THE TRACE FORMULA

Contents

1. Introduction

These are the notes of the second part of a course on étale cohomology taught by Johan de Jong at Columbia University in the Fall of 2009. The original note takers were Thibaut Pugin, Zachary Maddock and Min Lee. Over time we will add references to background material in the rest of the Stacks project and provide rigorous proofs of all the statements.

2. The trace formula

A typical course in étale cohomology would normally state and prove the proper and smooth base change theorems, purity and Poincaré duality. All of these can be found in [Del77, Arcata]. Instead, we are going to study the trace formula for the frobenius, following the account of Deligne in [Del77, Rapport]. We will only look at dimension 1, but using proper base change this is enough for the general case. Since all the cohomology groups considered will be étale, we drop the subscript $_{étale}$. Let us now describe the formula we are after. Let X be a finite type scheme of dimension 1 over a finite field k, ℓ a prime number and $\mathcal{F}$ a constructible, flat $\mathbf{Z}/\ell^n\mathbf{Z}$ sheaf. Then

$$\sum\nolimits_{x\in X(k)} \mathrm{Tr}(\mathrm{Frob}|\mathcal{F}_{\bar{x}}) = \sum\nolimits_{i=0}^{2}(-1)^i\mathrm{Tr}(\pi_X^*|H_c^i(X\otimes_k \bar{k}, \mathcal{F})) \tag{2.0.1}$$

as elements of $\mathbf{Z}/\ell^n\mathbf{Z}$. As we will see, this formulation is slightly wrong as stated. Let us nevertheless describe the symbols that occur therein.

3. Frobenii

In this section we will prove a “baffling” theorem. A topological analogue of the baffling theorem is the following.

Exercise 3.1. Let X be a topological space and $g : X \to X$ a continuous map such that $g^{-1}(U) = U$ for all opens U of X. Then g induces the identity on cohomology on X (for any coefficients).

We now turn to the statement for the étale site.

Lemma 3.2. *Let X be a scheme and $g : X \to X$ a morphism. Assume that for all $\varphi : U \to X$ étale, there is an isomorphism*

$$\begin{tikzcd} U \arrow[rr, "\sim"] \arrow[dr, "\varphi"'] & & U \times_{\varphi, X, g} X \arrow[dl, "pr_2"] \\ & X & \end{tikzcd}$$

functorial in U. Then g induces the identity on cohomology (for any sheaf).

Proof. The proof is formal and without difficulty. □

Please see Varieties, Section 36 for a discussion of different variants of the Frobenius morphism.

Theorem 3.3 (The Baffling Theorem)**.** *Let X be a scheme in characteristic $p > 0$. Then the absolute frobenius induces (by pullback) the trivial map on cohomology, i.e., for all integers $j \geq 0$,*

$$F_X^* : H^j(X, \underline{\mathbf{Z}/n\mathbf{Z}}) \longrightarrow H^j(X, \underline{\mathbf{Z}/n\mathbf{Z}})$$

is the identity.

This theorem is purely formal. It is a good idea, however, to review how to compute the pullback of a cohomology class. Let us simply say that in the case where cohomology agrees with Čech cohomology, it suffices to pull back (using the fiber products on a site) the Čech cocycles. The general case is quite technical, see Hypercoverings, Theorem 10.1. To prove the theorem, we merely verify that the assumption of Lemma 3.2 holds for the frobenius.

Proof of Theorem 3.3. We need to verify the existence of a functorial isomorphism as above. For an étale morphism $\varphi : U \to X$, consider the diagram

$$\begin{tikzcd}
U \arrow[dr, dashed] \arrow[drr, bend left, "F_U"] \arrow[ddr, bend right, "\varphi"'] & & \\
& U \times_{\varphi, X, F_X} X \arrow[r, "\mathrm{pr}_1"'] \arrow[d, "\mathrm{pr}_2"] & U \arrow[d, "\varphi"] \\
& X \arrow[r, "F_X"] & X.
\end{tikzcd}$$

The dotted arrow is an étale morphism and a universal homeomorphism, so it is an isomorphism. See Étale Morphisms, Lemma 14.3. □

Definition 3.4. Let k be a finite field with $q = p^f$ elements. Let X be a scheme over k. The *geometric frobenius* of X is the morphism $\pi_X : X \to X$ over $\mathrm{Spec}(k)$ which equals F_X^f.

Since π_X is a morphism over k, we can base change it to any scheme over k. In particular we can base change it to the algebraic closure $\bar{k}$ and get a morphism $\pi_X : X_{\bar{k}} \to X_{\bar{k}}$. Using π_X also for this base change should not be confusing as $X_{\bar{k}}$ does not have a geometric frobenius of its own.

Lemma 3.5. *Let $\mathcal{F}$ be a sheaf on $X_{étale}$. Then there are canonical isomorphisms $\pi_X^{-1}\mathcal{F} \cong \mathcal{F}$ and $\mathcal{F} \cong \pi_{X*}\mathcal{F}$.*

This is false for the fppf site.

Proof. Let $\varphi : U \to X$ be étale. Recall that $\pi_{X*}\mathcal{F}(U) = \mathcal{F}(U \times_{\varphi, X, \pi_X} X)$. Since $\pi_X = F_X^f$, it follows from the proof of Theorem 3.3 that there is a functorial isomorphism

$$\begin{tikzcd}
U \arrow[rr, "\gamma_U"'] \arrow[dr, "\varphi"'] & & U \times_{\varphi, X, \pi_X} X \arrow[dl, "\mathrm{pr}_2"] \\
& X &
\end{tikzcd}$$

where $\gamma_U = (\varphi, F_U^f)$. Now we define an isomorphism

$$\mathcal{F}(U) \longrightarrow \pi_{X*}\mathcal{F}(U) = \mathcal{F}(U \times_{\varphi, X, \pi_X} X)$$

by taking the restriction map of $\mathcal{F}$ along γ_U^{-1}. The other isomorphism is analogous. □

Remark 3.6. It may or may not be the case that F_U^f equals π_U.

We continue discussion cohomology of sheaves on our scheme X over the finite field k with $q = p^f$ elements. Fix an algebraic closure $\bar{k}$ of k and write $G_k = \mathrm{Gal}(\bar{k}/k)$ for the absolute Galois group of k. Let $\mathcal{F}$ be an abelian sheaf on $X_{\acute{e}tale}$. We will define a left G_k-module structure cohomology group $H^j(X_{\bar{k}}, \mathcal{F}|_{X_{\bar{k}}})$ as follows: if $\sigma \in G_k$, the diagram

$$\begin{tikzcd} X_{\bar{k}} \arrow[rr, "\mathrm{Spec}(\sigma)\times \mathrm{id}_X"] \arrow[dr] & & X_{\bar{k}} \arrow[dl] \\ & X & \end{tikzcd}$$

commutes. Thus we can set, for $\xi \in H^j(X_{\bar{k}}, \mathcal{F}|_{X_{\bar{k}}})$

$$\sigma \cdot \xi := (\mathrm{Spec}(\sigma) \times \mathrm{id}_X)^* \xi \in H^j(X_{\bar{k}}, (\mathrm{Spec}(\sigma) \times \mathrm{id}_X)^{-1}\mathcal{F}|_{X_{\bar{k}}}) = H^j(X_{\bar{k}}, \mathcal{F}|_{X_{\bar{k}}}),$$

where the last equality follows from the commutativity of the previous diagram. This endows the latter group with the structure of a G_k-module.

Lemma 3.7. *In the situation above denote $\alpha : X \to \mathrm{Spec}(k)$ the structure morphism. Consider the stalk $(R^j\alpha_*\mathcal{F})_{\mathrm{Spec}(\bar{k})}$ endowed with its natural Galois action as in Étale Cohomology, Section 56. Then the identification*

$$(R^j\alpha_*\mathcal{F})_{\mathrm{Spec}(\bar{k})} \cong H^j(X_{\bar{k}}, \mathcal{F}|_{X_{\bar{k}}})$$

from Étale Cohomology, Theorem 53.1 is an isomorphism of G_k-modules.

A similar result holds comparing $(R^j\alpha_!\mathcal{F})_{\mathrm{Spec}(\bar{k})}$ with $H^j_c(X_{\bar{k}}, \mathcal{F}|_{X_{\bar{k}}})$.

Proof. Omitted. □

Definition 3.8. The *arithmetic frobenius* is the map $\mathrm{frob}_k : \bar{k} \to \bar{k}$, $x \mapsto x^q$ of G_k.

Theorem 3.9. *Let $\mathcal{F}$ be an abelian sheaf on $X_{\acute{e}tale}$. Then for all $j \geq 0$, frob_k acts on the cohomology group $H^j(X_{\bar{k}}, \mathcal{F}|_{X_{\bar{k}}})$ as the inverse of the map π_X^*.*

The map π_X^* is defined by the composition

$$H^j(X_{\bar{k}}, \mathcal{F}|_{X_{\bar{k}}}) \xrightarrow{\pi_{X_{\bar{k}}}^*} H^j(X_{\bar{k}}, (\pi_X^{-1}\mathcal{F})|_{X_{\bar{k}}}) \cong H^j(X_{\bar{k}}, \mathcal{F}|_{X_{\bar{k}}}).$$

where the last isomorphism comes from the canonical isomorphism $\pi_X^{-1}\mathcal{F} \cong \mathcal{F}$ of Lemma 3.5.

Proof. The composition $X_{\bar{k}} \xrightarrow{\mathrm{Spec}(\mathrm{frob}_k)} X_{\bar{k}} \xrightarrow{\pi_X} X_{\bar{k}}$ is equal to $F^f_{X_{\bar{k}}}$, hence the result follows from the baffling theorem suitably generalized to nontrivial coefficients. Note that the previous composition commutes in the sense that $F^f_{X_{\bar{k}}} = \pi_X \circ \mathrm{Spec}(\mathrm{frob}_k) = \mathrm{Spec}(\mathrm{frob}_k) \circ \pi_X$. □

Definition 3.10. If $x \in X(k)$ is a rational point and $\bar{x} : \mathrm{Spec}(\bar{k}) \to X$ the geometric point lying over x, we let $\pi_x : \mathcal{F}_{\bar{x}} \to \mathcal{F}_{\bar{x}}$ denote the action by frob_k^{-1} and call it the *geometric frobenius*[1]

[1]This notation is not standard. This operator is denoted F_x in [Del77]. We will likely change this notation in the future.

We can now make a more precise statement (albeit a false one) of the trace formula (2.0.1). Let X be a finite type scheme of dimension 1 over a finite field k, ℓ a prime number and $\mathcal{F}$ a constructible, flat $\mathbf{Z}/\ell^n\mathbf{Z}$ sheaf. Then

$$\sum\nolimits_{x\in X(k)} \mathrm{Tr}(\pi_x|\mathcal{F}_{\bar{x}}) = \sum\nolimits_{i=0}^{2}(-1)^i\mathrm{Tr}(\pi_X^*|H_c^i(X_{\bar{k}},\mathcal{F})) \tag{3.10.1}$$

as elements of $\mathbf{Z}/\ell^n\mathbf{Z}$. The reason this equation is wrong is that the trace in the right-hand side does not make sense for the kind of sheaves considered. Before addressing this issue, we try to motivate the appearance of the geometric frobenius (apart from the fact that it is a natural morphism!).

Let us consider the case where $X = \mathbf{P}^1_k$ and $\mathcal{F} = \underline{\mathbf{Z}/\ell\mathbf{Z}}$. For any point, the Galois module $\mathcal{F}_{\bar{x}}$ is trivial, hence for any morphism φ acting on $\mathcal{F}_{\bar{x}}$, the left-hand side is

$$\sum\nolimits_{x\in X(k)} \mathrm{Tr}(\varphi|\mathcal{F}_{\bar{x}}) = \#\mathbf{P}^1_k(k) = q+1.$$

Now $\mathbf{P}^1_k$ is proper, so compactly supported cohomology equals standard cohomology, and so for a morphism $\pi : \mathbf{P}^1_k \to \mathbf{P}^1_k$, the right-hand side equals

$$\mathrm{Tr}(\pi^*|H^0(\mathbf{P}^1_{\bar{k}},\underline{\mathbf{Z}/\ell\mathbf{Z}})) + \mathrm{Tr}(\pi^*|H^2(\mathbf{P}^1_{\bar{k}},\underline{\mathbf{Z}/\ell\mathbf{Z}})).$$

The Galois module $H^0(\mathbf{P}^1_{\bar{k}},\underline{\mathbf{Z}/\ell\mathbf{Z}}) = \mathbf{Z}/\ell\mathbf{Z}$ is trivial, since the pullback of the identity is the identity. Hence the first trace is 1, regardless of π. For the second trace, we need to compute the pullback $\pi^* : H^2(\mathbf{P}^1_{\bar{k}},\underline{\mathbf{Z}/\ell\mathbf{Z}}))$ for a map $\pi : \mathbf{P}^1_{\bar{k}} \to \mathbf{P}^1_{\bar{k}}$. This is a good exercise and the answer is multiplication by the degree of π (for a proof see Étale Cohomology, Lemma 69.2). In other words, this works as in the familiar situation of complex cohomology. In particular, if π is the geometric frobenius we get

$$\mathrm{Tr}(\pi_X^*|H^2(\mathbf{P}^1_{\bar{k}},\underline{\mathbf{Z}/\ell\mathbf{Z}})) = q$$

and if π is the arithmetic frobenius then we get

$$\mathrm{Tr}(\mathrm{frob}_k^*|H^2(\mathbf{P}^1_{\bar{k}},\underline{\mathbf{Z}/\ell\mathbf{Z}})) = q^{-1}.$$

The latter option is clearly wrong.

Remark 3.11. The computation of the degrees can be done by lifting (in some obvious sense) to characteristic 0 and considering the situation with complex coefficients. This method almost never works, since lifting is in general impossible for schemes which are not projective space.

The question remains as to why we have to consider compactly supported cohomology. In fact, in view of Poincaré duality, it is not strictly necessary for smooth varieties, but it involves adding in certain powers of q. For example, let us consider the case where $X = \mathbf{A}^1_k$ and $\mathcal{F} = \underline{\mathbf{Z}/\ell\mathbf{Z}}$. The action on stalks is again trivial, so we only need look at the action on cohomology. But then π_X^* acts as the identity on $H^0(\mathbf{A}^1_{\bar{k}},\underline{\mathbf{Z}/\ell\mathbf{Z}})$ and as multiplication by q on $H^2_c(\mathbf{A}^1_{\bar{k}},\underline{\mathbf{Z}/\ell\mathbf{Z}})$.

4. Traces

We now explain how to take the trace of an endomorphism of a module over a noncommutative ring. Fix a finite ring Λ with cardinality prime to p. Typically, Λ is the group ring $(\mathbf{Z}/\ell^n\mathbf{Z})[G]$ for some finite group G. By convention, all the Λ-modules considered will be left Λ-modules.

We introduce the following notation: We set $\Lambda^\natural$ to be the quotient of Λ by its additive subgroup generated by the commutators (i.e., the elements of the form $ab - ba$, $a, b \in \Lambda$). Note that $\Lambda^\natural$ is not a ring.

For instance, the module $(\mathbf{Z}/\ell^n\mathbf{Z})[G]^\natural$ is the dual of the class functions, so

$$(\mathbf{Z}/\ell^n\mathbf{Z})[G]^\natural = \bigoplus\nolimits_{\text{conjugacy classes of } G} \mathbf{Z}/\ell^n\mathbf{Z}.$$

For a free Λ-module, we have $\mathrm{End}_\Lambda(\Lambda^{\oplus m}) = \mathrm{Mat}_n(\Lambda)$. Note that since the modules are left modules, representation of endomorphism by matrices is a right action: if $a \in \mathrm{End}(\Lambda^{\oplus m})$ has matrix A and $v \in \Lambda$, then $a(v) = vA$.

Definition 4.1. The *trace* of the endomorphism a is the sum of the diagonal entries of a matrix representing it. This defines an additive map $\mathrm{Tr} : \mathrm{End}_\Lambda(\Lambda^{\oplus m}) \to \Lambda^\natural$.

Exercise 4.2. Given maps

$$\Lambda^{\oplus m} \xrightarrow{a} \Lambda^{\oplus n} \quad \text{and} \quad \Lambda^{\oplus n} \xrightarrow{b} \Lambda^{\oplus m}$$

show that $\mathrm{Tr}(ab) = \mathrm{Tr}(ba)$.

We extend the definition of the trace to a finite projective Λ-module P and an endomorphism φ of P as follows. Write P as the summand of a free Λ-module, i.e., consider maps $P \xrightarrow{a} \Lambda^{\oplus n} \xrightarrow{b} P$ with

(1) $\Lambda^{\oplus n} = \mathrm{Im}(a) \oplus \mathrm{Ker}(b)$; and
(2) $b \circ a = \mathrm{id}_P$.

Then we set $\mathrm{Tr}(\varphi) = \mathrm{Tr}(a\varphi b)$. It is easy to check that this is well-defined, using the previous exercise.

5. Why derived categories?

With this definition of the trace, let us now discuss another issue with the formula as stated. Let C be a smooth projective curve over k. Then there is a correspondence between finite locally constant sheaves $\mathcal{F}$ on $C_{\acute{e}tale}$ whose stalks are isomorphic to $(\mathbf{Z}/\ell^n\mathbf{Z})^{\oplus m}$ on the one hand, and continuous representations $\rho : \pi_1(C, \bar{c}) \to \mathrm{GL}_m(\mathbf{Z}/\ell^n\mathbf{Z}))$ (for some fixed choice of $\bar{c}$) on the other hand. We denote $\mathcal{F}_\rho$ the sheaf corresponding to ρ. Then $H^2(C_{\bar{k}}, \mathcal{F}_\rho)$ is the group of coinvariants for the action of $\rho(\pi_1(C, \bar{c}))$ on $(\mathbf{Z}/\ell^n\mathbf{Z})^{\oplus m}$, and there is a short exact sequence

$$0 \longrightarrow \pi_1(C_{\bar{k}}, \bar{c}) \longrightarrow \pi_1(C, \bar{c}) \longrightarrow G_k \longrightarrow 0.$$

For instance, let $\mathbf{Z} = \mathbf{Z}\sigma$ act on $\mathbf{Z}/\ell^2\mathbf{Z}$ via $\sigma(x) = (1+\ell)x$. The coinvariants are $(\mathbf{Z}/\ell^2\mathbf{Z})_\sigma = \mathbf{Z}/\ell\mathbf{Z}$, which is not a flat $\mathbf{Z}/\ell^2\mathbf{Z}$-module. Hence we cannot take the trace of some action on $H^2(C_{\bar{k}}, \mathcal{F}_\rho)$, at least not in the sense of the previous section.

In fact, our goal is to consider a trace formula for ℓ-adic coefficients. But $\mathbf{Q}_\ell = \mathbf{Z}_\ell[1/\ell]$ and $\mathbf{Z}_\ell = \lim \mathbf{Z}/\ell^n\mathbf{Z}$, and even for a flat $\mathbf{Z}/\ell^n\mathbf{Z}$ sheaf, the individual cohomology groups may not be flat, so we cannot compute traces. One possible remedy is consider the total derived complex $R\Gamma(C_{\bar{k}}, \mathcal{F}_\rho)$ in the derived category $D(\mathbf{Z}/\ell^n\mathbf{Z})$ and show that it is a perfect object, which means that it is quasi-isomorphic to a finite complex of finite free module. For such complexes, we can define the trace, but this will require an account of derived categories.

