Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 65 (2019)
Heft: 3-4

Artikel: A note on Galois representations with big image
Autor: Katz, Nicholas M.
DOI: https://doi.org/10.5169/seals-869351

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 16.10.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

L'Enseignement Mathématique (2) 65 (2019), 271–301 DOI 10.4171/LEM/65-3/4-1

A note on Galois representations with big image

Nicholas M. Katz

Abstract. Given an integer $N \geq 3$, we will first construct motivic representations (i.e., built out of pieces of the cohomology of projective smooth varieties, in fact curves)

$$\rho : Gal\big(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_N)\big) \to GL(n, \mathbb{Q}_\ell)$$

with open image, for any ℓ which is 1 mod N and for certain n. We will do this in three different ways. The third of them has a descent to $\mathbb{Q}$ when N is 3 or 4. This provides us with motivic Galois representations of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ with open image in $GL(n, \mathbb{Q}_\ell)$ for any even $n \geq 6$ and any ℓ which is $\equiv 1$ mod 3 or mod 4.

Mathematics Subject Classification (2010). Primary: 11R32, 11T24, 34M35.

Keywords. Monodromy, Galois representation.

Contents

1 The case $N \geq 3$ 276
2 An alternate approach to the case $N \geq 3, N \neq 4$ 281
3 Yet another variant, for $N \geq 3$ 282
4 Working over $\mathbb{Q}$, when $N = 3$ and $\ell \equiv 1$ mod 3 287
5 Working over $\mathbb{Q}$, when $N = 4$ and $\ell \equiv 1$ mod 4 289
6 Independence of ℓ 291
7 Examples in higher dimension 292
8 Explicit one parameter families in higher dimension 294
9 Some open questions 297
References 298

Historical overview

We begin with a projective smooth curve $\mathcal{C}/\mathbb{Z}[1/N]$ with geometrically connected fibres, of genus ≥ 1. For example, we might take $\mathcal{C}$ to be the

hyperelliptic curve (whose affine points, in addition to which there is one point at ∞, are) defined by the equation

$$Y^2 = h(X)$$

with $h(X) \in \mathbb{Z}[X]$ a monic polynomial of degree $2g+1$ whose discriminant $\Delta \in \mathbb{Z}$ is nonzero. This is such a $\mathcal{C}$ over $\mathbb{Z}[1/(2\Delta)]$. By the end of the 1940's, Weil had proven the "Riemann Hypothesis" for curves over finite fields. This is the statement that for any prime p not dividing N, when we count the $\mathbb{F}_p$-points on the curve and define the integer a_p by

$$\#\mathcal{C}(\mathbb{F}_p) = p + 1 - a_p,$$

then we have the estimate

$$|a_p| \leq 2g\sqrt{p}.$$

More generally, for $\mathbb{F}_q/\mathbb{F}_p$ a finite extension, and a_q defined by

$$\#\mathcal{C}(\mathbb{F}_q) = q + 1 - a_q,$$

then we have the estimate

$$|a_q| \leq 2g\sqrt{q}.$$

One of Weil's proofs goes via the Jacobian $\mathcal{J}_p$ of $\mathcal{C}_p := \mathcal{C} \otimes_{\mathbb{Z}[1/N]} \mathbb{F}_p$. For a given p not dividing N, choose a prime $\ell \neq p$ and consider (what came to be called) the Tate module $T_\ell(\mathcal{J}_p)$, formed out of the points of ℓ power order on $\mathcal{J}_p(\overline{\mathbb{F}_p})$. This is a free $\mathbb{Z}_\ell$-module of rank $2g$ on which the arithmetic Frobenius $Frob_p$ $(x \mapsto x^p)$ acts. The connection to the a_p is given by the identities in $\mathbb{Z}_\ell$

$$\mathrm{Trace}\big(Frob_p | T_\ell(\mathcal{J}_p)\big) = a_p, \mathrm{Trace}\big(Frob_p^n | T_\ell(\mathcal{J}_p)\big) = a_{p^n} \text{ for all } n \geq 1.$$

These identities imply that the reversed characteristic polynomial $\det(1 - X Frob_p | T_\ell(\mathcal{J}_p))$ lies in $\mathbb{Z}[X]$, and is independent of the auxiliary choice of $\ell \neq p$. The Riemann Hypothesis then becomes the statement that when we factor this $\mathbb{Z}$-polynomial over $\mathbb{C}$, say

$$\det\big(1 - X Frob_p | T_\ell(\mathcal{J}_p)\big) = \prod_{i=1}^{2g} (1 - \alpha_i X),$$

then each α_i has

$$|\alpha_i| = \sqrt{p}.$$

By 1957, Taniyama [Tan] knew that if we look instead at the Jacobian $\mathcal{J}_{\overline{\mathbb{Q}}}$ of $\mathcal{C}_{\overline{\mathbb{Q}}} := \mathcal{C} \otimes_{\mathbb{Z}[1/N]} \overline{\mathbb{Q}}$, and view $T_\ell(\mathcal{J}_{\overline{\mathbb{Q}}})$ as a representation of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, then this representation is unramified outside $N\ell$, so defines a representation of (what came

to be called) the fundamental group $\pi_1(Spec(\mathbb{Z}[1/N\ell]))$. Moreover, he knew that for p not dividing $N\ell$, the action of the arithmetic Frobenius conjugacy class $Frob_{p,arith}$ in this π_1 is related to the situation in characteristic p by

$$\det\big(1 - X Frob_{p,arith} | T_\ell(\mathcal{J}_{\overline{\mathbb{Q}}})\big) = \det\big(1 - X Frob_p | T_\ell(\mathcal{J}_p)\big).$$

Thus was born the notion of a compatible system of ℓ-adic representations. In the same paper, Taniyama also initiates the study of abelian ℓ-adic representations, a theme later taken up by Serre [Ser5].

By the mid-1960's, Grothendieck and his school had developed ℓ-adic cohomology (see [KS, 9.0, 9.1] for a quick review). One of its consequences is this. For a projective smooth $X/\mathbb{Z}[1/N]$ with geometrically connected fibres of dimension d, and a prime ℓ, we have ℓ-adic representations $H^i(X, \mathbb{Q}_\ell)$ of $\pi_1(Spec(\mathbb{Z}[1/N\ell]))$. These $H^i(X, \mathbb{Q}_\ell)$ vanish for $i > 2d$, and their dimensions are the usual Betti numbers of the complex variety $X_{\mathbb{C}}$. For each prime p not dividing $N\ell$, we have

$$\#X(\mathbb{F}_p) = \sum_i (-1)^i \mathrm{Trace}\big(Frob_{p,geom} | H^i(X, \mathbb{Q}_\ell)\big),$$

$$\#X(\mathbb{F}_{p^n}) = \sum_i (-1)^i \mathrm{Trace}\big(Frob_{p,geom}^n | H^i(X, \mathbb{Q}_\ell)\big) \text{ for all } n \geq 1,$$

with $Frob_{p,geom}$ the inverse of $Frob_{p,arith}$. In 1973, Deligne proved that the individual traces $\mathrm{Trace}(Frob_{p,geom}^n | H^i(X, \mathbb{Q}_\ell))$ are integers independent of the auxiliary choice of $\ell \neq p$, and that the eigenvalues of $Frob_{p,geom} | H^i(X, \mathbb{Q}_\ell)$ all have complex absolute value $\sqrt{p}$.

To my knowledge, it is Serre who first considers the question of determining the image of these ℓ-adic representations, cf. [Ser1] and [Ser5, Chapter 4, 2.2]. Consider an elliptic curve E, whose H^1 is the dual of its $T_\ell \otimes \mathbb{Q}_\ell$. Serre proves that if $E_{\mathbb{C}}$ does not have complex multiplication, then for every ℓ, the image is an open subgroup of $\mathrm{GL}(2, \mathbb{Q}_\ell)$. In [Ser3] he proves that with finitely many exceptions, the image is the largest possible, $GL(2, \mathbb{Z}_\ell)$.

One key application of knowing the Galois image for non-CM elliptic curves is to clarify the Sato-Tate conjecture in this case (see [Tat, top of p. 107] for the first written mention of this conjecture, and see [Nam] for the history, in Japanese, of its 1963 discovery by Sato), and act as a harbinger of a conceptual understanding of what the conjecture says in general (cf. [Ser7, p. 6]). In the elliptic curve case, if instead of looking at the reversed characteristic polynomials

$$\det\big(1 - X Frob_{p,arith} | T_\ell(E_{\overline{\mathbb{Q}}})\big)$$

we "unitarize" them, and look at

$$\det\big(1 - X Frob_{p,arith}/\sqrt{p} | T_\ell(E_{\overline{\mathbb{Q}}})\big)$$

then these are characteristic polynomials of elements of the compact group SU(2), and as such determine conjugacy classes in that group. Equivalently, the space of conjugacy classes in SU(2) may be seen as the closed interval $[-2,2]$, by the map

$$\mathrm{Trace} : \mathrm{SU}(2) \to [-2,2].$$

Then each p not dividing N gives us an integer a_p with $|a_p| \leq 2\sqrt{p}$, and we view the real number

$$a_p/\sqrt{p} \in [-2,2]$$

as being a conjugacy class in SU(2). Via the isomorphism

$$2\cos : [0,\pi] \cong [-2,2]$$

we view $[0,\pi]$ as the space of conjugacy classes. In this "angle" picture, the conjugacy class attached to p is the unique angle $\theta_p \in [0,\pi]$ such that

$$a_p = 2\sqrt{p}\cos(\theta_p).$$

The Sato–Tate conjecture then asserts that these conjugacy classes $\{\theta_p\}_{p\nmid N}$ are equidistributed in the space of conjugacy classes of $SU(2)$ for its "Haar measure", which, in the $[0,\pi]$ picture, is the measure

$$(2/\pi)\sin^2(\theta)d\theta.$$

Let us return to the case of a projective smooth $X/\mathbb{Z}[1/N]$ with geometrically connected fibres. Then each H^i is selfdual, with a duality pairing

$$H^i(X,\mathbb{Q}_\ell) \times H^i(X,\mathbb{Q}_\ell) \to \mathbb{Q}_\ell(-i),$$

where $\mathbb{Q}_\ell(-i)$ is the one-dimensional representation on which $Frob_{p,geom}$ acts as p^i. This pairing is alternating when i is odd, and symmetric when i is even.

In the case when i is even, we can replace $H^i(X,\mathbb{Q}_\ell)$ by its Tate twist $H^i(X,\mathbb{Q}_\ell)(i/2)$. This space is orthogonally self dual in the usual sense, and so for $H^i(X,\mathbb{Q}_\ell)(i/2)$ the image of the ℓ-adic representation lies in the orthogonal group $O(h^i,\mathbb{Q}_\ell)$, with $h^i := \dim H^i$. If we combine the result of Beauville [Beau, Section 2, Thm. 2] with the trick of Terasoma [Ter, Thm. 2] we find that, for each ℓ, there exist smooth surfaces $X \subset \mathbb{P}^3$ over $\mathbb{Q}$ of any fixed degree $d \geq 4$ for which the ℓ-adic image on the quotient $Prim^2(X,\mathbb{Q}_\ell) := H^2(X,\mathbb{Q}_\ell)(1)/($ the hyperplane class $L)$ is open in $O(h^2-1,\mathbb{Q}_\ell)$ (and Zariski dense in $O(h^2-1)$).

