The propreties of an L-function from a geometric point of view

Ken-ichi Sugiyama

October 12, 2007

Abstract

We will discuss similarities of L-functions between in the number theory and in the geometry. In particular the Hesse-Weil congruent zeta function of a smooth curve defined over a finite field will be compared to the zeta function associated to a disrete dynamical system. Moreover a geometric analog of the Birch and Swinnerton-Dyre conjecture and of the Iwasawa Main Conjecture will be discussed. [1]

1 Introduction

About 40 years ago Mazur pointed out an analogy between the number theory and topology of threefolds. In particular he noticed that a similarity between the Iwasawa invariant and the Alexander polynomial which is the most well-known object in knot theory [15]. Recently such similarity between number theory and topology of threefolds has been recognized by many mathematicians.

The Iwasawa invariant appears in the Iwasawa theory which gives a deep insight into various L-functions from an arithmetic point of view. He has conjectured that his invariant should be the main part of a p-adic zeta function and his conjecture is referred as *the Iwasawa main conjecture*. It is sometimes compared with the Weil conjecture for a smooth projective curve over a finite field. In fact it was one of Iwasawa's motivation to develop his theory [10]. Because of similarity mentioned before it is natural to consider a corresponding model in geometry. An investigation of such a model was initiated by Artin and Mazur[2] and, following thier idea, Deninger[7] and Fried[8] have studied a zeta function associated to a dynamical system on a topological manifold with a foliation.

On the other hand Morishita has observed a certain analogies between primes and knots from Galois thoretic point of view. In fact, based on an analogy of the structure of a link group and a certain maximal pro l-Galois group, he

[1] 2000 Mathematics Subject Classification : 11F32, 11M36, 57M25, 57M27

has obtained invariants of a number field, which corresponds to the Alexander module and the Milnor invariants[19]. He has continued to pursue his line and has investigated the connection between his invariant and Massey product in Galois cohomology following link theory [20]. Nowadays a theory which study these analogies is called *arithmetic topology* and is also developped by Reznikov and Kapranov and thier collaborators [22][1]. In this note, following these philosophy, we will discuss an analogue of the Birch and Swinnerton-Dyer conjecture or the Iwasawa conjecture in low dimensional hyperbolic geometry.

The present paper is based on the lecture which I have given at Stekulov Institute at September 2007. The author wish to express deep appreciation to Professor A. Sergeev, Professor O. Sheinman and members of the institute for their kindness and hospitality. He also wants to express thanks to the attendents for thier stimulating questions.

2 Arithmetic geometry over a finite field and its geometric model

Everyone should know that the fundamental group of a circle S^1 is isomorphic to $\mathbb{Z}$ and that its universal covering is isomorphic to $\mathbb{R}$. On the other hand let $\mathbb{F}_q$ be a finite field of characteristic p. Then its étale fundamental which is the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ by definition is isomorphic to the profinite completion $\hat{\mathbb{Z}}$ of $\mathbb{Z}$:

$$\hat{\mathbb{Z}} = \lim_{\leftarrow} \mathbb{Z}/(f).$$

It is topologically generated by the Frobenius automorphism ϕ_q. Thus we may consider S^1 and $\mathbb{R}$ correspond to $\mathrm{Spec}\mathbb{F}_q$ and $\mathrm{Spec}\bar{\mathbb{F}}_q$, respectively and such an observation will play a key role in this section. In the following we will fix a generator g of $\pi_1(S^1) \simeq \mathbb{Z}$, which is a geometric substitute for ϕ_p.

2.1 A smooth curve over a finite field seems like to a mapping torus of a Riemann surface

In this section we will discuss a dymanical system on a mapping torus which is a geometric analogue of a Frobenius in number theory. Although there are more appropriate model due to Deninger[7] or Fried[8], we will treat the simplest one.

Let Σ be a smooth projective curve defined over $\mathbb{F}_q$ and $\overline{\Sigma}$ its base extension to $\bar{\mathbb{F}}_q$. We may write such objects in the diagram:

$$\begin{array}{ccc} \overline{\Sigma} & \xrightarrow{\rho} & \Sigma \\ \downarrow & & \downarrow \\ \mathrm{Spec}\bar{\mathbb{F}}_q & \rightarrow & \mathrm{Spec}\mathbb{F}_q. \end{array} \tag{2.1}$$

By the previous observation a corresponding geometric situation should be a Cartesian diagram:

$$\begin{array}{ccc} \overline{M} & \stackrel{\tau}{\to} & M \\ \downarrow & & \downarrow f \\ \mathbb{R} & \to & S^1. \end{array}$$

Here M is a compact Riemannian manifold and f is a smooth fibration. Since $\mathbb{R}$ is contractible $\bar{M}$ is isomorphic to a smooth compact manifold N with $\mathbb{R}$. By the fact

$$H^i_{et}(\overline{\Sigma},\, \mathbb{Q}_l) = 0, \quad i \geq 3$$

for $l \neq p$, the dimension of corresponding N should be 2. Thus for a geometric model of Σ it is natural to take M a mapping torus of an automorphism ϕ of N. Here the mapping torus of (N, ϕ) is defined as

$$N \times [0, 1]/ \sim,$$

where the relation is given by

$$(x,\, 0) \sim (\phi(x),\, 1), \quad x \in N.$$

Since (1) is Cartesian, ϕ_q induces an automorphism of $\bar{\Sigma}$, which will be denoted by the same letter. Then it is natural to regard ϕ its geometric substitute. Now we have obtained the following correspondence:

$$(\bar{\Sigma},\, \Sigma,\, \phi_p) \Longleftrightarrow (N,\, M,\, \phi).$$

Such a construction will be generalized to a local system. Let $\mathcal{L}$ be an l-adic local system (i.e. an l-adic flat vector bundle) on Σ. By Deligne it is known that to give such an object is equivalent to give a pair $(\bar{\mathcal{L}},\, \phi_{\mathcal{L}})$, where $\bar{\mathcal{L}}$ is an l-adic local system on $\bar{\Sigma}$ and $\phi_{\mathcal{L}}$ is its automorphism. Thus the corresponding geometric object for $\mathcal{L}$ should be a pair of a flat vector bundle L on N and its automorphism ϕ_L:

$$\begin{array}{ccc} L & \stackrel{\phi_L}{\longrightarrow} & L \\ \downarrow & & \downarrow \\ N & \stackrel{\phi}{\longrightarrow} & N \end{array} \tag{2.2}$$

2.2 A discrete dynamical system and its zeta function

We will review the definition of the Hasse-Weil zeta function. Let $\Sigma(\mathbb{F}_{q^n})$ be the set of $\mathbb{F}_{q^n}$-rational points of Σ. Then it has an action of ϕ_q and so does

$$\Sigma(\bar{\mathbb{F}}_q) = \cup_n \Sigma(\mathbb{F}_{q^n}).$$

The set of closed points $|\Sigma|$ is defined to be the orbit space of the action on $\Sigma(\bar{\mathbb{F}}_q)$. For $x \in \Sigma(\bar{\mathbb{F}}_q)$, the degree of extension of the residue field F_x over $\mathbb{F}_q$ will be denoted by $\deg x$. Then the map

$$\Sigma(\bar{\mathbb{F}}_q) \stackrel{\deg}{\to} \mathbb{Z}$$

factors through

$$|\Sigma| \stackrel{\deg}{\to} \mathbb{Z}.$$

Now the Hasse-Weil zeta function is defined to be

$$Z(\Sigma,\, t) = \prod_{x \in |\Sigma|} (1 - t^{\deg x})^{-1}. \tag{2.3}$$

The Weil conjecture predicts that $Z(\Sigma,\, t)$ should be a rational function. We will explain why this should be true by our geometric model. In order to do that, let us investigate properties of ϕ_q more closely.

By definition $\Sigma(\mathbb{F}_{q^n})$ is a finite subset of $\Sigma(\bar{\mathbb{F}}_q)$ which consists of fixed points of ϕ_q^n. Since ϕ_q is purely inseparable, its differential $d\phi_q$ vanishes and in particular we have

$$\det[1 - d\phi_q^n(x)] \neq 0$$

for any $x \in \Sigma(\mathbb{F}_{q^n})$. Every fixed point of ϕ_q^n is isolated and nondegenerate.