6. Derived categories

To set up notation, let $\mathcal{A}$ be an abelian category. Let $\text{Comp}(\mathcal{A})$ be the abelian category of complexes in $\mathcal{A}$. Let $K(\mathcal{A})$ be the category of complexes up to homotopy, with objects equal to complexes in $\mathcal{A}$ and morphisms equal to homotopy classes of morphisms of complexes. This is not an abelian category. Loosely speaking, $D(A)$ is defined to be the category obtained by inverting all quasi-isomorphisms in $\text{Comp}(\mathcal{A})$ or, equivalently, in $K(\mathcal{A})$. Moreover, we can define $\text{Comp}^+(\mathcal{A}), K^+(\mathcal{A}), D^+(\mathcal{A})$ analogously using only bounded below complexes. Similarly, we can define $\text{Comp}^-(\mathcal{A}), K^-(\mathcal{A}), D^-(\mathcal{A})$ using bounded above complexes, and we can define $\text{Comp}^b(\mathcal{A}), K^b(\mathcal{A}), D^b(\mathcal{A})$ using bounded complexes.

Remark 6.1. Notes on derived categories.

(1) There are some set-theoretical problems when $\mathcal{A}$ is somewhat arbitrary, which we will happily disregard.
(2) The categories $K(A)$ and $D(A)$ are endowed with the structure of a triangulated category.
(3) The categories $\text{Comp}(A)$ and $K(A)$ can also be defined when $\mathcal{A}$ is an additive category.

The homology functor $H^i : \text{Comp}(\mathcal{A}) \to \mathcal{A}$ taking a complex $K^\bullet \mapsto H^i(K^\bullet)$ extends to functors $H^i : K(\mathcal{A}) \to \mathcal{A}$ and $H^i : D(\mathcal{A}) \to \mathcal{A}$.

Lemma 6.2. *An object E of $D(\mathcal{A})$ is contained in $D^+(\mathcal{A})$ if and only if $H^i(E) = 0$ for all $i \ll 0$. Similar statements hold for D^- and D^+.*

Proof. Hint: use truncation functors. See Derived Categories, Lemma 11.5. □

Lemma 6.3. *Morphisms between objects in the derived category.*

(1) *Let $I^\bullet \in$ Comp$^+(\mathcal{A})$ with I^n injective for all $n \in \mathbf{Z}$. Then*
$$\text{Hom}_{D(\mathcal{A})}(K^\bullet, I^\bullet) = \text{Hom}_{K(\mathcal{A})}(K^\bullet, I^\bullet).$$
(2) *Let $P^\bullet \in$ Comp$^-(\mathcal{A})$ with P^n is projective for all $n \in \mathbf{Z}$. Then*
$$\text{Hom}_{D(\mathcal{A})}(P^\bullet, K^\bullet) = \text{Hom}_{K(\mathcal{A})}(P^\bullet, K^\bullet).$$
(3) *If $\mathcal{A}$ has enough injectives and $\mathcal{I} \subset \mathcal{A}$ is the additive subcategory of injectives, then $D^+(\mathcal{A}) \cong K^+(\mathcal{I})$ (as triangulated categories).*
(4) *If $\mathcal{A}$ has enough projectives and $\mathcal{P} \subset \mathcal{A}$ is the additive subcategory of projectives, then $D^-(\mathcal{A}) \cong K^-(\mathcal{P})$.*

Proof. Omitted. □

Definition 6.4. Let $F : \mathcal{A} \to \mathcal{B}$ be a left exact functor and assume that $\mathcal{A}$ has enough injectives. We define the *total right derived functor of F* as the functor $RF : D^+(\mathcal{A}) \to D^+(\mathcal{B})$ fitting into the diagram

$$\begin{tikzcd} D^+(\mathcal{A}) \arrow[r, "RF"] & D^+(\mathcal{B}) \\ K^+(\mathcal{I}) \arrow[u] \arrow[r, "F"] & K^+(\mathcal{B}). \arrow[u] \end{tikzcd}$$

This is possible since the left vertical arrow is invertible by the previous lemma. Similarly, let $G : \mathcal{A} \to \mathcal{B}$ be a right exact functor and assume that $\mathcal{A}$ has enough projectives. We define the *total left derived functor of* G as the functor $LG : D^-(\mathcal{A}) \to D^-(\mathcal{B})$ fitting into the diagram

$$\begin{tikzcd} D^-(\mathcal{A}) \arrow[r, "LG"] & D^-(\mathcal{B}) \\ K^-(\mathcal{P}) \arrow[u] \arrow[r, "G"] & K^-(\mathcal{B}). \arrow[u] \end{tikzcd}$$

This is possible since the left vertical arrow is invertible by the previous lemma.

Remark 6.5. In these cases, it is true that $R^iF(K^\bullet) = H^i(RF(K^\bullet))$, where the left hand side is defined to be ith homology of the complex $F(K^\bullet)$.

7. Filtered derived category

It turns out we have to do it all again and build the filtered derived category also.

Definition 7.1. Let $\mathcal{A}$ be an abelian category.

(1) Let $\mathrm{Fil}(\mathcal{A})$ be the category of filtered objects (A, F) of $\mathcal{A}$, where F is a filtration of the form

$$A \supset \ldots \supset F^nA \supset F^{n+1}A \supset \ldots \supset 0.$$

This is an additive category.

(2) We denote $\mathrm{Fil}^f(\mathcal{A})$ the full subcategory of $\mathrm{Fil}(\mathcal{A})$ whose objects (A, F) have finite filtration. This is also an additive category.

(3) An object $I \in \mathrm{Fil}^f(\mathcal{A})$ is called *filtered injective* (respectively *projective*) provided that $\mathrm{gr}^p(I) = \mathrm{gr}^p_F(I) = F^pI/F^{p+1}I$ is injective (resp. projective) in $\mathcal{A}$ for all p.

(4) The category of complexes $\mathrm{Comp}(\mathrm{Fil}^f(\mathcal{A})) \supset \mathrm{Comp}^+(\mathrm{Fil}^f(\mathcal{A}))$ and its homotopy category $K(\mathrm{Fil}^f(\mathcal{A})) \supset K^+(\mathrm{Fil}^f(\mathcal{A}))$ are defined as before.

(5) A morphism $\alpha : K^\bullet \to L^\bullet$ of complexes in $\mathrm{Comp}(\mathrm{Fil}^f(\mathcal{A}))$ is called a *filtered quasi-isomorphism* provided that

$$\mathrm{gr}^p(\alpha) : \mathrm{gr}^p(K^\bullet) \to \mathrm{gr}^p(L^\bullet)$$

is a quasi-isomorphism for all $p \in \mathbf{Z}$.

(6) We define $DF(\mathcal{A})$ (resp. $DF^+(\mathcal{A})$) by inverting the filtered quasi-isomorphisms in $K(\mathrm{Fil}^f(\mathcal{A}))$ (resp. $K^+(\mathrm{Fil}^f(\mathcal{A}))$).

Lemma 7.2. *If $\mathcal{A}$ has enough injectives, then $DF^+(\mathcal{A}) \cong K^+(\mathcal{I})$, where $\mathcal{I}$ is the full additive subcategory of $\mathit{Fil}^f(\mathcal{A})$ consisting of filtered injective objects. Similarly, if $\mathcal{A}$ has enough projectives, then $DF^-(\mathcal{A}) \cong K^+(\mathcal{P})$, where $\mathcal{P}$ is the full additive subcategory of $\mathit{Fil}^f(\mathcal{A})$ consisting of filtered projective objects.*

Proof. Omitted. □

8. Filtered derived functors

And then there are the filtered derived functors.

Definition 8.1. Let $T : \mathcal{A} \to \mathcal{B}$ be a left exact functor and assume that $\mathcal{A}$ has enough injectives. Define $RT : DF^+(\mathcal{A}) \to DF^+(\mathcal{B})$ to fit in the diagram

$$\begin{tikzcd} DF^+(\mathcal{A}) \arrow[r, "RT"] & DF^+(\mathcal{B}) \\ K^+(\mathcal{I}) \arrow[u] \arrow[r, "T"] & K^+(\mathrm{Fil}^f(\mathcal{B})). \arrow[u] \end{tikzcd}$$

This is well-defined by the previous lemma. Let $G : \mathcal{A} \to \mathcal{B}$ be a right exact functor and assume that $\mathcal{A}$ has enough projectives. Define $LG : DF^+(\mathcal{A}) \to DF^+(\mathcal{B})$ to fit in the diagram

$$\begin{tikzcd} DF^-(\mathcal{A}) \arrow[r, "LG"] & DF^-(\mathcal{B}) \\ K^-(\mathcal{P}) \arrow[u] \arrow[r, "G"] & K^-(\mathrm{Fil}^f(\mathcal{B})). \arrow[u] \end{tikzcd}$$

Again, this is well-defined by the previous lemma. The functors RT, resp. LG, are called the *filtered derived functor* of T, resp. G.

Proposition 8.2. *In the situation above, we have*

$$gr^p \circ RT = RT \circ gr^p$$

where the RT on the left is the filtered derived functor while the one on the right is the total derived functor. That is, there is a commuting diagram

$$\begin{tikzcd} DF^+(\mathcal{A}) \arrow[r, "RT"] \arrow[d, "gr^p"'] & DF^+(\mathcal{B}) \arrow[d, "gr^p"] \\ D^+(\mathcal{A}) \arrow[r, "RT"] & D^+(\mathcal{B}). \end{tikzcd}$$

Proof. Omitted. □

Given $K^\bullet \in DF^+(\mathcal{B})$, we get a spectral sequence

$$E_1^{p,q} = H^{p+q}(\mathrm{gr}^p K^\bullet) \Rightarrow H^{p+q}(\text{forget filt}(K^\bullet)).$$

9. Application of filtered complexes

Let $\mathcal{A}$ be an abelian category with enough injectives, and $0 \to L \to M \to N \to 0$ a short exact sequence in $\mathcal{A}$. Consider $\widetilde{M} \in \mathrm{Fil}^f(\mathcal{A})$ to be M along with the filtration defined by

$$F^1 M = L,\ F^n M = M \text{ for } n \leq 0, \text{ and } F^n M = 0 \text{ for } n \geq 2.$$

By definition, we have

$$\text{forget filt}(\widetilde{M}) = M, \quad \mathrm{gr}^0(\widetilde{M}) = N, \quad \mathrm{gr}^1(\widetilde{M}) = L$$

and $\mathrm{gr}^n(\widetilde{M}) = 0$ for all other $n \neq 0, 1$. Let $T : \mathcal{A} \to \mathcal{B}$ be a left exact functor. Assume that $\mathcal{A}$ has enough injectives. Then $RT(\widetilde{M}) \in DF^+(\mathcal{B})$ is a filtered complex with

$$\mathrm{gr}^p(RT(\widetilde{M})) \overset{\text{qis}}{=} \begin{cases} 0 & \text{if } \ p \neq 0, 1, \\ RT(N) & \text{if } \ p = 0, \\ RT(L) & \text{if } \ p = 1. \end{cases}$$

and forget $\mathrm{filt}(RT(\widetilde{M})) \stackrel{\mathrm{qis}}{=} RT(M)$. The spectral sequence applied to $RT(\widetilde{M})$ gives

$$E_1^{p,q} = R^{p+q}T(\mathrm{gr}^p(\widetilde{M})) \Rightarrow R^{p+q}T(\text{forget filt}(\widetilde{M})).$$

Unwinding the spectral sequence gives us the long exact sequence

$$\begin{tikzcd} 0 \arrow[r] & T(L) \arrow[r] & T(M) \arrow[r] & T(N) \arrow[dll, out=-90, in=90] \\ & R^1T(L) \arrow[r] & R^1T(M) \arrow[r] & \ldots \end{tikzcd}$$

This will be used as follows. Let X/k be a scheme of finite type. Let $\mathcal{F}$ be a flat constructible $\mathbf{Z}/\ell^n\mathbf{Z}$-module. Then we want to show that the trace

$$\mathrm{Tr}(\pi_X^* | R\Gamma_c(X_{\bar{k}}, \mathcal{F})) \in \mathbf{Z}/\ell^n\mathbf{Z}$$

is additive on short exact sequences. To see this, it will not be enough to work with $R\Gamma_c(X_{\bar{k}}, -) \in D^+(\mathbf{Z}/\ell^n\mathbf{Z})$, but we will have to use the filtered derived category.

10. Perfectness

Let Λ be a (possibly noncommutative) ring, Mod_Λ the category of left Λ-modules, $K(\Lambda) = K(\mathrm{Mod}_\Lambda)$ its homotopy category, and $D(\Lambda) = D(\mathrm{Mod}_\Lambda)$ the derived category.

Definition 10.1. We denote by $K_{perf}(\Lambda)$ the category whose objects are bounded complexes of finite projective Λ-modules, and whose morphisms are morphisms of complexes up to homotopy. The functor $K_{perf}(\Lambda) \to D(\Lambda)$ is fully faithful (Derived Categories, Lemma 19.8). Denote $D_{perf}(\Lambda)$ its essential image. An object of $D(\Lambda)$ is called *perfect* if it is in $D_{perf}(\Lambda)$.

Proposition 10.2. *Let $K \in D_{perf}(\Lambda)$ and $f \in End_{D(\Lambda)}(K)$. Then the trace $Tr(f) \in \Lambda^\natural$ is well defined.*

Proof. We will use Derived Categories, Lemma 19.8 without further mention in this proof. Let $P^\bullet$ be a bounded complex of finite projective Λ-modules and let $\alpha : P^\bullet \to K$ be an isomorphism in $D(\Lambda)$. Then $\alpha^{-1} \circ f \circ \alpha$ corresponds to a morphism of complexes $f^\bullet : P^\bullet \to P^\bullet$ well defined up to homotopy. Set

$$\mathrm{Tr}(f) = \sum_i (-1)^i \mathrm{Tr}(f^i : P^i \to P^i) \in \Lambda^\natural.$$

Given $P^\bullet$ and α, this is independent of the choice of $f^\bullet$. Namely, any other choice is of the form $\tilde{f}^\bullet = f^\bullet + dh + hd$ for some $h^i : P^i \to P^{i-1} (i \in \mathbf{Z})$. But

$$\begin{aligned} \mathrm{Tr}(dh) &= \sum_i (-1)^i \mathrm{Tr}(P^i \xrightarrow{dh} P^i) \\ &= \sum_i (-1)^i \mathrm{Tr}(P^{i-1} \xrightarrow{hd} P^{i-1}) \\ &= -\sum_i (-1)^{i-1} \mathrm{Tr}(P^{i-1} \xrightarrow{hd} P^{i-1}) \\ &= -\mathrm{Tr}(hd) \end{aligned}$$

and so $\sum_i (-1)^i \text{Tr}((dh+hd)|_{P^i}) = 0$. Furthermore, this is independent of the choice of $(P^\bullet, \alpha)$: suppose $(Q^\bullet, \beta)$ is another choice. The compositions

$$Q^\bullet \xrightarrow{\beta} K \xrightarrow{\alpha^{-1}} P^\bullet \quad \text{and} \quad P^\bullet \xrightarrow{\alpha} K \xrightarrow{\beta^{-1}} Q^\bullet$$

are representable by morphisms of complexes $\gamma_1^\bullet$ and $\gamma_2^\bullet$ respectively, such that $\gamma_1^\bullet \circ \gamma_2^\bullet$ is homotopic to the identity. Thus, the morphism of complexes $\gamma_2^\bullet \circ f^\bullet \circ \gamma_1^\bullet : Q^\bullet \to Q^\bullet$ represents the morphism $\beta^{-1} \circ f \circ \beta$ in $D(\Lambda)$. Now

$$\begin{aligned} \text{Tr}(\gamma_2^\bullet \circ f^\bullet \circ \gamma_1^\bullet|_{Q^\bullet}) &= \text{Tr}(\gamma_1^\bullet \circ \gamma_2^\bullet \circ f^\bullet|_{P^\bullet}) \\ &= \text{Tr}(f^\bullet|_{P^\bullet}) \end{aligned}$$

by the fact that $\gamma_1^\bullet \circ \gamma_2^\bullet$ is homotopic to the identity and the independence of the choice of $f^\bullet$ we saw above. □

11. Filtrations and perfect complexes

We now present a filtered version of the category of perfect complexes. An object (M, F) of $\text{Fil}^f(\text{Mod}_\Lambda)$ is called *filtered finite projective* if for all p, $\text{gr}^p_F(M)$ is finite and projective. We then consider the homotopy category $KF_{\text{perf}}(\Lambda)$ of bounded complexes of filtered finite projective objects of $\text{Fil}^f(\text{Mod}_\Lambda)$. We have a diagram of categories

$$\begin{array}{ccc} KF(\Lambda) & \supset & KF_{\text{perf}}(\Lambda) \\ \downarrow & & \downarrow \\ DF(\Lambda) & \supset & DF_{\text{perf}}(\Lambda) \end{array}$$

where the vertical functor on the right is fully faithful and the category $DF_{\text{perf}}(\Lambda)$ is its essential image, as before.

Lemma 11.1 (Additivity). *Let $K \in DF_{perf}(\Lambda)$ and $f \in End_{DF}(K)$. Then*

$$Tr(f|_K) = \sum\nolimits_{p \in \mathbf{Z}} Tr(f|_{gr^p K}).$$

Proof. By Proposition 10.2, we may assume we have a bounded complex $P^\bullet$ of filtered finite projectives of $\text{Fil}^f(\text{Mod}_\Lambda)$ and a map $f^\bullet : P^\bullet \to P^\bullet$ in $\text{Comp}(\text{Fil}^f(\text{Mod}_\Lambda))$. So the lemma follows from the following result, which proof is left to the reader. □

Lemma 11.2. *Let $P \in Fil^f(Mod_\Lambda)$ be filtered finite projective, and $f : P \to P$ an endomorphism in $Fil^f(Mod_\Lambda)$. Then*

$$Tr(f|_P) = \sum\nolimits_p Tr(f|_{gr^p(P)}).$$

Proof. Omitted. □

12. Characterizing perfect objects

For the commutative case see More on Algebra, Sections 64, 66, and 74.

Definition 12.1. Let Λ be a (possibly noncommutative) ring. An object $K \in D(\Lambda)$ has *finite Tor-dimension* if there exist $a, b \in \mathbf{Z}$ such that for any right Λ-module N, we have $H^i(N \otimes^{\mathbf{L}}_\Lambda K) = 0$ for all $i \notin [a, b]$.

This in particular means that $K \in D^b(\Lambda)$ as we see by taking $N = \Lambda$.

Lemma 12.2. *Let Λ be a left Noetherian ring and $K \in D(\Lambda)$. Then K is perfect if and only if the two following conditions hold:*

(1) *K has finite Tor-dimension, and*
(2) *for all $i \in \mathbf{Z}$, $H^i(K)$ is a finite Λ-module.*

Proof. See More on Algebra, Lemma 74.2 for the proof in the commutative case. $\square$

The reader is strongly urged to try and prove this. The proof relies on the fact that a finite module on a finitely left-presented ring is flat if and only if it is projective.

Remark 12.3. A variant of this lemma is to consider a Noetherian scheme X and the category $D_{perf}(\mathcal{O}_X)$ of complexes which are locally quasi-isomorphic to a finite complex of finite locally free $\mathcal{O}_X$-modules. Objects K of $D_{perf}(\mathcal{O}_X)$ can be characterized by having coherent cohomology sheaves and bounded tor dimension.

13. Cohomology of nice complexes

The following is a special case of a more general result about compactly supported cohomology of objects of $D_{ctf}(X, \Lambda)$.

Proposition 13.1. *Let X be a projective curve over a field k, Λ a finite ring and $K \in D_{ctf}(X, \Lambda)$. Then $R\Gamma(X_{\bar{k}}, K) \in D_{perf}(\Lambda)$.*

Sketch of proof. The first step is to show:

(1) *The cohomology of $R\Gamma(X_{\bar{k}}, K)$ is bounded.*

Consider the spectral sequence

$$H^i(X_{\bar{k}}, \underline{H}^j(K)) \Rightarrow H^{i+j}(R\Gamma(X_{\bar{k}}, K)).$$

Since K is bounded and Λ is finite, the sheaves $\underline{H}^j(K)$ are torsion. Moreover, $X_{\bar{k}}$ has finite cohomological dimension, so the left-hand side is nonzero for finitely many i and j only. Therefore, so is the right-hand side.