When i is odd, no such Tate twisting trick is available, and the image for H^i lies in the group of symplectic similitudes $GSp(H^i,\mathbb{Q}_\ell)$. [In the case of the two-dimensional H^1 of an elliptic curve, this group of symplectic similitudes is

just $\mathrm{GL}(2, \mathbb{Q}_\ell)$.] In contrast to the even dimensional case, where we know the existence of $X/\mathbb{Q}$ with suitable open image but do *not* know how to write down particular examples, Serre's theorem gives us open image for *every* $E/\mathbb{Q}$ without complex multiplication. In higher genus, we have Zarhin's result, who has shown that for hyperelliptic curves over $\mathbb{Q}$ (or indeed over any field K which is finitely generated over $\mathbb{Q}$) of the form $Y^2 = h(X)$, with h a polynomial of degree $n = 2g+1$ or $2g+2$, various explicit conditions on n and on the Galois group of h over K guarantee that the ℓ-adic representation on H^1 has image which is open in the group of symplectic similitudes $GSp(2g, \mathbb{Q}_\ell)$. For example, if h has degree $n \geq 5$ and has Galois group over $\mathbb{Q}$ either S_n or A_n, then this holds, cf. [Zar1]. See the papers [Zar2, Zar3, Zar4] for more such spectacular results.

We cannot hope to attain an open subgroup of $\mathrm{GL}(n, \mathbb{Q}_\ell)$ for $n \geq 3$ just from looking at the cohomology of projective smooth varieties. What we can hope to do is find a suitable X and an automorphism ϕ of finite order of X, such that when we break its H^i into eigenspaces for the induced action of ϕ, then for a well chosen i and a well chosen eigenspace, the ℓ-adic image of the representation on this piece of this H^i will be an open subgroup of $\mathrm{GL}(n, \mathbb{Q}_\ell)$ for n the dimension of this piece. This is the theme we will pursue here.

Introduction

Given an integer $N \geq 3$, we will first construct motivic representations (i.e., built out of pieces of the cohomology of projective smooth varieties, in fact curves)

$$\rho : Gal\big(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_N)\big) \to GL(n, \mathbb{Q}_\ell)$$

with open image, for any ℓ which is 1 mod N and for certain n. We will do this in three different ways. The third of them has a descent to $\mathbb{Q}$ when N is 3 or 4. This provides us with motivic Galois representations of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ with open image in $GL(n, \mathbb{Q}_\ell)$ for any even $n \geq 6$ and any ℓ which is $\equiv 1$ mod 3 or mod 4.

The underlying idea in all the cases considered is this. First, we find families of (projective, smooth, geometrically connected) curves over open sets of $\mathbb{P}^1$ over suitable rings of S-integers together with an action of a finite cyclic group G such that suitable G-isotypical components of the H^1 along the fibres have complex monodromy groups which are Zariski dense in $SL(n, \mathbb{C})$ (for n the rank of the isotypical component in question). The Zariski density is proven by specializing into finite characteristic, where on the one hand old results of the author (especially [Kat3] and [Kat4]) give such Zariski density results for the geometric monodromy groups in characteristic p, and where on the other hand

a fundamental semicontinuity theorem of Pink, [Kat3, 8.18.2] or [Kat7, 2.1], tells us that knowing this Zariski density in any single characteristic p forces its truth in characteristic zero. The second step is to apply a form of Hilbert irreducibility, along the lines of Serre [Ser6, Theorem, p. 149] or Terasoma [Ter, Thm. 2]. This shows the existences of infinitely many rational points in the parameter space such the isotypical component of the H^1 at that rational point is a Galois representation with the desired large image. We should point out that our method does *not* give explicit rational points with this property.

The descents from $\mathbb{Q}(\zeta_N)$ to $\mathbb{Q}$ in the cases $N = 3$ and $N = 4$ are in some sense tricks. They make explicit use of well-chosen elements of $PGL(2, \mathbb{Q})$ of orders 3 and 4 respectively, namely $W \mapsto \frac{1}{1-W}$ and $W \mapsto \frac{W-1}{W+1}$. We do not understand the general setting, if there is one, to which these tricks should belong. With the exception of these tricks, whose "discovery" we stumbled up in 2001, there is virtually nothing in this article that could not have been written 25 years ago.

The problem of constructing Galois representations with large image has also been considered by Upton [Upt] in the case GL_3, by Greenberg [Gre] for GL_n, and by Cornut–Ray [CR] for more general groups. The construction of Upton is motivic, those of Greenberg and Cornut-Ray are spectacularly non-motivic (in the sense of making no appeal or reference to cohomology). Motivic Galois representations with images which are Zariski dense in exceptional groups have been constructed by Dettweiler–Reiter [DR3] (for G_2, by local system methods), by Yun [Yun] (for G_2, E_7, E_8, by automorphic methods), and by Boxer–Celegari-Emerton–Levin–Madapusi Pera–Patrikis [BCE+] (for E_6, also by automorphic methods).

It is a pleasure to thank Peter Sarnak and Laurent Clozel, who awakened in 2001, respectively reawakened in 2016, my interest in this question.

1. The case $N \geq 3$

In this section, we fix an integer $N \geq 3$, an integer $n \geq 5$ such that $n+1$ is nonzero mod N, a prime number ℓ which is 1 mod N, and an embedding of $\mathbb{Q}(\zeta_N)$ into $\mathbb{Q}_\ell$. We also fix a monic polynomial

$$f = f_{n+1}(X) \in \mathbb{Z}[X]$$

of degree $n+1$, which, over $\mathbb{C}$, is a *Morse polynomial*, meaning that the derivative $f'(X)$ has n distinct zeroes, say $\alpha_1, \ldots, \alpha_n$, and f separates these zeroes:

$$f(\alpha_i) \neq f(\alpha_j) \text{ if } i \neq j.$$

The values $f(\alpha_i)$ are called the critical values of f. The critical values are integral over $\mathbb{Z}[1/(n+1)]$. We define a polynomial $F_{crit.val.}(T) \in \mathbb{Z}[1/(n+1)][T]$ by

$$F_{crit.val.}(T) := \prod_{roots\ \alpha_i\ of\ f'} \big(T - f(\alpha_i)\big)$$

and denote by

$$\Delta_{Morse}(f) := \text{Discriminant } (F_{crit.val.}).$$

For any $t \in \mathbb{C}$ which is not a critical value of f, the polynomial $t - f(X)$ has all distinct roots. For any prime p which is prime to $n+1$ and to the numerator of $\Delta_{Morse}(f)$, the coefficient-wise reduction mod p of f is a Morse polynomial in characteristic p.

For example, the polynomial $X^{n+1} - (n+1)X$ is a Morse polynomial. The zeroes of its derivative are the n'th roots of unity. Its critical values are $\{-n\zeta\}_{\zeta \in \mu_n}$, and $F_{crit.val.}(T) = T^n - (-n)^n$. Its reduction mod any prime p not dividing $n(n+1)$ is a Morse polynomial in characteristic p.

Over the parameter space

$$S := Spec\big(\mathbb{Z}[\zeta_N, 1/N, 1/(n+1), 1/\Delta_{Morse}(f)][T][1/F_{crit.val.}(T)]\big)$$

we have the one parameter family of curves $\pi : \mathcal{C} \to S$ given by

$$\mathcal{C} : Y^N = T - f(X).$$

The group $\mu_N := \mu_N(\mathbb{Z}[\zeta_N, 1/N])$ acts on this family, by $(X, Y) \mapsto (X, \zeta Y)$. The sheaf $\mathcal{F}_{\ell,f} := R^1\pi_!\mathbb{Q}_\ell$ is lisse on $S[1/\ell]$, and carries the action of μ_N. For a character χ of μ_N of full order N, the χ-isotypical component $\mathcal{F}_{\ell,f,\chi}$ of $\mathcal{F}_{\ell,f}$ is lisse on $S[1/\ell]$ of rank n and pure of weight one. [It is to insure the purity that we need $n+1$ to be nonzero mod N, otherwise the rank of $\mathcal{F}_{\ell,f,\chi}$ remains n but its quotient of (highest) weight one has rank $n-1$, cf. [Kat4, 5.16 and 5.18].] We denote by

$$\rho_{\ell,f,\chi} : \pi_1(S[1/\ell]) \to GL(n, \mathbb{Q}_\ell)$$

the ℓ-adic representation which "is" $\mathcal{F}_{\ell,f,\chi}$.

Theorem 1.1. *The image of $\pi_1(S[1/\ell])$ in $GL(n, \mathbb{Q}_\ell)$ is open. Moreover, if we embed $\mathbb{Z}[\zeta_N]$ into $\mathbb{C}$, the image of*

$$\pi_1^{geom}(S[1/\ell]) := \pi_1(S \otimes_{\mathbb{Z}[\zeta_N]} \mathbb{C})$$

contains an open subgroup of $SL(n, \mathbb{Q}_\ell)$.

Proof. It suffices to prove the "moreover", as the determinant, being pure of weight $n \neq 0$, certainly has open image in $\mathbb{Z}_\ell^\times$. Let us denote by Γ the image of $\pi_1^{geom}(S[1/\ell])$ in $GL(n, \mathbb{Q}_\ell)$. Fix a prime p not dividing either $n+1$ or the numerator of $\Delta_{Morse}(f)$, and a p-adic place of $\mathbb{Z}[\zeta_N, 1/N]$ with residue field some $\mathbb{F}_q$ with $q \equiv 1 \bmod N$. We denote by $\Gamma(p)$ the image of $\pi_1^{geom}(S[1/\ell] \otimes \mathbb{F}_q)$ in $GL(n, \mathbb{Q}_\ell)$. By Pink's specialization theorem, cf. [Kat3, 8.18.2] or [Kat7, 2.1], Γ contains (a conjugate of) $\Gamma(p)$. So it suffices to show that $\Gamma(p)$ contains an open subgroup of $SL(n, \mathbb{Q}_\ell)$. For this, we argue as follows. It is proven in [Kat4, 5.13] that the Zariski closure $G_{geom,p}$ of $\Gamma(p)$ sits in

$$SL(n) \subset G_{geom,p} \subset GL(n)$$

and has determinant of finite order. Let us denote by

$$\Gamma(p)_1 \subset \Gamma(p)$$

the subgroup of elements of determinant one. This is a subgroup of finite index, so its Zariski closure contains the identity component $G^0_{geom,p} = SL(n)$. Hence $\Gamma(p)_1$ is Zariski dense in $SL(n)$. We then conclude by the following well-known lemma, cf. [Ser2, Cor, p. 120], which we record for ease of reference.