We assume that the pair (N, ϕ) enjoys the same property i.e. fixed points of ϕ^n are isolated and nondegenerate. The set of fixed points of ϕ^n will be denoted by $N(\phi^n)$ and let $N(\phi^\infty)$ be their union. Then ϕ acts on $N(\phi^\infty)$ and its orbit space will be denoted by $|M|$. The degree of $x \in N(\phi^\infty)$ is defined to be

$$\deg x = \mathrm{Min}\{n \geq 1 \,|\, \phi^n(x) = x\},$$

which induces a map

$$|M| \xrightarrow{\deg} \mathbb{Z}.$$

Now our geometric analog of (2.2) is defined to be

$$\zeta(M,\, t) = \prod_{x \in |M|} (1 - t^{\deg x})^{-1}. \tag{2.4}$$

After \$1 of [6], its logarithmic derivative is computed as

$$\begin{aligned} t\frac{t}{dt} \log \zeta(M,\, t) &= \sum_{x \in |M|} \frac{\deg x \cdot t^{\deg x}}{1 - t^{\deg x}} \\ &= \sum_{x \in |M|} \sum_{n=1}^{\infty} \deg x \cdot t^{n \cdot \deg x} \\ &= \sum_{n=1}^{\infty} |N(\phi^n)| t^n. \end{aligned}$$

The assumption of (N, ϕ) and the Lefschetz trace formula shows

$$|N(\phi^n)| = \sum_i (-1)^i \mathrm{Tr}[(\phi^*)^n \,|\, H^i(N,\, \mathbb{Q})],$$

and

$$t\frac{t}{dt}\log\zeta(M,\,t) = \sum_i (-1)^i \sum_{n=1}^{\infty} \mathrm{Tr}[(\phi^*)^n \,|\, H^i(N,\,\mathbb{Q})]t^n.$$

Now the formula

$$t\frac{t}{dt}\log\det(1_n - At) = -\sum_{n=1}^{\infty} \mathrm{Tr}A^n \cdot t^n$$

for an $n \times n$-matrix A implies

$$t\frac{t}{dt}\log\zeta(M,\,t) = -\sum_i (-1)^i t\frac{t}{dt}\log\det[1_n - \phi^* t \,|\, H^i(N,\,\mathbb{Q})],$$

and we finally have

$$\zeta(M,\,t) = \prod_{i=0}^{2} \det[1 - \phi^* t \,|\, H^i(N,\,\mathbb{Q})]^{(-1)^{i+1}}. \tag{2.5}$$

The RHS is visibly a rational function.

We expect that there should exsist a suitable theory of cohomology and the Lefschetz trace formula in arithmetic geometry over a finite field. In fact it does exist. They are nothing but the theory of *étale cohomology* and *the Grotendieck-Lefschetz trace formula*. Thus we can repeat the same computation as above for Σ (more generally for any smooth projective variety over a finite field) and can prove the rationality of the Hasse-Weil zeta function. ([6]).

The above construction is generalized to an l-adic local system $\mathcal{L}$ on a Zarisiki open subset Σ_0 of Σ. For simplicity we will assume that Σ_0 and Σ are equal. Let $\rho_{\mathcal{L}}$ be the corresponding representation of étale fundamental group $\pi_1^{et}(\Sigma,\,\sigma_0)$ with respect to a geometric base point σ_0. Since $\rho_{\mathcal{L}}$ is unramified everywhere $\rho_{\mathcal{L}}(\phi_x)$ is well defined for $x \in \Sigma(\bar{\mathbb{F}}_q)$. Here $\phi_x \in \pi_1^{et}(\Sigma,\,\sigma_0)$ is a Frobenius automorphism at x, which is only well defined up to conjugation of an element of the inertia group at x. Moreover it is easy to see that a polynomial

$$P_{\mathcal{L},x}(t) = \det[1 - \rho_{\mathcal{L}}(\phi_x)t^{\deg x}]$$

is only determined by the orbit of x and thus we may define *the L-function* associated to $\mathcal{L}$ to be

$$L(\Sigma,\,\mathcal{L},\,t) = \prod_{x\in|\Sigma|} P_{\mathcal{L},x}(t)^{-1}.$$

Next we will discuss its topological model. Let F be a flat vector bundle on M and ρ_F the corresponding representation of $\pi_1(M, m_0)$. A point $x \in N(\infty)$ determines a closed loop in M and connecting it to m_0 by a curve c we will obtain an element γ_x of $\pi_1(M, m_0)$. Then

$$P_{F,x}(t) = \det[1 - \rho_F(\phi_x)t^{\deg x}]$$

does not depend on a choice of c and moreover it only depends on the orbit of x. Thus our geometric model of the L-function is

$$L(M,\, F,\, t) = \prod_{x \in |M|} P_{L,x}(t)^{-1}.$$

Since to give a flat vector bundle over M is equivalant to give a pair of a flat vector bundle L over N and its automorphism ϕ_L as (2.2), we have more geometric description of $P_{F,x}(t)$. Notice that $\phi^{\deg x}$ fixes x and ϕ_L induces an automorphism $\phi_{L,x}$ of L_x. Then it is easy to see that

$$P_{F,x}(t) = \det[1 - \phi_{L,x} t^{\deg x}].$$

Now using the Lefschetz trace formula for a local system the computation as before will show

$$L(M,\, F,\, t) = \prod_{i=0}^{2} \det[1 - \phi_L^* t \,|\, H^i(N,\, L)]^{(-1)^{i+1}}.$$

If we use the Grothendieck-Lefschetz trace the same argument is still available for an l-adic local system on Σ and we will obtain

$$L(\Sigma,\, \mathcal{L},\, t) = \prod_{i=0}^{2} \det[1 - \phi_{\mathcal{L}}^* t \,|\, H^i_{et}(\bar{\Sigma},\, \bar{\mathcal{L}})]^{(-1)^{i+1}}. \tag{2.6}$$

2.3 The Birch and Swinnerton-Dyer conjecture and its geometric model over a finite field

Let E be an elliptic curve defined over $\mathbb{Q}$ and we will fix a prime l. The integral l-adic Tate module of E is defined to be the inverse limit of l^n-torsion of E:

$$T_l(E) = \lim_{\leftarrow} E[l^n], \quad E[l^n] = \mathrm{Ker}[E \xrightarrow{l^n} E],$$

and we set

$$V_l(E) = T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

It is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module which is unramified at a prime p other than l which does not divide the discriminant Δ_E of E. Let $\rho_{E,l}$ be the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $V_l(E)$. Then for such a prime p, the characteristic polynomial of a Frobenius ϕ_p

$$\det[1 - \rho_{E,l}(\phi_p) t]$$

is well defined and the L-function of E is defined as

$$L(E,\, s) = \prod_p \det[1 - \rho_{E,l}(\phi_p) p^{-s}]^{-1},$$

where p runs through primes not dividing $l \cdot \Delta_E$. Then it absolutely converges for $\mathrm{Re}\, s > \frac{3}{2}$. Wiles has proved that the function

$$\xi_E(s) = N_E^{\frac{s}{2}} (2\pi)^{-s} \Gamma(s) L(E,\, s), \quad N_E \text{ is the conductor of } E,$$

satisfies a functional equation

$$\xi_E(s) = \pm \xi_E(2-s),$$

and that that $L(E, s)$ is entirely continued to the whole plane [29]. We are mainly interested in a behavior of the L-function at $s = 1$. By the Mordell-Weil theorem, the set of rational points $E(\mathbb{Q})$ of E becomes a finitely generated abelian group and its rank is referred as *the Mordell-Weil rank*. Now here is a crude form of the Birch and Swinnerton-Dyer.

Conjecture 2.1. *([4] [5]) The order of $L(E, s)$ at $s = 1$ should be equal to the Mordell-Weil rank of E.*

In [27] Tate has studied an analog of the conjecture for an elliptic fibration over a finite field. (In fact more generally he has considered the conjecture for an abelian fibration.) Let X be a smooth projective surface defined over a finite field $\mathbf{F}_q$ which has a morphism onto a smooth complete curve S whose generic fibre is an elliptic curve:

$$X \xrightarrow{f} S. \tag{2.7}$$

We assume that the moduli of the fibration is non-constant. Moreover for simplicity we also assume that (2.6) is a smooth fibration. (In general we do not have to assume this.) We set

$$V = R^1 f_* \mathbf{Q}_l,$$

which is a local system on S and let ρ_V be the corresponding representation of an étale fundamental group of S.

Then the L-function of the fibration is defined to be

$$\begin{aligned} L_{X/S}(s) &= L(S, V, t)|_{t=q^{-s}} \\ &= \prod_{x \in |S|} \det(1 - \rho_V(\phi_x) q^{-s \deg x})^{-1}. \end{aligned}$$

Now the assumption of moduli of the fibration and the Poincaré duality imply

$$H^0_{et}(S, V) = H^2_{et}(S, V) = 0.$$

Therefore by (2.5) we have

$$L(S, V, t) = \det(1 - \phi_q^* t \mid H^1(\overline{S}, \overline{V}))$$

and

$$\mathrm{ord}_{s=1} L_{X/S}(s) = \mathrm{ord}_{t=q^{-1}} \det(1 - \phi_q^* t \mid H^1(\overline{S}, \overline{V})).$$

The latter is equal to the multiplicity of q in eigenvalues of ϕ_q^*, which is greater than or equal to $\dim [H^1(\overline{S}, \overline{V})(1)]^{\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)}$. Here for an l-adic representation

W of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ $W(m)$ is its m-th Tate twist, which is defined as follows. We set

$$\mathbb{Z}_l(1) = \lim_{\leftarrow} \mu_{l^n}, \quad \mathbb{Q}_l(1) = \mathbb{Z}_l(1) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l,$$

and

$$\mathbb{Q}_l(-1) = \mathrm{Hom}_{\mathbb{Q}_l}(\mathbb{Q}_l(1), \mathbb{Q}_l),$$

where μ_N is a group of N-th roots of unity. Then for a positive integer m, $\mathbb{Q}_l(m)$ and $\mathbb{Q}_l(-m)$ are defined to be the m-th tensor product of $\mathbb{Q}_l(1)$ and $\mathbb{Q}_l(-1)$, respectively. Now we set

$$W(m) = W \otimes_{\mathbb{Q}_l} \mathbb{Q}_l(m).$$

Notice that by definition $\dim[H^1(\overline{S}, \overline{V})(1)]^{\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)}$ is equal to the dimension of the eigenspace of ϕ_q^* on $H^1(\overline{S}, \overline{V})$ whose eigenvalue is q.

