$|f(u) - f_m(u)| \leq \sup_{n\geq m} |a_n| R^n \to 0 \text{ when } m \to \infty.$$

• The set of analytic functions on an open subset $U \subseteq K$ is a ring. Furthermore, if ϕ is analytic and nonzero at every point of U, then $1/\phi$ is analytic.

More precisely, suppose that ϕ and ψ are analytic on U, and they are given on $D_r^\circ(a) \subseteq U$ as $\phi(u) = f(u-a)$ and $\psi(u) = g(u-a)$, for some $f, g \in K[\![t]\!]$ $r(f), r(g) \geq r$. In this case the radii of convergence of $f+g$ and fg are both $\geq r$, and $\phi(u) + \psi(u) = (f+g)(u-a)$ and $\phi(u)\psi(u) = fg(u-a)$ for $u \in D_r^\circ(a)$. Furthermore, if $\phi(u) \neq 0$ for every $u \in D_r^\circ(a)$, then in particular $f(0) \neq 0$, hence f

is invertible. The radius of convergence of f^{-1} is $\geq r$, and $1/\phi(u) = f^{-1}(u-a)$ for every $u \in D_r^\circ(a)$.

• If $\phi\colon U \to V$ and $\psi\colon V \to K$ are analytic functions, then the composition $\psi \circ \phi$ is analytic. More precisely, given $a \in U$, suppose that $D_r^\circ(a) \subseteq U$ and $D_{r'}^\circ(\phi(a)) \subseteq V$ are such that $\phi(u) = f(u-a)$ and $\psi(v) = g(v-\phi(a))$ for suitable $f, g \in K[\![t]\!]$, such that the radii of convergence of f and g are $\geq r, r'$, respectively. Note that $f(0) = \phi(a)$, and let $\widetilde{f} = f - f(0)$, and $h = g \circ \widetilde{f} \in K[\![t]\!]$. After possibly replacing r by a smaller value, we may assume that $\phi(D_r^\circ(a)) \subseteq D_{r'}^\circ(\phi(a))$. In this case the radius of convergence of h is $\geq r$, and we have $\phi(\psi(u)) = h(u-a)$ for $u \in D_r^\circ(a)$.

• If $f, g \in K[\![t]\!]$ have radii of convergence $\geq R > 0$, and $f(u) = g(u)$ for every u with $0 < |u| < R$, then $f = g$

One can differentiate analytic functions, and the result is again analytic. One can also consider, more generally, analytic functions of several variables. However, while such functions show up in Chapter 8, we do not need to develop any theory in this setting.

We end this section with the following result that is needed in Chapter 8. For simplicity, we assume that $|K^*|$ is dense in $\mathbf{R}_0$. For example, this always holds if K is algebraically closed. Indeed, if $u \in K$ is such that $|u| > 1$, then $|u|^q \in |K^*|$ for every $q \in \mathbf{Q}$, hence $|K^*|$ is dense in $\mathbf{R}_{>0}$.

PROPOSITION B.21. *Suppose that $|K^*|$ is dense in $\mathbf{R}_{>0}$, and let $R > 0$ and $f \in K[\![t]\!]$ be such that $r(f) > R$. In this case, there is a polynomial $P \in K[t]$ and an invertible power series $g \in K[\![t]\!]$ such that both g and g^{-1} are convergent on $D_R(0)$, and $f = Pg$.*

Before giving the proof of the proposition, we introduce some notation. Let $A_K = \{u \in R, |u| \leq 1\}$ and $\mathfrak{m}_K = \{u \in A_K, |u| < 1\}$. It is clear that A_K is a subring of K, $\mathfrak{m}_K$ is an ideal in A_K, and the quotient $A_K/\mathfrak{m}_K$ is a field, that we denote by k. If $f \in A[\![t]\!]$, we denote by $\overline{f}$ its image in $k[\![t]\!]$.

Let T denote the set of formal power series in $K[\![t]\!]$ that are convergent on $D_1(0)$. If $f = \sum_{n\geq 0} a_n t^n$, then $f \in T$ if and only if $\lim_{n\to\infty} a_n = 0$. It follows that if we put $\| f \| := \max_n |a_n|$, then this maximum is well-defined, and it is attained for only finitely many n. Note that if $f \in R[\![t]\!] \cap T$, then $\overline{f}$ is a polynomial.

EXERCISE B.22. Show that if $f, g \in T$, then $\| f \cdot g \| = \| f \| \cdot \| g \|$.