Lemma 1.2. *Over $\mathbb{Q}_\ell$, let $G \subset SL(n)$ be an irreducible connected (and hence semisimple) algebraic group. Suppose $\Gamma \subset G(\mathbb{Q}_\ell)$ is a closed subgroup which is Zariski dense in G. Then Γ contains an open subgroup of $G(\mathbb{Q}_\ell)$.*

Proof. The group Γ is an ℓ-adic Lie group. Every open subgroup Γ_1 of Γ is also Zariski dense in G (because G is connected, and replacing Γ by Γ_1 does not change the identity component of the Zariski closure). Its Lie algebra $\mathrm{Lie}(\Gamma) = \mathrm{Lie}(\Gamma_1)$ is reductive, because Γ_1 has, via G, an irreducible representation, cf. [Bou, p. 78, Prop. 5, a $\Longleftrightarrow$ e]. Because this irreducible representation has trivial determinant, $\mathrm{Lie}(\Gamma)$ has no nonzero abelian factor. Thus $\mathrm{Lie}(\Gamma)$ is semisimple. One knows [Bor, 7.9] that a semisimple Lie algebra is algebraic. Visibly we have the inclusion $\mathrm{Lie}(\Gamma) \subset \mathrm{Lie}(G)$. Thus $\mathrm{Lie}(\Gamma)$ is $\mathrm{Lie}(H)$ for some connected semisimple group $H \subset G$, and for a small enough Γ_1, Γ_1 is open in $H(\mathbb{Q}_\ell)$ (because they have the same Lie algebra) and hence is Zariski dense in H. Therefore $H = G$. □

This concludes the proof of the theorem. □

Remark 1.3. In fact, for any ℓ which is $1 \bmod N$, the image of $\rho_{\ell,f,\chi}$ contains $SL(n, \mathbb{Z}_\ell)$ (via some $\mathbb{Z}_\ell$-lattice in $\mathcal{F}_{\ell,f,\chi}$). [See [HL] for another approach to this sort of question.] To see this, we use the theory of middle convolution

with mod ℓ coefficients (written in a different language by Dettweiler–Reiter in [DR1] and [DR2], and also by Stambach–Vöklein in [SV]), applied in any good characteristic p. The sheaf $\mathcal{F}_{\ell,f,\chi}$ is the middle additive convolution

$$\mathcal{L}_\chi \star_{mid,+} (f_\star \mathbb{Q}_\ell/\mathbb{Q}_\ell).$$

Its reduction mod ℓ is the middle additive convolution

$$\mathcal{L}_\chi \star_{mid,+} (f_\star \mathbb{F}_\ell/\mathbb{F}_\ell).$$

Because f is Morse, the second factor is irreducible, tame at ∞, and all of its local monodromies at finite distance are reflections, cf. [Kat5, 3.3.6]. Therefore the middle convolution is irreducible, tame at ∞, and all of its local monodromies at finite distance are pseudoreflections with determinant $\chi\chi_{quad}$, which is always of order ≥ 3 because $N \geq 3$. Thus the mod ℓ image of $\Gamma(p)$ is an irreducible subgroup of $GL(n, \mathbb{F}_\ell)$ which is generated by pseudoreflections of order ≥ 3. By a theorem of Wagner [Wag, Thm. 1.2 and following paragraph], an irreducible subgroup of $GL(n, \mathbb{F}_\ell)$ generated by pseudoreflections of order ≥ 3 necessarily contains $SL(n, \mathbb{F}_\ell)$ provided that $n \geq 5$.

The inverse image, call it $\Gamma(p)_1$, in $\Gamma(p)$ of $SL(n, \mathbb{F}_\ell)$ lies in $SL(n, \mathbb{Z}_\ell)$ (because the determinants of elements of $\Gamma(p)$ are roots of unity of order dividing $\ell-1$). Then $\Gamma(p)_1$ is a closed subgroup of $SL(n, \mathbb{Z}_\ell)$ which maps onto $SL(n, \mathbb{F}_\ell)$. One knows [Ser5, Exc. 1, p. IV-27] that if $n \geq 2$ and $\ell \geq 5$, the only closed subgroup of $SL(n, \mathbb{Z}_\ell)$ which maps onto $SL(n, \mathbb{F}_\ell)$ is $SL(n, \mathbb{Z}_\ell)$ itself. Thus $\Gamma(p)_1$ is $SL(n, \mathbb{Z}_\ell)$. Hence $\Gamma(p)$ contains $SL(n, \mathbb{Z}_\ell)$. As Γ contains $\Gamma(p)$, we are done.

Here is another approach to this question, which gives the result for all but a finite set of ℓ which are 1 mod N and does not use the theory of mod ℓ middle convolution. Over the Riemann surface $S^{an} := (S \otimes_{\mathbb{Z}[\zeta_N]} \mathbb{C})^{an}$, with

$$K := \mathbb{Q}(\zeta_n)$$

we have the K-local system

$$\mathcal{F}_{K,f} := R(\pi^{an})_! K$$

and its χ component $\mathcal{F}_{K,f,\chi}$. We know that each of its local monodromies at finite distance is a pseudoreflection of known order ≥ 3, and that (correctly chosen conjugates of each of) these elements generate the entire image of $\pi_1(S^{an})$ in $GL(n, K)$. So if we invert some highly divisible integer M, we can find an $\mathcal{O}_K[1/M]$-lattice $\mathcal{F}_{\mathcal{O}_K[1/M],f,\chi}$ in $\mathcal{F}_{K,f,\chi}$ whose monodromy representation lands in $GL(n, \mathcal{O}_K[1/M])$. Because our K-representation was absolutely irreducible, the entire matrix ring $Mat_n(K)$ is spanned over K by the the image of the

K-groupring of $\pi_1(S^{an})$. At the expense of increasing M, we may assume that $Mat_n(\mathcal{O}_K[1/M]))$ is spanned by the image of the $\mathcal{O}_K[1/M]$-groupring. Once we are in this situation, then the reduction mod any prime $\mathcal{P}$ of $\mathcal{O}_K[1/M]$ of this $\mathcal{O}_K[1/M]$-form of our monodromy representation will be absolutely irreducible. Take a $\mathcal{P}$ whose residue field is a prime field $\mathbb{F}_\ell$ and at which the completion of K is $\mathbb{Q}_\ell$. We apply Wagner's theorem to conclude that the monodromy representation of $\mathcal{F}_{\mathcal{O}_K[1/M],f,\chi} \otimes \mathbb{Z}_\ell$ on S^{an} has image containing $SL(n, \mathbb{Z}_\ell)$. On the scheme

$$S_{\mathbb{C}} := S \otimes_{\mathbb{Z}[\zeta_N]} \mathbb{C},$$

we have our $\mathbb{Q}_\ell$ local system $\mathcal{F}_{\ell,\chi}$, which is the "partner" (in the sense of [AGV, XI, 4.4] via [AGV, XVI, 4.1]) of the transcendental local system $\mathcal{F}_{\mathcal{O}_K[1/M],f,\chi} \otimes \mathbb{Q}_\ell$ on S^{an}. So the image of the monodromy representation of $\mathcal{F}_{\ell,\chi}$ on the scheme $S_{\mathbb{C}}$ contains $SL(n, \mathbb{Z}_\ell)$.

Remark 1.4. The description of the local system $\mathcal{F}_{\ell,f,\chi}$ as the middle additive convolution

$$\mathcal{L}_\chi \star_{mid,+} (f_\star \mathbb{Q}_\ell / \mathbb{Q}_\ell)$$

tells us what its local monodromies are in terms of those of $f_\star \mathbb{Q}_\ell / \mathbb{Q}_\ell$, cf. [Kat5, 3.3.6]. According to [Kat5, 3.3.3, 3)], this local system will be rigid if and only if $f_\star \mathbb{Q}_\ell / \mathbb{Q}_\ell$ is rigid. But only for a Morse polynomial f of degree ≤ 3 will $f_\star \mathbb{Q}_\ell / \mathbb{Q}_\ell$ be rigid. This lack of rigidity means that we can't have an a priori description, in terms of local monodromies alone, of the local system on S^{an} which is its "partner".

Corollary 1.5. *There exist infinitely many $t \in \mathbb{Q}(\zeta_N)$ with $F_{crit.val.}(t) \neq 0$ for which the representation of $Gal(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_N)$ given by specializing T to t (i.e., by composing the maps*

$$Gal\big(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_N)\big) = \pi_1(Spec\big(\mathbb{Q}(\zeta_N)\big) \to \pi_1(S \otimes_{\mathbb{Z}} \mathbb{Q}) \to \pi_1(S[1/\ell]) \to GL(n, \mathbb{Q}_\ell),$$

the last map being the representation $\rho_{\ell,f,\chi}$) has open image, indeed the same open image as the representation $\rho_{\ell,f,\chi}$.

Proof. This follows from Theorem 1.1 by the form of Hilbert Irreducibility given in [Ter, Thm. 2] or in [Ser6, Theorem, p. 149]. □

Remark 1.6. When we specialize T to $t \in \mathbb{Q}(\zeta_N)$, the ℓ-adic representation we get is the χ-component of

$$H^1_c(\mathcal{C}_t \otimes \overline{\mathbb{Q}}, \mathbb{Q}_\ell)$$

for $\mathcal{C}_t$ the curve

$$\mathcal{C}_t : Y^N = t - f(X)$$

over $\mathbb{Q}(\zeta_N)$. It would be interesting to exhibit specific values of t for which the image is open.

2. An alternate approach to the case $N \geq 3, N \neq 4$

Fix an integer $n \geq 1$ such that $n+1$ is nonzero mod N. Fix $f = f_n(X) \in \mathbb{Z}[X]$ a monic polynomial of degree n whose discriminant $\Delta(f_n)$ is nonzero. [For example, we might take $\prod_{i=1}^{n}(X-i)$, whose discriminant is nonzero mod every prime $p \geq n$.] Over the parameter space

$$S := Spec\big(\mathbb{Z}[\zeta_N, 1/N][T][1/f_n(T)][1/\Delta(f_n)]\big)$$

we have the family of affine curves

$$\pi : \mathcal{C} \to S$$

of equation

$$\mathcal{C} : Y^N = f_n(X)(T-X).$$

The group $\mu_N(\mathbb{Q}(\zeta_N))$ has an obvious action on this family, namely $(x, y) \mapsto (x, \zeta y)$. For any ℓ, the relevant H^1 along the fibres,

$$\mathcal{F}_\ell := R^1\pi_!(\mathbb{Q}_\ell),$$

is lisse on $S[1/\ell]$, and carries an action of $\mu_N(\mathbb{Q}(\zeta_N))$.

Suppose now that ℓ is 1 mod N. Then we can choose an embedding of $\mathbb{Q}(\zeta_N)$ into $\mathbb{Q}_\ell$, and diagonalize the action. For a character χ of $\mu_N(\mathbb{Q}(\zeta_N))$ of full order N, the χ isotypical component $\mathcal{F}_{\ell,\chi}$ of $\mathcal{F}_\ell$ is lisse of rank n and pure of weight one.

Theorem 2.1. *Fix an integer $n \geq 5$ such that $n+1$ is nonzero mod N. Suppose that ℓ is 1 mod N. Let χ be a character of order N. Then the local system $\mathcal{F}_{\ell,\chi}$ on $S[1/\ell]$, viewed as a representation*

$$\rho_\chi : \pi_1(S[1/\ell]) \to GL(n, \mathbb{Q}_\ell)$$

has open image. Moreover, after extension of scalars from $\mathbb{Q}(\zeta_N)$ to $\mathbb{C}$ (e.g., by mapping ζ_N to $\exp(2\pi i/N)$), the image of $\pi_1^{geom}(S[1/\ell]) := \pi_1(S \otimes_{(\mathbb{Z}[\zeta_N,1/N]} \mathbb{C})$ contains an open subgroup of $SL(n, \mathbb{Q}_\ell)$, and for all but at most finitely many ℓ the image contains $SL(n, \mathbb{Z}_\ell)$.

