BASIC RESULTS IN THE DEFORMATION THEORY OF GALOIS REPRESENTATIONS

DANIEL MILLER

Contents

This is a review of useful results in the study of deformations of (mostly two-dimensional) representations of $\pi_1(\mathbf{Q}) = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. References to the literature will be given whenever possible.

1. Group cohomology

1.1. **Inflation-restriction.** This is from [NSW08, 1.6.7]. Let $H \subset G$ be a closed normal subgroup of a profinite group. If A is a G-module, then there is a canonical exact sequence

$$0 \longrightarrow \mathrm{H}^1(G/H, A^H) \xrightarrow{\text{inf}} \mathrm{H}^1(G, A) \xrightarrow{\text{res}} \mathrm{H}^1(H, A)^{G/H}.$$

1.2. **Duality theorems for Galois cohomology.** Let l be a prime, X a connected noetherian scheme on which l is invertible. Let $\mathbf{Z}_l = \varprojlim \boldsymbol{\mu}_{l^n}$, considered as a smooth l-adic sheaf on X. For any l-adic sheaf F on X, put $F(n) = F \otimes_{\mathbf{Z}_l} \mathbf{Z}_l(1)^{\otimes n}$.

We call a *p-adic field* a nonarchimedean local field of characteristic zero with residue characteristic p.

Theorem 1.3 (Tate). *Let k be a p-adic local field. Let M be a finite $\pi_1(k)$-module. Then the cup-product induces an isomorphism*

$$\mathrm{H}^\bullet(k, M^\vee(1)) = \mathrm{H}^{2-\bullet}(k, M)^\vee.$$

Let $\pi = \pi_1(k)$, and let M be a π-module. Suppose we want to compute $h^\bullet(M)$. It should be possible to compute $h^0(M)$ and $h^2(M) = h^0(M^\vee(1))$. We then use the Euler-Poincaré characteristic formula of Tate [NSW08, 7.3.1] to do this.

1.4. **Tate-Shafarevich groups and sets of places.** Let F be a number field, S a finite set of places of F. If M is a $G_{F,S}$-module, put

$$Ш^1_S(M) = \ker\left(\mathrm{H}^1(G_{F,S}, M) \to \bigoplus_{v \in S} \mathrm{H}^1(G_v, M)\right).$$

If $S \subset T$, then one can naturally identify $Ш^1_S(M)$ with a subgroup of $Ш^1_T(M)$. Indeed, there is a natural injection (inflation) $\mathrm{H}^1(G_{F,S}, M) \to \mathrm{H}^1(G_{F,T}, M)$ coming from the projection $G_{F,T} \twoheadrightarrow G_{F,S}$. The five-term inflation-restriction exact sequence [NSW08, 1.6.7] tells us that the image of the inflation map is the kernel of the restriction map $\mathrm{H}^1(G_{F,T}, M) \to \mathrm{H}^1(H, M)$, where $H = \ker(G_{F,T} \to G_{F,S})$. The point is that $H = \langle I_v : v \in T \smallsetminus S\rangle$. So if $c \in Ш_T(M)$, then $c|_v = 0$ for all $v \in T \smallsetminus S$, so certainly c is induced from an element of $\mathrm{H}^1(G_{F,S}, M)$. What remains is the easy verification of $c \in Ш_S(M)$. To be precise,

$Ш^1_T(M) \subset \mathrm{H}^1(G_{F,T}, M)$ is a subset of the image of $Ш^1_S(M) \subset \mathrm{H}^1(G_{F,S}, M)$ under the (injective) inflation map.

2. Galois representations associated to modular forms

Let $N \geqslant 1$ be an integer and $\varepsilon : (\mathbf{Z}/N)^\times \to S^1$ a character. We write $S_0(N,\varepsilon)$ for the space of cusp forms for $\Gamma_1(N)$ with nebentypus ε. We call a form $f = \sum_{n\geqslant 0} a_n q^n$ in $S_0(N,\varepsilon)$ *normalized* if $a_0 = 1$.

