PSEUDOCHARACTERS AND THE LENGTH BOUND

Prerequisites. Complete local noetherian rings and Hensel's lemma; lengths of modules; elementary divisors of matrices over $\mathbb{Z}_p$; graded rings. From Chapter 30, *Tate–Shafarevich groups of Tate twists*: the groups $G_{\mathbb{Q},p}$, G_p, $\mathrm{Sha}_p(\mathbb{Q}, e)$, Problem 30.1.1 and Theorem 30.1.2. From Chapter 32, *Eisenstein congruences and Selmer classes*: Problem 32.1.1, the congruence (1), the lattices of Section 32.2 (Problems 32.2.1–32.2.4), the inputs (D), (I), (O) of Section 32.3 with Problems 32.3.1 and 32.3.3, and Section 32.4, in particular Problems 32.4.6–32.4.8.

Chapter 32 ended with the observation that the Hecke algebra sees a Galois representation only through its traces. A Hecke algebra is not a domain: it has an Eisenstein component and cuspidal components, and its traces do not in general come from a representation over it. What structure do traces alone carry, and how do they measure Sha? The structure is a pseudocharacter; the ideal of products $b \cdot c$ of Chapter 32 can be read off from the traces; and the quotient by it carries extension classes. In a graded model of the deformation ring we then bound the length of the cotangent module that stands for the Selmer group by the length of a quotient of the model's Hecke algebra, and so by valuations of trace differences. Throughout, p is an odd prime.

33.1. Pseudocharacters of dimension two

Let G be a group and R a commutative ring in which 2 is invertible. A *pseudocharacter of dimension* 2 of G with values in R is a pair (T, D) of a function $T\colon G \to R$ and a homomorphism $D\colon G \to R^\times$ such that $T(1) = 2$ and, for all $g, h \in G$,

$$T(gh) = T(hg), \qquad T(gh) + D(g)\,T(g^{-1}h) = T(g)\,T(h).$$

By [Ch, Lemma 1.9] such pairs are the same as Chenevier's determinants of dimension 2. The function T is then a pseudocharacter of dimension 2 in the sense of Taylor [Ta, §1] and Rouquier [Ro], and conversely every such T arises in this way [Ch, Prop. 1.29]; see also [BC, §1.2]. The notion is due to Wiles in dimension two and to Taylor in general [BC, §1.1].

Problem 33.1.1. For every homomorphism $\rho\colon G \to \mathrm{GL}_2(R)$, $(\operatorname{tr}\rho, \det\rho)$ is a pseudocharacter. In particular, so is $(\psi_1 + \psi_2, \psi_1\psi_2)$ for any two characters $\psi_1, \psi_2\colon G \to R^\times$.

Problem 33.1.2. If (T, D) is a pseudocharacter, then $D(g) = \frac{1}{2}\big(T(g)^2 - T(g^2)\big)$ and $T(g^{-1}) = D(g)^{-1}T(g)$ for all $g \in G$.

So D is determined by T, and we often write T for the pair.

Problem 33.1.3. Let $R \subseteq R_1 \times R_2$ be a subring in which 2 is invertible, and let (T_i, D_i) be pseudocharacters with values in R_i. If $(T_1(g), T_2(g)) \in R$ for every g, then $((T_1, T_2), (D_1, D_2))$ is a pseudocharacter with values in R.

Date: November 25, 2026.

The first example of a pseudocharacter that is not visibly a trace is the one carried by a Hecke algebra with one Eisenstein and one cuspidal point. Let G be profinite, let $\chi\colon G \to \mathbb{Z}_p^\times$ be a continuous character whose reduction $\bar\chi$ is not trivial, and let $\rho\colon G \to \mathrm{GL}_2(\mathbb{Q}_p)$ be a continuous representation with $\operatorname{tr}\rho(G) \subseteq \mathbb{Z}_p$, $\operatorname{tr}\rho \equiv 1+\chi \pmod p$ and $\operatorname{tr}\rho \neq 1+\chi$. Put

$$e := \min_{g\in G} v_p\big(\operatorname{tr}\rho(g) - 1 - \chi(g)\big), \qquad \mathcal{T}(g) := \big(1+\chi(g), \operatorname{tr}\rho(g)\big) \in \mathbb{Z}_p \times \mathbb{Z}_p.$$

Problem 33.1.4. The $\mathbb{Z}_p$-subalgebra of $\mathbb{Z}_p \times \mathbb{Z}_p$ generated by the $\mathcal{T}(g)$ is $\mathbf{T}_e := \{(u,v) : u \equiv v \pmod{p^e}\}$, and $x \mapsto (0,p^e)$ induces $\mathbb{Z}_p[x]/(x(x-p^e)) \cong \mathbf{T}_e$. The function $\mathcal{T}$ is a pseudocharacter with values in $\mathbf{T}_e$.

