代数幾何学シンポジウム記録
2002年度 pp.84-94

ALGEBRAIC NUMBER THEORY AND LOW DIMENSIONAL TOPOLOGY

KAZUHIRO FUJIWARA

Nagoya University
Graduate school of Mathematics

December 10, 2002

§0. Introduction

The aim of this short article is to give a formulation of the celebrated conjecture of Leopoldt in terms of p-adic Hecke algebra of Hida. This is seen as a p-adic gauge method approach in number theory, and gives also a mysterious link between the works of A. Wiles and W. Thurston.

Let F be a totally real number field of degree g. We denote the integer ring by $\mathcal{O}_F$. The classical theorem of Dirichlet states that the group of units $\mathcal{O}_F^\times$ has the following structure:

$$\mathcal{O}_F^\times \simeq \{\pm 1\} \times \mathbf{Z}^{g-1}.$$

More precisely, for any $\mathbf{Z}$-basis $\langle \epsilon_1, \ldots, \epsilon_{g-1}\rangle$ of the free part,

$$\operatorname{rank}(\log|\iota(\epsilon_i)|)_{1\leq i\leq g-1, \iota: F\hookrightarrow \mathbf{C}} = g-1,$$

which is equivalent to the non-vanishing of the regulator R_F of F.

The Leopoldt conjecture means that a p-adic analogue of this classical theorem should be true.

Conjecture(Leopoldt).

$$\operatorname{rank}(\log_p \iota(\epsilon_i))_{1\leq i\leq g-1, \iota: F\hookrightarrow \bar{\mathbf{Q}}_p} = g-1.$$

This is also equivalent to the non-vanishing of the p-adic regulator $R_{F,p}$.

By the classical class field theory, the conjecture is equivalent to

$$\dim_{\mathbf{Q}_p} H^1_{\mathrm{et}}(\operatorname{Spec}\mathcal{O}_F[\frac{1}{p}],\ \mathbf{Q}_p) = 1.$$

Note that the dimension is positive by the existence of the cyclotomic $\mathbf{Z}_p$-tower. We put

$$\dim_{\mathbf{Q}_p} H^1_{\mathrm{et}}(\operatorname{Spec}\mathcal{O}_F[\frac{1}{p}],\ \mathbf{Q}_p) = 1 + \delta_{F,p}, \quad \delta_{F,p} \geq 0,$$

and call $\delta_{F,p}$ the Leopoldt defect.

Remark. The conjecture is known when F is abelian over $\mathbf{Q}$ [B]. The essential point is to factorize R_p into linear factors, and then to use a p-adic version of Baker's theory of linear combination of logarithms. So one need to use a deep result from transcendental number theory. For general F, $\delta_{F,p} < \frac{g}{2}$ holds [Wa].

§1. Analogy with 3-dimensional hyperbolic geometry

Since the nineteenth century, the analogy between algebraic number fields and function fields over finite fields has been quite useful and fruitful (Dedekind, Hilbert, Artin, Weil, Iwasawa, ...). In the following, we explain new dictionaries coming from a "topological" aspect of number fields, which leads to a striking relation with 3-dimensional hyperbolic geometry.

1.1 For a connected scheme X and a geometric point x of X, $\pi_1(X, x)$ means the arithmetic fundamental group. For a finite field $\mathbf{F}_q$, there is a canonical isomoprhism $\pi_1(\operatorname{Spec}\mathbf{F}_q) \simeq \hat{\mathbf{Z}}$ given by $\mathrm{Fr}_q \mapsto 1$. Here $\mathrm{Fr}_q : \bar{\mathbf{F}}_q \to \bar{\mathbf{F}}_q$, $\alpha \mapsto \alpha^{\frac{1}{q}}$, is the geometric Frobenius element. At the level of étale homotopy, the étale homotopy type of $\operatorname{Spec}\mathbf{F}_q$ is $K(\hat{\mathbf{Z}}, 1)$, which is isomorphic to the profinite completion of S^1. So one should regard $\operatorname{Spec}\mathbf{F}_q$ as an analogue of S^1, and the fundamental dictionary is

(Dict. 0) $$\operatorname{Spec}\mathbf{F}_q \Leftrightarrow S^1.$$

The standard dictionary in number theory, which is already mentioned, is stated as

$$C = \operatorname{Spec}\ \mathcal{O}_F \Leftrightarrow X/\mathbf{F}_q : \quad \text{proper smooth curve.}$$

On the other hand, a curve $X \to \operatorname{Spec}\mathbf{F}_q$ is an analogue of a surface fibration on a circle $M \to S^1$, so X itself should be an analogue of a topological 3-manifold (note that the ℓ-cohomological dimension of X (not of $\bar{X} = X \times_{\operatorname{Spec}\mathbf{F}_q} \operatorname{Spec}\bar{\mathbf{F}}_q$) is 3 for $\ell \neq p$).

This observation leads to the following analogy

(Dict. 1) C : regular arithmetic curve $\Leftrightarrow$ X : smooth curve over $\mathbf{F}_q$ $\Leftrightarrow$ M : 3-dimensional manifold

Dict. 1 was first found by B. Mazur. One should think that $\operatorname{Spec}\mathbf{Z}$ is the analogue of the 3-dimensional sphere S^3.