PROOF OF PROPOSITION B.21. The assertion holds trivially if $f = 0$, hence from now on we assume $f \neq 0$. Since $|K^*|$ is dense in $\mathbf{R}_{>0}$, after possibly replacing R by a larger value, we may assume that $R \in |K^*|$. We first note that if $\alpha \in D_{r(f)}^\circ(0)$ is such that $f(\alpha) = 0$, then $f = (t-\alpha)f_1$ for some $f_1 \in K[\![t]\!]$ with $r(f_1) \geq r(f)$. Indeed, by Lemma B.19 there is $g \in K[\![t]\!]$ with $r(g) \geq r(f)$ such that $f(u) = g(u-\alpha)$ for $|u| < r(f)$. Since $f(\alpha) = 0$, it follows that $g = tg_1$ for some $g_1 \in K[\![t]\!]$, and we clearly have $r(g_1) = r(g)$. Another application of Lemma B.19 gives $f_1 \in K[\![t]\!]$ with $r(f_1) \geq r(g_1) \geq r(f)$ such that $g_1(u) = f_1(u+\alpha)$ whenever $|u| < r(f)$. Therefore

$$f(u) = g(u-\alpha) = (u-\alpha)g_1(u-\alpha) = (u-\alpha)f_1(u)$$

for all u with $|u| < r(f)$, hence $f = (t-\alpha)f_1$.

We now show that there are $\alpha_1, \ldots, \alpha_r \in D_R(0)$ (possibly not distinct) such that

$$f = (t-\alpha_1)\cdots(t-\alpha_r)g \tag{B.2}$$

for some $g \in K[\![t]\!]$ with $r(g) \geq r(f)$, and such that $g(\alpha) \neq 0$ for every $\alpha \in D_R(0)$. If $\lambda \in K$ is such that $|\lambda| = R$, then after replacing f by $f(\lambda t)$, we may assume that $R = 1$. Let us write $f = \sum_{n \geq 0} a_n t^n$. By assumption, we have $f \in T$, and let N be the largest n with $|a_n| = \| f \|$. After replacing f by $a_N^{-1} f$, we may assume that $a_N = 1$. Therefore $f \in A_K[\![t]\!]$, and $\overline{f}$ is a monic polynomial of degree N. By what we have already proved, it is enough to show that given any expression as in (B.2), we have $r \leq N$. Since $\| t - \alpha_i \| = 1$ for all i, it follows from Exercise B.22 that $\| g \| = 1$. In particular, we have $g \in A_K[\![t]\!]$, and if we take the image in $k[\![t]\!]$, we get $\overline{f} = \overline{g} \cdot \prod_{i=1}^{r} (t - \overline{\alpha_i})$. Since $\overline{f}$ is a polynomial of degree N, we deduce that $r \leq N$.

In order to complete the proof of the proposition, it is enough to show that if we write f as in (B.2), with g not vanishing anywhere on $D_R(0)$, then g^{-1} converges on $D_R(0)$: indeed, we then take $P = \prod_{i=1}^{r} (t - \alpha_i)$. Since $|K^*|$ is dense in $\mathbf{R}_{>0}$, there is $R' \in |K^*|$ with $R < R' < r(f)$. Applying what we have already proved for g and $D_{R'}(0)$, we see that there are only finitely many $\alpha \in D_{R'}(0)$ with $g(\alpha) = 0$. It follows that after replacing R' by a smaller one, we may assume that g does not vanish on $D_{R'}(0)$, and in this case the radius of convergence of g^{-1} is $\geq R' > R$. This completes the proof of the proposition. □

B.5. Examples of analytic functions

In this section we discuss the p-adic version of some familiar complex analytic functions Let us start with the exponential function. In this section we assume that $K = \mathbf{C}_p$.

Consider $f = \sum_{n \geq 0} \frac{t^n}{n!} \in \mathbf{C}_p[\![t]\!]$, and let us determine the radius of convergence of f. Note that unlike in the complex case, the large denominators make the radius of convergence small. For every n we have

$$\mathrm{ord}_p(n!) = \sum_{i \geq 1} \lfloor n/p^i \rfloor \leq \sum_{i \geq 1} \frac{n}{p^i} = \frac{n}{p-1},$$

hence $(|1/n!|_p)^{1/n} \leq \left(\frac{1}{p}\right)^{-1/(p-1)}$. On the other hand, if $n = p^m$, then

$$\mathrm{ord}_p(n!) = p^{m-1} + \ldots + p + 1 = \frac{p^m - 1}{p-1},$$

hence $\mathrm{ord}_p(p^m!)/p^m$ converges to $\frac{1}{p-1}$. We thus conclude that $\limsup_n (|1/n!|_p)^{1/n} = \left(\frac{1}{p}\right)^{-1/(p-1)}$, hence by Proposition B.18 the radius of convergence of f is $\left(\frac{1}{p}\right)^{1/(p-1)} < 1$. This implies that the *p-adic exponential function* $\exp_p$ given by $\exp_p(u) = f(u)$ is not defined, for example, on all $\mathbf{Z}_p$.