Let $X(S)$ be the abelian group of the section of the fibration, which is a finitely generated abelian group by the Mordell-Weil's theorem for a function field. Then the cycle map embeds $X(S) \otimes_{\mathbb{Z}} \mathbb{Q}_l$ in a subspace of $H^1(\overline{S}, \overline{V})(1)$ fixed by the absolute Galois group. We will explain it briefly. Since $X \xrightarrow{f} S$ is an elliptic fibration, in the category of sheaves with respect to an étale topology on S, there is an exact sequence:

$$0 \to X[l^n] \to X \xrightarrow{l^n} X \to 0,$$

where the l^n-th power is taken for fibre direction. This induces injection of Galois modules

$$X(S) \otimes_{\mathbb{Z}} \mathbb{Z}/(l^n) \hookrightarrow H^1(S, X[l^n]). \tag{2.8}$$

If we set

$$V_l(X/S) = (\lim_{\leftarrow} X[l^n]) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l,$$

(2.8) implies an injection

$$X(S) \otimes_{\mathbb{Z}} \mathbb{Q}_l \hookrightarrow [H^1(\overline{S}, V_l(X/S))]^{\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)}.$$

Since $V_l(X/S)$ is the dual of $R^1 f_* \mathbb{Q}_l$ the Weil pairing

$$V_l(X/S) \times V_l(X/S) \to \mathbb{Q}_l(1)$$

shows

$$R^1 f_* \mathbb{Q}_l(1) \simeq V_l(X/S),$$

and thus we have the desired embedding

$$\begin{aligned} X(S) \otimes_{\mathbb{Z}} \mathbb{Q}_l &\hookrightarrow [H^1(\overline{S}, R^1 f_* \mathbb{Q}_l(1))]^{\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)} \\ &= [H^1(\overline{S}, \overline{V})(1)]^{\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)}. \end{aligned}$$

Now Tate conjectured the following.

Conjecture 2.2. *The order of $L_{X/S}(s)$ at $s = 1$ should be equal to the rank of $X(S)$.*

Remark 2.1. *He has also conjectured that the leading term of the L-function should be interpreted in terms of arithmetic invariant of a fibration.*

The above discussion shows that this is equivalent to that the cycle map

$$X(S) \otimes_{\mathbb{Z}} \mathbb{Q}_l \to [H^1(\overline{S}, \overline{V})(1)]^{\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)}$$

is surjective and moreover that multiplicity of 1 in eigenvalues of ϕ_q^* on $H^1(\overline{S}, \overline{V})(1)$ is equal to $\dim[H^1(\overline{S}, \overline{V})(1)]^{\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)}$. The latter statement implies a certain semisimplicity of the action of ϕ_q^*. In [11] Kato and Trihan have shown that the Tate conjecture is true if the l-primary part of the Shafarevic-Tate group of a fibration is finite. (Notice that in their theorem a fibration may have singular fibers). Moreover they have computed the leading term of the L-function, which implies the original Tate conjecture.

2.4 An analog of the Birch and Swinnerton-Dyer conjecture over $\mathbb{C}$

In each model due to Tate, Deninger[7] and Fried[8] a discrete dynamical system is used in a very efficient way. But since the Birch and Swinnerton-Dyer conjecture is formulated over $\mathbb{Q}$ there does not exist such a system *a priori.* Therefore there arises a natural question.

Is it possible to formulate a geometric analog of the conjecture without any discrete dynamical system?

This was our motivation. Now we will formulate a geomeric analog of the Birch and Swinnerton-Dyer conjecture over $\mathbb{C}$. Although we do not have any discrete dynamical sytem, replacing étale cohomology groups in Tate's model by spaces of L^2-sections of a certain vector bundles over a Zariski open subset of a compact Riemann surface, *the heat kernel* of a Laplacian will play the same role as Frobenius. For the proof of the statements see [24].

Let X be a smooth projective variety of dimension $d + 1$. Suppose there is a map from X to a smooth projective curve S

$$X \xrightarrow{f} S$$

with a section σ. Suppose that X admits a structure of a commutative group scheme over S with the identity section σ whose generic fibre is an abelian variety. Moreover we assume the fibration satisfies all of the following conditions.

Condition 2.1. *1. Let Σ be a subset of S where the fibration degenerates. Then it has a semistable reduction at each point of Σ.*

2. *We set*
$$S_0 = S \setminus \Sigma.$$
Then the Euler-Poincaré characteristic of S_0 is negative. (Thus S_0 is a quotient of the Poicaré upper halfplane $\mathbb{H}^2$ by a discrete subgroup Γ of $SL_2(\mathbb{R})$.)

3. -1_2 *is not contained in* Γ.

4. *Let fix a base point x_0 of S_0 and we will identify $\pi_1(S_0, x_0)$ and Γ. Let ρ_X be the monodromy representation:*
$$\Gamma \simeq \pi_1(S_0, x_0) \xrightarrow{\rho_X} \mathrm{Aut}(V), \quad V = H^1(f^{-1}(x_0), \mathbf{R}).$$
Then there is a positive constants α and C such that
$$|\mathrm{Tr}\rho_X(\gamma)| \leq Ce^{\alpha l(\gamma)}$$
is satisfied for any hyperbolic element γ of Γ.

5. *The moduli of the fibration is not a constant. Namely it satisfies*
$$H^0(S, R^1 f_* \mathcal{O}_X) = 0.$$

By the monodromy theorem [21], (1) implies Γ has no elliptic element. The (3) and (4) are not so restrictive. For example, if neccessary taking a subgroup of finite index, (3) will be always satisfied. Also it is easy to see (4) is satisfied if the monodromy representation is a restriction of a homomorphism of algebraic groups from $SL_2(\mathbf{R})$ to $GL_{2d}(\mathbf{R})$ to Γ.

In order to define the Selberg and the Ruelle L functions of the fibration, we will fix notation.

Let Γ^*_{conj} be the set of non trivial conjugacy classes of Γ and let $\Gamma^*_{h,conj}$ be its subset consisting of hyperbolic conjugacy classes. There is a natural bijection between $\Gamma^*_{h,conj}$ and the set of non trivial closed geodesics and we will identify them. Then $\gamma \in \Gamma^*_{h,conj}$ is uniquely written as
$$\gamma = \gamma_0^{\mu(\gamma)},$$
where γ_0 is a prime closed geodesic(i.e. not a positive multiple of an another one) and $\mu(\gamma)$ is a positive integer, which will be referred as *a multiplicity*. The subset of $\Gamma^*_{h,conj}$ consisiting of prime closed geodesics will be denoted by $\Gamma^*_{pr,conj}$. The *length* $l(\gamma)$ of $\gamma \in \Gamma^*_{h,conj}$ is defined by the length of the corresponding closed geodesic. Finally we set
$$D(\gamma) = e^{\frac{1}{2}l(\gamma)} - e^{-\frac{1}{2}l(\gamma)}.$$

Now *the Selberg L function* $L_{S,f}(s)$ is defined by
$$L_{S,f}(s) = \exp(-\sum_{\gamma \in \Gamma^*_{h,conj}} \frac{2\mathrm{Tr}\rho_X(\gamma)}{D(\gamma)\mu(\gamma)} e^{-sl(\gamma)}).$$

We also define the *Ruelle L function* $L_{R,f}(s)$ to be

$$L_{R,f}(s) = \frac{L_{S,f}(s-\frac{1}{2})}{L_{S,f}(s+\frac{1}{2})}.$$

It is easy to see that $L_{S,f}(s)$ absolutely convergents on $\{s \in \mathbf{C} \mid \mathrm{Re}\, s > \frac{1}{2} + \alpha\}$. One can prove that it is meromorphically continued to the whole plane and that $L_{S,f}(s)$ (resp. $L_{R,f}(s)$) is regular at $s = 0$ (resp. $s = \frac{1}{2}$). Our interest is $\mathrm{ord}_{s=0} L_{S,f}(s)$ and $\mathrm{ord}_{s=\frac{1}{2}} L_{R,f}(s)$.

Theorem 2.1. *Let $X(S)$ be the Mordell-Weil group of the fibration. Then we have*

$$2 \dim_{\mathbf{Q}} X(S) \otimes \mathbf{Q} \leq \mathrm{ord}_{s=0} L_{S,f}(s) = \mathrm{ord}_{s=\frac{1}{2}} L_{R,f}(s).$$

Moreover if $H^2(X, \mathcal{O}_X) = 0$, they are equal.