Dict. 0 and Dict. 1 have important consequences. For any (finite) place v of F, there is an inclusion $\operatorname{Spec} k(v) \hookrightarrow \operatorname{Spec}\mathcal{O}_F$ ($k(v)$ is the residue field at v). By Dict. 0 and Dict. 1, this is an analogue of embedding $S^1 \hookrightarrow M$, i.e., an analogue of a knot in a 3-manifold M! So we are lead to:

(Dict. 2) $\Sigma \subset \mathcal{O}_F$: a finite set of finite places $\Leftrightarrow$ $L \subset M$: a link

This dictionary is due to M. Morishita [M]. He establishes an analogy between the quadratic reciprocity law and the linking number of knots, and generalized it to a "higher linking number" situation.

There are further dictionaries. W. Thurston found that, especially when $M = S^3$ and $L = K$ is a knot, $M \setminus L$ often carries a complete hyperbolic structure, which is unique by the Mostow rigidity, and hence

$$M \setminus L \simeq \Gamma\backslash\mathbf{H}^3$$

where $\mathbf{H}^3 = \mathrm{SL}(2, \mathrm{C})/\mathrm{SU}(2)$ is the Riemannian symmetric space associated to $\mathrm{SL}(2, \mathbf{C})$. So we get

(Dict. 3) $\operatorname{Spec}\mathcal{O}_F \setminus \Sigma \quad (\Sigma \neq \emptyset) \Leftrightarrow N = M \setminus L$: 3-dimensional hyperbolic manifold

Remarks. 1. One should think that each $v \in \operatorname{Spec}\mathcal{O}_F$ is a primitive geodesic in $\operatorname{Spec}\mathcal{O}_F$ of length $\log q_v$ ($q_v = \sharp k(v)$). This is compatible with the analogy between the Riemann's zeta function and the Selberg zeta function, and also with T. Sunada's viewpoint that primes are analogues of closed geodesics of a complete Riemannian manifold.

2. Dict. 3 is compatible with anabelian geometry: for a number field F, $\operatorname{Spec} F$ itself should be seen as a (projective limit of) hyperbolic manifold, and we expect that a Mostow type rigidity holds for F:

$$\pi_1(\operatorname{Spec} F) \simeq \pi_1(\operatorname{Spec} F') \Rightarrow F \simeq F'.$$

This is in fact the theorem of Neukrich-Uchida.

The final dictionary concerns with the local monodromy. Let $o_v = \varprojlim \mathcal{O}_F/v^n$ be the local ring at v, and F_v be the local field at v. $\operatorname{Spec} k(v) \hookrightarrow \operatorname{Spec} o_v$ induces an equivalence of étale homotopy type, and

$\operatorname{Spec} F_v = \operatorname{Spec} o_v \setminus \{v\}$. For a topological situation, take a 3-manifold M and a knot K inside M. Let $N(K)$ be an open tubular neighbourhood of K in M.

(Dict. 4) $\qquad \operatorname{Spec} o_v \Leftrightarrow N(K), \quad \operatorname{Spec} F_v \Leftrightarrow N(K) \setminus K$

Under Dict. 4, $G_v = \operatorname{Gal}(\bar{F}_v/F_v)$ should be the analogue of $\pi_1(N(K) \setminus K)$. In fact, homotopically, $N(K) \setminus K$ has a natural S^1-fibration structure over K, and we have an exact sequence

$$0 \to I_K \to \pi_1(N(K) \setminus K) \to \pi_1(K) \to 0$$

Here I_K is isomorphic to $\mathbf{Z}$ (one can choose the class $[m_K]$ of a meridian m_K as a generator). $\pi_1(K)$ is spanned by K itself, and a splitting of the above sequence is obtained by choosing a longitude l_K. Moreover, $N(K) \setminus K$ is homotopic to a two dimensional torus, and hence

$$[l_K] \cdot [m_K] = [m_K] \cdot [l_K].$$

On the other hand, the tame part G_v^{tame} of G_v has the following structure:

$$0 \to I_v^{\text{tame}} \to G_v^{\text{tame}} \to \operatorname{Gal}(\overline{k(v)}/k(v)) \to 0,$$

where $I_v^{\text{tame}} \simeq \prod_{\ell \neq p} \mathbf{Z}_\ell$ (p = the residual characteristic, written additively). It is well-known that for a Frobenius lift Fr_v and a topological generator x of I_v^{tame}

$$\mathrm{Fr}_v \cdot x = q_v x \cdot \mathrm{Fr}_v\,.$$

So Spec F_v looks like a non-commutative torus, and 3-dimensinal manifolds are seen as specializations of arithmetic objects under $q \to 1$!

1.2 We try to use the dictionaries in 1.1 to understand the Leopoldt conjecture. We are trying to determine $\dim_{\mathbf{Q}_p} H^1_{\text{et}}(\operatorname{Spec} \mathcal{O}_F[\frac{1}{p}], \mathbf{Q}_p)$. So our problem is seen as an analogue of the determination of $H^1(N, \mathbf{Q})$ for an open hyperbolic manifold (or a link complement) N.

First we try to use ideas from 4-dimensional topology (instead of 3-dimensional topology). Let M be a closed, simply-connected, oriented smooth 4-manifold, and

$$I : H_2(M, \mathbf{Z}) \times H_2(M, \mathbf{Z}) \to \mathbf{Z}$$

be the intersection form. The celebrated theorem of S. Donaldson is

Theorem (Donaldson). *If I is positive definite, then I is isomorphic to the standard form $x_1y_1 + \cdots + x_\ell y_\ell$*

For the proof, Donaldson used the gauge theory. Let $\mathcal{X}$ be the moduli space of anti self-dual SU(2)-connections on M (for a generic Riemannian metric on M). Then the following properties are known:

(1) $\mathcal{X}$ is 5-dimensional, and there is a singular compactification $\bar{\mathcal{X}}$ of $\mathcal{X}$.
(2) The boundary of $\bar{\mathcal{X}}$ is $M \cup \Sigma$. $\Sigma = \{p_1, \ldots, p_\ell\} \neq \emptyset$ is zero dimensional, and consists of a finite number of points called cusps. Those cusps correspond to reducible connections.
(3) Near a cusp p, a tubular neighbourhood of p in $\bar{\mathcal{X}}$ is homeomorhic to a cone over $\mathbf{P}^2_{\mathbf{C}}$.