Let us consider also the *p-adic logarithm function* $\log_p(1+u) = g(u)$, where $g(t) = \sum_{n \geq 1} (-1)^{n-1} \frac{t^n}{n}$. We now are in better shape: if $\mathrm{ord}_p(n) = i$, then $n \geq p^i$, hence $\frac{i}{n} \leq \frac{\log(n)}{n \cdot \log(p)}$, which converges to zero when n goes to infinity. It then follows from Proposition B.18 that the radius of convergence of g is 1, hence $\log_p(1+u)$ is defined in $D_1^\circ(0)$, precisely as in the complex case.

We now consider the *p-adic binomial series*. Let us recall first the formula for the binomial series in the case of complex functions. If $a \in \mathbf{C}$, then we may consider the analytic function $\phi(u) = (1+u)^a$. More precisely, we have $\phi(u) = \exp(a \cdot \log(1+u))$, which is defined and analytic for $|u| < 1$. The Taylor expansion

at 0 is given by

$$\phi(u) = \sum_{m \geq 0} \frac{\phi^{(m)}(0)}{m!} u^m.$$

Since we have $\phi'(u) = a(1+u)^{a-1}$, one sees immediately by induction on m that $\phi^{(m)}(0) = a(a-1)\cdots(a-m+1)$.

We will now use the same formal power series in the p-adic setting, by allowing the exponent to lie in $\mathbf{C}_p$. More precisely, for $a \in \mathbf{C}_p$, consider the formal power series

$$B_{a,p}(y) = \sum_{m \geq 0} \frac{a(a-1)\cdots(a-m+1)}{m!} y^m \in \mathbf{C}_p[\![y]\!].$$

For obvious reasons, we also write $(1+y)^a$ for $B_{a,p}(y)$, and $(1+u)^a$ for $B_{a,p}(u)$, when $u \in \mathbf{C}_p$ is such that $|u|$ is smaller than the radius of convergence of $B_{a,p}$. Let us first discuss the radius of convergence of $B_{a,p}$.

LEMMA B.23. *Let $a \in \mathbf{C}_p$, and denote by R the radius of convergence of $B_{a,p}$.*

i) *If $|a|_p > 1$, then $R = \frac{1}{|a|_p}\left(\frac{1}{p}\right)^{1/(p-1)}$.*
ii) *If $|a|_p \leq 1$, then $R \geq \left(\frac{1}{p}\right)^{1/(p-1)}$.*
iii) *If $a \in \mathbf{Z}_p$, then $R \geq 1$.*

PROOF. Suppose first that $|a|_p > 1$. In this case $|a-i|_p = |a|_p$ for every $i \in \mathbf{Z}$. Therefore

$$\left(\frac{|a(a-1)\cdots(a-m+1)|_p}{|m!|_p}\right)^{1/m} = \frac{|a|_p}{|m!|_p^{1/m}},$$

and the computation that we have done for $\exp_p$ shows that in this case the radius of convergence of $B_{a,p}(x)$ is $\frac{1}{|a|_p}\left(\frac{1}{p}\right)^{1/(p-1)}$.

If $|a|_p \leq 1$, then $|a-i|_p \leq 1$ for every $i \in \mathbf{Z}$, and we deduce from Proposition B.18 and the computation in the case of the exponential function that $R \geq \left(\frac{1}{p}\right)^{1/(p-1)}$. For the assertion in iii), it is enough to show that if $a \in \mathbf{Z}_p$, then $\frac{a(a-1)\cdots(a-m+1)}{m!} \in \mathbf{Z}_p$. This is clear when $a \in \mathbf{Z}$, and the general case follows since $\mathbf{Z}$ is dense in $\mathbf{Z}_p$ (recall that $\mathbf{Z}_p$ consists of those $u \in \mathbf{Q}_p$ with $|u|_p \leq 1$). □

REMARK B.24. It is clear from definition that if m is a nonnegative integer, then $B_{m,p}(1+y)$ is, as expected, the m^{th} power of $1+y$.