The ring $\mathbf{T}_e$ is the *toy Hecke algebra*: $x=0$ is the Eisenstein point, $x=p^e$ the cuspidal point, and e measures how close they are. It occurs in nature.

Problem 33.1.5. The $\mathbb{Z}_{691}$-subalgebra of $\mathrm{End}(M_{12}\otimes\mathbb{Q}_{691})$ generated by the Hecke operators T_n, $n \geq 1$, on modular forms of weight 12 and level 1 is isomorphic to $\mathbb{Z}_{691}[x]/(x(x-691))$.

33.2. The reducibility ideal

Let R be a complete local noetherian ring with maximal ideal $\mathfrak{m}$ and residue field $\mathbb{F}$ of characteristic $\neq 2$, and let (T,D) be a pseudocharacter of G with values in R such that $T \equiv \chi_1 + \chi_2 \pmod{\mathfrak{m}}$ for two distinct characters $\chi_1, \chi_2\colon G \to \mathbb{F}^\times$. Fix $\sigma_0 \in G$ with $\chi_1(\sigma_0) \neq \chi_2(\sigma_0)$.

Problem 33.2.1. The polynomial $X^2 - T(\sigma_0)X + D(\sigma_0)$ has roots $\lambda_1, \lambda_2 \in R$ with $\lambda_i \equiv \chi_i(\sigma_0) \pmod{\mathfrak{m}}$, and $\lambda_1 - \lambda_2 \in R^\times$.

Define $a, d\colon G \to R$ by

$$a(g) := \frac{T(\sigma_0 g) - \lambda_2 T(g)}{\lambda_1 - \lambda_2}, \qquad d(g) := T(g) - a(g).$$

Problem 33.2.2. Suppose that $T = \operatorname{tr}\rho$ for $\rho\colon G \to \mathrm{GL}_2(R)$ with $\rho(\sigma_0) = \mathrm{diag}(\lambda_1,\lambda_2)$, and write $\rho = \left(\begin{smallmatrix} a' & b \\ c & d' \end{smallmatrix}\right)$. Then $a = a'$, $d = d'$, and $a(gh) - a(g)a(h) = b(g)c(h)$.

So a and d are the diagonal entries of a representation that need not exist, and the defect of a from being multiplicative stands in for the products $b(g)c(h)$.

Problem 33.2.3. $a \equiv \chi_1$ and $d \equiv \chi_2 \pmod{\mathfrak{m}}$. In particular $a(g) \in R^\times$.

Problem 33.2.4. $D(g) = a(g)T(g) - a(g^2)$ for every $g \in G$.

The *reducibility ideal* $I \subseteq R$ is the ideal generated by the elements $a(gh) - a(g)a(h)$, $g,h \in G$.

Problem 33.2.5. Modulo I, a and d are characters $G \to (R/I)^\times$, $T \equiv a + d$ and $D \equiv ad$.

Problem 33.2.6. Let $J \subsetneq R$ be an ideal, and let $\psi_1, \psi_2\colon G \to (R/J)^\times$ be characters with $\psi_i \equiv \chi_i \pmod{\mathfrak{m}}$ and $T \equiv \psi_1 + \psi_2 \pmod J$. Then $\psi_1 \equiv a$ and $\psi_2 \equiv d \pmod J$, and $I \subseteq J$.

Problems 33.2.5 and 33.2.6 prove the following; in particular I does not depend on σ_0. For pseudocharacters of any dimension whose residual constituents are absolutely irreducible and pairwise distinct, this is due to Bellaïche and Chenevier [BC, Prop. 1.5.1].