(2) *The cohomology groups $H^{i+j}(R\Gamma(X_{\bar{k}}, K))$ are finite.*

Since the sheaves $\underline{H}^j(K)$ are constructible, the groups $H^i(X_{\bar{k}}, \underline{H}^j(K))$ are finite (Étale Cohomology, Section 83) so it follows by the spectral sequence again.

(3) *$R\Gamma(X_{\bar{k}}, K)$ has finite Tor-dimension.*

Let N be a right Λ-module (in fact, since Λ is finite, it suffices to assume that N is finite). By the projection formula (change of module),

$$N \otimes_\Lambda^{\mathbf{L}} R\Gamma(X_{\bar{k}}, K) = R\Gamma(X_{\bar{k}}, N \otimes_\Lambda^{\mathbf{L}} K).$$

Therefore,

$$H^i(N \otimes_\Lambda^{\mathbf{L}} R\Gamma(X_{\bar{k}}, K)) = H^i(R\Gamma(X_{\bar{k}}, N \otimes_\Lambda^{\mathbf{L}} K)).$$

Now consider the spectral sequence

$$H^i(X_{\bar{k}}, \underline{H}^j(N \otimes_\Lambda^{\mathbf{L}} K)) \Rightarrow H^{i+j}(R\Gamma(X_{\bar{k}}, N \otimes_\Lambda^{\mathbf{L}} K)).$$

Since K has finite Tor-dimension, $\underline{H}^j(N \otimes_\Lambda^{\mathbf{L}} K)$ vanishes universally for j small enough, and the left-hand side vanishes whenever $i < 0$. Therefore $R\Gamma(X_{\bar{k}}, K)$ has finite Tor-dimension, as claimed. So it is a perfect complex by Lemma 12.2. $\square$

14. Lefschetz numbers

The fact that the total cohomology of a constructible complex of finite tor dimension is a perfect complex is the key technical reason why cohomology behaves well, and allows us to define rigorously the traces occurring in the trace formula.

Definition 14.1. Let Λ be a finite ring, X a projective curve over a finite field k and $K \in D_{ctf}(X, \Lambda)$ (for instance $K = \underline{\Lambda}$). There is a canonical map $c_K : \pi_X^{-1} K \to K$, and its base change $c_K|_{X_{\bar{k}}}$ induces an action denoted π_X^* on the perfect complex $R\Gamma(X_{\bar{k}}, K|_{X_{\bar{k}}})$. The *global Lefschetz number* of K is the trace $\mathrm{Tr}(\pi_X^*|_{R\Gamma(X_{\bar{k}}, K)})$ of that action. It is an element of $\Lambda^\natural$.

Definition 14.2. With Λ, X, k, K as in Definition 14.1. Since $K \in D_{ctf}(X, \Lambda)$, for any geometric point $\bar{x}$ of X, the complex $K_{\bar{x}}$ is a perfect complex (in $D_{perf}(\Lambda)$). As we have seen in Section 3, the Frobenius π_X acts on $K_{\bar{x}}$. The *local Lefschetz number* of K is the sum

$$\sum\nolimits_{x \in X(k)} \mathrm{Tr}(\pi_X|_{K_{\overline{x}}})$$

which is again an element of $\Lambda^\natural$.

At last, we can formulate precisely the trace formula.

Theorem 14.3 (Lefschetz Trace Formula)**.** *Let X be a projective curve over a finite field k, Λ a finite ring and $K \in D_{ctf}(X, \Lambda)$. Then the global and local Lefschetz numbers of K are equal, i.e.,*

$$Tr(\pi_X^*|_{R\Gamma(X_{\bar{k}}, K)}) = \sum\nolimits_{x \in X(k)} Tr(\pi_X|_{K_{\bar{x}}}) \tag{14.3.1}$$

in $\Lambda^\natural$.

Proof. See discussion below. $\square$

We will use, rather than prove, the trace formula. Nevertheless, we will give quite a few details of the proof of the theorem as given in [Del77] (some of the things that are not adequately explained are listed in Section 21).

We only stated the formula for curves, and in some weak sense it is a consequence of the following result.

Theorem 14.4 (Weil)**.** *Let C be a nonsingular projective curve over an algebraically closed field k, and $\varphi : C \to C$ a k-endomorphism of C distinct from the identity. Let $V(\varphi) = \Delta_C \cdot \Gamma_\varphi$, where Δ_C is the diagonal, Γ_φ is the graph of φ, and the intersection number is taken on $C \times C$. Let $J = \underline{\mathrm{Pic}}^0_{C/k}$ be the jacobian of C and denote $\varphi^* : J \to J$ the action induced by φ by taking pullbacks. Then*

$$V(\varphi) = 1 - Tr_J(\varphi^*) + \deg \varphi.$$

Proof. The number $V(\varphi)$ is the number of fixed points of φ, it is equal to

$$V(\varphi) = \sum\nolimits_{c \in |C| : \varphi(c) = c} m_{\mathrm{Fix}(\varphi)}(c)$$

where $m_{\mathrm{Fix}(\varphi)}(c)$ is the multiplicity of c as a fixed point of φ, namely the order or vanishing of the image of a local uniformizer under $\varphi - \mathrm{id}_C$. Proofs of this theorem can be found in [Lan02] and [Wei48]. $\square$

Example 14.5. Let $C = E$ be an elliptic curve and $\varphi = [n]$ be multiplication by n. Then $\varphi^* = \varphi^t$ is multiplication by n on the jacobian, so it has trace $2n$ and degree n^2. On the other hand, the fixed points of φ are the points $p \in E$ such that $np = p$, which is the $(n-1)$-torsion, which has cardinality $(n-1)^2$. So the theorem reads

$$(n-1)^2 = 1 - 2n + n^2.$$

Jacobians. We now discuss without proofs the correspondence between a curve and its jacobian which is used in Weil's proof. Let C be a nonsingular projective curve over an algebraically closed field k and choose a base point $c_0 \in C(k)$. Denote by $A^1(C \times C)$ (or $\mathrm{Pic}(C \times C)$, or $\mathrm{CaCl}(C \times C)$) the abelian group of codimension 1 divisors of $C \times C$. Then

$$A^1(C \times C) = \mathrm{pr}_1^*(A^1(C)) \oplus \mathrm{pr}_2^*(A^1(C)) \oplus R$$

where

$$R = \{Z \in A^1(C \times C) \mid Z|_{C \times \{c_0\}} \sim_{\mathrm{rat}} 0 \text{ and } Z|_{\{c_0\} \times C} \sim_{\mathrm{rat}} 0\}.$$

In other words, R is the subgroup of line bundles which pull back to the trivial one under either projection. Then there is a canonical isomorphism of abelian groups $R \cong \mathrm{End}(J)$ which maps a divisor Z in R to the endomorphism

$$\begin{array}{ccc} J & \to & J \\ [\mathcal{O}_C(D)] & \mapsto & (\mathrm{pr}_1|_Z)_*(\mathrm{pr}_2|_Z)^*(D). \end{array}$$

The aforementioned correspondence is the following. We denote by σ the automorphism of $C \times C$ that switches the factors.

$\mathrm{End}(J)$	R
composition of α, β	$\mathrm{pr}_{13*}(\mathrm{pr}_{12}{}^*(\alpha) \circ \mathrm{pr}_{23}{}^*(\beta))$
id_J	$\Delta_C - \{c_0\} \times C - C \times \{c_0\}$
φ^*	$\Gamma_\varphi - C \times \{\varphi(c_0)\} - \sum_{\varphi(c)=c_0} \{c\} \times C$
the trace form $\alpha, \beta \mapsto \mathrm{Tr}(\alpha\beta)$	$\alpha, \beta \mapsto -\int_{C \times C} \alpha.\sigma^*\beta$
the Rosati involution $\alpha \mapsto \alpha^\dagger$	$\alpha \mapsto \sigma^*\alpha$
positivity of Rosati $\mathrm{Tr}(\alpha\alpha^\dagger) > 0$	Hodge index theorem on $C \times C$ $-\int_{C \times C} \alpha\sigma^*\alpha > 0.$

In fact, in light of the Kunneth formula, the subgroup R corresponds to the $1,1$ hodge classes in $H^1(C) \otimes H^1(C)$.

Weil's proof. Using this correspondence, we can prove the trace formula. We have

$$\begin{aligned} V(\varphi) &= \int_{C\times C} \Gamma_\varphi.\Delta \\ &= \int_{C\times C} \Gamma_\varphi.\left(\Delta_C - \{c_0\}\times C - C\times\{c_0\}\right) + \int_{C\times C} \Gamma_\varphi.\left(\{c_0\}\times C + C\times\{c_0\}\right). \end{aligned}$$

Now, on the one hand

$$\int_{C\times C} \Gamma_\varphi.\left(\{c_0\}\times C + C\times\{c_0\}\right) = 1 + \deg\varphi$$

and on the other hand, since R is the orthogonal of the ample divisor $\{c_0\}\times C + C\times\{c_0\}$,

$$\begin{aligned} &\int_{C\times C} \Gamma_\varphi.\left(\Delta_C - \{c_0\}\times C - C\times\{c_0\}\right) \\ = &\int_{C\times C} \left(\Gamma_\varphi - C\times\{\varphi(c_0)\} - \sum_{\varphi(c)=c_0}\{c\}\times C\right).\left(\Delta_C - \{c_0\}\times C - C\times\{c_0\}\right) \\ = &-\mathrm{Tr}_J(\varphi^*\circ \mathrm{id}_J). \end{aligned}$$

Recapitulating, we have

$$V(\varphi) = 1 - \mathrm{Tr}_J(\varphi^*) + \deg\varphi$$

which is the trace formula.

Lemma 14.6. *Consider the situation of Theorem 14.4 and let ℓ be a prime number invertible in k. Then*

$$\sum\nolimits_{i=0}^{2}(-1)^i\, Tr(\varphi^*|_{H^i(C,\underline{\mathbf{Z}/\ell^n\mathbf{Z}})}) = V(\varphi) \mod \ell^n.$$

Sketch of proof. Observe first that the assumption makes sense because $H^i(C,\underline{\mathbf{Z}/\ell^n\mathbf{Z}})$ is a free $\mathbf{Z}/\ell^n\mathbf{Z}$-module for all i. The trace of φ^* on the 0th degree cohomology is 1. The choice of a primitive ℓ^nth root of unity in k gives an isomorphism

$$H^i(C,\underline{\mathbf{Z}/\ell^n\mathbf{Z}}) \cong H^i(C,\mu_{\ell^n})$$

compatibly with the action of the geometric Frobenius. On the other hand, $H^1(C,\mu_{\ell^n}) = J[\ell^n]$. Therefore,

$$\begin{aligned} \mathrm{Tr}(\varphi^*|_{H^1(C,\underline{\mathbf{Z}/\ell^n\mathbf{Z}})})) &= \mathrm{Tr}_J(\varphi^*) \mod \ell^n \\ &= \mathrm{Tr}_{\mathbf{Z}/\ell^n\mathbf{Z}}(\varphi^* : J[\ell^n]\to J[\ell^n]). \end{aligned}$$

Moreover, $H^2(C,\mu_{\ell^n}) = \mathrm{Pic}(C)/\ell^n\,\mathrm{Pic}(C) \cong \mathbf{Z}/\ell^n\mathbf{Z}$ where φ^* is multiplication by $\deg\varphi$. Hence

$$\mathrm{Tr}(\varphi^*|_{H^2(C,\underline{\mathbf{Z}/\ell^n\mathbf{Z}})}) = \deg\varphi.$$

Thus we have

$$\sum_{i=0}^{2}(-1)^i\mathrm{Tr}(\varphi^*|_{H^i(C,\underline{\mathbf{Z}/\ell^n\mathbf{Z}})}) = 1 - \mathrm{Tr}_J(\varphi^*) + \deg\varphi \mod \ell^n$$

and the corollary follows from Theorem 14.4. $\square$

An alternative way to prove this corollary is to show that

$$X \mapsto H^*(X, \mathbf{Q}_\ell) = \mathbf{Q}_\ell \otimes \lim_n H^*(X, \mathbf{Z}/\ell^n\mathbf{Z})$$

defines a Weil cohomology theory on smooth projective varieties over k. Then the trace formula

$$V(\varphi) = \sum_{i=0}^{2} (-1)^i \mathrm{Tr}(\varphi^*|_{H^i(C,\mathbf{Q}_\ell)})$$

is a formal consequence of the axioms (it's an exercise in linear algebra, the proof is the same as in the topological case).

15. Preliminaries and sorites

Notation: We fix the notation for this section. We denote by A a commutative ring, Λ a (possibly noncommutative) ring with a ring map $A \to \Lambda$ which image lies in the center of Λ. We let G be a finite group, Γ a *monoid extension of G by* $\mathbf{N}$, meaning that there is an exact sequence

$$1 \to G \to \tilde{\Gamma} \to \mathbf{Z} \to 1$$

and Γ consists of those elements of $\tilde{\Gamma}$ which image is nonnegative. Finally, we let P be an $A[\Gamma]$-module which is finite and projective as an $A[G]$-module, and M a $\Lambda[\Gamma]$-module which is finite and projective as a Λ-module.

Our goal is to compute the trace of $1 \in \mathbf{N}$ acting over Λ on the coinvariants of G on $P \otimes_A M$, that is, the number

$$\mathrm{Tr}_\Lambda \left(1; (P \otimes_A M)_G\right) \in \Lambda^\natural.$$

The element $1 \in \mathbf{N}$ will correspond to the Frobenius.

Lemma 15.1. *Let $e \in G$ denote the neutral element. The map*

$$\begin{array}{ccc} \Lambda[G] & \longrightarrow & \Lambda^\natural \\ \sum \lambda_g \cdot g & \longmapsto & \lambda_e \end{array}$$

factors through $\Lambda[G]^\natural$. We denote $\varepsilon : \Lambda[G]^\natural \to \Lambda^\natural$ the induced map.

Proof. We have to show the map annihilates commutators. One has

$$\left(\sum \lambda_g g\right)\left(\sum \mu_g g\right) - \left(\sum \mu_g g\right)\left(\sum \lambda_g g\right) = \sum_g \left(\sum_{g_1 g_2 = g} \lambda_{g_1}\mu_{g_2} - \mu_{g_1}\lambda_{g_2}\right) g$$

The coefficient of e is

$$\sum_g \left(\lambda_g \mu_{g^{-1}} - \mu_g \lambda_{g^{-1}}\right) = \sum_g \left(\lambda_g \mu_{g^{-1}} - \mu_{g^{-1}} \lambda_g\right)$$

which is a sum of commutators, hence it zero in $\Lambda^\natural$. □

Definition 15.2. Let $f : P \to P$ be an endomorphism of a finite projective $\Lambda[G]$-module P. We define

$$\mathrm{Tr}_\Lambda^G(f; P) := \varepsilon\left(\mathrm{Tr}_{\Lambda[G]}(f; P)\right)$$

to be the *G-trace of f on* P.

Lemma 15.3. *Let $f : P \to P$ be an endomorphism of the finite projective $\Lambda[G]$-module P. Then*

$$Tr_\Lambda(f; P) = \#G \cdot Tr_\Lambda^G(f; P).$$

Proof. By additivity, reduce to the case $P = \Lambda[G]$. In that case, f is given by right multiplication by some element $\sum \lambda_g \cdot g$ of $\Lambda[G]$. In the basis $(g)_{g\in G}$, the matrix of f has coefficient $\lambda_{g_2^{-1}g_1}$ in the (g_1, g_2) position. In particular, all diagonal coefficients are λ_e, and there are $\#G$ such coefficients. $\square$

Lemma 15.4. *The map $A \to \Lambda$ defines an A-module structure on $\Lambda^\natural$.*

Proof. This is clear. $\square$

Lemma 15.5. *Let P be a finite projective $A[G]$-module and M a $\Lambda[G]$-module, finite projective as a Λ-module. Then $P \otimes_A M$ is a finite projective $\Lambda[G]$-module, for the structure induced by the diagonal action of G.*

Note that $P \otimes_A M$ is naturally a Λ-module since M is. Explicitly, together with the diagonal action this reads

$$\left(\sum \lambda_g g\right)(p \otimes m) = \sum gp \otimes \lambda_g gm.$$

Proof. For any $\Lambda[G]$-module N one has

$$\mathrm{Hom}_{\Lambda[G]}\left(P \otimes_A M, N\right) = \mathrm{Hom}_{A[G]}\left(P, \mathrm{Hom}_\Lambda(M, N)\right)$$

where the G-action on $\mathrm{Hom}_\Lambda(M, N)$ is given by $(g \cdot \varphi)(m) = g\varphi(g^{-1}m)$. Now it suffices to observe that the right-hand side is a composition of exact functors, because of the projectivity of P and M. $\square$

Lemma 15.6. *With assumptions as in Lemma 15.5, let $u \in End_{A[G]}(P)$ and $v \in End_{\Lambda[G]}(M)$. Then*

$$Tr^G_\Lambda\left(u \otimes v; P \otimes_A M\right) = Tr^G_A(u; P) \cdot Tr_\Lambda(v; M).$$

Sketch of proof. Reduce to the case $P = A[G]$. In that case, u is right multiplication by some element $a = \sum a_g g$ of $A[G]$, which we write $u = R_a$. There is an isomorphism of $\Lambda[G]$-modules

$$\begin{array}{cccc} \varphi: & A[G] \otimes_A M & \cong & (A[G] \otimes_A M)' \\ & g \otimes m & \longmapsto & g \otimes g^{-1}m \end{array}$$

where $(A[G] \otimes_A M)'$ has the module structure given by the left G-action, together with the Λ-linearity on M. This transport of structure changes $u \otimes v$ into $\sum_g a_g R_g \otimes g^{-1}v$. In other words,

$$\varphi \circ (u \otimes v) \circ \varphi^{-1} = \sum_g a_g R_g \otimes g^{-1}v.$$

Working out explicitly both sides of the equation, we have to show

$$\mathrm{Tr}^G_\Lambda\left(\sum_g a_g R_g \otimes g^{-1}v\right) = a_e \cdot \mathrm{Tr}_\Lambda(v; M).$$

This is done by showing that

$$\mathrm{Tr}^G_\Lambda\left(a_g R_g \otimes g^{-1}v\right) = \begin{cases} 0 & \text{if } g \neq e \\ a_e \mathrm{Tr}_\Lambda(v; M) & \text{if } g = e \end{cases}$$

by reducing to $M = \Lambda$. $\square$

Notation: Consider the monoid extension $1 \to G \to \Gamma \to \mathbf{N} \to 1$ and let $\gamma \in \Gamma$. Then we write $Z_\gamma = \{g \in G | g\gamma = \gamma g\}$.

Lemma 15.7. *Let P be a $\Lambda[\Gamma]$-module, finite and projective as a $\Lambda[G]$-module, and $\gamma \in \Gamma$. Then*

$$Tr_\Lambda(\gamma, P) = \#Z_\gamma \cdot Tr_\Lambda^{Z_\gamma}(\gamma, P)\,.$$

Proof. This follows readily from Lemma 15.3. □

Lemma 15.8. *Let P be an $A[\Gamma]$-module, finite projective as $A[G]$-module. Let M be a $\Lambda[\Gamma]$-module, finite projective as a Λ-module. Then*

$$Tr_\Lambda^{Z_\gamma}(\gamma, P \otimes_A M) = Tr_A^{Z_\gamma}(\gamma, P) \cdot Tr_\Lambda(\gamma, M).$$

Proof. This follows directly from Lemma 15.6. □

Lemma 15.9. *Let P be a $\Lambda[\Gamma]$-module, finite projective as $\Lambda[G]$-module. Then the coinvariants $P_G = \Lambda \otimes_{\Lambda[G]} P$ form a finite projective Λ-module, endowed with an action of $\Gamma/G = \mathbf{N}$. Moreover, we have*

$$Tr_\Lambda(1; P_G) = {\sum}'_{\gamma \mapsto 1} Tr_\Lambda^{Z_\gamma}(\gamma, P)$$

where ${\sum}'_{\gamma\mapsto 1}$ means taking the sum over the G-conjugacy classes in Γ.

