Linear Representations of the Grothendieck-Teichmüller group

Ted Chinburg

joint work with Frauke Bleher and Alexander Lubotzky

ICTS, January 2024

Overview.

Transplanting techniques from discrete groups to profinite groups leads to two unexpected outcomes:

1. The profinite case is sometimes easier, with sharper results.
2. Applying the profinite results to number theory resolves an old question about constructing representations of the Grothendieck-Teichmüller group.

Group theory.

Let F_d be the discrete free group on d elements, and let $\mathrm{Aut}(F_d)$ be its automorphism group.

Goal:(Grunewald-Lubotzky 2009) One can construct linear representations of finite index subgroups of $\mathrm{Aut}(F_d)$ with image a "large" arithmetic group.

The Construction:

Choose a surjection $\pi : F_d \to H$ onto a finite group H and let $\mathcal{R} = \mathrm{Kernel}(\pi)$. Then $A(\pi) = \{\alpha \in \mathrm{Aut}(F_d) : \pi \circ \alpha = \pi\}$ has finite index in $\mathrm{Aut}(F_d)$. We have an exact sequence

$$1 \to \frac{\mathcal{R}}{[\mathcal{R},\mathcal{R}]} \to \frac{F_d}{[\mathcal{R},\mathcal{R}]} \xrightarrow{\pi} H \to 1 \qquad (1)$$

Grunewald and Lubotzky use Fox calculus and work of Vaserstein to show that when

$$\overline{\mathcal{R}} = \frac{\mathcal{R}}{[\mathcal{R},\mathcal{R}]}$$

$d \geq 4$ and $\pi(x_0) = 1 \in H$ for some generator $x_0 \in F_d$, we get a homomorphism

$$\rho : A(\pi) \to \mathrm{Aut}_{\mathbb{Z}[H]}(\overline{\mathcal{R}}) = \mathcal{G}$$

whose image has finite index in the arithmetic group $\mathcal{G}^1$ that is the kernel of all homomorphsms $\mathcal{G} \to \mathrm{GL}_1$ defined over $\mathbb{Q}$.

An Example:

$H = \mathbb{Z}/p$, p a prime.

$$\mathbb{Z}[H] \subset \mathbb{Q}[H] \equiv \mathbb{Q} \oplus \mathbb{Q}(\zeta_p)$$

as algebras.

$\mathbb{Q} \otimes_{\mathbb{Z}} \overline{\mathcal{R}}$ is commensurable with

$$\mathbb{Q} \oplus \mathbb{Q}[H]^{d-1} \equiv \mathbb{Q}^d \oplus \mathbb{Q}(\zeta_p)^{d-1}$$

as $\mathbb{Q}[H]$-module.

$\mathcal{G}(\mathbb{Z})$ is commensurable with $\mathrm{GL}_d(\mathbb{Z}) \times \mathrm{GL}_{d-1}(\mathbb{Z}[\zeta_p])$.

$\mathcal{G}^1(\mathbb{Z})$ is commensurable with $\mathrm{SL}_d(\mathbb{Z}) \times \mathrm{SL}_{d-1}(\mathbb{Z}[\zeta_p])$.

Note: It is hard to identify the image of

$$\rho : A(\pi) \to \mathrm{Aut}_{\mathbb{Z}[H]}(\overline{\mathcal{R}})^1 = \mathcal{G}^1(\mathbb{Z}).$$

The profinite case

Moral: Everything is easier!

Replace F_d by its profinite completion $\hat{F}_d$. Use a surjection $\pi : \hat{F}_d \to H$ with kernel we'll still call $\mathcal{R}$. Let $\beta \in H^2(H, \overline{\mathcal{R}})$ be the extension class of

$$1 \to \overline{\mathcal{R}} \;=\; \frac{\mathcal{R}}{[\mathcal{R},\mathcal{R}]} \to \frac{\hat{F}_d}{[\mathcal{R},\mathcal{R}]} \xrightarrow{\pi} H \to 1 \qquad (2)$$

Theorem (Bleher, C, Lubotzky) Let $\mathrm{Aut}_{\mathbb{Z}[H],\beta}(\overline{R})$ be the finite index subgroup of $\gamma \in \mathrm{Aut}_{\mathbb{Z}[H]}(\overline{R})$ that preserve β. Then

$$A(\pi) \to \mathrm{Aut}_{\mathbb{Z}[H],\beta}(\overline{R}) \quad \text{is surjective.}$$

Why is the profinite case easier?