Theorem 33.2.1. *I is the smallest ideal J of R such that T is congruent modulo J to a sum of two characters lifting χ_1 and χ_2.*

For a representation ρ over a discrete valuation ring as in Section 32.2, Problems 33.2.2 and 32.4.6 give $I = \pi^{m+n}\mathcal{O}$, where $m+n$ is the length of the segment of stable lattices. Return to the toy Hecke algebra.

Problem 33.2.7. In Problem 33.1.4, suppose that ρ is irreducible, and let $m+n$ be the length of its segment of stable lattices (Problem 32.2.3, with $\chi_1 = 1$, $\chi_2 = \bar{\chi}$). Then $m+n \geq e$, and the reducibility ideal of $\mathcal{T}$ is $\{0\} \times p^{m+n}\mathbb{Z}_p = p^{m+n-e}\, x\mathbf{T}_e$.

The *Eisenstein ideal* of a pseudocharacter T with respect to two given characters $\psi_1, \psi_2 \colon G \to R^\times$ is the ideal I_{Eis} generated by the $T(g) - \psi_1(g) - \psi_2(g)$. By Theorem 33.2.1, $I \subseteq I_{\mathrm{Eis}}$ whenever the ψ_i lift the χ_i. In the setting of Chapter 32 the two ideals coincide.

Problem 33.2.8. Let k, p, f, λ be as in Section 32.3, and let $m+n$ be the length of the segment of stable lattices of ρ_f. Then

$$m+n = \min_{\ell \neq p} v\big(a_\ell(f) - 1 - \ell^{k-1}\big),$$

the minimum over primes. So the reducibility ideal of $\operatorname{tr}\rho_f$ equals its Eisenstein ideal for $(1, \chi^{k-1})$.

For Δ and $p = 691$ both sides are 1 (Problem 32.4.8). When $K = \mathbb{Q}_p$, in the toy Hecke algebra built from $\rho = \rho_f$ and χ^{k-1} we get $e = m+n$, and the reducibility ideal is $x\mathbf{T}_e$: the Eisenstein component $\mathbf{T}_e/x\mathbf{T}_e = \mathbb{Z}_p$ is the largest quotient on which $\mathcal{T}$ is reducible.

33.3. The quotient by the reducibility ideal and Ext^1

Ribet's lemma produced a class modulo π. The reducibility ideal produces a class modulo I, which generates a copy of $\mathcal{O}/I$. Keep the notation of Section 32.2, with $\chi_1 \neq \chi_2$, and write ρ in the basis $\pi^m e_1, e_2$ of L_m as $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then the values of b generate $\mathcal{O}$, the values of c generate $I = \pi^{m+n}\mathcal{O}$, and by Problem 33.2.5 the reductions ψ_1, ψ_2 of a, d modulo I are characters. Put $\psi := \psi_1\psi_2^{-1}$.

Problem 33.3.1. $\kappa(g) := b(g)\, d(g)^{-1} \bmod I$ is a cocycle on G with values in $(\mathcal{O}/I)(\psi)$.

Problem 33.3.2. The $\mathcal{O}$-submodule of $H^1(G, (\mathcal{O}/I)(\psi))$ generated by the class of κ is isomorphic to $\mathcal{O}/I$.

Thus the quotient $\mathcal{O}/I$ embeds in a group of extensions of ψ_2 by ψ_1. For such pseudocharacters over a henselian local ring, Bellaïche and Chenevier [BC, Thm. 1.5.5] construct an injection of the dual, modulo I, of a module of off-diagonal entries into the corresponding Ext^1; this is the general form of the embedding. Now take $G = G_{\mathbb{Q},p}$, and f, λ, $\mathcal{O}$ as in Problem 33.2.8, so that $\psi \equiv \chi^{1-k} \pmod I$. As in Section 32.5, $\mathrm{Sha}_p(\mathbb{Q}, k-1) \otimes_{\mathbb{Z}_p} \mathcal{O}$ is the group of classes in $H^1(G_{\mathbb{Q},p}, (K/\mathcal{O})(1-k))$ that vanish on G_p.

Problem 33.3.3. The class of κ vanishes on G_p, and its image in $H^1(G_{\mathbb{Q},p}, (K/\mathcal{O})(1-k))$ generates a submodule isomorphic to $\mathcal{O}/I$. Hence $\operatorname{length}_{\mathcal{O}}\big(\mathrm{Sha}_p(\mathbb{Q}, k-1)\otimes\mathcal{O}\big) \geq m+n$.