Proof. The overall structure of the proof is the same as that of Theorem 1.1. It suffices to prove the "moreover" statement, and for this it is enough to

specialize to a good characteristic $p \neq \ell$ (one not dividing $\Delta(f_n)$) and a residue field $\mathbb{F}_q$ at a p-adic place of $\mathbb{Q}(\zeta_N)$. Then our local system, pulled back to $Spec(\mathbb{F}_q[T][1/f_n(T)]$, is tame at ∞ (as it comes from characteristic zero, cf. [Kat1, 4.7.1]). Its trace function is as follows: for $k/\mathbb{F}_q$ a finite extension, and χ extended to $k^\times$ by composition with the norm,

$$\mathrm{Trace}(Frob_{t,k}|\mathcal{F}_{\ell,\chi}) = -\sum_{x\in k} \chi\big(f_n(x)(t-x)\big).$$

This is the trace function of the middle additive convolution [Kat5]

$$\mathcal{L}_\chi \star_{mid,+} \mathcal{L}_{\chi(f_n(x))}.$$

Thus our local system is geometrically irreducible [Kat5, 2.9.6 and 2.9.8], and its local monodromies at finite distance (i.e., at the zeroes of $f_n(t)$) are all pseudoreflections of determinant χ^2, cf. [Kat5, 3.3.6]. Because $N \geq 3$ but $N \neq 4$, χ^2 has order ≥ 3. It then follows from [Kat4, 5.11] that in our chosen characteristic p, the image $\Gamma(p)$ of $\pi_1^{geom}(S \otimes \mathbb{F}_q)$ has Zariski closure $G_{geom,p}$ with $G^0_{geom,p} = SL(n)$. Exactly as in the proof of Theorem 1.1, we infer that $\Gamma(p)$ contains an open subgroup of $SL(n,\mathbb{Q}_\ell)$. To show that, for all but at most finitely many ℓ, it contains all of $SL(n,\mathbb{Z}_\ell)$ for a suitable $\mathbb{Z}_\ell$-lattice in $\mathcal{F}_{\ell,\chi}$, we repeat that Wagner argument of Remark 1.3. □

Remark 2.2. On $S^{an}_{\mathbb{C}}$, the ("partner" of the) χ component

$$\mathcal{L}_\chi \star_{mid,+} \mathcal{L}_{\chi(f_n(x))}$$

of the local system $\mathcal{F}_{\mathbb{C}} := R^1\pi_!^{an}\mathbb{C}$ is rigid (by [Kat5, 3.3.3, 3)]. It is the sheaf of germs of local holomorphic solutions of a Pochhammer hypergeometric equation, cf. [DM, bottom of p. 6] and [Poc, pp. 322–325]. This situation is in stark contrast with that of Remark 1.4, where we in general lack such rigidity.

Remark 2.3. Exactly as in the previous section, Hilbert Irreducibility ensures that there are infinitely many $t \in \mathbb{Q}(\zeta_N)$ with $f_n(t) \neq 0$ for which the ℓ-adic representation given by the χ component of the H^1_c of the curve

$$Y^N = f_n(X)(t-X)$$

over $\mathbb{Q}(\zeta_N)$ has open image in $GL(n,\mathbb{Q}_\ell)$.

3. Yet another variant, for $N \geq 3$

In this section, we fix an integer $N \geq 3$, a nonzero element $A \in \mathbb{Z}[\zeta_N]$, an integer $n \geq 2$, a prime number ℓ which is $1 \bmod N$, an embedding of $\mathbb{Q}(\zeta_N)$

into $\mathbb{Q}_\ell$, and a monic polynomial $f = f_n(X) \in \mathbb{Z}[\zeta_N][X]$ of degree n which, over $\mathbb{C}$ (by any choice of embedding) is a Morse polynomial. For any $t \in \mathbb{C}$ which is not a critical value of either f or of $f + A$, the rational function

$$\frac{t - f(X) - A}{t - f(X)}$$

has n simple zeroes and n simple poles at finite distance, no other zeroes or poles, and takes the value 1 at ∞. We denote by

$$F := F_{crit.val.}(T)$$

the monic polynomial whose roots are the $n-1$ distinct critical values of f. We make the additional hypothesis

(CritDiff$_\mathrm{A}$) The polynomial $F(T)F(T-A)$ has $2n-2$ i.e., all distinct, roots.

Equivalently, the condition on f is that A is not the difference of two distinct critical values of f. We denote by $\Delta_{crit,A} \in \mathbb{Z}[\zeta_N, 1/(2n)]$ the discriminant of $F(T)F(T-A)$.

Notice that if f is a Morse polynomial satisfying (CritDiff$_\mathrm{A}$), then for any constant $a \in \mathbb{Z}[\zeta_N]$, the polynomial $f(X) + a$ is also a Morse polynomial satisfying (CritDiff$_\mathrm{A}$).

Here is an example, to show that for any $A \neq 0$, we can find a Morse $f = f_n$ which satisfies (CritDiff$_\mathrm{A}$). For an integer $M \neq 0$, consider the polynomial

$$X^n - nM^{n-1}X.$$

Its critical values are $\{M^n(1-n)\zeta\}_{\zeta \in \mu_{n-1}}$. Using the archimedean inequality

$$|e^{i\alpha} - 1| \geq 2\alpha/\pi \text{ for } 0 \leq \alpha \leq \pi,$$

we see that for every complex embedding of $\mathbb{Q}(\zeta_{n-1})$, and any two distinct $n-1$ roots of unity ζ and ζ', we have

$$|(n-1)(\zeta - \zeta')| \geq 4.$$

So taking M large enough that $4M^n$ exceeds every archimedean absolute value of A provides a suitable f_n.

More generally, if $f = f_n$ is a Morse polynomial, then for any integer M, the polynomial $M^n f(X/M)$ has critical values M^n times those of f (and critical points M times those of f). So if we take M sufficiently large, $M^n f(X/M)$ will satisfy (CritDiff$_\mathrm{A}$).

Fix now a Morse function f and an $A \neq 0$ in $\mathbb{Z}[\zeta_N]$, such that (CritDiff$_\mathrm{A}$) holds for f. Over the parameter space

$$S := Spec\Big(\mathbb{Z}[\zeta_N, 1/N, 1/(2n), 1/A, 1/\Delta_{crit,A}][T]\big[1/\big(F(T)F(T-A)\big)\big]\Big)$$

we have the complete nonsingular model (add N sections along ∞)

$$\pi : \overline{\mathcal{C}} \to S$$

of the family of smooth affine curves

$$\mathcal{C} : y^N = \frac{T - f(X) - A}{T - f(X)}.$$

The sheaf $\mathcal{F}_\ell := R^1\pi_!\mathbb{Q}_\ell$ is lisse on $S[1/\ell]$ of rank $(N-1)(2n-2)$ and pure of weight one. For any character χ of μ_N of full order N, the χ component $\mathcal{F}_\ell^\chi$ is lisse of rank $2n-2$ and pure of weight one. [In fact, this is true for every nontrivial χ of order dividing N.]

We denote by

$$\rho_{\ell,f,A,\chi} : \pi_1(S[1/\ell]) \to GL(2n-2, \mathbb{Q}_\ell)$$

the ℓ-adic representation which "is" $\mathcal{F}_{\ell,\chi}$.

Theorem 3.1. *Suppose we are in one of the two following situations.*

(1) $n \geq 4$, f *satisfies* (CritDiff$_\mathrm{A}$) *and is of the form* $X^n - M^{n-1}nX + a$ *for some* $a \in \mathbb{Z}[\zeta_N]$.

(2) $n \geq 6$, f *satisfies* (CritDiff$_\mathrm{A}$) *and is of the form* $M^n h(X/M) + a$ *for some* $a \in \mathbb{Z}[\zeta_N]$ *and some monic* $h = h_n \in \mathbb{Z}[X]$ *whose derivative* h' *has Galois group over* $\mathbb{Q}$ *the full symmetric group* S_{n-1}.

Then the image of $\pi_1(S[1/\ell])$ *in* $GL(2n-2, \mathbb{Q}_\ell)$ *is open. Moreover, if we embed* $\mathbb{Z}[\zeta_N]$ *into* $\mathbb{C}$, *the image of*

$$\pi_1^{geom}(S[1/\ell]) := \pi_1(S \otimes_{\mathbb{Z}[\zeta_N]} \mathbb{C})$$

contains an open subgroup of $SL(2n-2, \mathbb{Q}_\ell)$.

Proof. Exactly as in the proof of Theorem 1.1, it suffices to prove the "moreover". And for this it suffices to pass to an $\mathbb{F}_q$-valued point of $\mathbb{Z}[\zeta_N, 1/N, 1/(2n), 1/\Delta_{crit,A}, 1/\ell]$, and show that over $S \otimes \mathbb{F}_q$ the image of $\pi_1^{geom}(S \otimes \mathbb{F}_q)$ contains an open subgroup of $SL(2n-2, \mathbb{Q}_\ell)$. We will choose such a point whose characteristic p is sufficiently large so that, in case (1), [Kat3, 7.10.5] applies, and in case (2) [Kat3, 7.10.6] applies. What this choice of p ensures is that in our characteristic p situation, when we consider the Fourier Transform

$$FT(f_\star\mathbb{Q}_\ell/\mathbb{Q}_\ell)$$

its geometric monodromy group G_{geom} sits in

$$Sp(n-1) \subset G_{geom} \subset \mu_p Sp(n-1), \text{ in case (1), } n \text{ odd,}$$
$$SL(n-1) \subset G_{geom} \subset \pm 1\mu_p SL(n-1), \text{ in case (1), } n \text{ even,}$$
$$SL(n-1) \subset G_{geom} \subset \pm 1\mu_p SL(n-1), \text{ in case (2), any } n.$$

[The references cited apply to an f to which a suitable constant has been added. The effect of such an addition is to perform an additive translation on $f_\star \mathbb{Q}_\ell/\mathbb{Q}_\ell$, which in turn has the effect of tensoring its Fourier Transform by a character of order p, hence the μ_p factor in the above statement.]

Using Lemma 1.2, it suffices to show that $G^0_{geom} = SL(2n-2)$ in this characteristic p situation.

Henceforth we work in characteristic p. The trace function of our sheaf $\mathcal{F}_{\ell,\chi}$ at points t of a finite field extension $k/\mathbb{F}_q$ with $F(t)F(t-A) \neq 0$ is the character sum

$$-1 - \sum_{x \in k} (\chi \circ \mathrm{Norm}_{k/\mathbb{F}_q}) \left(\frac{t - f(x) - A}{t - f(x)} \right),$$

with the usual convention that $\chi(0) = \chi(\infty) = 0$.

Write

$$\frac{t - f(x) - A}{t - f(x)} = 1 - \frac{A}{t - f(x)}.$$

Then we see that this character sum is the additive convolution

$$-\sum_{u \in k} (\chi \circ \mathrm{Norm}_{k/\mathbb{F}_q})\big(1 - A/(t-u)\big)\big(\#\{x \in k \,|\, f(x) = u\} - 1\big).$$

of the trace functions of $\mathcal{L}_\chi(1 - A/x)$ and $f_\star \mathbb{Q}_\ell/\mathbb{Q}_\ell$. In other words, $\mathcal{F}_{\ell,\chi}$ has the same trace function on $S \otimes \mathbb{F}_q$ as the ! additive convolution

$$\mathcal{L}_\chi(1 - A/x) \star_{!,+} f_\star \mathbb{Q}_\ell/\mathbb{Q}_\ell.$$

Let us admit for a moment the following key lemma.