Sketch of proof. We first prove this after multiplying by $\#G$.

$$\#G \cdot \mathrm{Tr}_\Lambda(1; P_G) = \mathrm{Tr}_\Lambda\Big(\sum_{\gamma\mapsto 1}\gamma, P_G\Big) = \mathrm{Tr}_\Lambda\Big(\sum_{\gamma\mapsto 1}\gamma, P\Big)$$

where the second equality follows by considering the commutative triangle

$$\begin{tikzcd} P^G \arrow[dr, "a"'] & & P_G \arrow[ll, "c"'] \\ & P \arrow[ur, "b"'] & \end{tikzcd}$$

where a is the canonical inclusion, b the canonical surjection and $c = \sum_{\gamma\mapsto 1}\gamma$. Then we have

$$\Big(\sum_{\gamma\mapsto 1}\gamma\Big)\Big|_P = a \circ c \circ b \quad \text{and} \quad \Big(\sum_{\gamma\mapsto 1}\gamma\Big)\Big|_{P_G} = b \circ a \circ c$$

hence they have the same trace. We then have

$$\#G \cdot \mathrm{Tr}_\Lambda(1; P_G) = {\sum_{\gamma\mapsto 1}}' \frac{\#G}{\#Z_\gamma}\mathrm{Tr}_\Lambda(\gamma, P) = \#G {\sum_{\gamma\mapsto 1}}' \mathrm{Tr}_\Lambda^{Z_\gamma}(\gamma, P).$$

To finish the proof, reduce to case Λ torsion-free by some universality argument. See [Del77] for details. □

Remark 15.10. Let us try to illustrate the content of the formula of Lemma 15.8. Suppose that Λ, viewed as a trivial Γ-module, admits a finite resolution $0 \to P_r \to \ldots \to P_1 \to P_0 \to \Lambda \to 0$ by some $\Lambda[\Gamma]$-modules P_i which are finite and projective as $\Lambda[G]$-modules. In that case

$$H_*\left((P_\bullet)_G\right) = \mathrm{Tor}_*^{\Lambda[G]}(\Lambda, \Lambda) = H_*(G, \Lambda)$$

and

$$\mathrm{Tr}_\Lambda^{Z_\gamma}(\gamma, P_\bullet) = \frac{1}{\#Z_\gamma}\mathrm{Tr}_\Lambda(\gamma, P_\bullet) = \frac{1}{\#Z_\gamma}\mathrm{Tr}(\gamma, \Lambda) = \frac{1}{\#Z_\gamma}.$$

Therefore, Lemma 15.8 says

$$\mathrm{Tr}_\Lambda(1, P_G) = \mathrm{Tr}\left(1|_{H_*(G,\Lambda)}\right) = \sum_{\gamma\mapsto 1}{}' \frac{1}{\# Z_\gamma}.$$

This can be interpreted as a point count on the stack BG. If $\Lambda = \mathbf{F}_\ell$ with ℓ prime to $\# G$, then $H_*(G,\Lambda)$ is $\mathbf{F}_\ell$ in degree 0 (and 0 in other degrees) and the formula reads

$$1 = \sum\nolimits_{\frac{\sigma\text{-conjugacy}}{\text{classes}\langle\gamma\rangle}} \frac{1}{\# Z_\gamma} \mod \ell.$$

This is in some sense a "trivial" trace formula for G. Later we will see that (14.3.1) can in some cases be viewed as a highly nontrivial trace formula for a certain type of group, see Section 30.

16. Proof of the trace formula

Theorem 16.1. *Let k be a finite field and X a finite type, separated scheme of dimension at most 1 over k. Let Λ be a finite ring whose cardinality is prime to that of k, and $K \in D_{ctf}(X,\Lambda)$. Then*

$$Tr(\pi_X^*|_{R\Gamma_c(X_{\bar{k}},K)}) = \sum\nolimits_{x\in X(k)} Tr(\pi_x|_{K_{\bar{x}}}) \tag{16.1.1}$$

in $\Lambda^\natural$.

Please see Remark 16.2 for some remarks on the statement. Notation: For short, we write

$$T'(X,K) = \sum\nolimits_{x\in X(k)} \mathrm{Tr}(\pi_x|_{K_{\bar{x}}})$$

for the right-hand side of (16.1.1) and

$$T''(X,K) = \mathrm{Tr}(\pi_x^*|_{R\Gamma_c(X_{\bar{k}},K)})$$

for the left-hand side.

Proof of Theorem 16.1. The proof proceeds in a number of steps.

Step 1. *Let $j : \mathcal{U} \hookrightarrow X$ be an open immersion with complement $Y = X - \mathcal{U}$ and $i : Y \hookrightarrow X$. Then $T''(X,K) = T''(\mathcal{U}, j^{-1}K) + T''(Y, i^{-1}K)$ and $T'(X,K) = T'(\mathcal{U}, j^{-1}K) + T'(Y, i^{-1}K)$.*

This is clear for T'. For T'' use the exact sequence

$$0 \to j_!j^{-1}K \to K \to i_*i^{-1}K \to 0$$

to get a filtration on K. This gives rise to an object $\widetilde{K} \in DF(X,\Lambda)$ whose graded pieces are $j_!j^{-1}K$ and $i_*i^{-1}K$, both of which lie in $D_{ctf}(X,\Lambda)$. Then, by filtered derived abstract nonsense (INSERT REFERENCE), $R\Gamma_c(X_{\bar{k}},K) \in DF_{perf}(\Lambda)$, and it comes equipped with π_x^* in $DF_{perf}(\Lambda)$. By the discussion of traces on filtered complexes (INSERT REFERENCE) we get

$$\begin{aligned} \mathrm{Tr}(\pi_X^*|_{R\Gamma_c(X_{\bar{k}},K)}) &= \mathrm{Tr}(\pi_X^*|_{R\Gamma_c(X_{\bar{k}},j_!j^{-1}K)}) + \mathrm{Tr}(\pi_X^*|_{R\Gamma_c(X_{\bar{k}},i_*i^{-1}K)}) \\ &= T''(U, i^{-1}K) + T''(Y, i^{-1}K). \end{aligned}$$

Step 2. *The theorem holds if* $\dim X \leq 0$.

Indeed, in that case

$$R\Gamma_c(X_{\bar{k}},K) = R\Gamma(X_{\bar{k}},K) = \Gamma(X_{\bar{k}},K) = \bigoplus\nolimits_{\bar{x}\in X_{\bar{k}}} K_{\bar{x}} \leftarrow \pi_X * .$$

Since the fixed points of $\pi_X : X_{\bar{k}} \to X_{\bar{k}}$ are exactly the points $\bar{x} \in X_{\bar{k}}$ which lie over a k-rational point $x \in X(k)$ we get

$$\mathrm{Tr}\big(\pi_X^*|_{R\Gamma_c(X_{\bar{k}},K)}\big) = \sum\nolimits_{x\in X(k)} \mathrm{Tr}(\pi_{\bar{x}}|_{K_{\bar{x}}}).$$

Step 3. *It suffices to prove the equality $T'(\mathcal{U},\mathcal{F}) = T''(\mathcal{U},\mathcal{F})$ in the case where*

- *$\mathcal{U}$ is a smooth irreducible affine curve over k,*
- *$\mathcal{U}(k) = \emptyset$,*
- *$K = \mathcal{F}$ is a finite locally constant sheaf of Λ-modules on $\mathcal{U}$ whose stalk(s) are finite projective Λ-modules, and*
- *Λ is killed by a power of a prime ℓ and $\ell \in k^*$.*

Indeed, because of Step 2, we can throw out any finite set of points. But we have only finitely many rational points, so we may assume there are none[2]. We may assume that $\mathcal{U}$ is smooth irreducible and affine by passing to irreducible components and throwing away the bad points if necessary. The assumptions of $\mathcal{F}$ come from unwinding the definition of $D_{ctf}(X,\Lambda)$ and those on Λ from considering its primary decomposition.

For the remainder of the proof, we consider the situation

$$\begin{tikzcd} \mathcal{V} \arrow[r] \arrow[d, "f"'] & Y \arrow[d, "\bar{f}"] \\ \mathcal{U} \arrow[r] & X \end{tikzcd}$$

where $\mathcal{U}$ is as above, f is a finite étale Galois covering, $\mathcal{V}$ is connected and the horizontal arrows are projective completions. Denoting $G = \mathrm{Aut}(\mathcal{V}|\mathcal{U})$, we also assume (as we may) that $f^{-1}\mathcal{F} = \underline{M}$ is constant, where the module $M = \Gamma(\mathcal{V}, f^{-1}\mathcal{F})$ is a $\Lambda[G]$-module which is finite and projective over Λ. This corresponds to the trivial monoid extension

$$1 \to G \to \Gamma = G \times \mathbf{N} \to \mathbf{N} \to 1.$$

In that context, using the reductions above, we need to show that $T''(\mathcal{U},\mathcal{F}) = 0$.

Step 4. *There is a natural action of G on $f_*f^{-1}\mathcal{F}$ and the trace map $f_*f^{-1}\mathcal{F} \to \mathcal{F}$ defines an isomorphism*

$$(f_*f^{-1}\mathcal{F}) \otimes_{\Lambda[G]} \Lambda = (f_*f^{-1}\mathcal{F})_G \cong \mathcal{F}.$$

To prove this, simply unwind everything at a geometric point.

Step 5. *Let $A = \mathbf{Z}/\ell^n\mathbf{Z}$ with $n \gg 0$. Then $f_*f^{-1}\mathcal{F} \cong (f_*\underline{A}) \otimes_{\underline{A}} \underline{M}$ with diagonal G-action.*

Step 6. *There is a canonical isomorphism $(f_*\underline{A} \otimes_{\underline{A}} \underline{M}) \otimes_{\Lambda[G]} \underline{\Lambda} \cong \mathcal{F}$.*

In fact, this is a derived tensor product, because of the projectivity assumption on $\mathcal{F}$.

Step 7. *There is a canonical isomorphism*

$$R\Gamma_c(\mathcal{U}_{\bar{k}},\mathcal{F}) = (R\Gamma_c(\mathcal{U}_{\bar{k}}, f_*A) \otimes_A^{\mathbf{L}} M) \otimes_{\Lambda[G]}^{\mathbf{L}} \Lambda,$$

compatible with the action of $\pi_{\mathcal{U}}^*$.

---

[2]At this point, there should be an evil laugh in the background.

This comes from the universal coefficient theorem, i.e., the fact that $R\Gamma_c$ commutes with $\otimes^{\mathbf{L}}$, and the flatness of $\mathcal{F}$ as a Λ-module.

We have

$$\begin{aligned}\mathrm{Tr}(\pi_{\mathcal{U}}^*|_{R\Gamma_c(\mathcal{U}_{\bar{k}},\mathcal{F})}) &= {\sum_{g\in G}}' \mathrm{Tr}_{\Lambda}^{Z_g}\left((g,\pi_{\mathcal{U}}^*)|_{R\Gamma_c(\mathcal{U}_{\bar{k}},f_*A)\otimes_A^{\mathbf{L}}M}\right)\\ &= {\sum_{g\in G}}' \mathrm{Tr}_{A}^{Z_g}((g,\pi_{\mathcal{U}}^*)|_{R\Gamma_c(\mathcal{U}_{\bar{k}},f_*A)})\cdot \mathrm{Tr}_{\Lambda}(g|_M)\end{aligned}$$

where Γ acts on $R\Gamma_c(\mathcal{U}_{\bar{k}},\mathcal{F})$ by G and $(e,1)$ acts via $\pi_{\mathcal{U}}^*$. So the monoidal extension is given by $\Gamma = G\times \mathbf{N}\to\mathbf{N}$, $\gamma\mapsto 1$. The first equality follows from Lemma 15.9 and the second from Lemma 15.8.

Step 8. *It suffices to show that* $Tr_A^{Z_g}((g,\pi_{\mathcal{U}}^*)|_{R\Gamma_c(\mathcal{U}_{\bar{k}},f_*A)})\in A$ *maps to zero in* Λ.

Recall that

$$\begin{aligned}\#Z_g\cdot \mathrm{Tr}_A^{Z_g}((g,\pi_{\mathcal{U}}^*)|_{R\Gamma_c(\mathcal{U}_{\bar{k}},f_*A)}) &= \mathrm{Tr}_A((g,\pi_{\mathcal{U}}^*)|_{R\Gamma_c(\mathcal{U}_{\bar{k}},f_*A)})\\ &= \mathrm{Tr}_A((g^{-1}\pi_{\mathcal{V}})^*|_{R\Gamma_c(\mathcal{V}_{\bar{k}},A)}).\end{aligned}$$

The first equality is Lemma 15.7, the second is the Leray spectral sequence, using the finiteness of f and the fact that we are only taking traces over A. Now since $A=\mathbf{Z}/\ell^n\mathbf{Z}$ with $n\gg 0$ and $\#Z_g=\ell^a$ for some (fixed) a, it suffices to show the following result.

Step 9. *We have* $Tr_A((g^{-1}\pi_{\mathcal{V}})^*|_{R\Gamma_c(\mathcal{V},A)})=0$ *in* A.

By additivity again, we have

$$\begin{aligned}&\mathrm{Tr}_A((g^{-1}\pi_{\mathcal{V}})^*|_{R\Gamma_c(\mathcal{V}_{\bar{k}}A)})+\mathrm{Tr}_A((g^{-1}\pi_{\mathcal{V}})^*|_{R\Gamma_c(Y-\mathcal{V})_{\bar{k}},A)})\\ &\quad = \mathrm{Tr}_A((g^{-1}\pi_Y)^*|_{R\Gamma(Y_{\bar{k}},A)})\end{aligned}$$

The latter trace is the number of fixed points of $g^{-1}\pi_Y$ on Y, by Weil's trace formula Theorem 14.4. Moreover, by the 0-dimensional case already proven in step 2,

$$\mathrm{Tr}_A((g^{-1}\pi_{\mathcal{V}})^*|_{R\Gamma_c(Y-\mathcal{V})_{\bar{k}},A)})$$

is the number of fixed points of $g^{-1}\pi_Y$ on $(Y-\mathcal{V})_{\bar{k}}$. Therefore,

$$\mathrm{Tr}_A((g^{-1}\pi_{\mathcal{V}})^*|_{R\Gamma_c(\mathcal{V}_{\bar{k}},A)})$$

is the number of fixed points of $g^{-1}\pi_Y$ on $\mathcal{V}_{\bar{k}}$. But there are no such points: if $\bar{y}\in Y_{\bar{k}}$ is fixed under $g^{-1}\pi_Y$, then $\bar{f}(\bar{y})\in X_{\bar{k}}$ is fixed under π_X. But $\mathcal{U}$ has no k-rational point, so we must have $\bar{f}(\bar{y})\in(X-\mathcal{U})_{\bar{k}}$ and so $\bar{y}\notin\mathcal{V}_{\bar{k}}$, a contradiction. This finishes the proof. □

Remark 16.2. Remarks on Theorem 16.1.

(1) This formula holds in any dimension. By a dévissage lemma (which uses proper base change etc.) it reduces to the current statement – in that generality.

(2) The complex $R\Gamma_c(X_{\bar{k}},K)$ is defined by choosing an open immersion $j: X\hookrightarrow \bar{X}$ with $\bar{X}$ projective over k of dimension at most 1 and setting

$$R\Gamma_c(X_{\bar{k}},K):=R\Gamma(\bar{X}_{\bar{k}},j_!K).$$

This is independent of the choice of $\bar{X}$ follows from (insert reference here). We define $H_c^i(X_{\bar{k}},K)$ to be the ith cohomology group of $R\Gamma_c(X_{\bar{k}},K)$.

Remark 16.3. Even though all we did are reductions and mostly algebra, the trace formula Theorem 16.1 is much stronger than Weil's geometric trace formula (Theorem 14.4) because it applies to coefficient systems (sheaves), not merely constant coefficients.

17. Applications

OK, having indicated the proof of the trace formula, let's try to use it for something.

18. On l-adic sheaves

Definition 18.1. Let X be a Noetherian scheme. A $\mathbf{Z}_\ell$*-sheaf* on X, or simply an ℓ*-adic sheaf* $\mathcal{F}$ is an inverse system $\{\mathcal{F}_n\}_{n\geq 1}$ where

(1) $\mathcal{F}_n$ is a constructible $\mathbf{Z}/\ell^n\mathbf{Z}$-module on $X_{étale}$, and
(2) the transition maps $\mathcal{F}_{n+1} \to \mathcal{F}_n$ induce isomorphisms $\mathcal{F}_{n+1} \otimes_{\mathbf{Z}/\ell^{n+1}\mathbf{Z}} \mathbf{Z}/\ell^n\mathbf{Z} \cong \mathcal{F}_n$.

We say that $\mathcal{F}$ is *lisse* if each $\mathcal{F}_n$ is locally constant. A *morphism* of such is merely a morphism of inverse systems.

Lemma 18.2. *Let $\{\mathcal{G}_n\}_{n\geq 1}$ be an inverse system of constructible $\mathbf{Z}/\ell^n\mathbf{Z}$-modules. Suppose that for all $k \geq 1$, the maps*

$$\mathcal{G}_{n+1}/\ell^k\mathcal{G}_{n+1} \to \mathcal{G}_n/\ell^k\mathcal{G}_n$$

are isomorphisms for all $n \gg 0$ (where the bound possibly depends on k). In other words, assume that the system $\{\mathcal{G}_n/\ell^k\mathcal{G}_n\}_{n\geq 1}$ is eventually constant, and call $\mathcal{F}_k$ the corresponding sheaf. Then the system $\{\mathcal{F}_k\}_{k\geq 1}$ forms a $\mathbf{Z}_\ell$-sheaf on X.

Proof. The proof is obvious. □

Lemma 18.3. *The category of $\mathbf{Z}_\ell$-sheaves on X is abelian.*

Proof. Let $\Phi = \{\varphi_n\}_{n\geq 1} : \{\mathcal{F}_n\} \to \{\mathcal{G}_n\}$ be a morphism of $\mathbf{Z}_\ell$-sheaves. Set

$$\mathrm{Coker}(\Phi) = \left\{\mathrm{Coker}\left(\mathcal{F}_n \xrightarrow{\varphi_n} \mathcal{G}_n\right)\right\}_{n\geq 1}$$

and $\mathrm{Ker}(\Phi)$ is the result of Lemma 18.2 applied to the inverse system

$$\left\{\bigcap_{m\geq n} \mathrm{Im}\left(\mathrm{Ker}(\varphi_m) \to \mathrm{Ker}(\varphi_n)\right)\right\}_{n\geq 1}.$$

That this defines an abelian category is left to the reader. □

Example 18.4. Let $X = \mathrm{Spec}(\mathbf{C})$ and $\Phi : \mathbf{Z}_\ell \to \mathbf{Z}_\ell$ be multiplication by ℓ. More precisely,

$$\Phi = \left\{\mathbf{Z}/\ell^n\mathbf{Z} \xrightarrow{\ell} \mathbf{Z}/\ell^n\mathbf{Z}\right\}_{n\geq 1}.$$

To compute the kernel, we consider the inverse system

$$\ldots \to \mathbf{Z}/\ell\mathbf{Z} \xrightarrow{0} \mathbf{Z}/\ell\mathbf{Z} \xrightarrow{0} \mathbf{Z}/\ell\mathbf{Z}.$$

Since the images are always zero, $\mathrm{Ker}(\Phi)$ is zero as a system.