This is the direction of Ribet and of Mazur and Wiles [MW], for one eigenform: a congruence of exponent $m+n$ produces a cyclic piece of Sha of that length. For Δ it gives $\operatorname{length}\mathrm{Sha}_{691}(\mathbb{Q}, 11) \geq 1$, and Theorem 30.1.2 gives equality. Alpöge's argument needs the reverse inequality, an upper bound for the length of Sha by trace differences. Traces cannot see a single class (Problem 32.4.5); they see only products of a class of weight -1 with a class of weight $+1$.

33.4. A graded model and the length bound

The torus $\{\mathrm{diag}(1,t)\}$ of Section 32.4 acts on a deformation ring of $\rho_0 = 1\oplus\omega^{k-1}$, and so grades it: upper right entries have weight -1, lower left entries weight $+1$, and traces weight 0. The reconstruction [Adr, §17.4] reduces the bound for Sha to four statements (G1)–(G4) about such a graded deformation ring: (G1) a class of Sha gives a tangent vector of weight -1 at the Eisenstein point; (G2) under hypotheses (M1)–(M5), the cotangent module of weight -1, modulo the differentials of the Selmer equations, has length at most $2\sum_\xi v(\xi(a))$, where a is a trace difference and ξ runs over representatives of the torus orbits of points with both upper and lower entries nonzero; (G3) the deformation problem is finite and these points are automorphic; (G4) a rigidity condition at these points. None of them is proved there; they are steps of its sketch towards the Selmer bound on windows, which in [Adr] is [Adr, Hyp. 17.11]; see the ledger in Section 58.7 of Chapter 58. Moreover (G3) is not a published theorem: it lies outside the hypotheses of the published automorphy lifting theorems for residually reducible representations, such as [ANT, Thm. 1.1]. We test (G2) on a model in which everything can be computed.

Let $P \in \mathbb{Z}_p[u]$ be a polynomial with $P(0) \neq 0$ and leading coefficient in $\mathbb{Z}_p^\times$, and let

$$A := \mathbb{Z}_p[y,z]/\big(y\,P(yz)\big),$$

graded by giving y weight -1 and z weight $+1$; the relation is homogeneous of weight -1. Think of y as an upper right entry and z as a lower left entry, so that $u = yz$ plays the role of $b\cdot c$. Let $x\colon A \to \mathbb{Z}_p$ be the Eisenstein point $y = z = 0$, with ideal $I_x = (y,z)$. The *cotangent module* I_x/I_x^2 is graded; write $(I_x/I_x^2)_{-1}$ for its part of weight -1, the model for the dual of the Selmer group.

Problem 33.4.1. $A_0 = \mathbb{Z}_p[u]/(uP(u))$ with $u = yz$, and $(I_x/I_x^2)_{-1} \cong \mathbb{Z}_p/P(0)\mathbb{Z}_p$. For $P(u) = p^r - u$, A_0 is the toy Hecke algebra $\mathbf{T}_r$ of Problem 33.1.4.

Problem 33.4.2. A point $(y,z) \in \overline{\mathbb{Q}}_p^2$ of $\operatorname{Spec} A$ has $y = 0$, or else yz is a root of P and $z \neq 0$. For each root u_0 of P, the points with $yz = u_0$ form one orbit of the torus.

So the points with both entries nonzero, the *two-signed* points, correspond to the roots of P; they are the cuspidal points. Let $\mathbf{T}^0 := \mathbb{Z}_p[u]/(P(u))$, the cuspidal quotient of A_0, and let $I_{\mathrm{Eis}} := u\mathbf{T}^0$, the image of the ideal of x in A_0; as in Section 33.2, it is generated by the product of an upper and a lower entry.

Problem 33.4.3. $\mathbf{T}^0$ is free over $\mathbb{Z}_p$. For $a \in \mathbb{Z}_p[u]$ with $a(\xi) \neq 0$ at every root ξ of P,

$$\operatorname{length}_{\mathbb{Z}_p} \mathbf{T}^0/a\mathbf{T}^0 = \sum_{\xi} v(a(\xi)),$$

the sum over the roots of P in $\overline{\mathbb{Q}}_p$ with multiplicity, where $v(p) = 1$.