Lemma 3.2. *The canonical surjection of perverse sheaves is an isomorphism*

$$\mathcal{L}_\chi(1 - A/x) \star_{!,+} f_\star \mathbb{Q}_\ell/\mathbb{Q}_\ell \cong \mathcal{L}_\chi(1 - A/x) \star_{mid,+} f_\star \mathbb{Q}_\ell/\mathbb{Q}_\ell.$$

This middle convolution is geometrically irreducible, and all its monodromies at finite distance are pseudoreflections of determinant $\chi\chi_{quad}$.

Then $\mathcal{F}_{\ell,\chi}$ has the same trace function on $S \otimes \mathbb{F}_q$ as the geometrically, and hence arithmetically, irreducible perverse middle convolution above. By Chebotarev, it follows that $\mathcal{F}_{\ell,\chi}$ is isomorphic to this middle convolution. Thus

$\mathcal{F}_{\ell,\chi}$ is lisse on $S \otimes \mathbb{F}_q$ of rank $2n-2 \geq 6$, geometrically irreducible, with all finite monodromies pseudoreflections of order ≥ 3. That $\mathcal{F}_{\ell,\chi}$ is tame at ∞ results from its "coming from characteristic zero", cf. [Kat1, 4.7.1 (i)]. The result then follows from [Kat4, 5.11]. □

It remains to give the proof of the key lemma.

Proof. To show that the ! convolution is equal to the middle convolution, it is equivalent to show that its Fourier Transform FT is a middle extension, and that its Fourier Transform is geometrically irreducible. Now FT turns ! convolution into $\otimes$, so the FT of the ! convolution is

$$FT\big(\mathcal{L}_\chi(1-A/x)\big) \otimes FT(f_\star \mathbb{Q}_\ell/\mathbb{Q}_\ell).$$

Both factors are lisse on $\mathbb{G}_m$. At 0, the first factor has unipotent local monodromy $Unip(2)$, cf. [Kat3, 7.12, SL-Example(3)], and the second factor has local monodromy $\oplus_{\chi:\chi^n=\mathbb{1},\chi\neq\mathbb{1}}\mathcal{L}_\chi$, cf. [Kat3, 7.10.4 (1)], so their tensor product correctly vanishes at 0.

It remains to show that this tensor product is geometrically irreducible. The first factor, being pure, has G_{geom} a (not necessarily connected) semisimple subgroup of $GL(2)$. So its identity component is either trivial or $SL(2)$. It is not trivial, because it contains $Unip(2)$.

As recalled above, by [Kat3, 7.10.5 and 7.10.6], the second factor has G^0_{geom} either $SL(n-1)$ or, if n is odd, possibly $Sp(n-1)$. As $n \geq 4$ in all cases, its Lie algebra is a simple Lie algebra which is not that of $SL(2)$. So by the Goursat–Kolchin–Ribet theorem [Kat3, 1.8.2], the direct sum object

$$FT\big(\mathcal{L}_\chi(1-A/x)\big) \oplus FT(f_\star \mathbb{Q}_\ell/\mathbb{Q}_\ell)$$

has

$$G^0_{geom} = SL(2) \times \big(\text{either } SL(n-1) \text{ or, if } n \text{ is odd, possibly } Sp(n-1)\big).$$

Consequently, the tensor product is irreducible.

That its local monodromies at finite distance are pseudoreflections of determinant $\chi\chi_{quad}$ is proven in [Kat6, 6.1.18].

This concludes the proof of the key lemma, and with it the proof of the theorem. □

Remark 3.3. Exactly as in the previous sections, Hilbert Irreducibility ensures that there are infinitely many $t \in \mathbb{Q}(\zeta_N)$ with $F(t)F(t-A) \neq 0$ for which the ℓ-adic representation given by the χ component of the H^1_c of the complete nonsingular model (add μ_N at ∞) of the curve

$$y^N = \frac{t-f(X)-A}{t-f(X)}$$

over $\mathbb{Q}(\zeta_N)$ has open image in $GL(2n-2, \mathbb{Q}_\ell)$.

4. Working over $\mathbb{Q}$, when $N = 3$ and $\ell \equiv 1 \bmod 3$

Consider the automorphism of the rational function field $\mathbb{Q}(W)$ given by the fractional linear transformation

$$\sigma : W \mapsto \frac{1}{1-W}.$$

One checks easily that σ^3 is the identity. We define the trace rational function

$$S(W) := W + \sigma(W) + \sigma^2(W) = W + \frac{1}{1-W} + 1 - \frac{1}{W} = \frac{W^3 - 3W + 1}{W(W-1)},$$

which is, of course, σ-invariant.

On the other hand, after we extend scalars to $\mathbb{Q}(\zeta)(W)$, for $\zeta = \zeta_3$ a primitive cube root of unity, the rational function

$$R(W) := \frac{W + \zeta^2}{W + \zeta}$$

is easily checked to satisfy

$$\sigma\big(R(W)\big) = \zeta R(W),$$

and hence $R(W)^3$ is σ-invariant.

We have the following miraculous identity, whose verification is left to the reader.

$$R(W)^3 := \left(\frac{W + \zeta^2}{W + \zeta}\right)^3 = \frac{S(W) + 3\zeta^2}{S(W) + 3\zeta}.$$

With these preliminaries out of the way, we fix an integer $n \geq 4$, an integer $M \geq 2$, and take

$$f(X) := X^n - nM^{n-1}X.$$

Consider the one parameter family of curves in (X, W) space over $\mathbb{Q}(T)$

$$T - f(X) = S(W).$$

This family has an automorphism of order three, which we will denote σ, given by

$$(X, W) \mapsto \big(X, \sigma(W)\big) = \big(X, 1/(1-W)\big).$$

If we extend scalars to $\mathbb{Q}(\zeta)(T)$, we can write this curve as

$$\frac{T - f(X) + 3\zeta^2}{T - f(X) + 3\zeta} = \left(\frac{W + \zeta^2}{W + \zeta}\right)^3.$$

Now define

$$Y := \frac{W + \zeta^2}{W + \zeta}.$$

Then in (X, Y) space, we have the curve

$$Y^3 = \frac{T - f(X) + 3\zeta^2}{T - f(X) + 3\zeta} = 1 - \frac{3\zeta - 3\zeta^2}{T - f(X) + 3\zeta},$$

on which the automorphism of order three has become the obvious automorphism $(X, Y) \mapsto (X, \zeta Y)$.

For $F(T) := F_{crit.val.}(T)$ the critical value polynomial for $f(X) - 3\zeta_3$, and for $A := 3\zeta - 3\zeta^2$, we saw in Section 3 that this last family has a projective smooth model over

$$S := Spec\Big(\mathbb{Z}[\zeta_3, 1/3, 1/(2n), 1/A, 1/\Delta_{crit,A}][T]\big[1/\big(F(T)F(T-A)\big)\big]\Big).$$

So if we replace each of the quantities

$$1/A, 1/\Delta_{crit,A}, \big(F(T)F(T-A)\big)$$

by its Norm from $\mathbb{Q}(\zeta)$ down to Q, we find that our family

$$T - f(X) = S(W)$$

has a projective smooth model

$$\pi : \mathcal{C} \to S_0$$

over S_0, the *Spec* of the ring

$$\mathbb{Z}\big[1/3, 1/(2n), 1/\mathrm{Norm}(A), 1/\mathrm{Norm}(\Delta_{crit,A})\big][T]\big[1/\mathrm{Norm}\big(F(T)F(T-A)\big)\big].$$

For any ℓ, we have the lisse $\mathbb{Q}_\ell$ sheaf $\mathcal{F}_\ell := R^1\pi_!\mathbb{Q}_\ell$ on $S_0[1/\ell]$. When $\ell \equiv 1$ mod 3, and χ is a character of full order three, we can extract the χ-component $\mathcal{F}_{\ell,\chi}$, which is lisse of rank $2n-2$ and pure of weight one. View it as an ℓ-adic representation

$$\rho_{f,\sigma} : \pi_1(S_0[1/\ell]) \to GL(2n-2, \mathbb{Q}_\ell).$$

Theorem 4.1. *The image of $\pi_1(S_0[1/\ell])$ in $GL(2n-2, \mathbb{Q}_\ell)$ is open. Moreover the image of*

$$\pi_1^{geom}(S_0[1/\ell]) := \pi_1(S_0 \otimes_{\mathbb{Z}} \mathbb{C})$$

contains an open subgroup of $SL(2n-2, \mathbb{Q}_\ell)$.

Proof. As always, the key statement is the "moreover". But $S_0 \otimes_{\mathbb{Z}} \mathbb{C}$ with its $\mathcal{F}_{\ell,\chi}$ is just the same as the $S \otimes_{\mathbb{Z}[\zeta_3]} \mathbb{C}$ with its $\mathcal{F}_{\ell,\chi}$ in Theorem 3.1, applied with $f(X) - 3\zeta$. □

Remark 4.2. Exactly as in the previous sections, Hilbert Irreducibility ensures that there are infinitely many $t \in \mathbb{Q}$ with $\mathrm{Norm}(F(t)F(t) - A)) \neq 0$ for which the ℓ-adic representation given by the χ component of the H^1 of the complete nonsingular model of the curve

$$t - f(X) = S(W)$$

over $\mathbb{Q}$ has open image in $GL(2n-2, \mathbb{Q}_\ell)$.

5. Working over $\mathbb{Q}$, when $N = 4$ and $\ell \equiv 1 \bmod 4$

This section is almost identical in idea and structure to the previous section, so we simply explain the relevant miraculous identity and leave the rest to the reader.

We have the automorphism of the rational function field $\mathbb{Q}(W)$ given by the fractional linear transformation

$$\sigma : W \mapsto \frac{W-1}{W+1}.$$

The trace rational function

$$S(W) := W + \sigma(W) + \sigma^2(W) + \sigma^3(W) = \frac{W^4 - 6W^2 + 1}{X(X^2-1)}$$

is σ-invariant. After extending scalars from $\mathbb{Q}(W)$ to $\mathbb{Q}(i)(W)$, i being a primitive fourth root of unity, the quantity

$$R(W) := \frac{W+i}{W-i}$$

transforms under σ by

$$\sigma\big(R(W)\big) = iR(W).$$

The miraculous identity is

$$R(W)^4 := \left(\frac{W+i}{W-i}\right)^4 = \frac{S(W)+4i}{S(W)-4i}.$$

With these preliminaries out of the way, we fix an integer $n \geq 4$, an integer $M \geq 2$, and take

$$f(X) := X^n - nM^{n-1}X.$$

Consider the one parameter family of curves in (X, W) space over $\mathbb{Q}(T)$

$$T - f(X) = S(W).$$

This family has an automorphism of order four, which we will denote σ if no confusion can occur, given by

$$(X, W) \mapsto \big(X, \sigma(W)\big) = \big(X, (W-1)/(W+1)\big).$$

If we extend scalars to $\mathbb{Q}(i)(T)$, we can write our curve as

$$\frac{T - f(X) + 4i}{T - f(X) - 4i} = \left(\frac{W+i}{W-i}\right)^4.$$

Now define

$$Y := \frac{W+i}{W-i}.$$

Then in (X, Y) space, we have the curve

$$Y^4 = \frac{T - f(X) + 4i}{T - f(X) - 4i} = 1 - \frac{-8i}{T - f(X) - 4i},$$

on which the automorphism of order four has become the obvious automorphism $(X, Y) \mapsto (X, iY)$.