Theorem 2.1. *Let $N \geqslant 3$ and $k \geqslant 1$ be integers, l an odd prime. Let $f_0 \in S_0(N,\varepsilon)$ be a normalized eigenfunction for the Hecke operators $\{T_p : p \nmid N\}$. Let $K = K_f = \mathbf{Q}(a_n : n \geqslant 1)$. Then there is a continuous irreducible representation $\rho_{f,l} : \pi_1\left(\mathbf{Z}[\frac{1}{lN}]\right) \to \mathrm{GL}_2(K_{f,l})$ such that for each prime $p \nmid lN$,*

$$\operatorname{tr} \rho_{f,l}(\mathrm{fr}_p) = a_p$$
$$\det \rho_{f,l}(\mathrm{fr}_p) = \varepsilon(p) p^{k-1}.$$

This representation is unique up to isomorphism.

Proof. **Do this!** □

3. Specific representations

Nice fact if ϕ, ψ are characters:

$$\mathrm{ad}(\phi \oplus \psi) = \phi^{-1}\psi \oplus \phi\psi^{-1} \oplus 2.$$

In particular,

$$h^0(\mathrm{ad}(\phi \oplus 1)) = 2 + 2h^0(\phi)$$

3.1. Peu ramifiée and très ramifée extensions.

The original source is [Ser87, 2.4.6]. Let $\bar\rho : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(\mathbf{F}_q)$ be an ordinary representation, i.e. $\bar\rho$ is the extension of an unramified character by an unramified twist of the cyclotomic character. Let $\mathbf{Q}_p^{\mathrm{ur}}(\bar\rho)$ be the extension of $\mathbf{Q}_p^{\mathrm{ur}}$ with Galois group cut out by $\bar\rho(I)$, where $I \subset G_{\mathbf{Q}_p}$ is the inertia group. It has a subextension $\mathbf{Q}_p^{\mathrm{ur}}(\bar\rho|_P)$, where $P \subset I$ is wild inertia. Kummer theory tells us that

$$\mathbf{Q}_p^{\mathrm{ur}}(\bar\rho) = \mathbf{Q}_p^{\mathrm{ur}}(\bar\rho|_P)(\sqrt[p]{x_1}, \ldots, \sqrt[p]{x_r}).$$

We say that $\bar\rho$ is *peu ramifiée* if $v_p(x_i) \equiv 0 \pmod p$ for each i, and $\bar\rho$ is *très ramifiée* otherwise.

In [Edi92, 8.2], we have an alternative definition. Consider the extension $\bar\rho$ as a finite étale group scheme V of $\mathbf{F}_q$-vector spaces over $\mathbf{Q}_p$. Then $\bar\rho$ is peu ramifiée if V can be extended to a finite flat group scheme over $\mathbf{Z}_p$, and très ramifiée otherwise.

3.2. Fundamental characters.

The reference is [Tat97, 4.4]. Let $(\mathcal{O}, \mathfrak{m}, k)$ be a complete mixed-characteristic discrete valuation ring with perfect residue field. Then the projection $\mathcal{O} \twoheadrightarrow k$ admits a multiplicative section $\omega : k \to \mathcal{O}$. If k_0 is a field, then the induced map $k_0 \to \mathcal{O}$ coming from any embedding $k_0 \hookrightarrow k$ is called a *fundamental character*. The main example is when $\mathcal{O}$ is the ring of integers in a finite extension of $\mathbf{Q}_p$ and $k = \mathbf{F}_{p^f}$, in which case the fundamental characters $k^\times \to \mathcal{O}^\times$ form a $\mathbf{Z}/f$-torsor under $r \cdot \chi = \chi^{p^r}$.

A better reference is [Ser72, 1.7].

4. Modular representations

4.1. Hecke operators.

A good (concise) summary of the diamond operators, Atkin-Lehner involution, and Hecke operators is [MW84, ch.2 §5].

4.2. **New parts of Jacobians.** The following is from [Maz78, §2]. For $n \geqslant 1$, let $J_0(n)$ be the jacobian of the modular curve $X_0(n)$. If $n = n'd$, there is a "degeneracy map" $B_d : X_0(n) \to X_0(n')$ that sends a pair (E, C) consisting of an elliptic curve and $C \subset E[n]$ of order n to the pair $(E/C[d], (C/C[d])[n'])$. There are induced maps $B_d^* : J_0(n') \to J_0(n)$. Let $J_0(n)_{\text{old}} \subset J_0(n)$ be the abelian subvariety generated by the images of the B_d for $n' < n$, and define $J_0(n)^{\text{new}}$ by the short exact sequence

$$0 \to J_0(n)_{\text{old}} \to J_0(n) \to J_0(n)^{\text{new}} \to 0.$$

By general theory, there is an isogeny $J_0(n) \sim J_0(n)_{\text{old}} \times J_0(n)^{\text{new}}$, thus an isomorphism of Galois representations

$$V_\ell J_0(n) \simeq V_\ell J_0(n)_{\text{old}} \oplus V_\ell J_0(n)^{\text{new}}.$$

There is an induced action of the Hecke algebra on $J_0(n)^{\text{new}}$.