Problem 33.4.4. Let $a \in A_0$ vanish at x, and let its image in $\mathbf{T}^0$ be nonzero at every root of P. Then

$$\operatorname{length}(I_x/I_x^2)_{-1} = \operatorname{length} \mathbf{T}^0/I_{\mathrm{Eis}} \leq \sum_{\xi} v(\xi(a)),$$

where $\xi(a)$ is the value of a at $u = \xi$ and the sum is over the roots ξ of P in $\overline{\mathbb{Q}}_p$, with multiplicity; that is, over the torus orbits of two-signed points (Problem 33.4.2), each counted with the multiplicity of its root. Equality holds for $a = u$.

Problems 33.4.1–33.4.4 prove the following.

Theorem 33.4.1. *In the model A, the length of the cotangent module of weight -1 equals* $\operatorname{length} \mathbf{T}^0/I_{\mathrm{Eis}}$*, and is at most $\sum_\xi v(\xi(a))$ for every a as in Problem 33.4.4. Equality holds for $a = u$.*

For $P = 691 - u$ the model has $A_0 = \mathbb{Z}_{691}[x]/(x(x - 691))$, the Hecke algebra of Problem 33.1.5, one two-signed orbit, with $u = 691$, and a cotangent module of weight -1 of length $1 = \operatorname{length} Ш_{691}(\mathbb{Q}, 11)$. In the model, (G1) and (G3) are built in: the cotangent module stands for the dual of the Selmer group, and every two-signed point is cuspidal. The content of the argument is to prove them for the actual deformation ring.

33.5. The factor two

In the model the comparison holds with the factor 1, while (G2) carries a factor 2 for a graded ring with many coordinates of each weight. Does the factor 1 survive when there are more coordinates? Traces have weight 0, so add a coordinate t of weight 0, and with it one relation of weight 0. Let $P, R \in \mathbb{Z}_p[u, t]$ with $P(0, 0) \neq 0$ and $R(0, 0) = 0$, and let

$$B := \mathbb{Z}_p[y, z, t]/\big(yP(yz, t),\ R(yz, t)\big), \qquad S := \mathbb{Z}_p[u, t]/(P, R),$$

graded as before with t of weight 0. Now x is the point $y = z = t = 0$, with ideal $I_x = (y, z, t)$, and S is the cuspidal quotient of B_0.

Problem 33.5.1. $B_0 = \mathbb{Z}_p[u, t]/\big(uP, R\big)$ with $u = yz$, and $(I_x/I_x^2)_{-1} \cong \mathbb{Z}_p/P(0, 0)\mathbb{Z}_p$. For $R = t$, B is the model A with $P(u, 0)$ in place of P, provided $P(u, 0)$ has leading coefficient in $\mathbb{Z}_p^\times$.

Problem 33.5.2. Let $a \in (u, t) \subseteq \mathbb{Z}_p[u, t]$. Then $\operatorname{length}(I_x/I_x^2)_{-1} \leq \operatorname{length} S/aS$. If S is free of finite rank over $\mathbb{Z}_p$ and a is nonzero at every point ξ of $\operatorname{Spec} S$ over $\overline{\mathbb{Q}}_p$, then $\operatorname{length}(I_x/I_x^2)_{-1} \leq \sum_\xi v(\xi(a))$, where ξ is counted with multiplicity the length of the localization of $S \otimes \overline{\mathbb{Q}}_p$ at ξ; equivalently, the $\xi(a)$ are the eigenvalues of multiplication by a on $S \otimes \overline{\mathbb{Q}}_p$.

So the factor 1 survives whenever the cuspidal quotient is finite and free. When S is finite over $\mathbb{Z}_p$ but has torsion, and a is nonzero at every ξ, length S/aS exceeds $\sum_\xi v(\xi(a))$ by length $S[a]$, and a bound by the values $\xi(a)$ alone must be obtained otherwise.

The factor two is harmless in the argument: in [Adr, §17.4] it yields a nonzero integer N such that, for every ℓ, a sum of lengths of Tate–Shafarevich groups at ℓ is at most $2v_\ell(N)$, and only $\sum_\ell 2v_\ell(N)\log\ell = 2\log|N|$ is used. We do not know whether the factor two in (G2) can be replaced by 1 in general.