Remark 18.5. If $\mathcal{F} = \{\mathcal{F}_n\}_{n\geq 1}$ is a $\mathbf{Z}_\ell$-sheaf on X and $\bar{x}$ is a geometric point then $M_n = \{\mathcal{F}_{n,\bar{x}}\}$ is an inverse system of finite $\mathbf{Z}/\ell^n\mathbf{Z}$-modules such that $M_{n+1} \to M_n$ is surjective and $M_n = M_{n+1}/\ell^n M_{n+1}$. It follows that

$$M = \lim_n M_n = \lim \mathcal{F}_{n,\bar{x}}$$

is a finite $\mathbf{Z}_\ell$-module. Indeed, $M/\ell M = M_1$ is finite over $\mathbf{F}_\ell$, so by Nakayama M is finite over $\mathbf{Z}_\ell$. Therefore, $M \cong \mathbf{Z}_\ell^{\oplus r} \oplus \oplus_{i=1}^t \mathbf{Z}_\ell/\ell^{e_i}\mathbf{Z}_\ell$ for some $r, t \geq 0$, $e_i \geq 1$. The module $M = \mathcal{F}_{\bar{x}}$ is called the *stalk* of $\mathcal{F}$ at $\bar{x}$.

Definition 18.6. A $\mathbf{Z}_\ell$-sheaf $\mathcal{F}$ is *torsion* if $\ell^n : \mathcal{F} \to \mathcal{F}$ is the zero map for some n. The abelian category of $\mathbf{Q}_\ell$-sheaves on X is the quotient of the abelian category of $\mathbf{Z}_\ell$-sheaves by the Serre subcategory of torsion sheaves. In other words, its objects are $\mathbf{Z}_\ell$-sheaves on X, and if $\mathcal{F}, \mathcal{G}$ are two such, then

$$\mathrm{Hom}_{\mathbf{Q}_\ell}(\mathcal{F}, \mathcal{G}) = \mathrm{Hom}_{\mathbf{Z}_\ell}(\mathcal{F}, \mathcal{G}) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell.$$

We denote by $\mathcal{F} \mapsto \mathcal{F} \otimes \mathbf{Q}_\ell$ the quotient functor (right adjoint to the inclusion). If $\mathcal{F} = \mathcal{F}' \otimes \mathbf{Q}_\ell$ where $\mathcal{F}'$ is a $\mathbf{Z}_\ell$-sheaf and $\bar{x}$ is a geometric point, then the *stalk* of $\mathcal{F}$ at $\bar{x}$ is $\mathcal{F}_{\bar{x}} = \mathcal{F}'_{\bar{x}} \otimes \mathbf{Q}_\ell$.

Remark 18.7. Since a $\mathbf{Z}_\ell$-sheaf is only defined on a Noetherian scheme, it is torsion if and only if its stalks are torsion.

Definition 18.8. If X is a separated scheme of finite type over an algebraically closed field k and $\mathcal{F} = \{\mathcal{F}_n\}_{n\geq 1}$ is a $\mathbf{Z}_\ell$-sheaf on X, then we define

$$H^i(X, \mathcal{F}) := \lim_n H^i(X, \mathcal{F}_n) \quad \text{and} \quad H^i_c(X, \mathcal{F}) := \lim_n H^i_c(X, \mathcal{F}_n).$$

If $\mathcal{F} = \mathcal{F}' \otimes \mathbf{Q}_\ell$ for a $\mathbf{Z}_\ell$-sheaf $\mathcal{F}'$ then we set

$$H^i_c(X, \mathcal{F}) := H^i_c(X, \mathcal{F}') \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell.$$

We call these the *ℓ-adic cohomology* of X with coefficients $\mathcal{F}$.

19. L-functions

Definition 19.1. Let X be a scheme of finite type over a finite field k. Let Λ be a finite ring of order prime to the characteristic of k and $\mathcal{F}$ a constructible flat Λ-module on $X_{\acute{e}tale}$. Then we set

$$L(X, \mathcal{F}) := \prod\nolimits_{x \in |X|} \det(1 - \pi_x^* T^{\deg x}|_{\mathcal{F}_{\bar{x}}})^{-1} \in \Lambda[[T]]$$

where $|X|$ is the set of closed points of X, $\deg x = [\kappa(x) : k]$ and $\bar{x}$ is a geometric point lying over x. This definition clearly generalizes to the case where $\mathcal{F}$ is replaced by a $K \in D_{ctf}(X, \Lambda)$. We call this the *$L$-function of $\mathcal{F}$*.

Remark 19.2. Intuitively, T should be thought of as $T = t^f$ where $p^f = \#k$. The definitions are then independent of the size of the ground field.

Definition 19.3. Now assume that $\mathcal{F}$ is a $\mathbf{Q}_\ell$-sheaf on X. In this case we define

$$L(X, \mathcal{F}) := \prod\nolimits_{x \in |X|} \det(1 - \pi_x^* T^{\deg x}|_{\mathcal{F}_{\bar{x}}})^{-1} \in \mathbf{Q}_\ell[[T]].$$

Note that this product converges since there are finitely many points of a given degree. We call this the *L-function of $\mathcal{F}$*.

20. Cohomological interpretation

This is how Grothendieck interpreted the L-function.

Theorem 20.1 (Finite Coefficients)**.** *Let X be a scheme of finite type over a finite field k. Let Λ be a finite ring of order prime to the characteristic of k and $\mathcal{F}$ a constructible flat Λ-module on $X_{\acute{e}tale}$. Then*

$$L(X, \mathcal{F}) = \det(1 - \pi_X^* \ T|_{R\Gamma_c(X_{\bar{k}}, \mathcal{F})})^{-1} \in \Lambda[[T]].$$

Proof. Omitted. □

Thus far, we don't even know whether each cohomology group $H_c^i(X_{\bar{k}}, \mathcal{F})$ is free.

Theorem 20.2 (Adic sheaves)**.** *Let X be a scheme of finite type over a finite field k, and $\mathcal{F}$ a $\mathbf{Q}_\ell$-sheaf on X. Then*

$$L(X, \mathcal{F}) = \prod\nolimits_i \det(1 - \pi_X^* T|_{H_c^i(X_{\bar{k}}, \mathcal{F})})^{(-1)^{i+1}} \in \mathbf{Q}_\ell[[T]].$$

Proof. This is sketched below. □

Remark 20.3. Since we have only developed some theory of traces and not of determinants, Theorem 20.1 is harder to prove than Theorem 20.2. We will only prove the latter, for the former see [Del77]. Observe also that there is no version of this theorem more general for $\mathbf{Z}_\ell$ coefficients since there is no ℓ-torsion.

We reduce the proof of Theorem 20.2 to a trace formula. Since $\mathbf{Q}_\ell$ has characteristic 0, it suffices to prove the equality after taking logarithmic derivatives. More precisely, we apply $T\frac{d}{dT}\log$ to both sides. We have on the one hand

$$\begin{aligned} T\frac{d}{dT}\log L(X, \mathcal{F}) &= T\frac{d}{dT}\log \prod_{x\in|X|} \det(1 - \pi_x^* T^{\deg x}|_{\mathcal{F}_{\bar{x}}})^{-1} \\ &= \sum_{x\in|X|} T\frac{d}{dT}\log(\det(1 - \pi_x^* T^{\deg x}|_{\mathcal{F}_{\bar{x}}})^{-1}) \\ &= \sum_{x\in|X|} \deg x \sum_{n\geq 1} \mathrm{Tr}((\pi_x^n)^*|_{\mathcal{F}_{\bar{x}}}) T^{n\deg x} \end{aligned}$$

where the last equality results from the formula

$$T\frac{d}{dT}\log\left(\det\left(1 - fT|_M\right)^{-1}\right) = \sum_{n\geq 1}\mathrm{Tr}(f^n|_M)T^n$$

which holds for any commutative ring Λ and any endomorphism f of a finite projective Λ-module M. On the other hand, we have

$$\begin{aligned} &T\frac{d}{dT}\log\left(\prod\nolimits_i \det(1 - \pi_X^* T|_{H_c^i(X_{\bar{k}}, \mathcal{F})})^{(-1)^{i+1}}\right) \\ &= \sum\nolimits_i (-1)^i \sum\nolimits_{n\geq 1} \mathrm{Tr}\left((\pi_X^n)^*|_{H_c^i(X_{\bar{k}}, \mathcal{F})}\right) T^n \end{aligned}$$

by the same formula again. Now, comparing powers of T and using the Mobius inversion formula, we see that Theorem 20.2 is a consequence of the following equality

$$\sum_{d|n} d \sum_{\substack{x\in|X| \\ \deg x = d}} \mathrm{Tr}((\pi_X^{n/d})^*|_{\mathcal{F}_{\bar{x}}}) = \sum_i (-1)^i \mathrm{Tr}((\pi_X^n)^*|_{H_c^i(X_{\bar{k}}, \mathcal{F})}).$$

Writing k_n for the degree n extension of k, $X_n = X \times_{\operatorname{Spec} k} \operatorname{Spec}(k_n)$ and ${}_n\mathcal{F} = \mathcal{F}|_{X_n}$, this boils down to

$$\sum_{x \in X_n(k_n)} \operatorname{Tr}(\pi_X^*|_{{}_n\mathcal{F}_{\bar{x}}}) = \sum_i (-1)^i \operatorname{Tr}((\pi_X^n)^*|_{H_c^i((X_n)_{\bar{k}}, {}_n\mathcal{F})})$$

which is a consequence of Theorem 20.5.

Theorem 20.4. *Let X/k be as above, let Λ be a finite ring with $\#\Lambda \in k^*$ and $K \in D_{ctf}(X, \Lambda)$. Then $R\Gamma_c(X_{\bar{k}}, K) \in D_{perf}(\Lambda)$ and*

$$\sum_{x \in X(k)} Tr(\pi_x|_{K_{\bar{x}}}) = Tr\left(\pi_X^*|_{R\Gamma_c(X_{\bar{k}}, K)}\right).$$

Proof. Note that we have already proved this (REFERENCE) when $\dim X \leq 1$. The general case follows easily from that case together with the proper base change theorem. $\square$

Theorem 20.5. *Let X be a separated scheme of finite type over a finite field k and $\mathcal{F}$ be a $\mathbf{Q}_\ell$-sheaf on X. Then $\dim_{\mathbf{Q}_\ell} H_c^i(X_{\bar{k}}, \mathcal{F})$ is finite for all i, and is nonzero for $0 \leq i \leq 2 \dim X$ only. Furthermore, we have*

$$\sum_{x \in X(k)} Tr(\pi_x|_{\mathcal{F}_{\bar{x}}}) = \sum_i (-1)^i \, Tr\left(\pi_X^*|_{H_c^i(X_{\bar{k}}, \mathcal{F})}\right).$$

Proof. We explain how to deduce this from Theorem 20.4. We first use some étale cohomology arguments to reduce the proof to an algebraic statement which we subsequently prove.

Let $\mathcal{F}$ be as in the theorem. We can write $\mathcal{F}$ as $\mathcal{F}' \otimes \mathbf{Q}_\ell$ where $\mathcal{F}' = \{\mathcal{F}'_n\}$ is a $\mathbf{Z}_\ell$-sheaf without torsion, i.e., $\ell : \mathcal{F}' \to \mathcal{F}'$ has trivial kernel in the category of $\mathbf{Z}_\ell$-sheaves. Then each $\mathcal{F}'_n$ is a flat constructible $\mathbf{Z}/\ell^n\mathbf{Z}$-module on $X_{\acute{e}tale}$, so $\mathcal{F}'_n \in D_{ctf}(X, \mathbf{Z}/\ell^n\mathbf{Z})$ and $\mathcal{F}'_{n+1} \otimes^{\mathbf{L}}_{\mathbf{Z}/\ell^{n+1}\mathbf{Z}} \mathbf{Z}/\ell^n\mathbf{Z} = \mathcal{F}'_n$. Note that the last equality holds also for standard (non-derived) tensor product, since $\mathcal{F}'_n$ is flat (it is the same equality). Therefore,

(1) the complex $K_n = R\Gamma_c(X_{\bar{k}}, \mathcal{F}'_n)$ is perfect, and it is endowed with an endomorphism $\pi_n : K_n \to K_n$ in $D(\mathbf{Z}/\ell^n\mathbf{Z})$,
(2) there are identifications
$$K_{n+1} \otimes^{\mathbf{L}}_{\mathbf{Z}/\ell^{n+1}\mathbf{Z}} \mathbf{Z}/\ell^n\mathbf{Z} = K_n$$
in $D_{perf}(\mathbf{Z}/\ell^n\mathbf{Z})$, compatible with the endomorphisms π_{n+1} and π_n (see [Del77, Rapport 4.12]),
(3) the equality $\operatorname{Tr}(\pi_X^*|_{K_n}) = \sum_{x \in X(k)} \operatorname{Tr}\left(\pi_x|_{(\mathcal{F}'_n)_{\bar{x}}}\right)$ holds, and
(4) for each $x \in X(k)$, the elements $\operatorname{Tr}(\pi_x|_{\mathcal{F}'_{n,\bar{x}}}) \in \mathbf{Z}/\ell^n\mathbf{Z}$ form an element of $\mathbf{Z}_\ell$ which is equal to $\operatorname{Tr}(\pi_x|_{\mathcal{F}_{\bar{x}}}) \in \mathbf{Q}_\ell$.

It thus suffices to prove the following algebra lemma. $\square$

Lemma 20.6. *Suppose we have $K_n \in D_{perf}(\mathbf{Z}/\ell^n\mathbf{Z})$, $\pi_n : K_n \to K_n$ and isomorphisms $\varphi_n : K_{n+1} \otimes^{\mathbf{L}}_{\mathbf{Z}/\ell^{n+1}\mathbf{Z}} \mathbf{Z}/\ell^n\mathbf{Z} \to K_n$ compatible with π_{n+1} and π_n. Then*

(1) *the elements $t_n = Tr(\pi_n|_{K_n}) \in \mathbf{Z}/\ell^n\mathbf{Z}$ form an element $t_\infty = \{t_n\}$ of $\mathbf{Z}_\ell$,*
(2) *the $\mathbf{Z}_\ell$-module $H^i_\infty = \lim_n H^i(k_n)$ is finite and is nonzero for finitely many i only, and*

(3) *the operators* $H^i(\pi_n) : H^i(K_n) \to H^i(K_n)$ *are compatible and define* $\pi^i_\infty : H^i_\infty \to H^i_\infty$ *satisfying*

$$\sum (-1)^i \, Tr(\pi^i_\infty|_{H^i_\infty \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell}) = t_\infty.$$

Proof. Since $\mathbf{Z}/\ell^n\mathbf{Z}$ is a local ring and K_n is perfect, each K_n can be represented by a finite complex $K_n^\bullet$ of finite free $\mathbf{Z}/\ell^n\mathbf{Z}$-modules such that the map $K_n^p \to K_n^{p+1}$ has image contained in ℓK_n^{p+1}. It is a fact that such a complex is unique up to isomorphism. Moreover π_n can be represented by a morphism of complexes $\pi_n^\bullet : K_n^\bullet \to K_n^\bullet$ (which is unique up to homotopy). By the same token the isomorphism $\varphi_n : K_{n+1} \otimes^{\mathbf{L}}_{\mathbf{Z}/\ell^{n+1}\mathbf{Z}} \mathbf{Z}/\ell^n\mathbf{Z} \to K_n$ is represented by a map of complexes

$$\varphi_n^\bullet : K_{n+1}^\bullet \otimes_{\mathbf{Z}/\ell^{n+1}\mathbf{Z}} \mathbf{Z}/\ell^n\mathbf{Z} \to K_n^\bullet.$$

In fact, $\varphi_n^\bullet$ is an isomorphism of complexes, thus we see that

- there exist $a, b \in \mathbf{Z}$ independent of n such that $K_n^i = 0$ for all $i \notin [a, b]$, and
- the rank of K_n^i is independent of n.

Therefore, the module $K^i_\infty = \lim_n \{K_n^i, \varphi_n^i\}$ is a finite free $\mathbf{Z}_\ell$-module and $K^\bullet_\infty$ is a finite complex of finite free $\mathbf{Z}_\ell$-modules. By induction on the number of nonzero terms, one can prove that $H^i(K^\bullet_\infty) = \lim_n H^i(K_n^\bullet)$ (this is not true for unbounded complexes). We conclude that $H^i_\infty = H^i(K^\bullet_\infty)$ is a finite $\mathbf{Z}_\ell$-module. This proves *ii*. To prove the remainder of the lemma, we need to overcome the possible noncommutativity of the diagrams

$$\begin{tikzcd}
K_{n+1}^\bullet \arrow[r, "\varphi_n^\bullet"] \arrow[d, "\pi_{n+1}^\bullet"'] & K_n^\bullet \arrow[d, "\pi_n^\bullet"] \\
K_{n+1}^\bullet \arrow[r, "\varphi_n^\bullet"'] & K_n^\bullet.
\end{tikzcd}$$

However, this diagram does commute in the derived category, hence it commutes up to homotopy. We inductively replace $\pi_n^\bullet$ for $n \geq 2$ by homotopic maps of complexes making these diagrams commute. Namely, if $h^i : K^i_{n+1} \to K^{i-1}_n$ is a homotopy, i.e.,

$$\pi_n^\bullet \circ \varphi_n^\bullet - \varphi_n^\bullet \circ \pi_{n+1}^\bullet = dh + hd,$$

then we choose $\tilde{h}^i : K^i_{n+1} \to K^{i-1}_{n+1}$ lifting h^i. This is possible because K^i_{n+1} free and $K^{i-1}_{n+1} \to K^{i-1}_n$ is surjective. Then replace $\pi_n^\bullet$ by $\tilde{\pi}_n^\bullet$ defined by

$$\tilde{\pi}^\bullet_{n+1} = \pi^\bullet_{n+1} + d\tilde{h} + \tilde{h}d.$$

With this choice of $\{\pi_n^\bullet\}$, the above diagrams commute, and the maps fit together to define an endomorphism $\pi^\bullet_\infty = \lim_n \pi_n^\bullet$ of $K^\bullet_\infty$. Then part *i* is clear: the elements $t_n = \sum (-1)^i \mathrm{Tr}\left(\pi_n^i|_{K_n^i}\right)$ fit into an element t_∞ of $\mathbf{Z}_\ell$. Moreover

$$\begin{aligned}
t_\infty &= \sum (-1)^i \mathrm{Tr}_{\mathbf{Z}_\ell}(\pi^i_\infty|_{K^i_\infty}) \\
&= \sum (-1)^i \mathrm{Tr}_{\mathbf{Q}_\ell}(\pi^i_\infty|_{K^i_\infty \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell}) \\
&= \sum (-1)^i \mathrm{Tr}(\pi_\infty|_{H^i(K^\bullet_\infty \otimes \mathbf{Q}_\ell)})
\end{aligned}$$

where the last equality follows from the fact that $\mathbf{Q}_\ell$ is a field, so the complex $K^\bullet_\infty \otimes \mathbf{Q}_\ell$ is quasi-isomorphic to its cohomology $H^i(K^\bullet_\infty \otimes \mathbf{Q}_\ell)$. The latter is also equal to $H^i(K^\bullet_\infty) \otimes_{\mathbf{Z}} \mathbf{Q}_\ell = H^i_\infty \otimes \mathbf{Q}_\ell$, which finishes the proof of the lemma, and also that of Theorem 20.5. $\square$

21. List of things which we should add above

What did we skip the proof of in the lectures so far:

(1) curves and their Jacobians,
(2) proper base change theorem,
(3) inadequate discussion of $R\Gamma_c$,
(4) more generally, given $f : X \to S$ finite type, separated S quasi-projective, discussion of $Rf_!$ on étale sheaves.
(5) discussion of $\otimes^{\mathbf{L}}$
(6) discussion of why $R\Gamma_c$ commutes with $\otimes^{\mathbf{L}}$

22. Examples of L-functions

We use Theorem 20.2 for curves to give examples of L-functions

23. Constant sheaves

Let k be a finite field, X a smooth, geometrically irreducible curve over k and $\mathcal{F} = \underline{\mathbf{Q}_\ell}$ the constant sheaf. If $\bar{x}$ is a geometric point of X, the Galois module $\mathcal{F}_{\bar{x}} = \overline{\mathbf{Q}_\ell}$ is trivial, so

$$\det(1 - \pi_x^* \, T^{\deg x}|_{\mathcal{F}_{\bar{x}}})^{-1} = \frac{1}{1 - T^{\deg x}}.$$

Applying Theorem 20.2, we get

$$\begin{aligned} L(X, \mathcal{F}) &= \prod_{i=0}^{2} \det(1 - \pi_X^* T|_{H_c^i(X_{\bar{k}}, \mathbf{Q}_\ell)})^{(-1)^{i+1}} \\ &= \frac{\det(1 - \pi_X^* T|_{H_c^1(X_{\bar{k}}, \mathbf{Q}_\ell)})}{\det(1 - \pi_X^* T|_{H_c^0(X_{\bar{k}}, \mathbf{Q}_\ell)}) \cdot \det(1 - \pi_X^* T|_{H_c^2(X_{\bar{k}}, \mathbf{Q}_\ell)})}. \end{aligned}$$

To compute the latter, we distinguish two cases.