Lemma(Gaschütz) Suppose $\psi : G_1 \to G_2$ is a surjective homomorphism of finitely pro-generated profinite groups. Assume that the number of topological generators of G_1 is $\leq d$ and that $S_2 \subset G_2$ is a set of d topological generators of G_2. Then there is a set $S_1 \subset G_1$ of topological generators of G_1 so that $\psi(S_1) = S_2$.

For a nice proof by Roquette, see "Field arithmetic" by Fried and Jarden.

Corollary If N is a closed normal subgroup of $\hat{F}_d$, every automorphism of $\hat{F}_d/N$ can be lifted to an automorphism of $\hat{F}_d$ preserving N.

Number theoretic applications

Theorem(Belyi, 1979) There is a canonical injection

$$G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\hat{F}_2).$$

Where does this come from?

Let $\overline{\mathbb{Q}}(t)_{0,1,\infty}$ be the maximal extension of $\overline{\mathbb{Q}}(t)$ in an algebraic closure $\overline{\mathbb{Q}(t)}$ that is unramified over all discrete valuations that are trivial on $\overline{\mathbb{Q}}$ other than those that give t, $t-1$ and t^{-1} valuation 1. Then the tower of fields $\mathbb{Q}(t) \subset \overline{\mathbb{Q}}(t) \subset \overline{\mathbb{Q}}(t)_{0,1,\infty}$ gives an exact sequence of Galois groups

$$1 \to \mathrm{Gal}\left(\frac{\overline{\mathbb{Q}}(t)_{0,1,\infty}}{\overline{\mathbb{Q}}(t)}\right) \to \mathrm{Gal}\left(\frac{\overline{\mathbb{Q}}(t)_{0,1,\infty}}{\mathbb{Q}(t)}\right) \to \mathrm{Gal}\left(\frac{\overline{\mathbb{Q}}(t)}{\mathbb{Q}(t)}\right) \to 1$$

Now use

$$\mathrm{Gal}\left(\frac{\overline{\mathbb{Q}}(t)}{\mathbb{Q}(t)}\right) = \mathrm{Gal}\left(\frac{\overline{\mathbb{Q}}}{\mathbb{Q}}\right) = G_{\mathbb{Q}}$$

and identify

$$\mathrm{Gal}\left(\frac{\overline{\mathbb{Q}}(t)_{0,1,\infty}}{\overline{\mathbb{Q}}(t)}\right) = \pi_1^{etale}(\mathbb{P}^1_{\overline{\mathbb{Q}}} - \{0,1,\infty\})$$

with the profinite completion $\hat{F}_2$ of $F_2 = \pi_1^{top}(\mathbb{P}^1_{\mathbb{C}} - \{0,1,\infty\})$. We get an exact sequence

$$1 \to \hat{F}_2 \to \mathrm{Gal}\left(\frac{\overline{\mathbb{Q}}(t)_{0,1,\infty}}{\mathbb{Q}(t)}\right) \to G_{\mathbb{Q}} \to 1$$

and a canonical homomorphism

$$G_{\mathbb{Q}} \to \mathrm{Out}(\hat{F}_2).$$

Belyi shows how to use decomposition groups of points over 0 and 1 to lift this canonically to an injective homomorphism

$$G_{\mathbb{Q}} \to \mathrm{Aut}(\hat{F}_2).$$

The Grothendieck-Teichmüller group $\widehat{GT}$

Belyi's construction produces two canonical topological pro-generators x and y of $\hat{F}_2$ coming from generators of inertia groups over 0 and 1. These can be thought of as loops around 0 and 1 from a base point in $\mathbb{P}^1_{\mathbb{C}}$.

Theorem(Drinfeld and Grothendieck) There is an infinite index subgroup $\widehat{GT}$ of $\gamma \in \mathrm{Aut}(\hat{F}_2)$ defined by certain identities involving $\gamma(x)$ and $\gamma(y)$ such that Belyi's map $G_{\mathbb{Q}} \to \mathrm{Aut}(\hat{F}_2)$ gives an injection

$$G_{\mathbb{Q}} \to \widehat{GT}.$$

Main Question(Grothendieck) Is $G_{\mathbb{Q}} = \widehat{GT}$??

Consequence If so, every representation of $G_{\mathbb{Q}}$ lifts to $\widehat{GT}$.