A simple computation shows that the Ruelle L function has *an Euler product*:

$$L_{R,f}(s) = c_0 \prod_{\gamma_0 \in \Gamma^*_{pr,conj}} (\det[1_{2d} - \rho_X(\gamma_0) e^{-sl(\gamma_0)}])^2,$$

where c_0 is a certain constant and 1_{2d} be the $2d \times 2d$ identity matrix. Now **Theorem 3.1** implies the following.

Theorem 2.2. *(A geometric analogue of the BSD conjecture over* $\mathbf{C}$*) The Euler product*

$$L_{X/S}(s) = \prod_{\gamma_0 \in \Gamma^*_{pr,conj}} \det[1_{2d} - \rho_X(\gamma_0) e^{-sl(\gamma_0)}]^2$$

has a zero at $s = \frac{1}{2}$ whose order is greater than or equal to $2 \dim_{\mathbf{Q}} X(S) \otimes \mathbf{Q}$. *Moreover if $H^2(X, \mathcal{O}_X) = 0$, then they are equal.*

The condition $H^2(X, \mathcal{O}_X) = 0$ corresponds to the finiteness of l-primary part of the Brauer group in the Tate conjecture. In fact let us define the topological Brauer group $Br(X)_{top}$ of X by

$$Br(X)_{top} = H^2(X, \mathcal{O}_X^{\times}),$$

where the cohomology is taken with respect to the classical topology. Then using the exponential sequaence, we see that $Br(X)_{top}$ is finitely generated if and only if $H^2(X, \mathcal{O}_X)$ vanishes.

3 The Iwasawa Main Conjecture and its geometric analog

In this chapter we will pursue an analogy between number theory and topology of threefolds. In particular our interest will be focused on similarity of knot theory and the Iwsawasa theory.

Let us briefly review the definition of the Alexander polynomial of a knot[18]. (See $3.1 for more complete treatment.) Let K be a knot (i.e. an embedded circle) in the standard 3-dimensional sphere S^3 and X its complement. Then the Alexander duality shows $H_1(X, \mathbb{Z})$ is isomorphic to the infinite cyclic group $\mathbb{Z}$. Let X_∞ be an infinite cyclic covering of X determined by geometric Galois theory and g a generator of $\mathrm{Gal}(X_\infty/X)$. Then we will see that $H_1(X_\infty, \mathbb{Q})$ is a finite dimensional vector space over $\mathbb{Q}$ on which g acts. The Alexander polynomial is defined to be its characteristic polynomial.

The Iwasawa module and the Iwasawa invariant are arithmetic objects which correspond to $H_1(X_\infty, \mathbb{Q})$ and the Alexander polynomial, respectively. Before going into furthur we will explain why the integer ring of a number field corresponds to a topological threefold.

Let D be the ring of integers of a number field F and $Z = \mathrm{Spec}(D)$. Based on the Artin-Verdier duality Mazur has computed étale cohomology groups of Z with a finite coefficient([14], pp. 539). In particular he has shown that, if F is totally imaginary,

$$H^q(Z, \mathbb{Z}/(n)) = \begin{cases} \mathbb{Z}/(n) & \text{if} \quad q = 0 \\ (\mathrm{Pic(Z)} \otimes_{\mathbb{Z}} \mathbb{Z}/(n))^* & \text{if} \quad q = 1 \\ (\mathrm{Ext}_Z(\mathbb{Z}/(n), \mathbb{G}_m))^* & \text{if} \quad q = 2 \\ \mu_n(D) & \text{if} \quad q = 3 \\ 0 & \text{if} \quad q > 3 \end{cases}$$

Here $*$ is the Pontryagin dual and $\mu_n(D)$ is the set of n-th roots of unity contained in D. Thus Z has the same property as a topological threefold from a viewpoint of cohomology. Moreover his computation shows that an ideal class group will play the same role as the first cohomology group. Moreover since by the theorem of Minkowski $\mathbb{Q}$ does not possesses a non-trivial finite extension which is unramified everywhere, we may consider $\mathrm{Spec}(\mathbb{Z})$ corresponds to S^3. Now remember that we have explained a prime corresponds to a circle. Thus an arithmetic substitute of a knot complement X should be $\mathrm{Spec}\mathbb{Z}[\frac{1}{p}]$, where p is a prime. Let ζ_N be a primitive N-th root of unity. Then $\mathrm{Spec}\mathbb{Z}[\zeta_{p^n}]$ is an unramified $(\mathbb{Z}/(p^n))^*$-extension of $\mathrm{Spec}\mathbb{Z}[\frac{1}{p}]$ and it is natural to think about that its ideal class group should play the same role as $H_1(X_\infty, \mathbb{Q})$. Now we will explain this idea more precisely.

3.1 The Alexander invariant

In this section we will discuss *the Alexander invariant*, which is a generalization of the Alexander polynomial to a twisted case. We will see that it plays the same role as RHS of (2.5). Although Milnor has used homology groups, we rather prefer to work on cohomologies.

Let $\Lambda_\infty = \mathbb{C}[t, t^{-1}]$ be a Laurent polynomial ring of complex coefficients. The following lemma is easy to see.

Lemma 3.1. *Let f and g be elements of Λ_∞ such that*

$$f = ug,$$

where u is a unit. Then their order at $t = 1$ are equal:

$$\mathrm{ord}_{t=1} f = \mathrm{ord}_{t=1} g.$$

Let $(C_\cdot, \partial_\cdot)$ be a bounded complex of free Λ_∞-modules of finite rank whose homology groups are torsion Λ_∞-modules. Suppose that it is given a base $\mathbf{c}_i$ for each C_i. Such a complex will refered as *a based complex*. We set

$$C_{even} = \oplus_{i\equiv 0(2)} C_i, \quad C_{odd} = \oplus_{i\equiv 1(2)} C_i,$$

which are free Λ_∞-modules of finite rank with basis $\mathbf{c}_{even} = \oplus_{i\equiv 0(2)} \mathbf{c}_i$ and $\mathbf{c}_{odd} = \oplus_{i\equiv 1(2)} \mathbf{c}_i$ respectively. Choose a base $\mathbf{b}_{even}$ of a Λ_∞-submodule B_{even} of C_{even} (necessary free) which is the image of the differential and column vectors $\mathbf{x}_{odd}$ of C_{odd} so that

$$\partial \mathbf{x}_{odd} = \mathbf{b}_{even}.$$

Similarly we take $\mathbf{b}_{odd}$ and $\mathbf{x}_{even}$ satisfying

$$\partial \mathbf{x}_{even} = \mathbf{b}_{odd}.$$

Then $\mathbf{x}_{even}$ and $\mathbf{b}_{even}$ are expressed by a linear combination of $\mathbf{c}_{even}$:

$$\mathbf{x}_{even} = X_{even}\mathbf{c}_{even}, \quad \mathbf{b}_{even} = Y_{even}\mathbf{c}_{even},$$

and we obtain a square matrix

$$\begin{pmatrix} X_{even} \\ Y_{even} \end{pmatrix}.$$

Similarly equations

$$\mathbf{x}_{odd} = X_{odd}\mathbf{c}_{odd}, \quad \mathbf{b}_{odd} = Y_{odd}\mathbf{c}_{odd}$$

yield a square matrix

$$\begin{pmatrix} X_{odd} \\ Y_{odd} \end{pmatrix}.$$

Now *the Milnor-Reidemeister torsion* $\tau_{\Lambda_\infty}(C_\cdot, \mathbf{c}_\cdot)$ of the based complex $\{C_\cdot, \mathbf{c}_\cdot\}$ is defined as

$$\tau_{\Lambda_\infty}(C_\cdot, \mathbf{c}_\cdot) = \pm \frac{\det \begin{pmatrix} X_{even} \\ Y_{even} \end{pmatrix}}{\det \begin{pmatrix} X_{odd} \\ Y_{odd} \end{pmatrix}} \tag{3.1}$$

It is known $\tau_{\Lambda_\infty}(C., \mathbf{c}.)$ is independent of a choice of $\mathbf{b}.$.

Since $H.(C.)$ are torsion Λ_∞-modules, they are finite dimensional complex vector spaces. Let τ_{i*} be the action of t on $H_i(C.)$. Then *an Alexander invariant* is defined to be the alternating product of their characteristic polynomials:

$$A_{C.}(t) = \prod_i \det[t - \tau_{i*}]^{(-1)^i}. \tag{3.2}$$

Then **Assertion 7** of [18] shows fractional ideals generated by $\tau_{\Lambda_\infty}(C., \mathbf{c}.)$ and $A_{C.}(t)$ are equal:

$$(\tau_{\Lambda_\infty}(C., \mathbf{c}.)) = (A_{C.}(t)).$$

In particular **Lemma 3.1** implies

$$\mathrm{ord}_{t=1}\tau_{\Lambda_\infty}(C., \mathbf{c}.) = \mathrm{ord}_{t=1}A_{C.}(t), \tag{3.3}$$

and we know

$$\tau_{\Lambda_\infty}(C., \mathbf{c}.) = \delta \cdot t^k A_{C.}(t),$$

where δ is a non-zero complex number and k is an integer. δ will be referred as *the difference* of the Alexander invariant and the Milnor-Reidemeister torsion.