Projective case. Assume that X is projective, so $H_c^i(X_{\bar{k}}, \mathbf{Q}_\ell) = H^i(X_{\bar{k}}, \mathbf{Q}_\ell)$, and we have

$$H^i(X_{\bar{k}}, \mathbf{Q}_\ell) = \begin{cases} \mathbf{Q}_\ell & \pi_X^* = 1 & \text{if } i = 0, \\ \mathbf{Q}_\ell^{2g} & \pi_X^* = ? & \text{if } i = 1, \\ \mathbf{Q}_\ell & \pi_X^* = q & \text{if } i = 2. \end{cases}$$

The identification of the action of π_X^* on H^2 comes from Étale Cohomology, Lemma 69.2 and the fact that the degree of π_X is $q = \#(k)$. We do not know much about the action of π_X^* on the degree 1 cohomology. Let us call $\alpha_1, \ldots, \alpha_{2g}$ its eigenvalues in $\bar{\mathbf{Q}}_\ell$. Putting everything together, Theorem 20.2 yields the equality

$$\prod\nolimits_{x \in |X|} \frac{1}{1 - T^{\deg x}} = \frac{\det(1 - \pi_X^* T|_{H^1(X_{\bar{k}}, \mathbf{Q}_\ell)})}{(1 - T)(1 - qT)} = \frac{(1 - \alpha_1 T) \ldots (1 - \alpha_{2g} T)}{(1 - T)(1 - qT)}$$

from which we deduce the following result.

Lemma 23.1. *Let X be a smooth, projective, geometrically irreducible curve over a finite field k. Then*

(1) *the L-function $L(X, \mathbf{Q}_\ell)$ is a rational function,*
(2) *the eigenvalues $\alpha_1, \ldots, \alpha_{2g}$ of π_X^* on $H^1(X_{\bar{k}}, \mathbf{Q}_\ell)$ are algebraic integers independent of ℓ,*

(3) *the number of rational points of X on k_n, where $[k_n : k] = n$, is*

$$\#X(k_n) = 1 - \sum\nolimits_{i=1}^{2g} \alpha_i^n + q^n,$$

(4) *for each i, $|\alpha_i| < q$.*

Proof. Part (3) is Theorem 20.5 applied to $\mathcal{F} = \underline{\mathbf{Q}_\ell}$ on $X \otimes k_n$. For part (4), use the following result. $\square$

Exercise 23.2. Let $\alpha_1, \ldots, \alpha_n \in \mathbf{C}$. Then for any conic sector containing the positive real axis of the form $C_\varepsilon = \{z \in \mathbf{C} \mid |\arg z| < \varepsilon\}$ with $\varepsilon > 0$, there exists an integer $k \geq 1$ such that $\alpha_1^k, \ldots, \alpha_n^k \in C_\varepsilon$.

Then prove that $|\alpha_i| \leq q$ for all i. Then, use elementary considerations on complex numbers to prove (as in the proof of the prime number theorem) that $|\alpha_i| < q$. In fact, the Riemann hypothesis says that for all $|\alpha_i| = \sqrt{q}$ for all i. We will come back to this later.

Affine case. Assume now that X is affine, say $X = \bar{X} - \{x_1, \ldots, x_n\}$ where $j : X \hookrightarrow \bar{X}$ is a projective nonsingular completion. Then $H_c^0(X_{\bar{k}}, \mathbf{Q}_\ell) = 0$ and $H_c^2(X_{\bar{k}}, \mathbf{Q}_\ell) = H^2(\bar{X}_{\bar{k}}, \mathbf{Q}_\ell)$ so Theorem 20.2 reads

$$L(X, \mathbf{Q}_\ell) = \prod_{x \in |X|} \frac{1}{1 - T^{\deg x}} = \frac{\det(1 - \pi_X^* T|_{H_c^1(X_{\bar{k}}, \mathbf{Q}_\ell)})}{1 - qT}.$$

On the other hand, the previous case gives

$$\begin{aligned} L(X, \mathbf{Q}_\ell) &= L(\bar{X}, \mathbf{Q}_\ell) \prod_{i=1}^{n} \left(1 - T^{\deg x_i}\right) \\ &= \frac{\prod_{i=1}^n (1 - T^{\deg x_i}) \prod_{j=1}^{2g} (1 - \alpha_j T)}{(1 - T)(1 - qT)}. \end{aligned}$$

Therefore, we see that $\dim H_c^1(X_{\bar{k}}, \mathbf{Q}_\ell) = 2g + \sum_{i=1}^n \deg(x_i) - 1$, and the eigenvalues $\alpha_1, \ldots, \alpha_{2g}$ of $\pi_{\bar{X}}^*$ acting on the degree 1 cohomology are roots of unity. More precisely, each x_i gives a complete set of $\deg(x_i)$th roots of unity, and one occurrence of 1 is omitted. To see this directly using coherent sheaves, consider the short exact sequence on $\bar{X}$

$$0 \to j_! \mathbf{Q}_\ell \to \mathbf{Q}_\ell \to \bigoplus_{i=1}^{n} \mathbf{Q}_{\ell, x_i} \to 0.$$

The long exact cohomology sequence reads

$$0 \to \mathbf{Q}_\ell \to \bigoplus_{i=1}^{n} \mathbf{Q}_\ell^{\oplus \deg x_i} \to H_c^1(X_{\bar{k}}, \mathbf{Q}_\ell) \to H_c^1(\bar{X}_{\bar{k}}, \mathbf{Q}_\ell) \to 0$$

where the action of Frobenius on $\bigoplus_{i=1}^n \mathbf{Q}_\ell^{\oplus \deg x_i}$ is by cyclic permutation of each term; and $H_c^2(X_{\bar{k}}, \mathbf{Q}_\ell) = H_c^2(\bar{X}_{\bar{k}}, \mathbf{Q}_\ell)$.

24. The Legendre family

Let k be a finite field of odd characteristic, $X = \mathrm{Spec}(k[\lambda, \frac{1}{\lambda(\lambda-1)}])$, and consider the family of elliptic curves $f : E \to X$ on $\mathbf{P}_X^2$ whose affine equation is $y^2 = x(x-1)(x-\lambda)$. We set $\mathcal{F} = Rf_*^1 \mathbf{Q}_\ell = \left\{R^1 f_* \mathbf{Z}/\ell^n \mathbf{Z}\right\}_{n \geq 1} \otimes \mathbf{Q}_\ell$. In this situation, the following is true

- for each $n \geq 1$, the sheaf $R^1 f_*(\mathbf{Z}/\ell^n\mathbf{Z})$ is finite locally constant – in fact, it is free of rank 2 over $\mathbf{Z}/\ell^n\mathbf{Z}$,
- the system $\{R^1 f_* \mathbf{Z}/\ell^n\mathbf{Z}\}_{n\geq 1}$ is a lisse ℓ-adic sheaf, and
- for all $x \in |X|$, $\det(1 - \pi_x\ T^{\deg x}|_{\mathcal{F}_{\bar{x}}}) = (1 - \alpha_x T^{\deg x})(1 - \beta_x T^{\deg x})$ where α_x, β_x are the eigenvalues of the geometric frobenius of E_x acting on $H^1(E_{\bar{x}}, \mathbf{Q}_\ell)$.

Note that E_x is only defined over $\kappa(x)$ and not over k. The proof of these facts uses the proper base change theorem and the local acyclicity of smooth morphisms. For details, see [Del77]. It follows that

$$L(E/X) := L(X, \mathcal{F}) = \prod_{x\in|X|} \frac{1}{(1 - \alpha_x T^{\deg x})(1 - \beta_x T^{\deg x})}.$$

Applying Theorem 20.2 we get

$$L(E/X) = \prod_{i=0}^{2} \det\left(1 - \pi_X^* T|_{H^i_c(X_{\bar{k}}, \mathcal{F})}\right)^{(-1)^{i+1}},$$

and we see in particular that this is a rational function. Furthermore, it is relatively easy to show that $H^0_c(X_{\bar{k}}, \mathcal{F}) = H^2_c(X_{\bar{k}}, \mathcal{F}) = 0$, so we merely have

$$L(E/X) = \det(1 - \pi_X^* T|_{H^1_c(X, \mathcal{F})}).$$

To compute this determinant explicitly, consider the Leray spectral sequence for the proper morphism $f : E \to X$ over $\mathbf{Q}_\ell$, namely

$$H^i_c(X_{\bar{k}}, R^j f_* \mathbf{Q}_\ell) \Rightarrow H^{i+j}_c(E_{\bar{k}}, \mathbf{Q}_\ell)$$

which degenerates. We have $f_*\mathbf{Q}_\ell = \mathbf{Q}_\ell$ and $R^1 f_* \mathbf{Q}_\ell = \mathcal{F}$. The sheaf $R^2 f_* \mathbf{Q}_\ell = \mathbf{Q}_\ell(-1)$ is the *Tate twist* of $\mathbf{Q}_\ell$, i.e., it is the sheaf $\mathbf{Q}_\ell$ where the Galois action is given by multiplication by $\#\kappa(x)$ on the stalk at $\bar{x}$. It follows that, for all $n \geq 1$,

$$\begin{aligned}
\#E(k_n) &= \sum\nolimits_i (-1)^i \mathrm{Tr}(\pi_E^{n\,*}|_{H^i_c(E_{\bar{k}}, \mathbf{Q}_\ell)}) \\
&= \sum\nolimits_{i,j} (-1)^{i+j} \mathrm{Tr}(\pi_X^{n\,*}|_{H^i_c(X_{\bar{k}}, R^j f_* \mathbf{Q}_\ell)}) \\
&= (q^n - 2) + \mathrm{Tr}(\pi_X^{n\,*}|_{H^1_c(X_{\bar{k}}, \mathcal{F})}) + q^n(q^n - 2) \\
&= q^{2n} - q^n - 2 + \mathrm{Tr}(\pi_X^{n\,*}|_{H^1_c(X_{\bar{k}}, \mathcal{F})})
\end{aligned}$$

where the first equality follows from Theorem 20.5, the second one from the Leray spectral sequence and the third one by writing down the higher direct images of $\mathbf{Q}_\ell$ under f. Alternatively, we could write

$$\#E(k_n) = \sum_{x\in X(k_n)} \#E_x(k_n)$$

and use the trace formula for each curve. We can also find the number of k_n-rational points simply by counting. The zero section contributes $q^n - 2$ points (we omit the points where $\lambda = 0, 1$) hence

$$\#E(k_n) = q^n - 2 + \#\{y^2 = x(x - 1)(x - \lambda), \lambda \neq 0, 1\}.$$

Now we have

$$\#\{y^2 = x(x-1)(x-\lambda),\ \lambda \neq 0,1\}$$

$$= \#\{y^2 = x(x-1)(x-\lambda) \text{ in } \mathbf{A}^3\} - \#\{y^2 = x^2(x-1)\} - \#\{y^2 = x(x-1)^2\}$$

$$= \#\{\lambda = \tfrac{-y^2}{x(x-1)} + x,\ x \neq 0,1\} + \#\{y^2 = x(x-1)(x-\lambda), x = 0,1\} - 2(q^n - \varepsilon_n)$$

$$= q^n(q^n-2) + 2q^n - 2(q^n - \varepsilon_n)$$

$$= q^{2n} - 2q^n + 2\varepsilon_n$$

where $\varepsilon_n = 1$ if -1 is a square in k_n, 0 otherwise, i.e.,

$$\varepsilon_n = \frac{1}{2}\left(1 + \left(\frac{-1}{k_n}\right)\right) = \frac{1}{2}\left(1 + (-1)^{\frac{q^n-1}{2}}\right).$$

Thus $\#E(k_n) = q^{2n} - q^n - 2 + 2\varepsilon_n$. Comparing with the previous formula, we find

$$\mathrm{Tr}(\pi_X^{n\,*}|_{H_c^1(X_{\bar{k}},\mathcal{F})}) = 2\varepsilon_n = 1 + (-1)^{\frac{q^n-1}{2}},$$

which implies, by elementary algebra of complex numbers, that if -1 is a square in k_n^*, then $\dim H_c^1(X_{\bar{k}}, \mathcal{F}) = 2$ and the eigenvalues are 1 and 1. Therefore, in that case we have

$$L(E/X) = (1-T)^2.$$

25. Exponential sums

A standard problem in number theory is to evaluate sums of the form

$$S_{a,b}(p) = \sum_{x \in \mathbf{F}_p - \{0,1\}} e^{\frac{2\pi i x^a (x-1)^b}{p}}.$$

In our context, this can be interpreted as a cohomological sum as follows. Consider the base scheme $S = \mathrm{Spec}(\mathbf{F}_p[x, \frac{1}{x(x-1)}])$ and the affine curve $f : X \to \mathbf{P}^1 - \{0,1,\infty\}$ over S given by the equation $y^{p-1} = x^a(x-1)^b$. This is a finite étale Galois cover with group $\mathbf{F}_p^*$ and there is a splitting

$$f_*(\bar{\mathbf{Q}}_\ell^*) = \bigoplus_{\chi : \mathbf{F}_p^* \to \bar{\mathbf{Q}}_\ell^*} \mathcal{F}_\chi$$

where χ varies over the characters of $\mathbf{F}_p^*$ and $\mathcal{F}_\chi$ is a rank 1 lisse $\mathbf{Q}_\ell$-sheaf on which $\mathbf{F}_p^*$ acts via χ on stalks. We get a corresponding decomposition

$$H_c^1(X_{\bar{k}}, \mathbf{Q}_\ell) = \bigoplus_\chi H^1(\mathbf{P}^1_{\bar{k}} - \{0,1,\infty\}, \mathcal{F}_\chi)$$

and the cohomological interpretation of the exponential sum is given by the trace formula applied to $\mathcal{F}_\chi$ over $\mathbf{P}^1 - \{0,1,\infty\}$ for some suitable χ. It reads

$$S_{a,b}(p) = -\mathrm{Tr}(\pi_X^*|_{H^1(\mathbf{P}^1_{\bar{k}} - \{0,1,\infty\}, \mathcal{F}_\chi)}).$$

The general yoga of Weil suggests that there should be some cancellation in the sum. Applying (roughly) the Riemann-Hurwitz formula, we see that

$$2g_X - 2 \approx -2(p-1) + 3(p-2) \approx p$$

so $g_X \approx p/2$, which also suggests that the χ-pieces are small.

26. Trace formula in terms of fundamental groups

In the following sections we reformulate the trace formula completely in terms of the fundamental group of a curve, except if the curve happens to be $\mathbf{P}^1$.

27. Fundamental groups

This material is discussed in more detail in the chapter on fundamental groups. See Fundamental Groups, Section 1. Let X be a connected scheme and let $\overline{x} \to X$ be a geometric point. Consider the functor

$$\begin{array}{cccc} F_{\overline{x}} : & \substack{\text{finite étale} \\ \text{schemes over } X} & \longrightarrow & \text{finite sets} \\ & Y/X & \longmapsto & F_{\overline{x}}(Y) = \left\{ \substack{\text{geom points } \overline{y} \\ \text{of } Y \text{ lying over } \overline{x}} \right\} = Y_{\overline{x}} \end{array}$$

Set

$$\pi_1(X, \overline{x}) = Aut(F_{\overline{x}}) = \text{ set of automorphisms of the functor } F_{\overline{x}}$$

Note that for every finite étale $Y \to X$ there is an action

$$\pi_1(X, \overline{x}) \times F_{\overline{x}}(Y) \to F_{\overline{x}}(Y)$$

Definition 27.1. A subgroup of the form $\text{Stab}(\overline{y} \in F_{\overline{x}}(Y)) \subset \pi_1(X, \overline{x})$ is called *open*.

Theorem 27.2 (Grothendieck)**.** *Let X be a connected scheme.*

(1) *There is a topology on $\pi_1(X, \overline{x})$ such that the open subgroups form a fundamental system of open nbhds of $e \in \pi_1(X, \overline{x})$.*
(2) *With topology of (1) the group $\pi_1(X, \overline{x})$ is a profinite group.*
(3) *The functor*

$$\begin{array}{ccc} \substack{\textit{schemes finite} \\ \textit{étale over } X} & \to & \substack{\textit{finite discrete continuous} \\ \pi_1(X, \overline{x})\textit{-sets}} \\ Y/X & \mapsto & F_{\overline{x}}(Y) \textit{ with its natural action} \end{array}$$

is an equivalence of categories.

Proof. See [Gro71]. □

Proposition 27.3. *Let X be an integral normal Noetherian scheme. Let $\overline{y} \to X$ be an algebraic geometric point lying over the generic point $\eta \in X$. Then*

$$\pi_x(X, \overline{\eta}) = Gal(M/\kappa(\eta))$$

($\kappa(\eta)$, function field of X) where

$$\kappa(\overline{\eta}) \supset M \supset \kappa(\eta) = k(X)$$

is the max sub-extension such that for every finite sub extension $M \supset L \supset \kappa(\eta)$ the normalization of X in L is finite étale over X.

Proof. Omitted. □

Change of base point. For any $\overline{x}_1, \overline{x}_2$ geom. points of X there exists an isom. of fibre functions

$$\mathcal{F}_{\overline{x}_1} \cong \mathcal{F}_{\overline{x}_2}$$

(This is a path from $\overline{x}_1$ to $\overline{x}_2$.) Conjugation by this path gives isom

$$\pi_1(X, \overline{x}_1) \cong \pi_1(X, \overline{x}_2)$$

well defined up to inner actions.

Functoriality. For any morphism $X_1 \to X_2$ of connected schemes any $\overline{x} \in X_1$ there is a canonical map

$$\pi_1(X_1, \overline{x}) \to \pi_1(X_2, \overline{x})$$

(Why? because the fibre functor ...)