By these (1)–(3) and by removing a tubular neighbourhood of Σ, $\bar{\mathcal{X}}$ gives an oriented cobordism between M and an ℓ-disjoint union of $\mathbf{P}^2_{\mathbf{C}}$, and the theorem is shown.

From this argument of Donaldson, we get

Lesson. *One needs a non-abelian gauge theory to get information on homology.*

(Though the intersection form is rather homotopical existence in the sense that it determines the h-cobordism class.) I think that the Donaldson pattern is the same as in the case of Wiles' proof of the Fermat's Last Theorem: number theorists have used the classical class field theory to understand FLT for a long time, then failed. The only effective way (developped by Frey, Ribet and Wiles) to prove it is to interprete FLT by an elliptic curve over $\mathbf{Q}$, then apply the non-commutative class field theory for GL(2) (the Taniyama-Shimura conjecture in this case). Inspired by these results of Donaldson and Wiles, I propose the following strategy to the Leopoldt conjecture: use the non-abelian class field theory to solve GL(1)-problems.

§3. $SL(2)$-approach

3.1 We fix a prime p. Let E_λ be a p-adic field with the integer ring $\mathcal{O}_\lambda$ with the maximal ideal λ, $k_\lambda = \mathcal{O}_\lambda/\lambda$ be the residue field.

Assume that F is a totally real number field, $[F : \mathbf{Q}] = g$.

$C = \operatorname{Spec} \mathcal{O}_F$, $\Sigma \subset |C|$ a finite subset.

Assume that Σ contains any place v dividing p. $G_\Sigma = \pi_1(C \setminus \Sigma)$ is the arithmetic fundamental group of $C \setminus \Sigma$.

We fix an absolutely indecomposable Galois representation

$$\bar{\rho} : G_\Sigma \to \mathrm{GL}_2(k_\lambda).$$

($\bar{\rho}$ corresponds to a flat connection in the geometric setting.) We assume that $\bar{\rho}$ is nearly ordinary and G_v-distinguished at $v|p$ in the following sense:

$$\bar{\rho}|_{G_v} \simeq \begin{pmatrix} \bar{\chi}_{1,v} & * \\ 0 & \bar{\chi}_{2,v} \end{pmatrix}, \quad \bar{\chi}_{1,v} \neq \bar{\chi}_{2,v} \ \text{ for } v|p.$$

In the following, we fix $\bar{\chi}_{2,v}$ for each $v|p$, and choose a function $def : \Sigma \setminus \{v; v|p\} \to \{\mathbf{min},\ \mathbf{unres}\}$. Consider the following deformation theory on $Art_{\mathcal{O}_\lambda}$:

$$R \mapsto F_{\bar{\rho}}(R) = \{\text{the set of representations } \rho : G_\Sigma \to \mathrm{GL}_2(R) \text{ lifting } \bar{\rho}, \text{ which satisfies (G1), (L1), (L2)}\}$$

Here

(G1) The pro-p part of $\det \rho$ is equal to the pro-p part of χ_{cycle} (χ_{cycle} is the cyclotomic character).

(L1) $$\text{At } v|p, \quad \rho|_{G_v} \simeq \begin{pmatrix} \chi_{1,v} & * \\ 0 & \chi_{2,v} \end{pmatrix}, \quad \chi_{2,v} \text{ lifts } \bar{\chi}_{2,v}$$

(L2)
At $v \in \Sigma \setminus \{v; v|p\}$, $\rho|_{G_v}$ is a minimal, or unrestricted lift according to $def(v) = \mathbf{min}$, or $\mathbf{unres}$.

Cf. [Fu] for the meaning of minimal or unrestricted local lifting. Note that (G1) fixes the determinant, so our problem is an SL(2)-deformation.

Remark. The moduli space of rank 2 flat bundles of a complete hyperbolic 3 manifold plays a very important role in the theory of Thurston. The nearly ordinarity condition is seen as a parabolic structure given to a flat connection. The biggest difference between the arithmetic case and the diffeo-geometric case is, that on the arithmetic side, there is no global moduli of Galois representation.

3.2 We assume further that $\bar{\rho}$ is modular in the sense that it comes from some automorphic representation $\bar{\pi}$ of infinity type (k, w). In this case, by Hida theory, we have the nearly ordinary Hecke algebra T_Σ attached to $\bar{\rho}$ (with a fixed central character). Put

$$\gamma_F = \prod_{v|p} \gamma_v,$$

where γ_v is the maximal pro-p quotient of $o_v^\times$. $\operatorname{rank}_{\mathbf{Z}_p} \gamma_F = g$.

The basic structures of T_Σ are the following: T_Σ is a complete local $\mathcal{O}_\lambda$-algebra over the complete group algebra $\Lambda^{\mathrm{big}} = \mathcal{O}_\lambda[[\gamma_F]]$, finite and dominant over Λ^{big} (and hence the Krull dimension of T_Σ is $g+1$).