The binomial series satisfies the following "expected" properties.

PROPOSITION B.25. *If $a, b \in \mathbf{C}_p$, then the following hold.*

i) $(1+y)^a \cdot (1+y)^b = (1+y)^{a+b}$.
ii) $((1+y)^a)^b = (1+y)^{ab}$.

Regarding ii), note that $(1+y)^a = 1 + v(y)$ for some $v \in y\mathbf{C}_p[\![y]\!]$, hence $(1+v(y))^b$ is well-defined in $\mathbf{C}_p[\![y]\!]$. We will prove the assertions in the proposition by reducing them to the corresponding ones over $\mathbf{C}$. However, it is more convenient to first introduce a formal series over $\mathbf{Q}$ in two variables, by letting a become a formal variable. More precisely, we consider

$$(1+y)^x := \sum_{m \geq 0} \frac{x(x-1)\cdots(x-m+1)}{m!} y^m \in \mathbf{Q}[\![x, y]\!].$$

PROPOSITION B.26. *We have the following equalities in* $\mathbf{Q}[\![x_1, x_2, y]\!]$.

i) $(1+y)^{x_1} \cdot (1+y)^{x_2} = (1+y)^{x_1+x_2}$.

ii) $((1+y)^{x_1})^{x_2} = (1+y)^{x_1 x_2}$.

PROOF. Let us prove i). Let f and g denote the left-hand side (respectively, the right-hand side) in i). In order to show that $f = g$, it is enough to show that they are equal in $\mathbf{C}[\![x_1, x_2, y]\!]$, hence it is enough to show that if $u_1, u_2, v \in \mathbf{C}$ are such that $|v| < 1$, then $f(u_1, u_2, v) = g(u_1, u_2, v)$ in $\mathbf{C}$ (note that under the condition on v, both sides are well-defined. As we have seen,

$$\begin{aligned}(1+v)^{u_1} \cdot (1+v)^{u_2} &= \exp(u_1 \log(1+v)) \cdot \exp(u_2 \log(1+v)) \\ &= \exp((u_1+u_2)\log(1+v)) = (1+v)^{u_1+u_1}.\end{aligned}$$

This completes the proof of i), and the proof of ii) is entirely similar. □

PROOF OF PROPOSITION B.25. If $g \in \mathbf{C}_p[\![x_1, x_2, y]\!]$ is such that the coefficient of every y^m is in $\mathbf{C}_p[x_1, x_2]$, for every $a, b \in \mathbf{C}_p$ we may consider $g(a, b, y) \in \mathbf{C}_p[\![y]\!]$. By letting $x_1 = a$ and $x_2 = b$ in Proposition B.26, we get the assertions in Proposition B.25. □

EXAMPLE B.27. Suppose that m is a positive integer not divisible by p, hence $\frac{1}{m} \in \mathbf{Z}_p$. It follows from Proposition B.23 that for every $u \in \mathbf{C}_p$ with $|u|_p < 1$ (for example, for every $u \in p\mathbf{Z}_p$) $v = (1+u)^{1/m}$ is well-defined, and by Proposition B.25 we have $v^m = 1 + u$.

Bibliography

[AKMW] D. Abramovich, K. Karu, K. Matsuki, and J. Włodarczyk, Torification and factorization of birational maps, J. Amer. Math. Soc. **15** (2002), 531–572. 72

[AKOV] N. Avni, B. Klopsch, U. Onn, and C. Voll, Representation zeta functions of some compact p-adic analytic groups, arXiv:1011.6533. 5

[Ati] M. F. Atiyah, Resolution of singularities nd division of distributions, Comm. Pure Appl. Math. **23** (1970), 145–150. 3

[Bad] L. Bădescu, *Algebraic surfaces*, Universitext, Springer-Verlag, New York, 2001. 82

[Beau] A. Beauville, *Complex algebraic surfaces*, Second edition, London Mathematical Society Student Texts, 34, Cambridge University Press, Cambridge, 1996. 82

[Ber] P. Berthelot, *Cohomologie cristalline des schémas de caractristique* $p > 0$, Lecture Notes in Mathematics, Vol. 407, Springer-Verlag, Berlin-New York, 1974. 100