Let $\{\overline{C.}, \overline{\partial}\}$ be a bounded complex of a finite dimensional vector spaces over $\mathbb{C}$. Given basis $\mathbf{c}_i$ and $\mathbf{h}_i$ for each $\overline{C_i}$ and $H_i(\overline{C.})$ respectively, the Milnor-Reidemeister torsion $\tau_{\mathbb{C}}(\overline{C.}, \overline{\mathbf{c}.})$ is also defined ([17]). Such a complex will be referred as *a based complex* again. By definition, if the complex is acyclic, it coincides with (3.1). Let $(C., \mathbf{c}.)$ be a based bounded complex over Λ_∞ whose homology groups are torsion Λ_∞-modules. Suppose its annihilator $Ann_{\Lambda_\infty}(H_i(C.))$ does not contain $t-1$ for each i. Then

$$(\overline{C.}, \overline{\partial}) = (C., \mathbf{c}.) \otimes_{\Lambda_\infty} \Lambda_\infty/(t-1)$$

is a based acyclic complex over $\mathbb{C}$ with a preferred base $\overline{\mathbf{c}.}$ which is the reduction of $\mathbf{c}.$ modulo $(t-1)$. This observation shows the following proposition.

Proposition 3.1. *Let $(C., \mathbf{c}.)$ be a based bounded complex over Λ_∞ whose homology groups are torsion Λ_∞-modules. Suppose the annihilator $Ann_{\Lambda_\infty}(H_i(C.))$ does not contain $t-1$ for each i. Then we have*

$$\tau_{\Lambda_\infty}(C., \mathbf{c}.)|_{t=1} = \tau_{\mathbb{C}}(\overline{C.}, \overline{\mathbf{c}.})$$

For a later purpose we will consider duals.

Let $\{C^{\cdot}, d\}$ be the dual complex of $\{C., \partial\}$:

$$(C^{\cdot}, d) = Hom_{\Lambda_\infty}((C., \partial), \Lambda_\infty).$$

By the universal coefficient theorem we have

$$H^q(C^{\cdot}, d) = Ext^1_{\Lambda_\infty}(H_{q-1}(C., \partial), \Lambda_\infty)$$

and the cohomology groups are torsion Λ_∞-modules. Moreover the characteristic polynomial of $H^q(C^\cdot, d)$ is equal to one of $H_{q-1}(C_\cdot, \partial)$. Thus if we define *the Alexander invariant* $A_{C^\cdot}(t)$ of $\{C^\cdot, d\}$ by the same way as (3.2), we have

$$A_{C^\cdot}(t) = A_{C_\cdot}(t)^{-1}. \tag{3.4}$$

Let us apply the theory to a threefold. The proofs of theorems will be found in [23].

In general let X be a connected finite CW-complex and $\{c_{i,\alpha}\}_\alpha$ its i-dimensional cells. We will fix its base point x_0 and let Γ be the fundamental group of X. Let ρ be a unitary representation of finite rank and V_ρ its representation space. Suppose that there is a surjective homomorphism

$$\Gamma \xrightarrow{\epsilon} \mathbb{Z},$$

and let X_∞ be the infinite cyclic covering of X which corresponds to $\operatorname{Ker}\epsilon$ by the Galois theory. Finally let $\tilde{X}$ be the universal covering of X.

The chain complex $(C_\cdot(\tilde{X}), \partial)$ is a complex of free $\mathbf{C}[\Gamma]$-module of finite rank. We take a lift of $\mathbf{c}_i = \{c_{i,\alpha}\}_\alpha$ as a base of $C_i(\tilde{X})$, which will be also denoted by the same character. Note that such a choice of base has an ambiguity of the action of Γ.

Following [12] consider a complex over $\mathbb{C}$:

$$C_i(X, \rho) = C_i(\tilde{X}) \otimes_{\mathbb{C}[\Gamma]} V_\rho.$$

On the other hand, restricting ρ to $\operatorname{Ker}\epsilon$, we will make a chain complex

$$C_\cdot(X_\infty, \rho) = C_\cdot(\tilde{X}) \otimes_{\mathbb{C}[\operatorname{Ker}\epsilon]} V_\rho,$$

which has the following description. Let us consider $\mathbb{C}[\mathbb{Z}] \otimes_{\mathbb{C}} V_\rho$ as Γ-module by

$$\gamma(p \otimes v) = p \cdot t^{\epsilon(\gamma)} \otimes \rho(\gamma) \cdot v, \quad p \in \mathbb{C}[\mathbb{Z}],\, v \in V_\rho.$$

Then $C_\cdot(X_\infty, \rho)$ is isomorphic to a complex ([12] **Theorem 2.1**):

$$C_\cdot(X, V_\rho[\mathbb{Z}]) = C_\cdot(\tilde{X}) \otimes_{\mathbb{C}[\Gamma]} (\mathbb{C}[\mathbb{Z}] \otimes_{\mathbb{C}} V_\rho).$$

and we know $C_\cdot(X_\infty, \rho)$ is a bounded complex of free Λ_∞-modules of finite rank. We will fix a unitary base $\mathbf{v} = \{v_1, \cdots, v_m\}$ of V_ρ and make it a based complex with a preferred base $\mathbf{c}_\cdot \otimes \mathbf{v} = \{c_{i,\alpha} \otimes v_j\}_{\alpha,i,j}$.

In the following we will fix an isomorphism between $\mathbb{C}[\mathbb{Z}]$ and Λ_∞ which sends the generator 1 of $\mathbb{Z}$ to t and will identify them. By the surjection:

$$\Lambda_\infty \to \Lambda_\infty/(t-1) \simeq \mathbb{C},$$

$C.(X_\infty, \rho) \otimes_{\Lambda_\infty} \mathbb{C}$ is isomorphic to $C.(X, \rho)$. Moreover if we take $\mathbf{c}. \otimes \mathbf{v}$ as a base of the latter, they are isomorphic as based complexes.

Let $C^{\cdot}(\tilde{X})$ be the cochain complex of $\tilde{X}$:

$$C^{\cdot}(\tilde{X}) = Hom_{\mathbb{C}[\Gamma]}(C.(\tilde{X}), \mathbb{C}[\Gamma]),$$

which is a bounded complex of free $\mathbb{C}[\Gamma]$-module of finite rank. For each i we will take the dual $\mathbf{c}^i = \{c^i_\alpha\}_\alpha$ of $\mathbf{c}_i = \{c_{i,\alpha}\}_\alpha$ as a base of $C^i(\tilde{X})$. Thus $C^{\cdot}(\tilde{X})$ becomes a based complex with a preferred base $\mathbf{c}^{\cdot} = \{\mathbf{c}^i\}_i$. Since ρ is a unitary representation, it is easy to see that the dual complex of $C.(X_\infty, \rho)$ is isomorphic to

$$C^{\cdot}(X_\infty, \rho) = C^{\cdot}(\tilde{X}) \otimes_{\mathbb{C}[\Gamma]} (\Lambda_\infty \otimes_{\mathbb{C}} V_\rho),$$

if we twist its complex structure by the complex conjugation. Also we will make it a based complex by the base $\mathbf{c}^{\cdot} \otimes \mathbf{v} = \{c^i_\alpha \otimes v_j\}_{\alpha,i,j}$.

Dualizing the exact sequence

$$0 \to C.(X_\infty, \rho) \overset{t-1}{\to} C.(X_\infty, \rho) \to C.(X, \rho) \to 0$$

in the derived category of bounded complex of finitely generated Λ_∞-modules, we will obtain a distinguished triangle:

$$C^{\cdot}(X, \rho) \to C^{\cdot}(X_\infty, \rho) \overset{t-1}{\to} C^{\cdot}(X_\infty, \rho) \to C^{\cdot}(X, \rho)[1] \to . \tag{3.5}$$

Here we set

$$C^{\cdot}(X, \rho) = C^{\cdot}(\tilde{X}, \rho) \otimes_{\mathbb{C}[\Gamma]} V_\rho.$$

and for a bounded complex $C^{\cdot}$, $C^{\cdot}[n]$ denotes its *shift*, which is defined as

$$C^i[n] = C^{i+n}.$$

Note that $C^{\cdot}(X, \rho)$ is isomorphic to the reduction of $C^{\cdot}(X_\infty, \rho)$ modulo $(t-1)$.

Let τ^* be the action of t on $H^{\cdot}(X_\infty, \rho)$. Then (8) induces an exact sequence:

$$\to H^q(X, \rho) \to H^q(X_\infty, \rho) \overset{\tau^*-1}{\to} H^q(X_\infty, \rho) \to H^{q+1}(X, \rho) \to . \tag{3.6}$$

In the following, we will assume that the dimension of X is three and that all $H.(X_\infty, \mathbb{C})$ and $H.(X_\infty, \rho)$ are finite dimensional vector spaces over $\mathbb{C}$. The arguments of §4 of [18] will show the following theorem.