Hints

§33.1.

33.1.1: Cayley–Hamilton: $\rho(g) + \det\rho(g)\,\rho(g)^{-1} = \operatorname{tr}\rho(g)$.
33.1.2: Take $h = g$, then $h = 1$.
33.1.3: Problem 33.1.2.
33.1.4: Subtract the scalar $1+\chi(g)$ from $\mathcal{T}(g)$. Then Problems 33.1.2, 33.1.1 and 33.1.3.
33.1.5: Use the eigenbasis E_{12}, Δ, Problem 32.1.1, and $\tau(2) = -24$.

§33.2.

33.2.1: Hensel's lemma.
33.2.2: Compute $\operatorname{tr}(\rho(\sigma_0)\rho(g))$.
33.2.3: Reduce modulo $\mathfrak{m}$ and use $T(\sigma_0 g) \equiv \chi_1(\sigma_0 g) + \chi_2(\sigma_0 g)$.
33.2.4: Express $T(\sigma_0 g^2)$ by the defining identity with $(g, g\sigma_0)$, and $T(g^2)$ by Problem 33.1.2.
33.2.5: Problems 33.2.3 and 33.2.4.
33.2.6: Problem 33.1.2, and the polynomial of Problem 33.2.1 modulo J.
33.2.7: First, the reduction of a stable lattice has semisimplification $1\oplus\bar\chi$: its trace is $1+\bar\chi$, its determinant is $\bar\chi$ by Problem 33.1.2, and Brauer–Nesbitt applies. The roots of Problem 33.2.1 and the function a may be computed in each factor. Use Problem 33.2.2 in the second factor, and note that $\mathbf{T}_e$ projects onto the second factor.
33.2.8: One inequality is Problem 32.4.7. For the other, apply Problem 33.2.6 with J the ideal generated by the $a_\ell(f) - 1 - \ell^{k-1}$, and Chebotarev.

§33.3.

33.3.1: Modulo I the matrix is upper triangular; multiply two of them.
33.3.2: Evaluate at σ_0.
33.3.3: Run Problem 32.3.3 modulo I, as in Problem 32.4.7; $(\mathcal{O}/I)(1-k)$ has no invariants under I_p. Then Problem 30.1.1.

§33.4.

33.4.1: The monomials of weight 0, +1 and −1 are u^j, zu^j and yu^j. For the cotangent module, keep the linear term of the relation.
33.4.2: The torus acts by $(y,z) \mapsto (t^{-1}y, tz)$.
33.4.3: Elementary divisors: the length is the valuation of the determinant of multiplication by a. Compute that determinant over $\overline{\mathbb{Q}}_p$.
33.4.4: Problem 33.4.3.

§33.5.

33.5.1: As in Problem 33.4.1; the monomials of weight 0 and -1 are the monomials in u, t and y times them. Since $R(0,0) = 0$, $y\,R(yz,t) \in I_x^2$.

33.5.2: As in Problems 33.4.3 and 33.4.4, with $S/(u,t)S$.

References

[Adr] J. Adriazola, *The Alpöge proof of the Riemann hypothesis*, manuscript, revised 24 November 2026, `https://github.com/jimjamzola/RH-Alpoge-Reconstruction`.

[ANT] P. B. Allen, J. Newton and J. A. Thorne, *Automorphy lifting for residually reducible l-adic Galois representations, II*, Compos. Math. **156** (2020), 2399–2422.

[BC] J. Bellaïche and G. Chenevier, *Families of Galois representations and Selmer groups*, Astérisque **324** (2009).

[Ch] G. Chenevier, *The p-adic analytic space of pseudocharacters of a profinite group and pseudorepresentations over arbitrary rings*, in: Automorphic Forms and Galois Representations, Vol. 1, London Math. Soc. Lecture Note Ser. 414, Cambridge Univ. Press, 2014, 221–285; `https://arxiv.org/abs/0809.0415`.

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), 179–330.

[Ro] R. Rouquier, *Caractérisation des caractères et pseudo-caractères*, J. Algebra **180** (1996), 571–586.

[Ta] R. Taylor, *Galois representations associated to Siegel modular forms of low weight*, Duke Math. J. **63** (1991), 281–332.