So if we replace each of the quantities

$$1/A, 1/\Delta_{crit,A}, \big(F(T)F(T-A)\big)$$

by its Norm from $\mathbb{Q}(i)$ down to Q, we find that our family

$$T - f(X) = S(W)$$

has a projective smooth model

$$\pi : \mathcal{C} \to S_0$$

over S_0, the *Spec* of the ring

$$\mathbb{Z}\big[1/(2n), 1/\mathrm{Norm}(A), 1/\mathrm{Norm}(\Delta_{crit,A})\big][T]\big[1/\mathrm{Norm}\big(F(T)F(T-A)\big)\big].$$

For any ℓ, we have the lisse $\mathbb{Q}_\ell$ sheaf $\mathcal{F}_\ell := R^1\pi_!\mathbb{Q}_\ell$ on $S_0[1/\ell]$. When $\ell \equiv 1$ mod 4, and χ is a character of full order four, we can extract the χ-component $\mathcal{F}_{\ell,\chi}$, which is lisse of rank $2n-2$ and pure of weight one. View it as an ℓ-adic representation

$$\rho_{f,\sigma} : \pi_1\big(S_0[1\ell]\big) \to GL(2n-2, \mathbb{Q}_\ell).$$

Theorem 5.1. *The image of $\pi_1(S_0[1/\ell])$ in $GL(2n-2, \mathbb{Q}_\ell)$ is open. Moreover the image of*

$$\pi_1^{geom}\big(S_0[1/\ell]\big) := \pi_1(S_0 \otimes_{\mathbb{Z}} \mathbb{C})$$

contains an open subgroup of $SL(2n-2, \mathbb{Q}_\ell)$.

Proof. As always, the key statement is the "moreover". But $S_0 \otimes_{\mathbb{Z}} \mathbb{C}$ with its $\mathcal{F}_{\ell,\chi}$ is just the same as the $S \otimes_{\mathbb{Z}[\zeta_3]} \mathbb{C}$ with its $\mathcal{F}_{\ell,\chi}$ in Theorem 3.1, applied with $f(X) + 4i$. □

Remark 5.2. Exactly as in the previous sections, Hilbert Irreducibility ensures that there are infinitely many $t \in \mathbb{Q}$ with $\mathrm{Norm}(F(t)F(t) - A)) \neq 0$ for which the ℓ-adic representation given by the χ component of the H^1 of the complete nonsingular model of the curve

$$t - f(X) = S(W)$$

over $\mathbb{Q}$ has open image in $GL(2n-2, \mathbb{Q}_\ell)$.

6. Independence of ℓ

In each of the previous sections, we began with a cyclotomic field $K := \mathbb{Q}(\zeta_N)$, $N \geq 3$, a number field E, a proper smooth one-parameter family

$$\pi : \mathcal{C} \to S$$

of curves over a dense open set S of $Spec(\mathcal{O}_E[T])$, a character χ of either $\mathbb{Z}/N\mathbb{Z}$ or of $\mu_N(\mathbb{Q}(\zeta_N))$ with values in $\mu_N(\mathbb{Q}(\zeta_N))$ of full order N, and an action of either $\mathbb{Z}/N\mathbb{Z}$ or of $\mu_N(\mathbb{Q}(\zeta_N))$ on the family.

Over $\mathbb{C}$, $\mathcal{F}^{an} := R^1(\pi^{an})_! K$ is a K-local system on S^{an} whose χ component $(\mathcal{F}^{an})^\chi$, under the action of either $\mathbb{Z}/N\mathbb{Z}$ or of $\mu_N(\mathbb{Q}(\zeta_N))$, has rank

$$d := \mathrm{rank}(\mathcal{F}^{an})^\chi.$$

For each finite place λ of K, with completion K_λ, we have the K_λ-local system $R^1\pi_! K_\lambda$ on $S[1/\ell]$, whose χ component has the same rank d. For each $t \in S(E)$, the χ-component $H^1(\mathcal{C}_t \otimes_E \overline{E}, K_\lambda)^\chi$ is a representation of $Gal(\overline{E}/E)$, and for variable λ these form a compatible system of λ-adic representations

$$\rho_{\lambda,t} : Gal(\overline{E}/E) \to GL(d, K_\lambda).$$

For each λ, we denote by $G_{\lambda,t}$ the algebraic group over K_λ which is the Zariski closure in $GL(d)$ of the image of $\rho_{\lambda,t}$.

When we fix a place λ of K of residue characteristic $\ell \equiv 1 \bmod N$, then K_λ is $\mathbb{Q}_\ell$. For a fixed such λ, we showed the existence of infinitely many $t \in E$ for which the image of $\rho_{\lambda,t}$ is open in $GL(d, \mathbb{Q}_\ell)$.

Theorem 6.1. *Suppose that λ_1 is a place of K of residue characteristic $\ell_1 \equiv 1$ mod N, and $t \in S(E)$ is such that the image of $\rho_{\lambda_1,t}$ is open in $GL(d, \mathbb{Q}_{\ell_1})$. Then for every place λ_2 of residue characteristic $\ell_2 \equiv 1$ mod N, the image of $\rho_{\lambda_2,t}$ is open in $GL(d, \mathbb{Q}_{\ell_2})$.*

Proof. For any such λ_2 of K, $H^1(\mathcal{C}_t \otimes_E \overline{E}, \mathbb{Q}_{\ell_2})^\chi$ is a direct factor of $H^1(\mathcal{C}_t \otimes_E \overline{E}, \mathbb{Q}_{\ell_2})$. By Faltings[Fal, &5, Satz 4], $\rho_{\lambda_2,t}$ is completely reducible, and hence $G_{\lambda_2,t}$ is reductive . Denote by $\Gamma_{\lambda_2,t}$ the image of $\rho_{\lambda_2,t}$. By Bogomolov [Bog, Thm. 1], $\Gamma_{\lambda_2,t}$ is open in $G_{\lambda_2,t}(\mathbb{Q}_{\lambda_2})$. So it suffices to show that $G_{\lambda_2,t}$ is $GL(d)$. According to Hui [Hui, 3.22 and 3.19], the rank of the derived group $(G^0_{\lambda,t})^{der}$ is independent of the auxiliary choice of λ. For λ_1, we know that $G_{\lambda_1,t} = GL(d)$, so its derived group is $SL(d)$, of rank $d-1$. Therefore $(G^0_{\lambda_2,t})^{der}$ is a connected semisimple subgroup of $SL(d)$ of rank $d-1$. The only such subgroup is $SL(d)$ itself. The determinant of $\rho_{\lambda_2,t}$ is of infinite order, being pure of weight $d \neq 0$. Therefore $G_{\lambda_2,t}$ must be $GL(d)$. □

Remark 6.2. See [HL, Thm. 1] and [CHT, Thm. 1.2] for other results, in slightly different contexts, of the same type.

7. Examples in higher dimension

In this section, we give examples built with higher dimensional varieties. For given integers $n \geq 2$ and $d \geq 3$, and k a field in which d is invertible, a polynomial $f(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ is a "strong Deligne polynomial" if it satisfies the following two conditions.

(1) The affine hypersurface of equation $f = 0$ in $\mathbb{A}^n$ is smooth of dimension $n-1$.

(2) Write f as the sum of homogeneous forms $f = f_d + f_{d-1} + \ldots + f_0$. The projective hypersurface of equation $f_d = 0$ in $\mathbb{P}^{n-1}$ is smooth of dimension $n-2$.

Here is another way to think of these conditions. Pass to the homogeneous form

$$F(X_1, \ldots, X_n, Z) \in k[X_1, \ldots, X_n, Z] := f_d + Zf_{d-1} + Z^2 f_{d-2} + \ldots + Z^d f_0.$$

The conditions on F are that $F = 0$ defines a smooth hypersurface H_F of dimension $n-1$ in $\mathbb{P}^n$ and that the intersection $H_F \cap (Z = 0)$ defines a smooth hypersurface of dimension $n-2$ in $\mathbb{P}^{n-2}$.

This point of view makes clear that in the affine space Poly(n, d) over $\mathbb{Z}[1/d]$ of all degree d polynomials in n variables (the coefficients being the coordinate functions), the special Deligne polynomials form a dense (over any field k in which d is invertible, the polynomial $f := 1 + \sum_{i=1}^n X_i^d$ is a strong Deligne polynomial) open set $SD(n, d)$.

Now fix an integer $N \geq 3$, and write $K := \mathbb{Q}(\zeta_N)$. Over the parameter space

$$S := SD(n, d) \otimes_{\mathbb{Z}[1/d]} \mathcal{O}_K[1/N, 1/d]$$

of strong Deligne polynomials f, we have the family $\pi : \mathcal{H} \to S$ of smooth affine hypersurfaces of dimension n of equation

$$Y^N = f(X_1, \ldots, X_N)$$

and the obvious action on it of the group $\mu_N(K)$. We fix a character χ of $\mu_N(K)$ of full order N.

Theorem 7.1. *Suppose $n \geq 2$, $d \geq 3$, $N \geq 3$, and d is nonzero mod N (i.e., $\chi^d \neq \mathbb{1}$). For each finite place λ of K, denote by ℓ its residue characteristic. Then we have the following results.*

(1) *The sheaves $(R^i \pi_! K_\lambda)^\chi$ on $S[1/\ell]$ vanish for $i \neq n$.*

(2) *The sheaf $\mathcal{F}_{\lambda,\chi} := (R^n \pi_! K_\lambda)^\chi$ on $S[1/\ell]$ is pure of weight n and lisse of rank $(d-1)^n$. Its trace function is given by*

$$\mathrm{Trace}(Frob_{k,f} | \mathcal{F}_{\lambda,\chi}) = (-1)^n \sum_{x \in k^n} \chi_k\big(f(x)\big).$$

(3) *Over any field k in which $d\ell$ is invertible, the geometric monodromy group of $\mathcal{F}_{\lambda,\chi} | S \otimes k$ contains $SL((d-1)^n)$.*

Proof. This is proven in [Kat6, 5.1.9, 5.1.14, and 5.2.2 1)]. □

Exactly as in the first section, we get the following corollary.

Corollary 7.2. *Under the hypotheses of the theorem, for any λ of residue characteristic $\ell \equiv 1$ mod N, the image of the representation*

$$\rho_{\lambda,\chi} : \pi_1(S[1/\ell]) \to GL\big((d-1)^n, \mathbb{Q}_\ell\big)$$

which "is" the sheaf $\mathcal{F}_{\lambda,\chi}$ is open in $GL\big((d-1)^n, \mathbb{Q}_\ell\big)$.