[Bit] F. Bittner, The universal Euler characteristic for varieties of characteristic zero, Compos. Math. **140** (2004), 1011–1032. 71, 72

[Ber] I. N. Bernstein, The analytic continuation of generalized functions with respect to a parameter, Functional Anal. Appl. **6** (1972), 273–285. 3

[BG] I. N. Bernstein and S. I. Gelfand, Meromorphic property of the functions P^λ, Functional Anal. Appl. **3** (1969), 68–69. 3

[BCDT] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, On the modularity of elliptic curves over Q: wild 3-adic exercises, J. Amer. Math. Soc. 14 (2001), 843–939. 2, 68

[Con] B. Conrad, Several approaches to non-Archimedean geometry, in *p-adic geometry*, 963, Univ. Lecture Ser., 45, Amer. Math. Soc., Providence, RI, 2008. 118

[deJ1] A. J. de Jong, Weil cohomology theories, note available at *http://www.math.columbia.edu/˜ dejong/seminar/note_on_weil_cohomology.pdf*. 23

[deJ2] A. J. de Jong, Smoothness, semi-stability and alterations, Inst. Hautes Études Sci. Publ. Math. **83** (1996), 51–93. 27

[Del1] P. Deligne, Cohomologie étale: les points de départ, in *Cohomologie Étale* (SGA 4 1/2), Lecture Notes in Mathematics 569, 4–75, Springer-Verlag, Berlin-Heidelberg-New York, 1977. 32, 37

[Del2] P. Deligne, Fonctions L modulo ℓ^n et modulo p, in *Cohomologie Étale* (SGA 4 1/2), Lecture Notes in Mathematics 569, 110–128, Springer-Verlag, Berlin-Heidelberg-New York, 1977. 39

[Del3] P. Deligne, La conjecture de Weil, I, Publ. Math. IHES **43** (1974), 273–307. 2, 13

[DL] J. Denef and F. Loeser, Motivic Igusa zeta functions, J. Algebraic Geom. **7** (1998), 505–537. 4

[dSG] M. du Sautoy and F. Grunewald, Analytic properties of zeta functions and subgroup growth, Ann. of Math. (2) **152** (2000), 793–833. 4, 5

[Dwo] B. Dwork, On the rationality of the zeta function of an algebraic variety, Amer. J. Math. **82** (1960), 631–648. 2, 13, 87

[Ful1] W. Fulton, *Intersection theory*, Second edition, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, 2, Springer-Verlag, Berlin, 1998. 26

[Ful2] W. Fulton, *Introduction to toric varieties*, Ann. of Math. Stud. **131**, The William H. Rover Lectures in Geometry, Princeton Univ. Press, Princeton, NJ, 1993. 71

[Ful3] W. Fulton, A fixed point formula for varieties over finite fields, Math. Scand. **42** (1978), 189–196. 39, 42

[Göt1] L. Göttsche, On the motive of the Hilbert scheme of points on a surface, Math. Res. Lett. **8**, 2001, 613–627. 79

[Göt2] L. Göttsche, The Betti numbers of the Hilbert scheme of points on a smooth projective surface. Math. Ann. **286** (1990), 193–207. 14

[GS] L. Göttsche and W. Soergel, Perverse sheaves and the cohomology of Hilbert schemes of smooth algebraic surfaces, Math. Ann **296** (1993), 235–245. 84

[Gra] A. Granville, Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers, in *Organic mathematics (Burnaby, BC, 1995)*, 253–276, CMS Conf. Proc. 20, Amer. Math. Soc., Providence, RI, 1997. 109

[Gro] A. Grothendieck, Formule de Lefschetz et rationaité de fonctions L, Séminaire Bourbaki 279 (1965). 2

[SGA1] A. Grothendieck, *Revêtements étales et groupe fondamental.* Fasc I: Exposés 1 à 5, Séminaire de Géometrie Algébrique, 1960/1961, Institut de Hautes Études Scientifiques, Paris 1963. 101

[Har] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, No. 52, Springer-Verlag, New York-Heidelberg, 1977. 17, 22, 31, 77, 83, 108

[Igu] J.-i. Igusa, *An introduction to the theory of local zeta functions*, AMS/IP Studies in Advanced Mathematics 14, American Mathematical Society, Providence, RI, International Press, Cambridge, MA, 2000. 3

[Kap] M. Kapranov, The elliptic curve in the S-duality theory and Eisenstein series for Kac-Moody groups, arXiv: math.AG/0001005. 4, 76, 80