There is a big G_Σ-representation $\rho_{Q(\Lambda^{\mathrm{big}})}$ of Hida on $Q(\Lambda^{\mathrm{big}})^{\oplus 2}$ ($Q(\Lambda^{\mathrm{big}})$ is the fraction field of Λ^{big}). $\rho_{Q(\Lambda^{\mathrm{big}})}$ is nearly ordinary at $v|p$. When $\bar{\rho}$ is absolutely irreducible, there is a Galois stable free lattice in $Q(\Lambda^{\mathrm{big}})^{\oplus 2}$ which is unique up to isomoprhism.

By the compatibility of the local and the global Langlands correspondence at $v \nmid p$, there is a surjective ring homomorhism $R_\Sigma \to T_\Sigma$. Under this setting, the following theorem is proved by the theory of the Taylor-Wiles system [Fu] by using the systems from quaternion algebras.

Theorem. *Assume that $p \geq 3$, and $\bar{\rho}$ is an absolutely irreducible and modular representation. Assume moreover that $\bar{\rho}|_{G_{F(\zeta_p)}}$ is absolutely irreducible, and G_v-distinguished for $v|p$. Then*
a) The nearly ordinary Hecke algebra T_Σ is the universal deformation ring R_Σ.
b) T_Σ is finite flat over $\Lambda^{\rm big}$, and is a local complete intersection.

(cf. [Fu] for the special case. The general nearly ordinary case follows from it.)

3.3 Unfortunately, the local moduli space for absolutely irreducible representations does not give any information on the Leopoldt conjecture. Inspired by Donaldson and Wiles, we try to use reducible $\bar{\rho}$ to get information on F. Our expectation is the following:

Expectation. *Assume that F is totally real, and there is one totally odd character χ of G_F such that the Iwasawa μ-invariant $\mu_\chi = 0$ for a prime p. Then the Lepoldt conjecture is true for a pair (F, p).*

So we are dividing the Lepoldt conjecture into two parts. In the first part, we find a totally imaginary chracter χ satisfying the assumption. In the second part, we try to use the theory of the p-adic Hecke algebra.

The first part is easier. Of course, conjecturally, μ_χ should be zero for all such χ's. But even without any conjecture, we succeed to find a very good χ in many cases.

Assumption $(*)_{F,p}$ (existence of good quadratic characters). *Assume that $p \geq 3$. For any finite set Σ of finite places of F, there is a quadratic character $\chi : G_\Sigma \to \{\pm 1\}$ such that*
1. χ is totally imaginary.
2. χ is unramified at all $v \in \Sigma$ and $\chi(\mathrm{Fr}_v) = -1$.
3. The relative class number h_{F_χ}/h_F is not divisible by p. Here F_χ is the splitting field of χ.

From the conditions, it follows that $H^1_f(F, \chi) = 0$ for the finite part. For the existence of a good quadratic character, the following is known:

Theorem. *$(*)_{F,p}$ is satisfied if $p = 3$, or p is large enough compared to F [N].*

In the following we fix a good quadratic character χ, and choose a good $\bar{\rho}$ from χ so that the analysis of the deformation theory (and the structure of the local deformation space) is easy. This is a kind of a transversality argument in number theory.

Our $\bar{\rho}$ is the following:

$$0 \to k_\lambda \to \bar{\rho} \to \bar{\chi} \to 0.$$

We assume that the extension is non-split, but is split at all finite places except y, $y \nmid p$. The existence of such an extension (for a suitable y) follows from the Euler characteristic formula. $\chi(\mathrm{Fr}_y) = \omega(\mathrm{Fr}_y) = -1$.

We put $\Sigma = \{v|p,\ v|\operatorname{cond}\chi, y\}$. The deformation problem is as follows.

At $v|p$, the deformation is nearly ordinary.

$$\rho|_{G_v} \simeq \begin{pmatrix} \chi_{1,v} & * \\ 0 & \chi_{2,v} \end{pmatrix}.$$

Here $\chi_{2,v}$ lifts the trivial representation (*not $\bar{\chi}|_{G_v}$).*

At $v = y$, the deformation is the special deformation, i.e., $\rho|_{G_v}$ is of the form

$$\rho|_{G_v} \simeq \begin{pmatrix} \chi_{1,v} & * \\ 0 & \chi_{2,v} \end{pmatrix}.$$

Here $\chi_{2,v}$ lifts $\chi|_{G_v}$, and $\chi_{1,v} = \chi_{2,v}(1)$.

At $v \in \Sigma$, $v \neq y, v \nmid p$, the deformation is mininal.

To define an appropriate Hecke algebra, we need to know that $\bar{\rho}$ has a good lifting which is modular.

Proposition. *Assume that $p \geq 3$, and $\bar{\rho}$ is as above. Then $\bar{\rho}$ is modular in the following sense: by enlarging $\mathcal{O}_\lambda$ if necessary, $\bar{\rho} = \rho_{\pi,\lambda} \bmod \lambda$ for a cuspical representation π of type $((2,\dots,2),0)$ which is nearly ordinary at $v|p$, and $\rho_{\pi,\lambda}$ is a deformation of $\bar{\rho}$ which fits into the deformation problem given above.*

The proposition is proved by constructing an Eisenstein ideal using p-adic Eisenstein series by the technique of [W1]. By the proposition, we can define the Hecke algebra T_Σ attached to $\bar{\rho}$. It is a priori not clear whether there exists a natural ring homomorphism $R_\Sigma \to T_\Sigma$ (this is a usual difficulty in case of reducible residual representations). This amounts to saying that we have a good free Galois-stable lattice $\mathcal{L}$ inside the big G_Σ-representation $\rho_{Q(\Lambda^{\mathrm{big}})}$ of Hida on $Q(\Lambda^{\mathrm{big}})^{\oplus 2}$. The existence is assured by Assumption $(*)_{(F,p)}$, especially by 3, and $R_\Sigma \to T_\Sigma$ exists (cf. Appendix A2).