Because the parameter space S is rational, Hilbert irreducibility and the independence of ℓ results give us

Theorem 7.3. *Fix a place λ_1 of residue characteristic $\ell_1 \equiv 1$ mod N. There exist infinitely many strong Deligne polynomials $f \in K[X_1, \ldots, X_n]$ of degree d for which the action of $Gal(\overline{K}/K)$ on*

$$H_c^n\Big(\big(Y^N = f(x)\big) \otimes_K \overline{K}, K_{\lambda_1} = \mathbb{Q}_{\ell_1}\Big)^\chi$$

has open image in $GL((d-1)^n, K_{\lambda_1}) = GL((d-1)^n, \mathbb{Q}_{\ell_1})$. Moreover, given such an f, then for any other place λ_2 of residue characteristic $\ell_2 \equiv 1$ mod N, the action of $Gal(\overline{K}/K)$ on

$$H_c^n\Big(\big(Y^N = f(x)\big) \otimes_K \overline{K}, K_{\lambda_2} = \mathbb{Q}_{\ell_2}\Big)^\chi$$

has open image in $GL((d-1)^n, K_{\lambda_2}) = GL((d-1)^n, \mathbb{Q}_{\ell_2})$.

8. Explicit one parameter families in higher dimension

Thus far, we have worked over the *entire* parameter space of *all* strong Deligne polynomials of given degree d in a given number $n \geq 2$ of variables. Over a field in which d is invertible, suppose we have a polynomial $f(X) := f(X_1, \ldots, X_n)$ of degree d whose leading form f_d defines a smooth hypersurface in $\mathbb{P}^{n-1}$ (a "Deligne polynomial") and which has only finitely many critical points (points where all the $\partial f / \partial f X_i$ vanish). For any t which is not a critical value (the value of f at a critical point), $t - f(X)$ is a strong Deligne polynomial.

As before, we put $K := \mathbb{Q}(\zeta_N)$, $N \geq 3$. Fix a degree $d \geq 3$ which is nonzero mod N, and a number $n \geq 2$ of variables. Given a Deligne polynomial $f \in \mathcal{O}_K[X_1, \ldots, X_n]$ of degree d, with only finitely many critical points (in $\mathbb{C}^n$), denote by

$$F_{crit}(T) \in \mathcal{O}_K[T]$$

a choice of (not necessarily monic) polynomial whose roots are the distinct critical values of f, and by

$$\Delta_{crit} \in \mathcal{O}_K$$

its discriminant. We will exhibit such an f such that for any χ of full order N, the local system whose trace function is given by the one parameter ("t" the parameter) family of character sums

$$(-1)^n \sum_{x \in k^n} \chi\big(t - f(x)\big)$$

is lisse of rank $(d-1)^n$, pure of weight n, and its G_{geom} contains $SL((d-1)^n)$.

More precisely, over

$$S := Spec\big(\mathcal{O}_K[1/d, 1/\Delta_{crit}, 1/N, T][1/F_{crit}(T)]\big),$$

we have $\pi : \mathcal{H} \to S$, the family of varieties of equation

$$Y^N = t - f(X_1, \ldots, X_n).$$

The $(R^i \pi_! K_\lambda)^\chi$ will vanish for $i \neq n$, and

$$\mathcal{F}_{\lambda.\chi} := (R^n \pi_! K_\lambda)^\chi$$

will be lisse of rank $(d-1)^n$, pure of weight n, and its G_{geom} will contain $SL((d-1)^n)$.

Once we have such an f, then there are infinitely many $t \in K$ such that for every place λ_i of K with residue characteristic $\ell_i \equiv 1 \bmod N$, the action of $Gal(\overline{K}/K)$ on

$$H_c^n\Big(\big(Y^N = t - f(X)\big) \otimes_K \overline{K}, K_{\lambda_i} = \mathbb{Q}_{\ell_i}\Big)^\chi$$

has open image in $GL((d-1)^n, K_{\lambda_i}) = GL((d-1)^n, \mathbb{Q}_{\ell_i})$.

Here is our $f(X_1, \ldots, X_n)$, for given n and d. It is a variation on the idea behind [Kat6, 6.7]. Define

$$g(X) := X^d - dX,$$

Choose a prime p which is $1 \bmod d-1$ and take

$$f(X_1, \ldots, X_n) := \sum_{i=1}^n p^i g(X_i).$$

The critical points of this f are the points $(a_1, \ldots, a_n)$ where each a_i is a $d-1$ root of unity. The critical values are the sums

$$\sum_{i=1}^n p^i g(a_i) = \sum_{i=1}^n p^i (1-d) a_i.$$

We first show that these $(d-1)^n$ sums are all distinct. Because $p \equiv 1 \bmod d-1$, the a_i are Teichmüller points in $\mathbb{Z}_p$. After dividing by $1-d$, we are looking at the expression of $(d-1)^n$ distinct elements of $\mathbb{Z}_p$ expanded in the base p, using 0 and Teichmüller points as "digits".

The vanishing of the $(R^i \pi_! K_\lambda)^\chi$ on $S[1/\ell]$ for $i \neq n$ results by proper base change from the universal assertion (1) of Theorem 7.1, as does the fact that our $\mathcal{F}_{\lambda,\chi}$ on $S[1/\ell]$ is lisse of rank $(d-1)^n$ and pure of weight n. What must be proven is that its G_{geom} contains $SL((d-1)^n)$.

For $i = 1, \ldots, n$, and fixed λ, define

$$L_i := \big((p^i g)_\star \mathbb{Q}_\ell / \mathbb{Q}_\ell\big) \otimes K_\lambda.$$

Exactly as in [Kat6, 6.7.9–11], the purity of our $\mathcal{F}_{\lambda,\chi}$ shows that is the iterated middle convolution of the Kummer sheaf $\mathcal{L}_\chi$ with the L_i:

$$\mathcal{F}_{\lambda,\chi} \cong \mathcal{L}_\chi \star_{mid,+} L_1 \star_{mid,+} L_2 \ldots \star_{mid,+} L_n.$$

This sheaf is tame at ∞, lisse outside the $(d-1)^n$ critical values, and at each critical value its local monodromy is a pseudoreflection of determinant $\chi\chi_{quad}^n$.

There is a further property, nonpunctuality, our argument requires of the multiple middle convolution $L_1 \star_{mid,+} L_2 \ldots \star_{mid,+} L_n$, namely that it is the direct sum of irreducible middle extension sheaves. To see that this holds, we work successively from the right. Applying [Kat6, 6.1.12] successively, it suffices to verify that for each $m = 1, \ldots, n-1$,

$$(**) \qquad \text{all ratios} \quad \frac{\sum_{i=1}^{m} p^i(a_i - b_i)}{a_0 - b_0} \neq 1,$$

for all choices of $d-1$ roots of unity $a_0 \neq b_0, a_1, \ldots, a_m, b_1, \ldots, b_m$. To see that this holds, simply cross multiply and rewrite this as

$$b_0 + \sum_{i=1}^{m} p^i a_i \neq a_0 + \sum_{i=1}^{m} p^i b_i.$$

Viewed in $\mathbb{Z}_p$, this inequality is obvious, already the first digits are different.

If in addition we knew that $\mathcal{F}_{\lambda,\chi}$ was geometrically irreducible, then by [Kat4, 5.11], we would know that its G_{geom} contains $SL((d-1)^n)$ provided that $n \geq 2$ and either

$$(d-1)^n > 4$$

or

$$d = 3, n = 2, \qquad \text{and} \qquad \chi \text{ does not have order } 3.$$

[When $d = 3$ and $n = 2$ the requirement that N be nonzero mod $d = 3$ forces our χ to have order prime to 3.] To show the geometric irreducibility, it is enough to work in some large characteristic P which is 1 mod $d-1$ (not to be confused with p used in defining f as the sum of $p^i g(X_i)$), with $P > p^{2n(d-1)} - 1$ (to be sure that none of $p, p^2, \ldots, p^n$ is a $2d-2$ root of unity mod P), with $P > 2d-2$, and such that (**) above holds in $\mathbb{F}_P$, and to show there that

$$L_1 \star_{mid,+} L_2 \ldots \star_{mid,+} L_n$$

is geometrically irreducible (because middle convolution with $\mathcal{L}_\chi$ preserves geometric irreducibility). For this, it suffices to show that on $\mathbb{G}_m$, the tensor product of the (lisse on $\mathbb{G}_m$) Fourier Transforms

$$FT(L_1) \otimes FT(L_2) \ldots \otimes FT(L_n)$$

is geometrically irreducible (its extension by direct image across 0 is the Fourier Transform of $L_1 \star_{mid,+} L_2 \ldots \star_{mid,+} L_n$, by the nonpunctuality of the latter).

From [Kat3, 7.10.4], we know that, in our sufficiently large characteristic P, each individual $FT(L_i)$ has G_{geom} either $Sp(d-1)$, if d is odd, or $\pm SL(d-1)$, if d is even. So it suffices to show that the G_{geom} of the direct sum is the n-fold self product $(Sp(d-1))^n$ in the d odd case, and contains the n-fold self product $(SL(d-1))^n$ in the d even case. For then the tensor product is the product of irreducible representations of the factors, so is an irreducible representation of that product.

By Goursat–Kolchin–Ribet, cf. [Kat3, 1.8.2], it suffices to show that for $i \neq j$, there is no lisse rank one $\mathcal{L}$ on $\mathbb{G}_m$ for which $FT(L_i) \cong \mathcal{L} \otimes FT(L_j)$ or for

which $FT(L_i)^\vee \cong \mathcal{L} \otimes FT(L_j)$. In the d odd case, $\mathcal{L}$ must have order dividing 2, as the only scalars in $Sp(d-1)$ are ± 1. The $I(\infty)$ representation of $FT(L_i)$ is, by [7.9.4, line 4 of proof, or 7.10.4, line 12 of proof]Ka-ESDE, the direct sum

$$\oplus_{\zeta \in \mu_{d-1}} \mathcal{L}_{\chi_{quad}} \otimes \mathcal{L}_{\psi(p^i(1-d)\zeta x)}.$$

The only $\mathcal{L}$ of order dividing 2 is either $\mathbb{Q}_\ell$ or $\mathcal{L}_{\chi_{quad}}$. The second is not allowed, because it "removes" the factor $\mathcal{L}_{\chi_{quad}}$ from each piece of the $I(\infty)$-representation. The first is not allowed, because the $I(\infty)$-representation of $FT(L_j)$ is

$$\oplus_{\zeta \in \mu_{d-1}} \mathcal{L}_{\chi_{quad}} \otimes \mathcal{L}_{\psi(p^j(1-d)\zeta x)},$$

and for $i \neq j$, no $p^i\zeta$ is any $p^j\zeta'$, for ζ, ζ' any $d-1$ roots of unity.

In the d even case, where each factor's G_{geom} is $\pm SL(d-1)$, $\mathcal{L}$ must have order dividing $2(d-1)$. As $P > 2d-2$, such an $\mathcal{L}$ is necessarily tame, so of the form $\mathcal{L}_\chi$ for a character χ of order dividing $2d-2$. If χ is nontrivial, we multiply the $\mathcal{L}_{\chi_{quad}}$ factors in the $I(\infty)$ summands by χ, not allowed. So it remains only to rule out both $FT(L_i) \cong FT(L_j)$ and $FT(L_i)^\vee \cong FT(L_j)$ Again we compare $I(\infty)$ summands. The first case cannot happen, for the same reason as above: no $p^i\zeta$ is any $p^j\zeta'$. The second case cannot happen because no $-p^i\zeta$ is any $p^j\zeta'$. This concludes the proof that our $\mathcal{F}_{\lambda,\chi}$ on $S[1/\ell]$ is geometrically irreducible.