Theorem 3.1. *([18])*

1. *For $i \geq 3$, $H^i(X_\infty, \rho)$ vanishes.*
2. *For $0 \leq i \leq 2$, $H^i(X_\infty, \rho)$ is a finite dimensional vector space over $\mathbb{C}$ and there is a perfect pairng:*

$$H^i(X_\infty, \rho) \times H^{2-i}(X_\infty, \rho) \to \mathbb{C}.$$

The perfect pairing will be referred as *the Milnor duality.*

Let $A_{\rho *}(t)$ and $A^*_\rho(t)$ be the Alexander invariants of $C_\cdot(X_\infty,\,\rho)$ and $C^\cdot(X_\infty,\,\rho)$ respectively. Since the latter complex is the dual of the previous one, (3.4) implies

$$A^*_\rho(t) = A_{\rho *}(t)^{-1}.$$

Let $\tau^*_{\Lambda_\infty}(X_\infty,\,\rho)$ be the Milnor-Reidemeister torsion of $C^\cdot(X_\infty,\,\rho)$ with respect to a preferred base $\mathbf{c}^\cdot \otimes \mathbf{v}$. Because of an ambiguity of a choice of $\mathbf{c}^\cdot$ and $\mathbf{v}$, it is well-defined modulo

$$\{zt^n \mid z \in \mathbb{C},\, |z| = 1,\, n \in \mathbb{Z}\}.$$

Let δ_ρ be the absolute value of the difference between $A^*_\rho(t)$ and $\tau^*_{\Lambda_\infty}(X_\infty,\,\rho)$. The previous discussion of the torsion of a complex implies the following theorem.

Theorem 3.2. *The order of $\tau^*_{\Lambda_\infty}(X_\infty,\,\rho)$, $A^*_\rho(t)$ and $A_{\rho *}(t)^{-1}$ at $t = 1$ are equal. Let β be the order. Then we have*

$$\begin{aligned}\lim_{t\to 1} |(t-1)^{-\beta}\tau^*_{\Lambda_\infty}(X_\infty,\,\rho)| &= \delta_\rho \lim_{t\to 1} |(t-1)^{-\beta}A^*_\rho(t)| \\ &= \delta_\rho \lim_{t\to 1} |(t-1)^{-\beta}A_{\rho *}(t)^{-1}|.\end{aligned}$$

By **Theorem 3.1** we see that the Alexander invariant becomes

$$A^*_\rho(t) = \frac{\det[t-\tau^* \mid H^0(X_\infty,\,\rho)]\cdot \det[t-\tau^* \mid H^2(X_\infty,\,\rho)]}{\det[t-\tau^* \mid H^1(X_\infty,\,\rho)]}. \tag{3.7}$$

Suppose $H^0(X_\infty,\,\rho)$ vanishes. Then the Milnor duality implies

$$A^*_\rho(t)^{-1} = \det[t-\tau^* \mid H^1(X_\infty,\,\rho)],$$

which is a generator of the characteristic ideal of $H^1(X_\infty,\,\rho)$. Thus if we think X_∞ corresponds to the $\mathbb{Z}_p$-extension of $\mathbb{Q}$, a similarity between the $char_\Lambda(X_{\infty,i})$ and the ideal generated by the Alexander invariant is clear.

Let $h^i(\rho)$ be the dimension of $H^i(X,\,\rho)$. Then the standard argument shows the following theorem.

Theorem 3.3. *Suppose $H^0(X_\infty,\,\rho)$ vanishes. Then we have*

$$\mathrm{ord}_{t=1} A^*_\rho(t) \le -h^1(\rho),$$

and the identity holds if the action of τ^* on $H^1(X_\infty,\,\rho)$ is semisimple.

Theorem 3.4. *Suppose $H^i(X,\,\rho)$ vanishes for all i. Then we have*

$$|\tau^*_{\mathbb{C}}(X,\,\rho)| = \delta_\rho |A^*_\rho(1)| = \frac{\delta_\rho}{|A_{\rho *}(1)|}.$$

Proof. The exact sequence (3.6) and the assumption implies $t-1$ is not contained in the annihilator of $H^{\cdot}(X_\infty,\,\rho)$. Now the theorem will follow from **Proposition 3.1** and **Theorem 3.2**.

□

When X is a mapping torus, we obtain a finer information of the absolute value of the leading term of the Alexander invariant. A proof of the following theorem is essentially contained in [7] or [8].

Theorem 3.5. *Let f be an automorphism of a connected finite CW-complex of dimension two S and X its mapping torus. Let ρ be a unitary representation of the fundamental group of X which satisfies $H^0(S,\,\rho)=0$. Suppose that the surjective homomorphism*

$$\Gamma \xrightarrow{\epsilon} \mathbb{Z}$$

is induced from the structure map

$$X \to S^1,$$

and that the action of f^* on $H^1(S,\,\rho)$ is semisimple. Then the order of $A^*_\rho(t)$ is $-h^1(\rho)$ and

$$\lim_{t\to 1} |(t-1)^{h^1(\rho)} A^*_\rho(t)| = |\tau^*_{\mathbb{C}}(X,\rho)|.$$

In particular we know that $|\tau^*_{\mathbb{C}}(X,\rho)|$ is determined by the homotopy class of f. As before without semisimplicity of f^*, we only have

$$\mathrm{ord}_{t=1} A^*_\rho(t) \le -h^1(\rho).$$

Let X is the complement of a knot K in S^3 and ρ a unitary representation of its fundamental group. Since, by the Alexander duality, $H_1(X,\,\mathbb{Z})$ is isomorphic to $\mathbb{Z}$, X admits an infinite cyclic covering X_∞. Suppose $H_i(X_\infty,\,\rho)$ are finite dimensional complex vector spaces for all i. Then our twisted Alexander invariant is essentially the inverse of the twisted Alexander polynomial $\Delta_{K,\rho}(t)$ defined by Kitano [13]. More precisely

Theorem 3.6. *Suppose $H^0(X_\infty,\,\rho)$ vanishes. Then we have*

$$\mathrm{ord}_{t=1}\Delta_{K,\rho}(t) = -\mathrm{ord}_{t=1}A^*_\rho(t) \ge h^1(\rho),$$

and the identity holds if the action of τ^* on $H^1(X_\infty,\,\rho)$ is semisimple. Moreover suppose $H^i(X,\,\rho)$ vanishes for all i. Then

$$|\tau^*_{\mathbb{C}}(X,\,\rho)| = \frac{1}{|\Delta_{K,\rho}(1)|}.$$

3.2 The Iwasawa module and the Iwasawa invariant

We will explain arithmetic substitute for the Alezander inavariant, *the Iwasawa module* and *the Iwasawa invariant.* This is also an object which corresponds to RHS of (2.6).

We will fix a p^n-th root of unity ζ_{p^n} as

$$\zeta_{p^n} = \exp(\frac{2\pi i}{p^n}),$$

and let μ_{p^n} be the subgroup of $\mathbb{C}^\times$ generated by ζ_{p^n}. Since $\zeta_{p^n}^p = \zeta_{p^{(n-1)}}$ for any n, the invese limit with respect to the p-th power:

$$\zeta_{p^\infty} = \lim_{\leftarrow} \zeta_{p^n} \in \lim_{\leftarrow} \mu_{p^n}.$$

is defined.

There is a canonical decomposition of Galois group:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}),$$

where $\mathbb{Q}_n$ is a finite abelian extension of $\mathbb{Q}$. In the decomposition, the former and the latter are isomorphic to $(\mathbb{Z}/(p))^\times$ and the kernel of the mod p reduction map:

$$\Gamma_n = \mathrm{Ker}[(\mathbb{Z}/(p^n))^\times \to (\mathbb{Z}/(p))^\times] \simeq \mathbb{Z}/(p^{n-1}),$$

respectively. Taking the inverse limit with respect to n, we have an infinite extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$ such that

$$\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = \lim_{\leftarrow} \Gamma_n \overset{\kappa}{\simeq} (1 + p\mathbb{Z}_p)^\times \overset{\log}{\simeq} \mathbb{Z}_p.$$

Here the cyclotomic character κ is defined as

$$\gamma(\zeta_{p^\infty}) = \zeta_{p^\infty}^{\kappa(\gamma)}, \quad \gamma \in \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}).$$

Then a topological ring

$$\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]] = \lim_{\leftarrow} \mathbb{Z}_p[\Gamma_n],$$

is referred as *the Iwasawa algebra*. Choosing a topological generator γ_0 of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ (e.g. $\kappa(\gamma_0) = 1 + p$), Λ is isomorphic to a formal power series ring $\mathbb{Z}_p[[t]]$. Thus we have a isomorphism

$$\begin{aligned} \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\zeta_\infty)/\mathbb{Q})]] &\simeq \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})] \otimes_{\mathbb{Z}_p} \Lambda \\ &\simeq \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[t]], \end{aligned}$$

where $\mathbb{Q}(\zeta_{p^\infty})$ is the union of $\{\mathbb{Q}(\zeta_{p^n})\}_n$.

