Trends in Mathematics
Information Center for Mathematical Sciences
Volume 9, Number 1, June, 2006, Pages 75–79

MODULI OF GALOIS REPRESENTATIONS II — FINITENESS CONJECTURES

YUICHIRO TAGUCHI

Abstract. In this talk, I will recall the construction of moduli schemes which parametrize various kinds of Galois representations (which I talked about in the last Seminar at Kuju, 2004), and then discuss some finiteness conjectures related to the moduli schemes. Main topics include:

- Zeta functions as generating functions of the number of mod p Galois representations;
- A finiteness conjecture on the moduli scheme of representations of the Galois group of the maximal Galois extension of an algebraic number field unramified outside a finite number of primes;
- A moduli-theoretic reformulation of the finiteness conjecture of Khare and Moon on mod p Galois representations with bounded conductor.

In fact, most part of the theory is purely algebraic, and is applicable to representations of a rather general class of non-commutative rings (instead of group rings of Galois groups). It is a generalization of Mazur's deformation theory [6] and is, at the same time, a topological version of Procesi's theory [8]. Main differences of our theory from Mazur's are:

— We do not fix a residual representation ρ_0 to start with, so that we can construct a moduli space which parametrizes all absolutely irreducible representations having various residual representations;
— We are interested in parametrizing the isomorphism classes of absolutely irreducible $\mathbb{Q}_p$-representations as well as $\mathbb{Z}_p$-representations;
— To parametrize absolutely irreducible p-adic representations having a fixed residual representation ρ_0 defined over a finite field k, we do not need an assumption such as $\mathrm{End}(\rho_0) \simeq k$ to ensure the universality of the moduli space, although this is only at the expense of localization of the coefficient rings (e.g. making the prime p invertible).

In this paper, a *ring* means a (not necessarily commutative) associative ring with unity.

1. The moduli scheme.

First we define the type of rings whose representations we want to parametrize. Fix a category $\mathfrak{a}$ of rings which is closed under taking subobjects, quotients and tensor products. A *pro-$\mathfrak{a}$ ring* is a topological ring R which is canonically isomorphic to the projective limit $\varprojlim_\lambda (R/I_\lambda)$, where I_λ are open two-sided ideals of R such that R/I_λ are in $\mathfrak{a}$. An *f-pro-$\mathfrak{a}$ ring* is a topological ring which contains an open pro-$\mathfrak{a}$ subring (this is named after Huber's "f-adic rings" ([3])). If $\mathfrak{a}$ is the category of finite rings (resp. artinian Λ-algebras which are finite over a fixed commutative ring Λ), we say "f-profinite" (resp. "f-proartinian over Λ") instead of "f-pro-$\mathfrak{a}$". Typically, f-pro-$\mathfrak{a}$ rings are obtained from pro-$\mathfrak{a}$ rings by localization. For example, the matrix algebra $\mathrm{M}_n(\widehat{\mathbb{Z}})$ is a profinite ring, where $\widehat{\mathbb{Z}}$ is the profinite completion of the integer ring $\mathbb{Z}$, and $\mathrm{M}_n(\widehat{\mathbb{Z}}) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathrm{M}_n(\mathbb{A})$ is an f-profinite ring, where $\mathbb{A} = \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ is the ring of finite adèles of $\mathbb{Q}$. If p is a prime number and G is a profinite group, then the completed group ring $\mathbb{Z}_p[\![G]\!]$ is a profinite ring, and $\mathbb{Z}_p[\![G]\!][1/p]$ is an f-profinite ring.

The following lemma is at the basis of our construction of moduli schemes of absolutely irreducible representations of f-pro-$\mathfrak{a}$ rings:

Lemma 1. *Let R be an f-pro-$\mathfrak{a}$ ring, and $n \geq 1$ an integer. Then there exist a commutative f-pro-$\mathfrak{a}$ ring $\mathrm{F}_n(R)$ and a morphism $\Phi_{R,n} : R \to \mathrm{M}_n(\mathrm{F}_n(R))$ of f-pro-$\mathfrak{a}$ rings which is universal for morphisms of R into matrix algebras; i.e., if $\phi : R \to \mathrm{M}_n(F)$ is a morphism of f-pro-$\mathfrak{a}$ rings with F a commutative f-pro-$\mathfrak{a}$ ring, then there exists a unique morphism $f : \mathrm{F}_n(R) \to F$ such that $\phi = \mathrm{M}_n(f) \circ \Phi_{R,n}$:*

$$\begin{array}{ccc} & & \mathrm{M}_n(\mathrm{F}_n(R)) \\ & \overset{\Phi_{R,n}}{\nearrow} & \downarrow{\scriptstyle \mathrm{M}_n(f)} \\ R & \xrightarrow[\phi]{} & \mathrm{M}_n(F). \end{array}$$