The precise definition of $\widehat{GT}$ (optional)

Elements of $\widehat{GT}$ are specified by pairs $(\lambda, f) \in \hat{\mathbb{Z}}^* \times \hat{F}_2'$ where $\hat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$ and $\hat{F}_2'$ is the commutator subgroup of $\hat{F}_2$. These must satisfy some identities listed below, and they give automorphisms of $\hat{F}_2$ by

$$x \to x^\lambda \quad \text{and} \quad y \to f^{-1} y^\lambda f.$$

The identities are:

$$f(x,y) \cdot f(y,x) = 1$$

$$f(x,y)x^m f(z,x) z^m f(y,z) y^m = 1 \quad \text{with} \quad m = \frac{\lambda - 1}{2} \quad \text{when} \quad xyz = 1$$

$$f(x_{12}, x_{23}) f(x_{34}, x_{45}) f(x_{51}, x_{12}) f(x_{23}, x_{34}) f(x_{45}, x_{51}) = 1 \quad \text{in} \quad \hat{\kappa}_{0,5}$$

when $\hat{\kappa}_{0,5} = \mathrm{Kernel}(M(0,5) \to S_5)$ and $M(0,5)$ is the quotient of the profinite braid group $\hat{B}_5$ by the relations $(\sigma_1 \cdot \sigma_2 \cdot \sigma_3 \cdot \sigma_4)^2 = 1 = \sigma_4 \cdot \sigma_3 \cdot \sigma_2 \cdot \sigma_1^2 \cdot \sigma_2 \cdot \sigma_3 \cdot \sigma_4$ and $x_{ij} = \sigma_{j-1} \cdots \sigma_{i+1} \sigma_i^2 \sigma_{i+1}^{-1} \cdots \sigma_{j-1}^{-1}$ for $1 \le i < j \le n$.

The question of Lochak and Schneps, and the Leapfrog strategy

Question(Lochak and Schneps, 1997) Can one construct a non-abelian finite dimensional representation of $G_{\mathbb{Q}}$ that has infinite order image and that lifts to $\widehat{GT}$?

Theorem(Bleher, C, Lubotzky) The profinite version of the Grunewald-Lubotzky construction produces non-abelian representations of $G_{\mathbb{Q}}$ that lift to finite index subgroups of $\mathrm{Aut}(\hat{F}_2)$, and therefore to finite index subgroups of $\widehat{GT}$. These representations come from the adelic Tate modules of generalized Jacobians of curves.

Question:

Which "automorphic" representations of $G_{\mathbb{Q}}$ can be extended to finite index subgroups of $\mathrm{Aut}(\hat{F}_2)$?

Lifting Galois actions on Tate modules of generalized Jacobians

X = smooth projective irreducible curve over $\overline{\mathbb{Q}}$.

Theorem(Belyi) There is a non-constant morphism $\lambda : X \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ that is unramified outside $\{0, 1, \infty\}$.

Let Y be the smooth curve over $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ whose function field $\overline{\mathbb{Q}}(Y)$ is the Galois closure of $\overline{\mathbb{Q}}(X)$ over $\overline{\mathbb{Q}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}) = \overline{\mathbb{Q}}(t)$. Then $H = \mathrm{Gal}(\overline{\mathbb{Q}}(Y)/\overline{\mathbb{Q}}(t))$ is a finite quotient of

$$\hat{F}_2 = \mathrm{Gal}\left(\frac{\overline{\mathbb{Q}}(t)_{0,1,\infty}}{\overline{\mathbb{Q}}(t)}\right) = \pi_1^{etale}(\mathbb{P}^1_{\overline{\mathbb{Q}}} - \{0, 1, \infty\}).$$

As in the profinite Grunewald-Lubotzky construction, we have an exact sequence

$$1 \to \overline{\mathcal{R}} \;=\; \frac{\mathcal{R}}{[\mathcal{R},\mathcal{R}]} \to \frac{\hat{F}_2}{[\mathcal{R},\mathcal{R}]} \xrightarrow{\pi} H \to 1 \qquad (3)$$

Lemma:(Serre) $\overline{\mathcal{R}}$ is the Galois group of the maximal abelian cover of Y that is unramified outside the set S of points of Y lying over $\{0,1,\infty\} \subset \mathbb{P}^1_{\overline{\mathbb{Q}}}$. As such $\overline{\mathcal{R}}$ is isomorphic to the adelic Tate module $T_S(Y)$ of the generalized Jacobian of Y with respect to S.