9. Some open questions

As already noted in the "Historical Overview" section, Zarhin has shown that for hyperelliptic curves over $\mathbb{Q}$ (or indeed over any field K which is finitely generated over $\mathbb{Q}$) of the form $Y^2 = h(X)$, with h a polynomial of degree $n = 2g+1$ or $2g+2$, various explicit conditions on n and on the Galois group of h over K guarantee that the ℓ-adic representation on H^1 has image which is open in the group of symplectic similitudes $GSp(2g, \mathbb{Q}_\ell)$. For example, if h has degree $n \geq 5$ and has Galois group over $\mathbb{Q}$ either S_n or A_n, then this holds, cf. [Zar1]. What if any are the analogues of Zarhin's results for χ components of H^1_c of superelliptic[1] curves over cyclotomic fields, and their descents to $\mathbb{Q}$, when they exist?

[1] See [AP, Thm. 3.8] for the monodromy of the universal family of tri-elliptic curves.

References

[AP] J. Achter and R. Pries, The integral monodromy of hyperelliptic and trielliptic curves. *Math. Ann.* **338** (2007), 187–206. Zbl 1129.11027 MR 2295509

[AGV] M. Artin, A. Grothendieck, and J. L. Verdier, *Séminaire de Géometrie Algébrique du Bois Marie*, SGA 4, Tome III, Springer Lecture Notes in Mathematics 305, Springer Verlag, 1973. Zbl 0245.00002

[BCE+] G. Boxer, F. Calegari, M. Emerton, B. Levin, K. Madapusi Pera, and S. Patrikis, Compatible systems of Galois representations associated to the exceptional group E6. *Forum Math. Sigma* 7, Article ID e4 (2019). Zbl 07013705 MR 3910457

[Beau] A. Beauville, Le groupe de monodromie des familles universelles d'hypersurfaces et d'intersections complètes. Complex analysis and algebraic geometry (Göttingen, 1985), 8–18, Lecture Notes in Math., 1194, Springer, Berlin, 1986. Zbl 0603.14011 MR 0855873

[Bou] N. Bourbaki, *Éléments de mathématique.* Fasc. XXVI. Groupes et algèbres de Lie. Chapitre I: Algèbres de Lie. (French) Seconde édition. Actualités Scientifiques et Industrielles, No. 1285 Hermann, Paris 1971. Zbl 0213.04103 MR 0271276

[Bog] F. A. Bogomolov, Sur l'algébricité des représentations l-adiques. C. R. Acad. Sci. Paris Sér. A-B **290** (1980), A701–A703. Zbl 0457.14020 MR 0574307

[Bor] A. Borel, *Linear Algebraic Groups*, Second edition. Graduate Texts in Mathematics, 126. Springer-Verlag, New York, 1991. Zbl 0726.20030 MR 1102012

[CHT] A. Cadoret, C. Y. Hui, and A. Tamagawa, Geometric monodromy-semisimplicity and maximality. *Ann. of Math.* (2) **186** (2017), 205–236. Zbl 1369.14029 MR 3665003

[CR] C. Cornut and J. Ray, Generators of the pro-p Iwahori and Galois representations. *Int. J. Number Theory* **14** (2018), 37–53. Zbl 1430.20047 MR 3726241

[Del] P. Deligne, La conjecture de Weil II. *Pub. Math. I.H.E.S.* **52** (1981), 137–252. Zbl 0456.14014 MR 0601520

[DM] P. Deligne and G. D. Mostow, Monodromy of hypergeometric functions and non-lattice integral monodromy. *Pub. Math. I.H.E.S.* **63** (1986), 5–89. Zbl 0615.22008 MR 0849651

[DR1] M. Dettweiler and S. Reiter, On rigid tuples in linear groups of odd dimension. *J. Algebra* **222** (1999), 550–560. Zbl 0945.12001 MR 1734230

[DR2] —— An algorithm of Katz and its application to the inverse Galois problem. Algorithmic methods in Galois theory. *J. Symbolic Comput.* **30** (2000), 761–798. Zbl 1049.12005 MR 1800678

[DR3] —— Rigid local systems and motives of type G2. With an appendix by Michael Dettweiler and Nicholas M. Katz. *Compos. Math.* **146** (2010), 929–963. Zbl 1194.14036 MR 2660679

[Fal] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.* **73** (1983), 349–366. Zbl 0588.14026 MR 0718935

[Gre] R. Greenberg, Galois representations with open image. *Ann. Math. Qué.* **40** (2016), 83–119. Zbl 1414.11151 MR 3512524

[Gro] A. Grothendieck, Formule de Lefschetz et rationalité des fonctions L. *Seminaire Bourbaki* 1964–65, Exposé 279, reprinted in *Dix Exposés sur la cohomologie des schémas*, North-Holland, 1968. Zbl 0199.24802 MR 1608788

[HL] C. Y. Hui and M. Larsen, Type A images of Galois representations and maximality. *Math. Z.* **284** (2016), 989–1003. Zbl 1402.11081 MR 3563263

[Hui] C. Y. Hui, Monodromy of Galois representations and equal-rank subalgebra equivalence. *Math. Res. Lett.* **20** (2013), 705–728. Zbl 1287.11074

[Kat1] N. Katz, Sommes Exponentielles, Astérisque 79, Course taught at the University of Paris, Orsay, Fall 1979. With a preface by Luc Illusie. Notes written by Gérard Laumon. Astérisque 79. Sociét'e Mathématique de France, Paris, 1980. Zbl 0469.12007 MR 0617009

[Kat2] —— *Gauss Sums, Kloosterman Sums, and Monodromy Groups*. Annals of Mathematics Studies, 116. Princeton Univ. Press, Princeton, NJ, 1988. Zbl 0675.14004 MR 0955052

[Kat3] —— *Exponential Sums and Differential Equations*. Annals of Mathematics Studies, 124. Princeton Univ. Press, Princeton, NJ, 1990. Zbl 0731.14008 MR 1081536

[Kat4] —— Affine cohomological transforms, perversity, and monodromy. *J. Amer. Math. Soc.* **6** (1993), 149–222. Zbl 0815.14011 MR 1161307

[Kat5] —— *Rigid Local Systems*. Annals of Mathematics Studies, 139. Princeton University Press, Princeton, NJ, 1996. Zbl 0864.14013 MR 1366651

[Kat6] —— *Moments, Monodromy, and Perversity*. Annals of Mathematics Studies, 159. Princeton University Press, Princeton, NJ, 2005. Zbl 1079.14025 MR 2183396

[Kat7] —— Sato–Tate in the higher dimensional case: Elaboration of 9.5.4 in Serre's $N_X(p)$ book. *Enseign. Math.* **59** (2013), 359–377 Zbl 1320.14042 MR 3189042

[KS] N. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues, and Monodromy*. American Mathematical Society Colloquium Publications, 45. American Mathematical Society, Providence, RI, 1999. Zbl 0958.11004 MR 1659828

[Nam] K. Namba, Dedekind's η function and Sato's $\sin^2$ conjecture. *Reports of the Institute for Mathematics and Computer Science* **27**, 16th Symposium on the History of Mathematics, Inst. of Math. and Compt. Sci. Tsuda Univ. (2006), 95–167 (in Japanese).

[Poc] L. Pochhammer, Ueber hypergeometrische Functionen höherer Ordnung. *J. Reine Angew. Math (Crelle)* **71** (1870), 316–362. JFM 02.0265.01 MR 1579481

[Ser1] J. P. Serre, Groupes de Lie ℓ-adique attachés aux courbes elliptiques, Coll. Clermont-Ferrand, C.N.R.S., 1964, 3–20, published in *Les Tendances Géom. en Algèbre et Théorie des Nombres*, Éditions du Centre National de la Recherche Scientifique, Paris, 1966, pp. 239–256. Zbl 0148.41502 MR 0218366

[Ser2] —— Sur les groupes de Galois attachés aux groupes p-divisibles. *Proc. Conf. Local Fields (Driebergen, 1966)*, Springer, Berlin, 1967, pp. 118–131 Zbl 0189.02901 MR 0242839

[Ser3] —— Proprétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.* **15** (1972), 259–331. Zbl 0235.14012 MR 0387283

[Ser4] —— Représentations l-adiques. *Algebraic number theory* (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976), pp. 177–193. Japan Soc. Promotion Sci., Tokyo, 1977. Zbl 0406.14015 MR 0476753

[Ser5] —— *Abelian l-adic Representations and Elliptic Curves*. With the collaboration of Willem Kuyk and John Labute. Second edition. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. Zbl 0709.14002 MR 1043865

[Ser6] —— *Lectures on the Mordell–Weil Theorem*, Third Edition. Aspects of Mathematics E15, Springer Fachmedien Wiesbaden GmbH, 1997. Zbl 0863.14013 MR 1757192

[Ser7] —— (18 Mai 1966) Lettre à Armand Borel, pp. 1–9. *Frobenius Distributions: Lang–Trotter and Sato–Tate Conjectures*. Contemp. Math., 663, Amer. Math. Soc., Providence, RI, 2016. Zbl 1350.11001 MR 3502936

[SV] K. Strambach and J. Völklein, On linearly rigid tuples. (English summary) *J. Reine Angew. Math.* **510** (1999), 57–62. Zbl 0931.12006 MR 1696090

[Tan] Y. Taniyama, L-functions of number fields and zeta functions of abelian varieties. *J. Math. Soc. Japan* **9** (1957), 330–366. Zbl 0213.22803 MR 0095161

[Tat] J. Tate, Algebraic cycles and poles of zeta functions. *Arithmetical Algebraic Geometry* (Proc. Conf. Purdue Univ., 1963) pp. 93–110, Harper and Row, New York, 1965. Zbl 0213.22804 MR 0225778

[Ter] T. Terasoma, Complete intersections with middle Picard number 1 defined over Q. *Math. Z.* **189** (1985), 289–296. Zbl 0579.14006 MR 0779223

[Upt] M. G. Upton, Galois representations attached to Picard curves. *J. Algebra* **322** (2009), 1038–1059. Zbl 1230.11071 MR 2537671

[Wag] A. Wagner, Collineation groups generated by homologies of order greater than 2. *Geom. Dedicata* **7** (1978), 387–398. Zbl 0402.20036 MR 0512113

[Yun] Z. Yun, Motives with exceptional Galois groups and the inverse Galois problem. *Invent. Math.* **196** (2014), 267–337. Zbl 1374.14013 MR 3193750

[Zar1] Y. Zarhin, Very simple 2-adic representations and hyperelliptic Jacobians. Dedicated to Yuri I. Manin on the occasion of his 65th birthday. *Mosc. Math. J.* **2** (2002), 403–431. Zbl 1082.11039 MR 1944511

[Zar2] —— Families of absolutely simple hyperelliptic Jacobians. *Proc. Lond. Math. Soc. (3)* **100** (2010), 24–54. Zbl 1186.14031 MR 2578467

[Zar3] —— Galois groups of Mori trinomials and hyperelliptic curves with big monodromy. *Eur. J. Math.* **2** (2016), 360–381 Zbl 1344.14021 MR 3454107

[Zar4] —— Two-dimensional families of hyperelliptic Jacobians with big monodromy. *Trans. Amer. Math. Soc.* **368** (2016), 3651–3672. Zbl 1343.14025 MR 3451889

(*Reçu le 25 décembre 2018*)

Nicholas M. Katz, Fine Hall, Dept. Math.,
Princeton University, Princeton NJ 08544-1000, USA

e-mail: nmk@math.princeton.edu

© Fondation L'Enseignement Mathématique