Now we can compare R_Σ with T_Σ. Again we have the following theorem.

Theorem. *Assume that $p \geq 3$, and $\bar{\rho}$ is as above. Then*
a) The nearly ordinary Hecke algebra T_Σ is the universal deformation ring R_Σ.
b) T_Σ is finite flat over Λ^{big}, and is a local complete intersection.

We construct Taylor-Wiles systems from quaternion algebras. See [CS] for related works.

§4. Eisenstein locus

We study the same $\bar{\rho}$ as in §3. Note that our choice Σ is minimal. Let $Y = \mathrm{Spec}\ R_\Sigma = \mathrm{Spec}\ T_\Sigma$. We analyze the locus $Z = V(I_\Sigma)$ where the universal deformation ρ^{univ} is reducible (Eisenstein locus). Here I_Σ is the Eisenstein ideal (see A1 of the appendix).

Proposition.

$$\dim Z = \dim_{\mathbf{Q}_p} H^1_{\mathrm{et}}(\mathrm{Spec}\,\mathcal{O}_F[\frac{1}{p}],\ \mathbf{Q}_p) = 1 + \delta_{F,p}.$$

This follows from the following theorem by a dimension counting.

Theorem.

$$T_\Sigma / I_\Sigma \xrightarrow{\sim} \mathcal{O}_\lambda[[X_F]]/(L_y)$$

Here X_F is the maximal pro-p abelian quotient of $\pi_1(\mathrm{Spec}\,\mathcal{O}_F[\frac{1}{p}])$, $L_y = 1 - \chi^{-1} \cdot \chi_{\mathrm{cycle}} \cdot \chi^{\mathrm{univ}}(\mathrm{Fr}_y)$, $\chi^{\mathrm{univ}} : \pi_1(\mathrm{Spec}\,\mathcal{O}_F[\frac{1}{p}]) \to \mathcal{O}_\lambda[[X_F]]$ is the universal character.

(Sketch) We use $R_\Sigma = T_\Sigma$. Then T_Σ/I_Σ is the moduli space classifying extensions $0 \to \chi_1 \to \rho \to \chi_2 \to 0$ which is locally split except y with $\det \rho = \chi_1 \cdot \chi_2$ fixed. χ_1 is unramified except possibly at $v|p$. One can determine all the extensions by using the Euler characteristic formula and the Tate-Poitou duality by assumption $(*)_{(F,p)}$. □

Remark. Note that T_Σ/I_Σ does not carry a standard $\mathcal{O}_\lambda[[X_\Sigma]]$-algebra structure, nor T_Σ. The standard structure on T_Σ/I_Σ is an $\mathcal{O}_\lambda[[X'_\Sigma]]$-structure, where X'_Σ is the image of $\gamma_F \to X_\Sigma$. L_y is an Euler factor at y (by our assumption on χ, the p-adic L-fuction of $\chi^{-1}\omega$ is a unit in the Iwasawa algebra, and does not appear here).

§5. Counting argument

Lemma. *Notations are as in §4, and assume that $p \geq 3$. Then the Eisenstein ideal I_Σ is generated at most by g-elements.*

This is proved in the appendix, A3.

Here we give a non-rigorous but suggestive argument to the Leopoldt conjecture. Consider the following sequence

$$0 \to I_\Sigma \to T_\Sigma \to T_\Sigma/I_\Sigma \to 0.$$

Here T_Σ has Krull dimension $g+1$, and I_Σ is generated at most by g-elements. So the naive expectation should be $\dim T_\Sigma/I_\Sigma = 1$, which implies $\delta_{F,p} = 0$ by the proposition in §4.

The following proposition refines the above argument. A stronger result will be found in the next section.

Proposition. *Assume that $p \geq 3$. The following two conditions are equivalent.*

a) The Leopoldt conjecture is true for (F,p).

b) For minimal Σ, the Eisenstein ideal I_Σ of T_Σ is generated by a regular sequence of g-elements.

Proof. $b) \to a)$: let $(x_1, \ldots, x_g)$ be a regular sequence in I_Σ. Then $\dim T_\Sigma/I_\Sigma = 1$. On the other hand, $\dim T_\Sigma/I_\Sigma = 1 + \delta_{F,p}$, where $\delta_{F,p}$ is the Leopoldt defect.

$a) \to b)$: we use the basic estimate on the number of generators of I_Σ. Since $\delta_{F,p} = 0$ by our assumption, $T_{\Sigma,P}$ has Krull dimension g. On the other hand, T_Σ/I_Σ is reduced, and hence the localization $I_{\Sigma,P}$ at any minimal prime ideal P of I_Σ is the maximal ideal of $T_{\Sigma,P}$, and is generated by g-elements. So $T_{\Sigma,P}$ is a regular local ring, and g is the minimal number of the generators of $T_{\Sigma,P}$.