[Katz] N. Katz, Une formule de congruence pour la fonction ζ, Exposé XXII, in *Groupes de Monodromie en Géometrie Algébrique* (SGA 7 II), Lecture Notes in Mathematics 340, 401–438, Springer-Verlag, Berlin-Heidelberg-New York, 1973. 39

[KM] N. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, 108, Princeton University Press, Princeton, NJ, 1985. 109

[Knu] A. Knutson, Frobenius splitting, point counting, and degenerations, arXiv:0911.4941. 46

[Kob] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, Second edition, Graduate Texts in Mathematics, 58, Springer-Verlag, New York, 1984. 87, 111, 116

[Kol] J. Kollár, *Rational curves on algebraic varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, 32, Springer-Verlag, Berlin, 1996. 49

[Lang] S. Lang, *Algebraic number theory*, Graduate Texts in Mathematics, 110, Springer-Verlag, New York, 1994. 57, 67, 112

[LaWe] S. Lang and A. Weil, Number of points of varieties in finite fields, Amer. J. Math. **76** (1954), 819–827. 50

[LL1] M. Larsen and V. A. Lunts, Rationality criteria for motivic zeta functions, Compos. Math. **140** (2004), 1537–1560. 4, 81, 82

[LL2] M. Larsen and V. A. Lunts, Motivic measures and stable birational geometry, Mosc. Math. J. **3** (2003), 85–95. 74, 81, 82, 84

[Lau] G. Laumon, Transformation de Fourier, constantes d'équations fonctionnelles et conjecture de Weil, Inst. Hautes Études Sci. Publ. Math. **65** (1987), 131–210. 13

[LeS] B. Le Stum, *Rigid cohomology*, Cambridge Tracts in Mathematics, 172, Cambridge University Press, Cambridge, 2007. 100

[Lor] D. Lorenzini, *An invitation to arithmetic geometry*, Graduate studies in Mathematics 9, American Mathematical Society, Providence, RI, 1996. 18

[Mar] D. A. Marcus, *Number fields*, Universitext, Springer Verlag, New York-Heidelberg, 1977. 67

[Mat] H. Matsumura, *Commutative ring theory*, translated from the Japanese by M. Reid, Second edition, Cambridge Studies in Advanced Mathematics 8, Cambridge University Press, Cambridge, 1989. 111, 112

[Mil] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series, 33, Princeton University Press, Princeton, N.J., 1980. 28, 32, 37, 38

[MoVa] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, 97, Cambridge University Press, Cambridge, 2007. 58

[Mum1] D. Mumford, *Abelian varieties*, with appendices by C. P. Ramanujam and Y. I. Manin, corrected reprint of the second (1974) edition, Tata Institute of Fundamental Research Studies in Mathematics, 5, published for the Tata Institute of Fundamental Research, Bombay, by Hindustan Book Agency, New Delhi, 2008. 36

[Mum2] D. Mumford, Rational equivalence of 0-cycles on surfaces, J. Math. Kyoto Univ. **9** (1968), 195–204. 85

[Po] B. Poonen, The Grothendieck ring of varieties is not a domain, Math. Res. Lett. **9** (2002), 493–497. 75

[Sa] N. Sahasrabudhe, Grothendieck ring of varieties, Master thesis at Université de Bordeaux, available at *http://www.algant.eu/documents/theses/neeraja.pdf*. 74

[Se1] J.-P Serre, *A course in arithmetic*, Graduate Texts in Mathematics, No. 7, Springer-Verlag, New York-Heidelberg, 1973. 55

[Se2] J. P. Serre, Espaces fibrés algébriques, Séminaire Chevalley, 2^{e} année, 1958. 80

[TW] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, Ann. of Math. (2) **141** (1995), 553–572. 2, 68

[vdP] M. van der Put, The cohomology of Monsky and Washnitzer, in *Introductions aux cohomologies p-adiques (Luminy, 1984)*, Mém. Soc. Math. France (N.S.) No. **23** (1986), 33–59. 100

[Voll] C. Voll, Functional equations for zeta functions of groups and rings, Ann. of Math. (2) **172** (2010), 1181–1218. 5

[We1] A. Weil, *Varietés Abéliennes et Courbes Algébriques*, Hermann, Paris (1948). 1

[We2] A. Weil, Number of solutions of equations over finite fields, Bull. Amer. Math. Soc. **55** (1949), 497–508. 1, 2

[Wil] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. (2) **141** (1995), 443–551. 2, 68