Now let $\mathfrak{A}$ be the category of f-pro-$\mathfrak{a}$ rings (or any category of topological rings which has similar properties — I think it is not necessary here to make the axioms explicit), and let $\mathfrak{C}$ be the full subcategory of $\mathfrak{A}$ consisting of commutative objects. In what follows, all rings and morphisms are in $\mathfrak{A}$.

Definition 2. Let $F \in \mathfrak{C}$. An *Azumaya algebra* A over F of degree n is an F-algebra such that:

(1) A is a locally free F-module of rank n^2;
(2) The map

$$\begin{array}{rccc} \iota : & A \otimes_F A^{\mathrm{o}} & \to & \mathrm{End}_F(A) \\ & a \otimes b & \mapsto & (x \mapsto axb) \end{array}$$

is an isomorphism of rings.

For more on Azumaya algebras, see e.g. [2].

Definition 3. Let $R \in \mathfrak{A}$ and $F \in \mathfrak{C}$. A *representation* of R over F of *degree* n is a morphism $\rho : R \to A$ in $\mathfrak{A}$, where A is an Azumaya algebra over F of degree n. It is said to be *absolutely irreducible* if ρ is essentially surjective, meaning that the image $\rho(R)$ generates A as an F-module. Two representations $\rho_i : R \to A_i$ over F

are said to be *isomorphic* if there is an isomorphism $\phi : A_1 \to A_2$ of F-algebras in $\mathfrak{A}$ such that $\rho_2 = \phi \circ \rho_1$.

Let $\mathfrak{S}$ be the category of schemes obtained by patching affine pieces $\mathrm{Spec}(F)$ with $F \in \mathfrak{C}$. The notions of Azumaya algebra and (absolutely irreducible) representation of R can be globalized, so that we may talk about Azumaya algebras $\mathcal{A}$ over $S \in \mathfrak{S}$ and absolutely irreducible representations $\rho : R \to \mathfrak{A}$.

Let R be an object of $\mathfrak{A}$ and $n \geq 1$ an integer. We assume that R has the following property (this is weaker than what is ensured in Lemma 1):

($\mathrm{V}_n^{\mathrm{ai}}$) There exist an object $\boldsymbol{F}$ of $\mathfrak{C}$ and a morphism $\Phi : R \to \mathrm{M}_n(\boldsymbol{F})$ in $\mathfrak{A}$ such that, for any $F \in \mathfrak{C}$ and any absolutely irreducible representation $\phi : R \to \mathrm{M}_n(F)$ in $\mathfrak{A}$, there exists a morphism $f : \boldsymbol{F} \to F$ and an automorphism $\sigma \in \mathrm{Aut}_{F\text{-alg}}(\mathrm{M}_n(F))$ such that $\phi = \sigma \circ \mathrm{M}_n(f) \circ \Phi$.

Then we can construct the moduli scheme which parametrizes all absolutely irreducible representations of R of degree n as follows: Define

- $\boldsymbol{F}^{\mathrm{tr}}$ to be the closed subring of $\boldsymbol{F}$ generated by $\mathrm{Tr}(\Phi(R))$;
- $\boldsymbol{A}^{\mathrm{tr}}$ to be the closed $\boldsymbol{F}^{\mathrm{tr}}$-subalgebra of $\mathrm{M}_n(\boldsymbol{F})$ generated by the image $\Phi(R)$ of R.

The localizations of $\boldsymbol{A}^{\mathrm{tr}}$ at primes of $\boldsymbol{F}^{\mathrm{tr}}$ may happen to be Azumaya algebras. Define $X_{R,n}$ to be the open subscheme of $\mathrm{Spec}(\boldsymbol{F}^{\mathrm{tr}})$ over which $\boldsymbol{A}^{\mathrm{tr}}$ is Azumaya. It is an object of $\mathfrak{S}$, and will turn out to be the wanted moduli scheme. The morphism Φ in ($\mathrm{V}_n^{\mathrm{ai}}$) gives rise to an absolutely irreducible representation

$$\rho_{R,n} : R \to \mathcal{A}_{R,n},$$

where $\mathcal{A}_{R,n}$ is the restriction to $X_{R,n}$ of the sheafification of $\boldsymbol{A}^{\mathrm{tr}}$.