We show that conormal module I_Σ/I_Σ^2 is free of rank g over T_Σ/I_Σ. Since T_Σ is generated at most by g-elements, there is a surjection $\alpha : T_\Sigma^{\oplus g} \twoheadrightarrow I_\Sigma$, and hence $\alpha_I : (T_\Sigma/I_\Sigma)^{\oplus g} \twoheadrightarrow I_\Sigma/I_\Sigma^2$. α_I is bijective at any minimal prime ideal P containing I_Σ, and hence α_I is bijective.

To show that I_Σ is generated by a regular sequence of g-elements, it suffices to see the canonical map of graded modules

$$\operatorname{Sym} I_\Sigma/I_\Sigma^2 \twoheadrightarrow gr_I T_\Sigma = \oplus_{n\geq 0} I_\Sigma^n/I_\Sigma^{n+1}$$

is injective. Since T_Σ/I_Σ is reduced, it suffices to see it at each minimal prime ideal P, and the map is injective there since $T_{\Sigma,P}$ is a regular local ring. □

§6.Main Theorem

Theorem. *Assume that $p \geq 3$, and Σ is minimal. Then the conormal module I_Σ/I_Σ^2 has rank $g - \delta_F$ at any minimal prime ideal of T_Σ/I_Σ.*

To prove the theorem, one needs to control Selmer groups of the adjoint type using $R_\Sigma = T_\Sigma$. We omit the details.

As a consequence of the theorem, we get the following: if I_Σ/I_Σ^2 is free of rank g over T_Σ/I_Σ, then the Leopoldt conjecture is true for (F,p) under the existence of a good quadratic character (of course the condition is weeker than the proposition in §5).

This type of conditions for Hecke algebras appear in [K] when $F = \mathbf{Q}$. In [K], the condition is used as a hypothesis to show the cyclicity of the Iwasawa module for for powers of Teichmüller characters.

Appendix. Standard modules and their properties

A1. Standard modules

Here we give a formalism to construct good Galois stable lattices.

Axioms.

Ax 1 *T is a reduced noetherian complete local algebra, with the total fraction ring $L = Q(T)$. 2 is invertible in L, and has no 2-torsions.*

Ax 2 *G is a topological group with an involution $c \in G$.*

Ax 3 *$\rho_L : G \to \mathrm{Aut}_L V$ is a representation of G. V is L-free of rank 2. ρ is odd in the sense that $\det \rho(c) = -1$. At each minimal prime ideal P, the induced representation on V_P is irreducible.*

Ax 4 *T contains $\{\mathrm{Tr}\,\rho_L(\sigma), \sigma \in G\}$. ρ_L is continuous in the following sense: there is a G-stable finitely generated T-lattice M in V, and the G-action is continuous for the m-adic topology.*

Let p be the residual characteristic of T. For a G-module A,

$$A^+ = \{a \in A,\ c \cdot a = a\},\ A^- = \{a \in A,\ c \cdot a = -a\}.$$

$$A = A^+ \oplus A^-$$

is called the parity decomposition (when $p = 2$, we assume that A has no 2-torsions).

We fix a parity $s = +$, or $-$. By $-s$, we mean the opposite parity. For $\sigma \in G$, we put

$$a(\sigma) = 1/2(\mathrm{Tr}\,\rho_L(\sigma) - s \cdot \mathrm{Tr}\,\rho_L(\sigma \cdot c)),$$

$$d(\sigma) = 1/2(\mathrm{Tr}\,\rho_L(\sigma) + s \cdot \mathrm{Tr}\,\rho_L(\sigma \cdot c)).$$

Even when $p = 2$, these elements belong to T since T has no 2-torsions by $Ax1$.

Formulas. *Take an L-basis (e_+, e_-) of V so that $\rho_L(c) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. For the matrix representation*

$$\rho_L(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix},$$

$$x(\sigma, \tau) \stackrel{def}{=} a(\sigma\tau) - a(\sigma)a(\tau) = b(\sigma)c(\tau) \in T.$$

$$d(\sigma\tau) - d(\sigma)d(\tau) = c(\sigma)b(\tau) = x(\tau, \sigma).$$

$$\det \rho_L(\sigma) = a(\sigma)d(\sigma) - x(\sigma, \sigma)$$

Theorem. *For a rank one free T-lattice $\mathcal{L}$ of M^s, there is a unique minimal G-stable sublattice M of V with $M^s = \mathcal{L}$. The G-action is continuous.*

$$\rho_M : G \to \mathrm{Aut}_T M$$

satisfies $\rho_M \otimes_T L = \rho_L$.

Proof. Take an element $e_s \in M_L$ which generates $\mathcal{L}$ as a T-module.

Let $M_{\mathcal{L}}$ be the T-submodule spanned by $\rho_L(\sigma)e_s$, $\sigma \in G$, i.e., $M = T[G] \cdot \mathcal{L}$. $M_{\mathcal{L}}$ is G-stable, and gives a rank two lattice generically.

Sublemma. $M^s_{\mathcal{L}} = \mathcal{L}$.

Proof. This follows from the following formula

$$(\rho_L(\sigma)e_s)^s = d(\sigma)e_s.$$

The minimality and the uniqueness are clear.

We show that the action is continuous. We take $\alpha \in L^\times$ so that $\alpha\mathcal{L}$ is contained in some G-stable lattice. This ensures us $M_{\alpha\mathcal{L}}$ is finitely generated, and again a lattice. By the Artin-Rees lemma, the induced topology on $M_{\alpha\mathcal{L}}$ is again m-adic. For $\alpha \in L^\times$,

$$M_{\alpha L} = \alpha M_{\mathcal{L}}$$

as G-modules by the definition, and the claim follows.