Let A_n be the p-primary part of the ideal class group of $\mathbb{Q}(\zeta_{p^n})$. Then the *the Iwasawa module* is defined to be

$$X_\infty = \varprojlim A_n.$$

Here the inverse limit is taken with respect to the norm map. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$ acts on A_n, X_∞ becomes a $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})]]$-module. For an integer $i \in \mathbb{Z}/(p-1)$, let $X_{\infty,i}$ be its ω^i-component:

$$X_{\infty,i} = X_\infty \otimes_{\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})]} \mathbb{Z}_p(\omega^i).$$

Here $\mathbb{Z}_p(\omega^i)$ is isomorphic to $\mathbb{Z}_p$ as an abstract module but has a $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$-action by the character ω^i. It is known $X_{\infty,i}$ is a finitely generated torsion Λ-module and let $char_\Lambda(X_{\infty,i})$ be its characteristic ideal. Its generator will be referred as *the Iwasawa invariant.*

3.3 p-adic zeta function and the Iwasawa Main Conjecture

In the previous section we have explained an object in a p-adic world which plays the same role as RHS of (2.5) or (2.6). In this section we will explain *the Iwasawa main conjecture*, which predicts that we should have the same equation as them even in a p-adic setting. Intuitively an object which sits in LHS should be a Dirichlet L-function. But it lives in the complex world we have to replace it by a p-adic analytic function, which is nothing but *a p-adic L-function* due to Kubota and Leopoldt. For simplicity we assume p is an odd prime.

Let χ be a Dirichlet character of conductor f_χ. It is known special values of the Dirichlet L-function

$$L(s,\,\chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$$

at nonpositive integers are given by

$$L(1-n,\,\chi) = -\frac{B_{n,\chi}}{n}, \quad 1 \le n \in \mathbb{Z}. \tag{3.8}$$

Here $B_{n,\chi}$ is a generalized Bernoulli number defined by

$$\sum_{a=1}^{f_\chi} \frac{\chi(a) T e^{aT}}{e^{f_\chi T} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{T^n}{n!}.$$

By definition the Kubota-Leopoldt L-function is a p-adic analytic function which interpolates special values of Dirichlet's L-function. More precisely let us fix a completion of the algebraic closure of $\mathbb{Q}_p$, which will be denoted by $\mathbb{C}_p$. Let $|\cdot|_p$ be a p-adic norm on $\mathbb{C}_p$ normalized as

$$|p|_p = p^{-1}.$$

Fact 3.1. *For a non-trivial Dirichlet character χ (resp. the trivial character $\mathbf{1}$), there is the unique analytic function $L_p(s,\,\chi)$ (resp. meromorphic function $L_p(s,\,\mathbf{1})$) on a domain*

$$D = \{s \in \mathbb{C}_p \mid |s|_p < p^{-\frac{p-2}{p-1}}\},$$

which satisfies

$$L_p(1-n,\,\chi) = -(1-\chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}, \quad 1 \le n \in \mathbb{Z}, \tag{3.9}$$

where ω is the Teichmüller character. Moreover $L_p(s,\,\mathbf{1})$ is analytic outside $s=1$ and has a simple pole there whose residue is $1-p^{-1}$.

Let j be an integer such that $j \equiv n (\mathrm{mod} \quad p-1)$, $0 \le j < p-1$. Then combining (2.1) and (2.2) we obtain the following identity of special values of these two functions:

$$L_p(1-n,\,\chi) = (1-\chi\omega^{-j}(p)p^{n-1})L(1-n,\,\chi\omega^{-j}), \quad (1 \le n \in \mathbb{Z}).$$

Thus we may consider $L_p(s,\,\chi)$ as a p-adic analog of $L(s,\,\chi)$. Moreover it is known that, for an even integer such that $\omega^i \ne \mathbf{1}$, there is $f(t,\,\omega^i) \in \mathbb{Z}_p[[t]]$, which is called *the Iwasawa power series*, satisfying

$$f((1+p)^s-1,\,\omega^i) = L_p(s,\,\omega^i), \quad s \in \mathbb{Z}_p. \tag{3.10}$$

Let γ_0 be a topological generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ so that

$$\kappa(\gamma_0) = 1+p,$$

and φ an isomorphism

$$\Lambda = \mathbb{Z}_p[[\Gamma_\infty]] \overset{\varphi}{\simeq} \mathbb{Z}_p[[t]], \quad \varphi(\gamma_0) = 1+t.$$

By these identification a character κ^s ($s \in \mathbb{Z}_p$) induces a homomorphism of algebra

$$\mathbb{Z}_p[[t]] \xrightarrow{\kappa^s} \mathbb{Z}_p$$

which is

$$\kappa^s(t) = \kappa^s(\gamma_0) - 1 = (1+p)^s - 1.$$

In particular, by (2.3), we obtain

$$\kappa^s(f(t,\,\omega^i)) = f((1+p)^s-1,\,\omega^i) = L_p(s,\omega^i).$$

for an even integer i such that ω^i is nontrivial. Now we formulate the Iwasawa Main Conjecture.

Conjecture 3.1. *Let i be an odd integer such that $i \ne 1\,(\mathrm{mod}\,p-1)$. Then the characteristic ideal $char_\Lambda(X_{\infty,i})$ should be generated by $f(t,\,\omega^{1-i})$.*

The conjecture is first proved by Mazur and Wiles([16]). Today there is a much simpler proof which uses Kolyvagin's Euler system (e.g. [28] Chapter 15).

3.4 The Ruelle-Selberg L-function

In this section we will introduce a Ruelle-Selberg L-function which plays the same role as the p-adic function in the Iwasawa Main Conjecture.

Let X be a hyperbolic threefold of finite volume, which is a quotient of the Poincaré upper half space $\mathbb{H}^3$ by a torsion free discrete subgroup Γ_g of $PSL_2(\mathbb{C})$. Since there is a natural bijection between the set of closed geodesics and one of hyperbolic conjugacy classes $\Gamma_{g,conj}$, we will identify them. Using this identification, the length $l(\gamma)$ of $\gamma \in \Gamma_{g,conj}$ is defined as one of the corresponding closed geodesic.

Let ρ be a unitary representation of rank r. Then a Ruelle-Selberg L-function is formally defined to be

$$R_\rho(z) = \prod_\gamma \det[1 - \rho(\gamma)e^{-zl(\gamma)}],$$

where γ runs over prime closed geodesics, i.e. not a positive multiple of another one. It is known $R_\rho(z)$ absolutely convergents if $\mathrm{Re}\, z$ is sufficiently large. We will study it separately according to whether X is compact or noncompact.

Suppose X is compact. The following theorem is a special case of [9]**Theorem 3**.

Fact 3.2. *The Ruelle-Selberg L-function is meromorphically continued to the whole plane and its order at $z = 0$ is*

$$e = 4h^0(\rho) - 2h^1(\rho).$$

Moreover we have

$$\lim_{z \to 0} |z^{-e} R_\rho(z)| = |\tau^*_{\mathbb{C}}(X, \rho)|^2.$$

Although Fried has shown his results for an orthogonal representation, his proof is still valid for a unitary case.

Now we want to generalize Fried's theorem to a noncompact case. By a technical reason (which should be overcome), we assume that $r = 1$ (i.e. ρ is a unitary character) and that X has only one cusp. Let Γ_∞ be the fundamental group at the cusp and $\rho|_{\Gamma_\infty}$ the restriction. Then we have proved the following theorem [25].

Theorem 3.7. *The Ruelle-Selberg L-function is meromorphically continued to the whole plane. Suppose $\rho|_{\Gamma_\infty}$ is trivial. Then we have*

$$\mathrm{ord}_{z=0} R_\rho(z) = 2(2h^0(\rho) + 1 - h^1(\rho)).$$

On the contrary if $\rho|_{\Gamma_\infty}$ is nontrivial,

$$\mathrm{ord}_{z=0} R_\rho(z) = -2h^1(\rho).$$

As for a special value, we have shown the following result [26].

Theorem 3.8. *Suppose that $\rho|_{\Gamma_\infty}$ is nontrivial and that $h^1(\rho)$ vanishes. Then*

$$|R_\rho(0)| = |\tau^*_{\mathbb{C}}(X,\rho)|^2.$$

These theorems are proved by a computation based on the Selberg trace formula. In the course of the proof, we have also obtained an analogue of the Riemann hypothesis.

Theorem 3.9. *([25]) Suppose that $\rho|_{\Gamma_\infty}$ is nontrivial. Zeros and poles of $R_\rho(z)$ is, except for finitely many of them, are located on lines:*

$$\{s \in \mathbb{C} \,|\, \mathrm{Re}\, s = -1,\, 0,\, 1\}.$$

If $\rho|_{\Gamma_\infty}$ is trivial, there are another poles or zeros which are derived from a scattering term. These correspond to trivial zeros *of the Riemann's zeta function.*

3.5 A geometric analog of the Iwasawa Main Conjecture

Let X be a hyperbolic threefold of finite volume which admits an infinite cyclic covering X_∞. Let g be a generator of $\mathrm{Gal}(X_\infty/X)$. Let ρ be a unitary representation of the fundamental group of X and we will always assume that the pair $(X_\infty,\, \rho)$ satisfies the assumption of the Milnor duality.