4.3. **Eisenstein ideal.** This definition is from [Maz77, II.9]. Let $\mathbf{T} = \mathbf{T}_n$ be the Hecke algebra for $\Gamma_0(n)$. So $\mathbf{T}$ is generated as a $\mathbf{Z}$-algebra by the Hecke operators T_l, $l \nmid n$. The *Eisenstein ideal* $\mathfrak{I} \subset \mathbf{T}$ is generated by the $T_l - (l+1)$ for $l \nmid n$, and $1 + w$. So if $f \in S_k$ is an eigenform annihilated by $\mathfrak{I}$, one has $a_p(f) = p + 1$. This means $\rho_{f,l}$ should look like $\kappa_l \oplus 1$, where κ is the cyclotomic character.

5. Deformation problems

Let $\mathcal{O}$ be a complete dvr with residue field k. Our deformation problems will be covariant functors on the category $\mathsf{C}_{\mathcal{O}}$ of "test objects." These are local artinian $\mathcal{O}$-algebras A such that $\mathcal{O} \to A$ induces an isomorphism $k \xrightarrow{\sim} A/\mathfrak{m}_A$.

5.1. **Minimal deformations.** Here we follow [Kha03, §2.1]. Let k be a finite field of characteristic p and $\bar\rho : G_{\mathbf{Q},S} \to \mathrm{GL}_2(k)$ a continuous p-ordinary representation. One says a lift $\rho : G_{\mathbf{Q},S} \to \mathrm{GL}_2(A)$ is *minimally ramified* if for $v \in S \smallsetminus p$,

$$\rho|_{I_v} \sim \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}.$$

(This doesn't seem to be the same as [KR03, p.180]. Find out what's wrong.)

5.2. **New deformation rings.** We follow [KR03, df.1]. Let $\bar\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_q)$ be a continuous representation unramified outside S. Suppose $T \supset S$ is a finite set of primes such that $\bar\rho$ is nice for $T \smallsetminus S$. Then $R_{\bar\rho}^{T\text{-new}}$ represents minimally ramified deformations $\rho : G_{\mathbf{Q},S} \to \mathrm{GL}_2(A)$ such that for $v \in T \smallsetminus S$, ρ_v is a twist of $\begin{pmatrix} \varepsilon & * \\ & 1 \end{pmatrix}$.

6. Commutative algebra

6.1. **Weierstrass preparation theorem.** This is from [Bou98, VII §3.8, pr.6]. Let $\mathcal{O}$ be a complete discrete valuation ring with uniformizer π. Then any $f \in \mathcal{O}[\![X]\!]$ can be written as

$$f = u\pi^m \left(X^n + a_{n-1}X^{n-1} + \cdots + a_0\right),$$

where $u \in \mathcal{O}[\![X]\!]^\times$ and the $a_i \in \langle \pi \rangle$. In particular, the only way the quotient $\mathcal{O}[\![X]\!]/f$ can be flat over $\mathcal{O}$ is for $m = 0$, in which case the quotient has finite $\mathcal{O}$-rank.

6.2. **Specific presentations via small extensions.** Fix a finite field k of characteristic p. Recall that a *coefficient ring* over k is a complete local noetherian $\mathrm{W}(k)$-algebra with residue field k. If R is such a ring, write $\mathfrak{t}_R = \hom(\mathfrak{m}_R/\mathfrak{m}_R^2, k)$; this is a k-vector space. Recall that a *small extension* of coefficient rings over k is a surjection $R_1 \twoheadrightarrow R_0$ such that the kernel I is principle and annihilated by $\mathfrak{m}_1$.