Definition. *G-module $M = M_{\mathcal{L}}$ constructed as above is the standard module for $(\rho_L,\ V_L)$ with respect to $\mathcal{L}$.*

When we vary $\mathcal{L}$ with the same parity, standard modules are unique up to multiplication by an element of $L^{\times}$.

Remark. The notion of standard modules depends only on the pseudo-representation defined by ρ_L. One can define the standard module associated to pseudo-representations directly.

The following proposition, though the proof is rather trivial, shows an amazing property of a standard module.

Proposition. *A standard module $M = M_{\mathcal{L}}$ is s-deprived, i.e., there is no Galois stable module $M' \subset M$ such that $M^s = (M')^s$.*

Since $(M')^s = M^s = \mathcal{L}$, $M_{\mathcal{L}} = T_{\Sigma}[G] \cdot \mathcal{L} \subset M'$ since M' is Galois stable.

Proposition (Standard module criteria). *Let M be a G-stable lattice for $(\rho_L,\ V_L)$. Then M is standard if and only if the mod m-reduction $\bar{\rho}_M = M/mM$ satisfies the following:*

$\bar{\rho}_M$ is of the form

$$0 \to (\bar{\chi}^{-s})^{\oplus\alpha} \to \bar{\rho}_M \to \bar{\chi}^s \to 0,$$

and has no quotient isomorphic to $\bar{\chi}^{-s}$.

Especially, the notion of standard modules does not depend on any choice of c as long as $\bar{\chi}^s$ has parity s for the choice.

Proof. We prove $\Leftarrow$ direction. Since the parity decomposition is functorial, M^s/mM^s has dimension one. So there is an element e_s in M_s such that $Te_s \hookrightarrow M_s$ is an isomorphism after mod m reduction. Since T is noetherian, by Nakayama's lemma $M_s = Te_s$. This implies that M contains the standard module M_{Te_s}. Let A be the image of the reduction map $M_{Te_s} \otimes_T k \to M \otimes_T k$. If $A \neq \bar{\rho}_M$, $\bar{\rho}_M/A$ has a quotient which is isomorphic to $\bar{\chi}^{-s}$, and this contradicts to our assumption. This means $\bar{\rho}_M = A$, and by Nakayama's lemma again $M = M_{Te_s}$.

Lemma. *Let M be a standard module, $\bar{\rho} = \rho \bmod m_T$. Then the k-linear map*

$$\bar{\rho}^{\vee} \otimes \bar{\chi}^{-s}/(\bar{\chi}^{-s}/\bar{\chi}^s) \to H^1(G,\ \bar{\chi}^{-s}/\bar{\chi}^s)$$

obtained by pulling back the extension

$$0 \to \bar{\chi}^{-s}/\bar{\chi}^s \to \bar{\rho}^{\vee} \otimes \bar{\chi}^{-s} \to k^{\oplus\alpha} \to 0$$

by linear maps $k \to k^{\oplus\alpha}$, is injective.

Proof. If not, there is a quotient of $\bar{\rho}$ which is isomorphic to $\bar{\chi}^{-s}$. This contradicts to the fact that a standard module is $-s$-deprived.

Definition (Abstract Eisenstein ideal). *The ideal I of T generated by $d(\sigma\tau) - d(\sigma)d(\tau)$, $\sigma, \tau \in G_{\Sigma}$ is the (abstract) Eisenstein ideal.*

By our assumption 3, the Eisenstein ideal is a proper ideal of T. The following proposition shows that $V(I)$ gives "the locus where ρ_L can not be irreducible".

Proposition. *For a standard module M with parity s, $\rho_I = \rho \bmod I$ has the following form*

$$0 \to M^{-s}/IM^{-s}\tilde{\chi}^{-s} \to \rho_I \to \tilde{\chi}^s \to 0$$

where $\tilde{\chi}^{\pm s} : G \to (T/I)^{\times}$ are charaters which satisfies

$$\tilde{\chi}^s\tilde{\chi}^{-s} = \det \rho_L \bmod I.$$

At any $P \notin V(I)$, the localization M_P^{-s} at P is T_P-free of rank one, and the induced $\rho_P : G \to \mathrm{Aut}_{T_P} M_P$ is irreducible.

A2. Construction of a free lattice

In 3.3, a priori, there is no algebra homomorphism $R_\Sigma \to T_\Sigma$, so there is no way to compare two rings. For this, one needs to construct a free T_Σ-lattice.

Theorem. *Notations are the same as 3.3. Assume that Σ is minimal. Then there is*

$$\rho_{T_\Sigma} : G_\Sigma \to \mathrm{GL}_2(T_\Sigma)$$

which gives $\bar{\rho}$. Moreover, ρ_{T_Σ} is unique up to isomorphism, and is a deformation of $\bar{\rho}$.