Since $H^0(X,\, \rho)$ is a subspace of $H^0(X_\infty,\, \rho)$, **Theorem 3.3**, **Theorem 3.4**, **Theorem 3.5** and **Fact 3.2** imply the following theorem.

Theorem 3.10. *Suppose that X is compact and that $H^0(X_\infty,\, \rho)$ vanishes. Then*

$$-2h^1(\rho) = \mathrm{ord}_{z=0} R_\rho(z) \geq 2\mathrm{ord}_{t=1} A^*_\rho(t),$$

and the identity holds if the action of g on $H^1(X_\infty,\, \rho)$ is semisimple. If all $H^i(X,\, \rho)$ vanish, we have

$$|R_\rho(0)| = \delta_\rho^2 |A^*_\rho(1)|^2.$$

Moreover suppose that X is homeomorphic to a mapping torus of an automorphism of a CW-complex of dimension two and that the surjective homomorphism from the fundamental group to $\mathrm{Gal}(X_\infty/X) \simeq \mathbb{Z}$ is induced from the structure map:

$$X \to S^1.$$

Then if the action of g on $H^1(X_\infty,\, \rho)$ is semisimple, we have

$$\lim_{z\to 0} |z^{2h^1(\rho)} R_\rho(z)| = \lim_{t \to 1} |(t-1)^{h^1(\rho)} A^*_\rho(t)|^2 = |\tau^*_{\mathbb{C}}(X,\, \rho)|^2.$$

When X is noncompact, **Theorem 3.3**, **Theorem 3.4**, **Theorem 3.7** and **Theorem 3.8** show the following theorem.

Theorem 3.11. *Suppose X has only one cusp and let ρ be a unitary character of its fundamental group. Let us assume $H^0(X_\infty, \rho)$ vanishes.*

1. *If $\rho|_{\Gamma_\infty}$ is nontrivial, we have*

$$-2h^1(\rho) = \mathrm{ord}_{z=0} R_\rho(z) \geq 2\mathrm{ord}_{t=1} A^*_\rho(t).$$

   Moreover if all $H^i(X, \rho)$ vanish, we have

$$|R_\rho(0)| = \delta_\rho^2 |A^*_\rho(1)|^2.$$

2. *If $\rho|_{\Gamma_\infty}$ is trivial, we have*

$$-2h^1(\rho) = \mathrm{ord}_{z=0} R_\rho(z) \geq 2(1 + \mathrm{ord}_{t=1} A^*_\rho(t)).$$

Moreover if the action of g on $H^1(X_\infty, \rho)$ is semisimple, each inequality above becomes an identity.

Suppose that $H^0(X_\infty, \rho) = 0$ and that the action of g on $H^1(X_\infty, \rho)$ is semisimple. Let us make a change of variables:

$$z = t - 1.$$

Then if X is compact, two ideals $(R_\rho(z)^{-1})$ and $(A^*_\rho(z)^{-2})$ of $\mathbb{C}[[z]]$ are coincide. Thus we see that a geometric analog of the Iwasawa Main Conjecture holds for a unitary representaion of the fundamental group.

Notice that in the original Iwasawa main conjecture the Krull dimension of $\mathbb{Z}_p[[s]]$ is two and it is neccessary to care about a p-adic integral structure of the p-adic zeta function. But in our case the Krull dimension of $\mathbb{C}[[z]]$ is one and we do not have to worry about an integral structure of R_ρ. Thus our model is much simpler and easier than the p-adic one. The reader may wonder the reason of exceptional zeros of $R_\rho(z)$ in **Theorem 3.11 (2)** but such a phenomenon also occurs for a p-adic L-function associated to an elliptic curve defined over $\mathbb{Q}$ which has a split multiplicative reduction at p [3]. It is quite surprising that although p-adic analysis, the arithmetic algebraic geometry over a finite field and the theory of hyperbolic threefolds are quite different in their feature, L-functions in each field have common properties.

A main difference between the model of Deninger[7] or Fried[8] and ours is that in their models there exist *a dynamical system* which corresponds to the geometric Frobenius but not in ours. As in the case of a geometric analog of the Birch and Swinnerton-Dyer conjecture, we will use the heat kernel of the Laplacian and the Selberg trace formula instead of a geometric Frobenius and the Grotheidieck-Lefschetz trace formula in the Weil conjecture, respectively. Since our exceptional zeros are derived from a certain curious phenomenon in L^2 Hodge theory, we expect that exceptional zeros of a p-adic L-function will be also explained by p-adic Hodge theory.

Address : Department of Mathematics and Informatics
Faculty of Science
Chiba University
1-33 Yayoi-cho Inage-ku
Chiba 263-8522, Japan
e-mail address : sugiyama@math.s.chiba-u.ac.jp

The author is partially supported by the Grand-in-Aid for Scientific Research (C) No.18540203, the Ministry of Eduvation, Culture, Sports, Science and Technology, Japan.

References

[1] M. Kapranov A. Reznikov and P. Moree. Arithmetic Topology. lecture at hauptseminar, Max-Planck-Institute, August 1996.

[2] M. Artin and B. Mazur. On periodic orbits. *Ann. of Math.*, 81:82–99, 1965.

[3] J. Tate B. Mazur and J.Teitelbaum. On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Inventiones Math.*, 84:1–48, 1986.

[4] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves I. *Journ. reine u. angewandte Math.*, 212:7–25, 1963. MR0179168, Zbl0118.27601.

[5] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves II. *Journ. reine u. angewandte Math.*, 218:79–108, 1965. MR0146143, Zbl0147.02506.

[6] P. Deligne. La conjecture de Weil I. *Publ. I.H.E.S.*, 43:273–307, 1974.

[7] C. Deninger. A dynamical systems analogue of Lichtenbaum's conjecture on special values of Hasse-Weil zeta functions. math/0605724v2, May 2007.

[8] D. Fried. Homological identities for closed orbits. *Invent. Math.*, 71:419–442, 1983.

[9] D. Fried. Analytic torsion and closed geodesics on hyperbolic manifolds. *Inventiones Math.*, 84:523–540, 1986.

[10] K. Iwasawa. On Γ_l-extension of algebraic number fields. *Ann. of Math.*, 98:246–326, 1973.

[11] K. Kazuya and F. Trihan. On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$. *Inventiones Math.*, 153(3):537–592, 2003.

[12] P. Kirk and C. Livingston. Twisted Alexander invarinants, Reidemeister torsion, and Casson-Gordon invariants. *Topology*, 38(3):635–661, 1999.

[13] T. Kitano. Twisted Alexander polynomial and Reidemeister torsion. *Pacific Jour. Math.*, 174(2):431–442, 1996.

[14] B. Mazur. Note on étale cohomology of number field. *Ann. Sci. Ec. Norm. Sup.*, 6:521–552, 1973.

[15] B. Mazur. E-mail to Morishita. on his unpublished mimeographed note (circa 1965), October 17 2000.

[16] B. Mazur and A. Wiles. Class fields of abelian extensions of **Q**. *Inventiones Math.*, 76:179–330, 1984.

[17] J. Milnor. Whitehead torsion. *Bull. Amer. Math. Soc.*, 72:358–426, 1966.

[18] J. Milnor. Infinite cyclic coverings. In J. G. Hocking, editor, *Conference on the Topology of Manifolds*, pages 115–133. PWS Publishing Company, 1968.

[19] M. Morishita. On certain analogies between knots and primes. *J. Reine und Angew. Math.*, 550:141–167, 2002.

[20] M. Morishita. Milnor invariants and Massey products for prime numbers. *Compositio Math.*, 140:69–83, 2004.

[21] D. R. Morrison. The Clemens-Schmid exact sequence and applications. In P. Griffith, editor, *Topics in Transcendental Algebraic Geometry*, number 106 in Ann. of Math. Stud., pages 101–119. Princeton Univ Press, 1984. MR0756848, Zbl0576.32034.

[22] A. Reznikov. Three-manifolds class field theory. *Sel. Math. New Ser.*, 3:361–399, 1997.

[23] K. Sugiyama. An analog of the Iwasawa conjecture for a compact hyperbolic threefold. to appear in J. Reine Angew. Math.

[24] K. Sugiyama. A geometric analogue of the Birch and Swinnerton-Dyer conjecture over the complex number field. *J. Differential Geometry*, 68:73–98, 2004.

[25] K. Sugiyama. An analog of the Iwasawa conjecture for a complete hyperbolic threefold of a finite volume. Preprint, May 2006.

[26] K. Sugiyama. On a special value of the Ruelle L-function. Preprint, May 2006.

[27] J. Tate. Algebraic cycles and poles of zeta functions. In *Proc. of the Purdue Conference on Arithmetic Algebraic Geometry.* Harper and Row, 1964. MR0225778, Zbl0213.22804.

[28] L. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Math.* Springer-Verlag, 1982.

[29] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Ann. of Math.*, 141:443–551, 1995.