Base field. Let X be a variety over a field k. Then we get

$$\pi_1(X, \overline{x}) \to \pi_1(Spec(k), \overline{x}) =^{\text{prop}} Gal(k^{\text{sep}}/k)$$

This map is surjective if and only if X is geometrically connected over k. So in the geometrically connected case we get s.e.s. of profinite groups

$$1 \to \pi_1(X_{\overline{k}}, \overline{x}) \to \pi_1(X, \overline{x}) \to Gal(k^{\text{sep}}/k) \to 1$$

($\pi_1(X_{\overline{k}}, \overline{x})$: geometric fundamental group of X, $\pi_1(X, \overline{x})$: arithmetic fundamental group of X)

Comparison. If X is a variety over $\mathbf{C}$ then

$$\pi_1(X, \overline{x}) = \text{ profinite completion of } \pi_1(X(\mathbf{C})(\text{ usual topology}), x)$$

(have $x \in X(\mathbf{C})$)

Frobenii. X variety over k, $\#k < \infty$. For any $x \in X$ closed point, let

$$F_x \in \pi_1(x, \overline{x}) = \mathrm{Gal}(\kappa(x)^{\text{sep}}/\kappa(x))$$

be the geometric frobenius. Let $\overline{\eta}$ be an alg. geom. gen. pt. Then

$$\pi_1(X, \overline{\eta}) \leftarrow^{\cong} \pi_1(X, \overline{x}) \overset{\text{functoriality}}{\leftarrow} \pi_1(x, \overline{x})$$

Easy fact:

$$\begin{array}{ccc} \pi_1(X, \overline{\eta}) & \to^{\deg} \pi_1(\mathrm{Spec}(k), \overline{\eta})* & = Gal(k^{sep}/k) \\ & & || \\ & & \widehat{\mathbf{Z}} \cdot F_{\mathrm{Spec}(k)} \\ F_x & \mapsto & \deg(x) \cdot F_{\mathrm{Spec}(k)} \end{array}$$

Recall: $\deg(x) = [\kappa(x) : k]$

Fundamental groups and lisse sheaves. Let X be a connected scheme, $\overline{x}$ geom. pt. There are equivalences of categories

(Λ finite ring)	fin. loc. const. sheaves of Λ-modules of $X_{\acute{e}tale}$	$\leftrightarrow$	finite (discrete) Λ-modules with continuous $\pi_1(X,\overline{x})$-action
(ℓ a prime)	lisse ℓ-adic sheaves	$\leftrightarrow$	finitely generated $\mathbf{Z}_\ell$-modules M with continuous $\pi_1(X,\overline{x})$-action where we use ℓ-adic topology on M

In particular lisse $\mathbf{Q}_l$-sheaves correspond to continuous homomorphisms

$$\pi_1(X, \overline{x}) \to \mathrm{GL}_r(\mathbf{Q}_l), \quad r \geq 0$$

Notation: A module with action (M, ρ) corresponds to the sheaf $\mathcal{F}_\rho$.

Trace formulas. X variety over k, $\#k < \infty$.

(1) Λ finite ring $(\#\Lambda, \#k) = 1$

$$\rho : \pi_1(X, \overline{x}) \to \mathrm{GL}_r(\Lambda)$$

continuous. For every $n \geq 1$ we have

$$\sum_{d|n} d \left(\sum_{\substack{x \in |X|, \\ \deg(x) = d}} \mathrm{Tr}(\rho(F_x^{n/d})) \right) = \mathrm{Tr}\left((\pi_x^n)^* |_{R\Gamma_c(X_{\overline{k}}, \mathcal{F}_\rho)} \right)$$

(2) $l \neq char(k)$ prime, $\rho : \pi_1(X, \overline{x}) \to \mathrm{GL}_r(\mathbf{Q}_l)$. For any $n \geq 1$

$$\sum_{d|n} d \left(\sum_{\substack{x \in |X| \\ \deg(x)=d}} \mathrm{Tr}\left(\rho(F_x^{n/d})\right) \right) = \sum_{i=0}^{2\dim X} (-1)^i \mathrm{Tr}\left(\pi_X^*|_{H_c^i(X_{\overline{k}}, \mathcal{F}_\rho)}\right)$$

Weil conjectures. (Deligne-Weil I, 1974) X smooth proj. over k, $\#k = q$, then the eigenvalues of π_X^* on $H^i(X_{\overline{k}}, \mathbf{Q}_l)$ are algebraic integers α with $|\alpha| = q^{1/2}$.

Deligne's conjectures. (almost completely proved by Lafforgue + ...) Let X be a normal variety over k finite

$$\rho : \pi_1(X, \overline{x}) \longrightarrow \mathrm{GL}_r(\mathbf{Q}_l)$$

continuous. Assume: ρ irreducible $\det(\rho)$ of finite order. Then

(1) there exists a number field E such that for all $x \in |X|$(closed points) the char. poly of $\rho(F_x)$ has coefficients in E.
(2) for any $x \in |X|$ the eigenvalues $\alpha_{x,i}$, $i = 1, \ldots, r$ of $\rho(F_x)$ have complex absolute value 1. (these are algebraic numbers not necessary integers)
(3) for every finite place λ(not dividing p), of E (maybe after enlarging E a bit) there exists
$$\rho\lambda : \pi_1(X, \overline{x}) \to \mathrm{GL}_r(E_\lambda)$$
compatible with ρ. (some char. polys of F_x's)

Theorem 27.4 (Deligne, Weil II)**.** *For a sheaf $\mathcal{F}_\rho$ with ρ satisfying the conclusions of the conjecture above then the eigenvalues of π_X^* on $H_c^i(X_{\overline{k}}, \mathcal{F}_\rho)$ are algebraic numbers α with absolute values*

$$|\alpha| = q^{w/2}, \ \textit{for } w \in \mathbf{Z}, \ w \leq i$$

Moreover, if X smooth and proj. then $w = i$.

Proof. See [Del80]. □

28. Profinite groups, cohomology and homology

Let G be a profinite group.

Cohomology. Consider the category of discrete modules with continuous G-action. This category has enough injectives and we can define

$$H^i(G, M) = R^i H^0(G, M) = R^i(M \mapsto M^G)$$

Also there is a derived version $RH^0(G, -)$.

Homology. Consider the category of compact abelian groups with continuous G-action. This category has enough projectives and we can define

$$H_i(G, M) = L_i H_0(G, M) = L_i(M \mapsto M_G)$$

and there is also a derived version.

Trivial duality. The functor $M \mapsto M^\wedge = \mathrm{Hom}_{cont}(M, S^1)$ exchanges the categories above and

$$H^i(G, M)^\wedge = H_i(G, M^\wedge)$$

Moreover, this functor maps torsion discrete G-modules to profinite continuous G-modules and vice versa, and if M is either a discrete or profinite continuous G-module, then $M^\wedge = \mathrm{Hom}(M, \mathbf{Q}/\mathbf{Z})$.

Notes on Homology.

(1) If we look at Λ-modules for a finite ring Λ then we can identify

$$H_i(G, M) = Tor_i^{\Lambda[[G]]}(M, \Lambda)$$

where $\Lambda[[G]]$ is the limit of the group algebras of the finite quotients of G.

(2) If G is a normal subgroup of Γ, and Γ is also profinite then
   - $H^0(G, -)$: discrete Γ-module$\to$ discrete Γ/G-modules
   - $H_0(G, -)$: compact Γ-modules $\to$ compact Γ/G-modules

   and hence the profinite group Γ/G acts on the cohomology groups of G with values in a Γ-module. In other words, there are derived functors

$$RH^0(G, -) : D^+(\text{discrete } \Gamma\text{-modules}) \longrightarrow D^+(\text{discrete } \Gamma/G\text{-modules})$$

   and similarly for $LH_0(G, -)$.

29. Cohomology of curves, revisited

Let k be a field, X be geometrically connected, smooth curve over k. We have the fundamental short exact sequence

$$1 \to \pi_1(X_{\overline{k}}, \overline{\eta}) \to \pi_1(X, \overline{\eta}) \to \mathrm{Gal}(k^{sep}/k) \to 1$$

If Λ is a finite ring with $\#\Lambda \in k^*$ and M a finite Λ-module, and we are given

$$\rho : \pi_1(X, \overline{\eta}) \to \mathrm{Aut}_\Lambda(M)$$

continuous, then $\mathcal{F}_\rho$ denotes the associated sheaf on $X_{\acute{e}tale}$.

Lemma 29.1. *There is a canonical isomorphism*

$$H_c^2(X_{\overline{k}}, \mathcal{F}_\rho) = (M)_{\pi_1(X_{\overline{k}}, \overline{\eta})}(-1)$$

as Gal(k^{sep}/k)-modules.

Here the subscript $_{\pi_1(X_{\overline{k}}, \overline{\eta})}$ indicates co-invariants, and (-1) indicates the Tate twist i.e., $\sigma \in \mathrm{Gal}(k^{sep}/k)$ acts via

$$\chi_{cycl}(\sigma)^{-1}.\sigma \text{ on RHS}$$

where

$$\chi_{cycl} : \mathrm{Gal}(k^{sep}/k) \to \prod\nolimits_{l \neq char(k)} \mathbf{Z}_l^*$$

is the cyclotomic character.

Reformulation (Deligne, Weil II, page 338). For any finite locally constant sheaf $\mathcal{F}$ on X there is a maximal quotient $\mathcal{F} \to \mathcal{F}''$ with $\mathcal{F}''/X_{\overline{k}}$ a constant sheaf, hence

$$\mathcal{F}'' = (X \to \mathrm{Spec}(k))^{-1} F''$$

where F'' is a sheaf Spec(k), i.e., a Gal(k^{sep}/k)-module. Then

$$H_c^2(X_{\overline{k}}, \mathcal{F}) \to H_c^2(X_{\overline{k}}, \mathcal{F}'') \to F''(-1)$$

is an isomorphism.

Proof of Lemma 29.1. Let $Y \to^{\varphi} X$ be the finite étale Galois covering corresponding to $\mathrm{Ker}(\rho) \subset \pi_1(X, \overline{\eta})$. So

$$\mathrm{Aut}(Y/X) = Ind(\rho)$$

is Galois group. Then $\varphi^* \mathcal{F}_\rho = \underline{M}_Y$ and

$$\varphi_* \varphi^* \mathcal{F}_\rho \to \mathcal{F}_\rho$$

which gives

$$\begin{aligned} &H^2_c(X_{\overline{k}}, \varphi_* \varphi^* \mathcal{F}_\rho) \to H^2_c(X_{\overline{k}}, \mathcal{F}_\rho) \\ &= H^2_c(Y_{\overline{k}}, \varphi^* \mathcal{F}_\rho) \\ &= H^2_c(Y_{\overline{k}}, \underline{M}) = \bigoplus_{\substack{\text{irred. comp. of} \\ Y_{\overline{k}}}} M \end{aligned}$$

$$\mathrm{Im}(\rho) \to H^2_c(Y_{\overline{k}}, \underline{M}) = \bigoplus_{\substack{\text{irred. comp. of} \\ Y_{\overline{k}}}} M \to_{\mathrm{Im}(\rho)\text{equivalent}} H^2_c(X_{\overline{k}}, \mathcal{F}_\rho) \to^{\substack{\text{trivial Im}(\rho) \\ \text{action}}}$$

irreducible curve $C/\overline{k}$, $H^2_c(C, \underline{M}) = M$.

Since

$$\begin{matrix} \text{set of irreducible} \\ \text{components of } Y_k \end{matrix} = \frac{Im(\rho)}{Im(\rho|_{\pi_1(X_{\overline{k}}, \overline{\eta})})}$$

We conclude that $H^2_c(X_{\overline{k}}, \mathcal{F}_\rho)$ is a quotient of $M_{\pi_1(X_{\overline{k}}, \overline{\eta})}$. On the other hand, there is a surjection

$$\mathcal{F}_\rho \to \mathcal{F}'' = \begin{matrix} \text{sheaf on } X \text{ associated to} \\ (M)_{\pi_1(X_{\overline{k}}, \overline{\eta})} \leftarrow \pi_1(X, \overline{\eta}) \end{matrix}$$

$$H^2_c(X_{\overline{k}}, \mathcal{F}_\rho) \to M_{\pi_1(X_{\overline{k}}, \overline{\eta})}$$

The twist in Galois action comes from the fact that $H^2_c(X_{\overline{k}}, \mu_n) =^{\mathrm{can}} \mathbf{Z}/n\mathbf{Z}$. $\square$

Remark 29.2. Thus we conclude that if X is also projective then we have functorially in the representation ρ the identifications

$$H^0(X_{\overline{k}}, \mathcal{F}_\rho) = M^{\pi_1(X_{\overline{k}}, \overline{\eta})}$$

and

$$H^2_c(X_{\overline{k}}, \mathcal{F}_\rho) = M_{\pi_1(X_{\overline{k}}, \overline{\eta})}(-1)$$

Of course if X is not projective, then $H^0_c(X_{\overline{k}}, \mathcal{F}_\rho) = 0$.

Proposition 29.3. *Let X/k as before but $X_{\overline{k}} \neq \mathbf{P}^1_{\overline{k}}$ The functors $(M, \rho) \mapsto H^{2-i}_c(X_{\overline{k}}, \mathcal{F}_\rho)$ are the left derived functor of $(M, \rho) \mapsto H^2_c(X_{\overline{k}}, \mathcal{F}_\rho)$ so*

$$H^{2-i}_c(X_{\overline{k}}, \mathcal{F}_\rho) = H_i(\pi_1(X_{\overline{k}}, \overline{\eta}), M)(-1)$$

Moreover, there is a derived version, namely

$$R\Gamma_c(X_{\overline{k}}, \mathcal{F}_\rho) = LH_0(\pi_1(X_{\overline{k}}, \overline{\eta}), M(-1)) = M(-1) \otimes^{\mathbf{L}}_{\Lambda[[\pi_1(X_{\overline{k}}, \overline{\eta})]]} \Lambda$$

in $D(\Lambda[[\widehat{\mathbf{Z}}]])$. Similarly, the functors $(M, \rho) \mapsto H^i(X_{\overline{k}}, \mathcal{F}_\rho)$ are the right derived functor of $(M, \rho) \mapsto M^{\pi_1(X_{\overline{k}}, \overline{\eta})}$ so

$$H^i(X_{\overline{k}}, \mathcal{F}_\rho) = H^i(\pi_1(X_{\overline{k}}, \overline{\eta}), M)$$

Moreover, in this case there is a derived version too.

Proof. (Idea) Show both sides are universal δ-functors. $\square$

Remark 29.4. By the proposition and Trivial duality then you get

$$H_c^{2-i}(X_{\overline{k}}, \mathcal{F}_\rho) \times H^i(X_{\overline{k}}, \mathcal{F}_\rho^\wedge(1)) \to \mathbf{Q}/\mathbf{Z}$$

a perfect pairing. If X is projective then this is Poincare duality.

30. Abstract trace formula

Suppose given an extension of profinite groups,

$$1 \to G \to \Gamma \xrightarrow{\deg} \widehat{\mathbf{Z}} \to 1$$

We say Γ *has an abstract trace formula* if and only if there exist

(1) an integer $q \geq 1$, and
(2) for every $d \geq 1$ a finite set S_d and for each $x \in S_d$ a conjugacy class $F_x \in \Gamma$ with $\deg(F_x) = d$

such that the following hold

(1) for all ℓ not dividing q have $\mathrm{cd}_\ell(G) < \infty$, and
(2) for all finite rings Λ with $q \in \Lambda^*$, for all finite projective Λ-modules M with continuous Γ-action, for all $n > 0$ we have

$$\sum\nolimits_{d|n} d\left(\sum\nolimits_{x \in S_d} \mathrm{Tr}(F_x^{n/d}|_M)\right) = q^n \mathrm{Tr}(F^n|_{M \otimes^{\mathbf{L}}_{\Lambda[[G]]} \Lambda})$$

in $\Lambda^\natural$.

Here $M \otimes^{\mathbf{L}}_{\Lambda[[G]]} \Lambda = LH_0(G, M)$ denotes derived homology, and $F = 1$ in $\Gamma/G = \widehat{\mathbf{Z}}$.

Remark 30.1. Here are some observations concerning this notion.

(1) If modeling projective curves then we can use cohomology and we don't need factor q^n.
(2) The only examples I know are $\Gamma = \pi_1(X, \overline{\eta})$ where X is smooth, geometrically irreducible and $K(\pi, 1)$ over finite field. In this case $q = (\#k)^{\dim X}$. Modulo the proposition, we proved this for curves in this course.
(3) Given the integer q then the sets S_d are uniquely determined. (You can multiple q by an integer m and then replace S_d by m^d copies of S_d without changing the formula.)

Example 30.2. Fix an integer $q \geq 1$

$$\begin{array}{ccccccccc} 1 & \to & G = \widehat{\mathbf{Z}}^{(q)} & \to & \Gamma & \to & \widehat{\mathbf{Z}} & \to & 1 \\ & & = \prod_{l \nmid q} \mathbf{Z}_l & & F & \mapsto & 1 & & \end{array}$$

with $FxF^{-1} = ux$, $u \in (\widehat{\mathbf{Z}}^{(q)})^*$. Just using the trivial modules $\mathbf{Z}/m\mathbf{Z}$ we see

$$q^n - (qu)^n \equiv \sum\nolimits_{d|n} d\#S_d$$

in $\mathbf{Z}/m\mathbf{Z}$ for all $(m, q) = 1$ (up to $u \to u^{-1}$) this implies $qu = a \in \mathbf{Z}$ and $|a| < q$. The special case $a = 1$ does occur with

$$\Gamma = \pi_1^t(\mathbf{G}_{m,\mathbf{F}_p}, \overline{\eta}), \quad \#S_1 = q - 1, \quad \text{and} \quad \#S_2 = \frac{(q^2-1)-(q-1)}{2}$$

31. Automorphic forms and sheaves

References: See especially the amazing papers [Dri83], [Dri84] and [Dri80] by Drinfeld.

Unramified cusp forms. Let k be a finite field of characteristic p. Let X geometrically irreducible projective smooth curve over k. Set $K = k(X)$ equal to the function field of X. Let v be a place of K which is the same thing as a closed point $x \in X$. Let K_v be the completion of K at v, which is the same thing as the fraction field of the completion of the local ring of X at x. Denote $O_v \subset K_v$ the ring of integers. We further set

$$O = \prod\nolimits_v O_v \subset \mathbf{A} = \prod_v{}' K_v$$

and we let Λ be any ring with p invertible in Λ.

Definition 31.1. An *unramified cusp form on $GL_2(\mathbf{A})$ with values in* Λ[3] is a function

$$f : \mathrm{GL}_2(\mathbf{A}) \to \Lambda$$

such that

(1) $f(x\gamma) = f(x)$ for all $x \in \mathrm{GL}_2(\mathbf{A})$ and all $\gamma \in \mathrm{GL}_2(K)$
(2) $f(ux) = f(x)$ for all $x \in \mathrm{GL}_2(\mathbf{A})$ and all $u \in \mathrm{GL}_2(O)$
(3) for all $x \in \mathrm{GL}_2(\mathbf{A})$,
$$\int_{\mathbf{A} \mod K} f\left(x\begin{pmatrix}1 & z\\ 0 & 1\end{pmatrix}\right) dz = 0$$
see [dJ01, Section 4.1] for an explanation of how to make sense out of this for a general ring Λ in which p is invertible.

Hecke Operators. For v a place of K and f an unramified cusp form we set

$$T_v(f)(x) = \int_{g \in M_v} f(g^{-1}x)dg,$$

and

$$U_v(f)(x) = f\left(\begin{pmatrix}\pi_v^{-1} & 0\\ 0 & \pi_v^{-1}\end{pmatrix} x\right)$$

Notations used: here $\pi_v \in O_v$ is a uniformizer

$$M_v = \{h \in Mat(2 \times 2, O_v) | \det h = \pi_v O_v^*\}$$

and $dg =$ is the Haar measure on $\mathrm{GL}_2(K_v)$ with $\int_{\mathrm{GL}_2(O_v)} dg = 1$. Explicitly we have

$$T_v(f)(x) = f\left(\begin{pmatrix}\pi_v^{-1} & 0\\ 0 & 1\end{pmatrix} x\right) + \sum_{i=1}^{q_v} f\left(\begin{pmatrix}1 & 0\\ -\pi_v^{-1}\lambda_i & \pi_v^{-1}\end{pmatrix} x\right)$$

with $\lambda_i \in O_v$ a set of representatives of $O_v/(\pi_v) = \kappa_v$, $q_v = \#\kappa_v$.