Proof. Let $\rho : G_\Sigma \to \mathrm{Aut}(Q(\Lambda^{\mathrm{big}})^{\oplus 2})$ be the Hida's two dimensional representation attached to T_Σ. Put $T = T_\Sigma$, $V = Q(\Lambda^{\mathrm{big}})^{\oplus 2}$, and $\rho_L = \rho$. Take a rank one free lattice $\mathcal{L}$ in V^-, and consider the standard module $M_\mathcal{L}$. The reduction has the form

$$0 \to k^{\oplus\alpha} \to \bar{\rho} \to \bar{\chi} \to 0$$

where $\alpha = \dim_k M_\mathcal{L}^+/mM_\mathcal{L}^+$. At each $v|p$, there is a G_v-stable filtration

$$0 \to \mathcal{L}_{1,v} \to M_\mathcal{L} \to \mathcal{L}_{2,v} \to 0$$

where each $\mathcal{L}_{i,v}$ is T_Σ-torsion free. The G_v-action on $\mathcal{L}_{i,v}$ is via a character $\chi_{i,v}$ lifting $\bar{\chi}|_{G_v}$ or the trivial representation according to $i = 1, 2$. Note that $\bar{\chi}|_{G_v} \neq 1$, so we have that the image of

$$\mathcal{L}_{1,v} \otimes_{T_\Sigma} k \to M_\mathcal{L} \otimes_{T_\Sigma} k$$

is non-zero since $\bar{\chi}$ must appear in $\bar{\rho}$, and $\bar{\rho}|_{G_v}$ defines a split exact sequence. Similarly, we know that $\bar{\rho}$ is split at all $v \neq y$. Since $\bar{\rho}$ defines an injection

$$k^{\oplus\alpha} \hookrightarrow H^1_{\mathrm{et}}(\mathrm{Spec}\, O_F \setminus \{y\}, \bar{\chi}^{-1})$$

we get $\alpha = 1$. $M_\mathcal{L}$ is T_Σ-free of rank one, and the associated G_Σ-representation gives ρ_Σ. For the uniqueness, take any $\rho' : G_\Sigma \to \mathrm{Aut}_{T_\Sigma}(M)$ lifting $\bar{\rho}$ where M is T_Σ-free. Then M is standard with respect to parity $-$, and all standard modules for parity $-$ are isomorphic. To show that ρ_Σ is a deformation is standard. We need to check the local conditions, and only consider the case $v|p$ for simplicity. We show that $\mathcal{L}_{2,v}$ is free of rank one with the notation as above. $\mathcal{L}_{2,v} \otimes_{T_\Sigma} k$ has dimension one over k since G_v-action is trivial there. The claim follows by Nakayama's lemma again, and the T_Σ-freeness of $\mathcal{L}_{1,v}$ follows as a consequence. The form of $\chi_{i,v}|_{I_v}$ is the desired one by the specialization argument to Hilbert modular forms of type $((2, \dots, 2)), 0)$. $\square$

A3. Estimate of Eisenstein ideals: refinement of Mazur's method

Theorem. *Assume that Σ is minimal. Then I_Σ is generated at most by g-elements.*

Proof. The proof is based on a lattice chage technique. We already know the existence of a Galois deformation $\rho : G_\Sigma \to \mathrm{Aut}_{T_\Sigma} M_\Sigma$ where M_Σ is T_Σ-free of rank 2. $\mathcal{L} = M_\Sigma^+$. We calculate the standard module $M_\mathcal{L}$ with respect to the plus sign.

Sublemma. *$M_\mathcal{L}^- = I_\Sigma$ where I_Σ is the Eisenstein ideal.*

Proof. We take a basis (e_+, e_-) of M_Σ. We take the matrix representation

$$\rho(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}$$

with respect to this basis. The module J generated by $c(\sigma), \sigma \in G_\Sigma$, is $M_\mathcal{L}^-$ by the definition. We view J as an ideal of T_Σ. By

$$d(\sigma\tau) - d(\sigma)d(\tau) = c(\sigma)b(\tau),$$

$I_\Sigma \subset J$. On the other hand, since $\bar{\rho}$ is non-split, there is $\tau \in G_\Sigma$ such that $b(\tau) \bmod m \neq 0$. For such τ, $b(\tau)$ is a unit in T_Σ, and hence $J \subset I_\Sigma$ follows. □

Consider the Galois representation ρ' on $M_\mathcal{L}$. Then $\rho' \bmod m$ defines an injection

$$I_\Sigma \otimes_{T_\Sigma} k \hookrightarrow H^1(F, \bar{\chi})$$

By a similar argument as in A2, the obtained extensions split except possibly at $v|p$. $\dim_k H^1_{\mathrm{et}}(\mathrm{Spec}\, \mathcal{O}_F[\frac{1}{p}], \bar{\chi}) = g$, and the claim follows.

References

[B] Brumer, A., *On the units of algebraic number fields*, Mathematatika **14** (1967), 121-124.

[F] Fujiwara K., *Deformation rings and Hecke algebras in the totally real case, preprint.*

[H] Hida, H., *On nearly ordinary Hecke algebras for* GL(2) *over totally real fields*, Adv. Stud. Pure Math., vol. 17, Academic Press, pp. 139-169.

[Na] Naito, H., *Indivisibility of class numbers of totally imaginary quadratic extensions and their Iwasawa invariants*, J. Math. Soc. Japan **43** (1991), 185-194.

[K] Kurihara, M., *Ideal class groups of cyclotomic fields and modular forms of level* 1, J. Number Theory vol 45 (1993), 281-294.

[M] Morishita, M., *On certain analogies between knots and primes*, J. Reine Angew. Math. **550** (2002), 141-167.

[SW] Skinner, C., Wiles, A., *Residually reducible representations and modular forms*, Inst. Hautes Études Sci. Publ. Math. **89** (2000), 5-126.

[W1] Wiles, A., *The Iwasawa conjecture for totally real fields*, Ann. of Math. **131** (1990), 493-540.

[W2] ———, *Modular elliptic curves and Fermat's last theorem*, Ann, of Math. **141** (1995), 443-551.

[Wa] Waldshmidt, M., *A lower bound for the p-adic rank of the units of an algebraic number field*, Topics in classical number theory, Vol I, II, North-Holland, 1984, pp. 1617-1650.