We are interested in measuring the complexity of presentations of coefficient rings. Write $\mathrm{W}(k)[\![\boldsymbol{x}]\!] = \mathrm{W}(k)[\![x_1, \ldots, x_d]\!]$. For a polynomial $f \in \mathrm{W}(k)[\![\boldsymbol{x}]\!]$, put

$$v(f) = \min\{e : p^e \mid f\} + \sum_{i=1}^{r} \min\{n_i : x_i^{n_i} \mid f\}.$$

For a set $\boldsymbol{f} = \{f_1, \ldots, f_r\} \subset \mathrm{W}(k)[\![\boldsymbol{x}]\!]$, the *complexity* of $\boldsymbol{f}$, denoted $v(\boldsymbol{f})$, is by definition $\min\{v(f_i)\}_{1\leqslant i\leqslant r}$. Put $|\boldsymbol{n}| = n_1 + \cdots + n_r$. Note that if $v(\boldsymbol{f}) \geqslant e + |\boldsymbol{n}|$, then we have a surjection

$$R(e, \boldsymbol{n}) = \mathrm{W}(k)[\![\boldsymbol{x}]\!]/\langle p^e, x_1^{n_1}, \ldots, x_d^{n_d}\rangle \twoheadrightarrow R(\boldsymbol{f}) = \mathrm{W}(k)[\![\boldsymbol{x}]\!]/\langle f_1, \ldots, f_r\rangle.$$

We introduce an operation $\boldsymbol{f} \mapsto \boldsymbol{f}^+$ on sets of relations. Put

$$\{f_1, \ldots, f_r\}^+ = \{pf_1, x_1 f_1, \ldots, x_d f_1, \ldots, pf_r, x_1 f_r, \ldots, x_d f_r\}.$$

Note that $v(\boldsymbol{f}^+) > v(\boldsymbol{f})$, and that the natural map $R(\boldsymbol{f}^+) \twoheadrightarrow R(\boldsymbol{f})$ factors as

$$\begin{aligned} R(\boldsymbol{f}^+) &\twoheadrightarrow R(pf_1, x_1 f_1, \ldots, x_d f_1, \ldots, pf_{r-1}, x_1 f_{r-1}, \ldots, x_d f_{r-1}, f_r) \\ &\twoheadrightarrow R(pf_1, x_1 f_1, \ldots, x_d f_1, \ldots, pf_{r-2}, x_1 f_{r-2}, \ldots, x_d f_{r-2}, f_{r-1}, f_r) \\ &\twoheadrightarrow \cdots \\ &\twoheadrightarrow R(\boldsymbol{f}), \end{aligned}$$

in which each surjection is small.

Write $\boldsymbol{f}^{+0} = \boldsymbol{f}$, $\boldsymbol{f}^{+(n+1)} = (\boldsymbol{f}^{+n})^+$. Fix some $\boldsymbol{f}$. Then for all $(e, \boldsymbol{n})$ with $e + |\boldsymbol{n}| \geqslant v(\boldsymbol{f})$, there exists some m such that $v(\boldsymbol{f}^{+m}) \geqslant e + |\boldsymbol{n}|$. This gives quotients

$$R(e, \boldsymbol{n}) \twoheadleftarrow R(\boldsymbol{f}^{+m}) \twoheadrightarrow R(\boldsymbol{f}).$$

The key facts here are:

(1) The surjection $R(\boldsymbol{f}^{+m}) \twoheadrightarrow R(\boldsymbol{f})$ is a composite of small extensions.
(2) Rings of the form $R(e, \boldsymbol{n})$ surject onto any finite coefficient ring.

The latter fact holds because $\mathrm{W}(k)[\![\boldsymbol{x}]\!] = \varprojlim R(e, \boldsymbol{n})$.

References

[Bou98] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7.* Elements of Mathematics. Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[Edi92] Bas Edixhoven. The weight in Serre's conjectures on modular forms. *Invent. Math.*, 109(3):563–594, 1992.

[Kha03] Chandrashekhar Khare. On isomorphisms between deformation rings and Hecke rings. *Invent. Math.*, 154(2):199–222, 2003. With an appendix by Gebhard Böckle.

[KR03] Chandrashekhar Khare and Ravi Ramakrishna. Finiteness of Selmer groups and deformation rings. *Invent. Math.*, 154(1):179–198, 2003.

[Maz77] Barry Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186, 1977.

[Maz78] Barry Mazur. Rational isogenies of prime degree. *Invent. Math.*, 44(2):129–162, 1978. with an appendix by D. Goldfeld.

[MW84] Barry Mazur and Andrew Wiles. Class fields of abelian extensions of $\mathbf{Q}$. *Invent. Math.*, 76(2):179–330, 1984.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, second edition, 2008.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser87] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[Tat97] John Tate. Finite flat group schemes. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 121–154. Springer, 1997.