Eigenforms. An *eigenform* f is an unramified cusp form such that some value of f is a unit and $T_v f = t_v f$ and $U_v f = u_v f$ for some (uniquely determined) $t_v, u_v \in \Lambda$.

[3]This is likely nonstandard notation.

Theorem 31.2. *Given an eigenform f with values in $\overline{\mathbf{Q}}_l$ and eigenvalues $u_v \in \overline{\mathbf{Z}}_l^*$ then there exists*

$$\rho : \pi_1(X) \to GL_2(E)$$

continuous, absolutely irreducible where E is a finite extension of $\mathbf{Q}_\ell$ contained in $\overline{\mathbf{Q}}_l$ such that $t_v = Tr(\rho(F_v))$, and $u_v = q_v^{-1} \det(\rho(F_v))$ for all places v.

Proof. See [Dri80]. □

Theorem 31.3. *Suppose $\mathbf{Q}_l \subset E$ finite, and*

$$\rho : \pi_1(X) \to GL_2(E)$$

absolutely irreducible, continuous. Then there exists an eigenform f with values in $\overline{\mathbf{Q}}_l$ whose eigenvalues t_v, u_v satisfy the equalities $t_v = Tr(\rho(F_v))$ and $u_v = q_v^{-1}\det(\rho(F_v))$.

Proof. See [Dri83]. □

Remark 31.4. We now have, thanks to Lafforgue and many other mathematicians, complete theorems like this two above for GL_n and allowing ramification! In other words, the full global Langlands correspondence for GL_n is known for function fields of curves over finite fields. At the same time this does not mean there aren't a lot of interesting questions left to answer about the fundamental groups of curves over finite fields, as we shall see below.

Central character. If f is an eigenform then

$$\chi_f : \begin{array}{ccc} O^*\backslash\mathbf{A}^*/K^* & \to & \Lambda^* \\ (1,\ldots,\pi_v,1,\ldots,1) & \mapsto & u_v^{-1} \end{array}$$

is called the *central character*. If corresponds to the determinant of ρ via normalizations as above. Set

$$C(\Lambda) = \left\{ \begin{array}{c} \text{unr. cusp forms } f \text{ with coefficients in } \Lambda \\ \text{such that } U_v f = \varphi_v^{-1} f \forall v \end{array} \right\}$$

Proposition 31.5. *If Λ is Noetherian then $C(\Lambda)$ is a finitely generated Λ-module. Moreover, if Λ is a field with prime subfield $\mathbf{F} \subset \Lambda$ then*

$$C(\Lambda) = (C(\mathbf{F})) \otimes_{\mathbf{F}} \Lambda$$

compatibly with T_v acting.

Proof. See [dJ01, Proposition 4.7]. □

This proposition trivially implies the following lemma.

Lemma 31.6. *Algebraicity of eigenvalues. If Λ is a field then the eigenvalues t_v for $f \in C(\Lambda)$ are algebraic over the prime subfield $\mathbf{F} \subset \Lambda$.*

Proof. Follows from Proposition 31.5. □

Combining all of the above we can do the following very useful trick.

Lemma 31.7. *Switching l. Let E be a number field. Start with*

$$\rho : \pi_1(X) \to SL_2(E_\lambda)$$

absolutely irreducible continuous, where λ is a place of E not lying above p. Then for any second place λ' of E not lying above p there exists a finite extension $E'_{\lambda'}$ and a absolutely irreducible continuous representation

$$\rho' : \pi_1(X) \to SL_2(E'_{\lambda'})$$

which is compatible with ρ in the sense that the characteristic polynomials of all Frobenii are the same.

Note how this is an instance of Deligne's conjecture!

Proof. To prove the switching lemma use Theorem 31.3 to obtain $f \in C(\overline{\mathbf{Q}}_l)$ eigenform ass. to ρ. Next, use Proposition 31.5 to see that we may choose $f \in C(E')$ with $E \subset E'$ finite. Next we may complete E' to see that we get $f \in C(E'_{\lambda'})$ eigenform with $E'_{\lambda'}$ a finite extension of $E_{\lambda'}$. And finally we use Theorem 31.2 to obtain $\rho' : \pi_1(X) \to SL_2(E'_{\lambda'})$ abs. irred. and continuous after perhaps enlarging $E'_{\lambda'}$ a bit again. $\square$

Speculation: If for a (topological) ring Λ we have

$$\begin{pmatrix} \rho : \pi_1(X) \to SL_2(\Lambda) \\ \text{abs irred} \end{pmatrix} \leftrightarrow \text{ eigen forms in } C(\Lambda)$$

then all eigenvalues of $\rho(F_v)$ algebraic (won't work in an easy way if Λ is a finite ring. Based on the speculation that the Langlands correspondence works more generally than just over fields one arrives at the following conjecture.

Conjecture. (See [dJ01]) For any continuous

$$\rho : \pi_1(X) \to \mathrm{GL}_n(\mathbf{F}_l[[t]])$$

we have $\#\rho(\pi_1(X_{\overline{k}})) < \infty$.

A rephrasing in the language of sheaves: "For any lisse sheaf of $\overline{\mathbf{F}_l((t))}$-modules the geom monodromy is finite."

Theorem 31.8. *The Conjecture holds if $n \leq 2$.*

Proof. See [dJ01]. $\square$

Theorem 31.9. *Conjecture holds if $l > 2n$ modulo some unproven things.*

Proof. See [Gai07]. $\square$

It turns out the conjecture is useful for something. See work of Drinfeld on Kashiwara's conjectures. But there is also the much more down to earth application as follows.

Theorem 31.10. *(See* [dJ01, Theorem 3.5]*) Suppose*

$$\rho_0 : \pi_1(X) \to GL_n(\mathbf{F}_l)$$

is a continuous, $l \neq p$. Assume

1. *Conj. holds for X,*
2. *$\rho_0|_{\pi_1(X_{\overline{k}})}$ abs. irred., and*
3. *l does not divide n.*

Then the universal deformation ring R_{univ} of ρ_0 is finite flat over $\mathbf{Z}_l$.

Explanation: There is a representation $\rho_{\text{univ}} : \pi_1(X) \to \mathrm{GL}_n(R_{\text{univ}})$ (Univ. Defo ring) R_{univ} loc. complete, residue field $\mathbf{F}_l$ and $(R_{\text{univ}} \to \mathbf{F}_l) \circ \rho_{\text{univ}} \cong \rho_0$. And given any $R \to \mathbf{F}_l$, R local complete and $\rho : \pi_1(X) \to \mathrm{GL}_n(R)$ then there exists $\psi : R_{\text{univ}} \to R$ such that $\psi \circ \rho_{\text{univ}} \cong \rho$. The theorem says that the morphism

$$\mathrm{Spec}(R_{\text{univ}}) \longrightarrow \mathrm{Spec}(\mathbf{Z}_l)$$

is finite and flat. In particular, such a ρ_0 lifts to a $\rho : \pi_1(X) \to \mathrm{GL}_n(\overline{\mathbf{Q}}_l)$.

Notes:

(1) The theorem on deformations is easy.
(2) Any result towards the conjecture seems hard.
(3) It would be interesting to have more conjectures on $\pi_1(X)$!

32. Counting points

Let X be a smooth, geometrically irreducible, projective curve over k and $q = \#k$. The trace formula gives: there exists algebraic integers $w_1, \ldots, w_{2g}$ such that

$$\#X(k_n) = q^n - \sum\nolimits_{i=1}^{2g_X} w_i^n + 1.$$

If $\sigma \in \mathrm{Aut}(X)$ then for all i, there exists j such that $\sigma(w_i) = w_j$.

Riemann-Hypothesis. For all i we have $|\omega_i| = \sqrt{q}$.

This was formulated by Emil Artin, in 1924, for hyperelliptic curves. Proved by Weil 1940. Weil gave two proofs

- using intersection theory on $X \times X$, using the Hodge index theorem, and
- using the Jacobian of X.

There is another proof whose initial idea is due to Stephanov, and which was given by Bombieri: it uses the function field $k(X)$ and its Frobenius operator (1969). The starting point is that given $f \in k(X)$ one observes that $f^q - f$ is a rational function which vanishes in all the $\mathbf{F}_q$-rational points of X, and that one can try to use this idea to give an upper bound for the number of points.

33. Precise form of Chebotarev

As a first application let us prove a precise form of Chebotarev for a finite étale Galois covering of curves. Let $\varphi : Y \to X$ be a finite étale Galois covering with group G. This corresponds to a homomorphism

$$\pi_1(X) \longrightarrow G = \mathrm{Aut}(Y/X)$$

Assume $Y_{\overline{k}}$ = irreducible. If $C \subset G$ is a conjugacy class then for all $n > 0$, we have

$$|\#\{x \in X(k_n) \mid F_x \in C\} - \frac{\#C}{\#G} \cdot \#X(k_n)| \leq (\#C)(2g-2)\sqrt{q^n}$$

(Warning: Please check the coefficient $\#C$ on the right hand side carefuly before using.)

Sketch. Write

$$\varphi_*(\overline{\mathbf{Q}_l}) = \oplus_{\pi \in \widehat{G}} \mathcal{F}_\pi$$

where $\widehat{G}$ is the set of isomorphism classes of irred representations of G over $\overline{\mathbf{Q}}_l$. For $\pi \in \widehat{G}$ let $\chi_\pi : G \to \overline{\mathbf{Q}}_l$ be the character of π. Then

$$H^*(Y_{\overline{k}}, \overline{\mathbf{Q}}_l) = \oplus_{\pi\in\widehat{G}} H^*(Y_{\overline{k}}, \overline{\mathbf{Q}}_l)_\pi =_{(\varphi \text{ finite })} \oplus_{\pi\in\widehat{G}} H^*(X_{\overline{k}}, \mathcal{F}_\pi)$$

If $\pi \neq 1$ then we have

$$H^0(X_{\overline{k}}, \mathcal{F}_\pi) = H^2(X_{\overline{k}}, \mathcal{F}_\pi) = 0, \quad \dim H^1(X_{\overline{k}}, \mathcal{F}_\pi) = (2g_X - 2)d_\pi^2$$

(can get this from trace formula for acting on ...) and we see that

$$|\sum_{x\in X(k_n)} \chi_\pi(\mathcal{F}_x)| \leq (2g_X - 2)d_\pi^2 \sqrt{q^n}$$

Write $1_C = \sum_\pi a_\pi \chi_\pi$, then $a_\pi = \langle 1_C, \chi_\pi\rangle$, and $a_1 = \langle 1_C, \chi_1\rangle = \frac{\#C}{\#G}$ where

$$\langle f, h\rangle = \frac{1}{\#G} \sum_{g\in G} f(g)\overline{h(g)}$$

Thus we have the relation

$$\frac{\#C}{\#G} = ||1_C||^2 = \sum |a_\pi|^2$$

Final step:

$$\begin{aligned}
\#\left\{x \in X(k_n) \mid F_x \in C\right\} &= \sum_{x\in X(k_n)} 1_C(x) \\
&= \sum_{x\in X(k_n)} \sum_\pi a_\pi \chi_\pi(F_x) \\
&= \underbrace{\frac{\#C}{\#G} \#X(k_n)}_{\text{term for } \pi=1} + \underbrace{\sum_{\pi\neq 1} a_\pi \sum_{x\in X(k_n)} \chi_\pi(F_x)}_{\text{error term (to be bounded by } E)}
\end{aligned}$$

We can bound the error term by

$$\begin{aligned}
|E| &\leq \sum_{\substack{\pi\in\widehat{G},\\ \pi\neq 1}} |a_\pi|(2g-2)d_\pi^2\sqrt{q^n} \\
&\leq \sum_{\pi\neq 1} \frac{\#C}{\#G}(2g_X - 2)d_\pi^3\sqrt{q^n}
\end{aligned}$$

By Weil's conjecture, $\#X(k_n) \sim q^n$. □

34. How many primes decompose completely?

This section gives a second application of the Riemann Hypothesis for curves over a finite field. For number theorists it may be nice to look at the paper by Ihara, entitled "How many primes decompose completely in an infinite unramified Galois extension of a global field?", see [Iha83]. Consider the fundamental exact sequence

$$1 \to \pi_1(X_{\overline{k}}) \to \pi_1(X) \xrightarrow{\deg} \widehat{\mathbf{Z}} \to 1$$

Proposition 34.1. *There exists a finite set $x_1, \dots, x_n$ of closed points of X such that set of* **all** *frobenius elements corresponding to these points topologically generate $\pi_1(X)$.*

Another way to state this is: There exist $x_1, \ldots, x_n \in |X|$ such that the smallest normal closed subgroup Γ of $\pi_1(X)$ containing 1 frobenius element for each x_i is all of $\pi_1(X)$. i.e., $\Gamma = \pi_1(X)$.

Proof. Pick $N \gg 0$ and let

$$\{x_1, \ldots, x_n\} = \begin{array}{l}\text{set of all closed points of} \\ X \text{ of degree} \leq N \text{ over } k\end{array}$$

Let $\Gamma \subset \pi_1(X)$ be as in the variant statement for these points. Assume $\Gamma \neq \pi_1(X)$. Then we can pick a normal open subgroup U of $\pi_1(X)$ containing Γ with $U \neq \pi_1(X)$. By R.H. for X our set of points will have some x_{i_1} of degree N, some x_{i_2} of degree $N-1$. This shows $\deg : \Gamma \to \widehat{\mathbf{Z}}$ is surjective and so the same holds for U. This exactly means if $Y \to X$ is the finite étale Galois covering corresponding to U, then $Y_{\overline{k}}$ irreducible. Set $G = \mathrm{Aut}(Y/X)$. Picture

$$Y \to^G X, \quad G = \pi_1(X)/U$$

By construction all points of X of degree $\leq N$, split completely in Y. So, in particular

$$\#Y(k_N) \geq (\#G)\#X(k_N)$$

Use R.H. on both sides. So you get

$$q^N + 1 + 2g_Y q^{N/2} \geq \#G\#X(k_N) \geq \#G(q^N + 1 - 2g_X q^{N/2})$$

Since $2g_Y - 2 = (\#G)(2g_X - 2)$, this means

$$q^N + 1 + (\#G)(2g_X - 1) + 1)q^{N/2} \geq \#G(q^N + 1 - 2g_X q^{N/2})$$

Thus we see that G has to be the trivial group if N is large enough. □

Weird Question. Set $W_X = \deg^{-1}(\mathbf{Z}) \subset \pi_1(X)$. Is it true that for some finite set of closed points $x_1, \ldots, x_n$ of X the set of all frobenii corresponding to these points *algebraically* generate W_X?

By a Baire category argument this translates into the same question for all Frobenii.

35. How many points are there really?

If the genus of the curve is large relative to q, then the main term in the formula $\#X(k) = q - \sum \omega_i + 1$ is not q but the second term $\sum \omega_i$ which can (a priori) have size about $2g_X\sqrt{q}$. In the paper [VD83] the authors Drinfeld and Vladut show that this maximum is (as predicted by Ihara earlier) actually at most about $g\sqrt{q}$.

Fix q and let k be a field with k elements. Set

$$A(q) = \limsup_{g_X \to \infty} \frac{\#X(k)}{g_X}$$

where X runs over geometrically irreducible smooth projective curves over k. With this definition we have the following results:

- RH $\Rightarrow A(q) \leq 2\sqrt{q}$
- Ihara $\Rightarrow A(q) \leq \sqrt{2q}$
- DV $\Rightarrow A(q) \leq \sqrt{q} - 1$ (actually this is sharp if q is a square)

Proof. Given X let $w_1, \ldots, w_{2g}$ and $g = g_X$ be as before. Set $\alpha_i = \frac{w_i}{\sqrt{q}}$, so $|\alpha_i| = 1$. If α_i occurs then $\overline{\alpha}_i = \alpha_i^{-1}$ also occurs. Then

$$N = \#X(k) \leq X(k_r) = q^r + 1 - (\sum_i \alpha_i^r) q^{r/2}$$

Rewriting we see that for every $r \geq 1$

$$-\sum_i \alpha_i^r \geq N q^{-r/2} - q^{r/2} - q^{-r/2}$$

Observe that

$$0 \leq |\alpha_i^n + \alpha_i^{n-1} + \ldots + \alpha_i + 1|^2 = (n+1) + \sum_{j=1}^{n} (n+1-j)(\alpha_i^j + \alpha_i^{-j})$$

So

$$\begin{aligned} 2g(n+1) &\geq -\sum_i \left(\sum_{j=1}^{n} (n+1-j)(\alpha_i^j + \alpha_i^{-j}) \right) \\ &= -\sum_{j=1}^{n} (n+1-j) \left(\sum_i \alpha_i^j + \sum_i \alpha_i^{-j} \right) \end{aligned}$$

Take half of this to get

$$\begin{aligned} g(n+1) &\geq -\sum_{j=1}^{n} (n+1-j)(\sum_i \alpha_i^j) \\ &\geq N \sum_{j=1}^{n} (n+1-j) q^{-j/2} - \sum_{j=1}^{n} (n+1-j)(q^{j/2} + q^{-j/2}) \end{aligned}$$

This gives

$$\frac{N}{g} \leq \left(\sum_{j=1}^{n} \frac{n+1-j}{n+1} q^{-j/2} \right)^{-1} \cdot \left(1 + \frac{1}{g} \sum_{j=1}^{n} \frac{n+1-j}{n+1} (q^{j/2} + q^{-j/2}) \right)$$

Fix n let $g \to \infty$

$$A(q) \leq \left(\sum_{j=1}^{n} \frac{n+1-j}{n+1} q^{-j/2} \right)^{-1}$$

So

$$A(q) \leq \lim_{n\to\infty}(\ldots) = \left(\sum_{j=1}^{\infty} q^{-j/2} \right)^{-1} = \sqrt{q} - 1$$

□

36. Other chapters

Preliminaries

References

[Del77] Pierre Deligne, *Cohomologie étale*, Lecture Notes in Mathematics, no. 569, Springer-Verlag, 1977.

[Del80] ———, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. (1980), no. 52, 137–252.

[dJ01] Aise Johan de Jong, *A conjecture on arithmetic fundamental groups*, Israel J. Math. **121** (2001), 61–84.

[Dri80] Vladimir Gershonovich Drinfel'd, *Langlands' conjecture for* GL(2) *over functional fields*, Proceedings of the International Congress of Mathematicians (Helsinki, 1978) (Helsinki), Acad. Sci. Fennica, 1980, pp. 565–574.

[Dri83] ———, *Two-dimensional l-adic representations of the fundamental group of a curve over a finite field and automorphic forms on* GL(2), Amer. J. Math. **105** (1983), no. 1, 85–114.

[Dri84] ———, *Two-dimensional l-adic representations of the Galois group of a global field of characteristic p and automorphic forms on* GL(2), Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **134** (1984), 138–156, Automorphic functions and number theory, II.

[Gai07] Dennis Gaitsgory, *On de Jong's conjecture*, Israel J. Math. **157** (2007), 155–191.

[Gro71] Alexander Grothendieck, *Revêtements étales et groupe fondamental (sga 1)*, Lecture notes in mathematics, vol. 224, Springer-Verlag, 1971.

[Iha83] Yasutaka Ihara, *How many primes decompose completely in an infinite unramified Galois extension of a global field?*, J. Math. Soc. Japan **35** (1983), no. 4, 693–709.

[Lan02] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[VD83] Sergei Georgievich Vlèduţ and Vladimir Gershonovich Drinfel'd, *The number of points of an algebraic curve*, Funktsional. Anal. i Prilozhen. **17** (1983), no. 1, 68–69.

[Wei48] André Weil, *Courbes algébriques et variétés abéliennes*, Hermann, 1948.