For $S \in \mathfrak{S}$, let $\underline{\mathrm{Rep}}^{\mathrm{ai}}_{R,n}(S)$ be the set of isomorphism classes of absolutely irreducible representations of R over S of degree n. If $g : S \to X_{R,n}$ is a morphism in $\mathfrak{S}$, then the pull-back $g^*\rho_{R,n} : R \to g^*\mathcal{A}_{R,n}$ of $\rho_{R,n}$ by g is an absolutely irreducible representation of R over S. Thus we have a map of sets

$$\boldsymbol{r} : X_{R,n}(S) \to \underline{\mathrm{Rep}}^{\mathrm{ai}}_{R,n}(S).$$

We can show that $\boldsymbol{r}$ is bijective. In other words, we have:

Theorem 4. *The scheme $X_{R,n}$ represents the functor $\underline{\mathrm{Rep}}^{\mathrm{ai}}_{R,n}$.*

2. Zeta functions.

In this section, let R be a profinite ring. We could consider various kinds of zeta functions of R. In this paper, however, we concentrate on the following type of zeta functions: Let $\mathbb{F}_q$ be a finite field of q elements. For each $n \geq 1$, we define the nth zeta function of R to be

$$Z_{R,n,\mathbb{F}_q} := \exp\left(\sum_{\nu=1}^{\infty} \frac{N_\nu}{\nu} T^\nu\right),$$

where

$$N_\nu := \#\underline{\mathrm{Rep}}^{\mathrm{ai}}_{R,n}(\mathbb{F}_{q^\nu}).$$

It is *a priori* in the power series ring $\mathbb{Q}[\![T]\!]$.

Theorem 5. *If the scheme $X_{R,n} \otimes_{\widehat{\mathbb{Z}}} \mathbb{F}_q$ is of finite type over $\mathbb{F}_q$, then the power series $Z_{R,n,\mathbb{F}_q}(T)$ has radius of convergence > 0. If R is isomorphic to the profinite completion of a finitely generated (discrete) ring, then it is a rational function in T.*

The first assertion of the Theorem is trivial if R itself is topologically finitely generated. So our interest is in the case is where R is not known to be topologically finitely generated but still $X_{R,n}$ is known to be of finite type. So far, I have no such examples. A question related to this issue is the following: Let K be a global field (= a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(t)$), S a fintie set of places of K, and $G_{K,S}$ the Galois group over K of the maximal separable extension of K unramified outside S. It is known ([4]) that $G_{K,S}$ is generated by a finite number of conjugacy classes. Let $R_{K,S} := \widehat{\mathbb{Z}}[\![G_{K,S}]\!]$.

Question. Is the f-profinite scheme $X_{R_{K,S},n}$ of finite type over $\widehat{\mathbb{Z}}$?

This is equivalent to asking if the ring $\boldsymbol{F}^{\rm tr}$ generated by the image of $\operatorname{Tr}\Phi_{R_{K,S},n}$ is topologically finitely generated. The values of $\operatorname{Tr}\Phi_{R_{K,S},n}$ is of course constant on each conjugacy class of $G_{K,S}$. However, if $G_{K,S}$ is generated by a finitely many conjugacy classes $G_1, ..., G_r$, it may not be true that $\operatorname{Tr}(\Phi_{R_{K,S},n}(G_1)), ..., \operatorname{Tr}(\Phi_{R_{K,S},n}(G_r))$ generate $\boldsymbol{F}^{\rm tr}$ as a topological ring.

3. Finiteness conjectures on Galois representations.

Let K be a global field, and p a prime number. We consider two kinds of Galois representations of K, mod p representations and p-adic representations.

3-1. Mod p representations. Let $N = \prod \mathfrak{q}^{n_\mathfrak{q}}$ be an effective divisor of K. Khare ([5]) and Moon ([7]) independently formulated the following conjecture:

Conjecture ($\mathbb{F}$)**.** For any K, n, p and N as above, there exist only finitely many isomorphism classes of semisimple continuous representations $\rho : G_K \to \mathrm{GL}_n(\overline{\mathbb{F}}_p)$ with $N(\rho)|N$.

Here, $N(\rho)$ is the *Artin conductor* of ρ outside p, and is defined by the product

$$N(\rho) \;=\; \prod_{\mathfrak{q}} \mathfrak{q}^{n_\mathfrak{q}(\rho)}$$

over the primes $\mathfrak{q}$ of K (not dividing p, if K is an algebraic number field) with exponent

$$n_\mathfrak{q}(\rho) \;:=\; \sum_{i=0}^{\infty} \frac{1}{(G_{\mathfrak{q},0} : G_{\mathfrak{q},i})} \dim_{\overline{\mathbb{F}}_p}(V/V^{G_{\mathfrak{q},i}}),$$

where V is the representation space of ρ and $G_{\mathfrak{q},i}$ is the ith ramification subgroup of $\mathrm{Im}(\rho)$ at (an extension of) $\mathfrak{q}$.

In terms of our moduli scheme, this can be reformulated as follows: Let $G_K(N)$ be the quotient of G_K by the normal subgroup generated by $G_{K_\mathfrak{q}}^{n_\mathfrak{q}}$ (and its conjugates) for all[1] $\mathfrak{q}$, where $G_{K_\mathfrak{q}}^{n_\mathfrak{q}}$ is the $n_\mathfrak{q}$th ramification subgroup (in the upper numbering filtration) of the absolute Galois group $G_{K_\mathfrak{q}}$ of the completion $K_\mathfrak{q}$ of K at $\mathfrak{q}$. Let $X_{\mathbb{F}_p[G_K(N)],n}$ be the f-profinite scheme constructed in Theorem 4 for the profinite ring $R = \mathbb{F}_p[G_K(N)]$. It can be checked that Conjecture ($\mathbb{F}$) is equivalent to each of the following two statements:

Conjecture ($\mathbb{F}^*$)**.** For any K, n, p and N, there exist only finitely many isomorphism classes of semisimple continuous representations $\rho : G_K(N) \to \mathrm{GL}_n(\overline{\mathbb{F}}_p)$.

Conjecture ($\mathbb{X}$)**.** For any K, n, p and N, the set of $\overline{\mathbb{F}}_p$-rational points of $X_{\mathbb{F}_p[G_K(N)],n}$ is finite.

Note that the f-profinite scheme $X_{\mathbb{F}_p[G_K(N)],n}$ itself may not be finite over $\mathbb{F}_p$.

3-2. p-adic representations. Although we do not explain this in detail here, certain versions of the finiteness conjectures of Fontaine-Mazur on geometric Galois representations ([1], Conj. 2a, 2b, 2c) can also be formulated in terms of our moduli schemes. This is nicely done already in terms of Mazur's deformation theory if all the p-adic representations considered have the property that their residual representations ρ_0 have one-dimensional $\mathrm{End}(\rho_0)$ over the coefficient field. In general, however, this is far from reality, so that our theory is necessary.

References

[1] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, in: Elliptic curves, modular forms and Fermat's last theorem (Hong Kong, 1993), Internat. Press, Cambridge, MA, 1995, pp. 41–78 (190–227 in the 2nd ed.)

[2] A. Grothendieck, *Le groupe de Brauer, I. Algebres d'Azumaya et interpretations diverses*, Séminaire Bourbaki 1964/65, Exp. **290** (in the new edition: Vol. 9, Soc. Math. France, Paris, 1995, pp. 199–219); also in: "Dix Exposés sur la cohomologie des schémas", North Holland, Amsterdam et Masson, Paris, 1968

[3] R. Huber, *Continuous valuations*, Math. Z. **212** (1993), 455–477

[4] Y. Ihara, *How many primes decompose completely in an infinite unramified Galois extension of a global field?*, J. Math. Soc. Japan **35** (1983), 81–106

[5] C. Khare, *Conjectures on finiteness of mod p Galois representations*, J. Ramanujan Math. Soc. **15** (2000), 23–42

[6] B. Mazur, *Deforming Galois representations*, in: Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987), Y. Ihara, K. Ribet and J.-P. Serre (eds.), M.S.R.I. Publ. **16**, Springer-Verlag, New York, 1989, pp. 385–437

[7] H. Moon, *Finiteness results on certain mod p Galois representations*, J. Number Theory **84** (2000), 156–165

[8] C. Procesi, *Deformations of representations*, in: "Methods in ring theory" (Levico Terme, 1997), Lecture Notes in Pure and Appl. Math. **198**, Dekker, New York, 1998, pp. 247–276

[1]Note that $n_\mathfrak{q} = 0$ for almost all $\mathfrak{q}$ and that we omit those $\mathfrak{q}|p$ if K is an algebraic number field.