Remarks

1. There is a number field F such that X, Y and the action of H on Y are defined over F. For all such F, $G_F = \mathrm{Gal}(\overline{\mathbb{Q}}/F)$ acts on $T_S(Y)$.
2. If X is a modular curve, F can be taken to be abelian over $\mathbb{Q}$. In this case, the action of G_F on $T_S(Y)$ is related to modular forms of weight two via work of Shimura. This is one of the first cases of the Langlands program.

Main arithmetic result

Theorem(Bleher, C, Lubotzky) For a sufficiently large number field F, the action of G_F on $T_S(Y)$ extends to an action of a finite index subgroup $A_{S,Y}$ of $\mathrm{Aut}(\hat{F}_2)$ when we embed G_F into $\mathrm{Aut}(\hat{F}_2)$ via the Belyi embedding

$$G_F \subset G_{\mathbb{Q}} \to \mathrm{Aut}(\hat{F}_2).$$

Corollary For a sufficiently large number field F, the action of G_F on $T_S(Y)$ extends to the action of a finite index subgroup of the Grothendieck-Teichmüller group $\widehat{GT}$. This provides examples of the kind sought by Lochak and Schneps.

Remark One can prove a similar result for the action of G_F on $T_{S'}(X)$ when S' is the inverse image of $\{0, 1, \infty\}$ under $X \to \mathbb{P}^1_{\mathbb{Q}}$.

An example

Let $X = Y$ be the curve with function field $\overline{\mathbb{Q}}(t, (t(t-1))^{1/3})$, so that Y is the function field of the affine elliptic curve

$$y^3 = t(t-1).$$

Then Y is a cyclic $H = \mathbb{Z}/3$ cover of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$. There is an exact sequence of Tate modules

$$0 \to \hat{\mathbb{Z}}(1) \oplus \hat{\mathbb{Z}}(1) \to T_S(Y) \to T(Y) \to 0$$

in which

$$\hat{\mathbb{Z}}(1) = \varprojlim_n \mu_n$$

when μ_n is the Galois module of n^{th} roots of unity, and $T(Y)$ is the adelic Tate module of the elliptic curve. In this case (and in fact, whenever H is abelian), the action of G_F on $T(Y)$ can also be lifted to an action of a finite index subgroup of $\mathrm{Aut}(\hat{F}_2)$.

Final comments

1. We can construct some (very large) finite Galois covers $Y \to \mathbb{P}^1$ branched over $\{0, 1, \infty\}$ defined over $\mathbb{Q}$ such that the Galois action of $G_{\mathbb{Q}}$ on $T_S(Y)$ extends to all of $\mathrm{Aut}(\hat{F}_2)$. So this action automatically extends to $\widehat{GT}$.

In general, there will be obstructions to extending the Galois action on $T_S(Y)$ to all of $\mathrm{Aut}(\hat{F}_2)$ in a way that is consistent with Belyi's embedding $G_{\mathbb{Q}} \to \mathrm{Aut}(\hat{F}_2)$ and with the identification of $T_S(Y)$ with a subquotient of
$\hat{F}_2 = \mathrm{Gal}(\overline{\mathbb{Q}}_{0,1,\infty}(t)/\overline{\mathbb{Q}}(t)) = \pi_1^{et}(\mathbb{P}^1_{\overline{\mathbb{Q}}} - \{0, 1, \infty\})$.

Future work has to do with identifying maximal subgroups $\tilde{A}$ of finite index in $\mathrm{Aut}(\hat{F}_2)$ for which such an extension exists. One can then try to show that at least one such $\tilde{A}$ contains $\widehat{GT}$ by showing the conditions specifying when $\alpha \in \mathrm{Aut}(\hat{F}_2)$ lies in $\widehat{GT}$ imply the finitely many conditions that determine whether $\alpha \in \tilde{A}$.

2. To expand on # 1, any family of Galois representations (e.g. the Tate modules $T_S(Y)$ as Y varies) that are constructed "group theoretically" from $\hat{F}_2 = \mathrm{Gal}(\overline{\mathbb{Q}}(t)_{0,1,\infty}/\overline{\mathbb{Q}}(t))$ defines a family of lifting problems relative to the Belyi embedding $G_{\mathbb{Q}} \to \mathrm{Aut}(\hat{F}_2)$. Such a family defines a system of obstructions to lifting the representations to all of $\mathrm{Aut}(\hat{F}_2)$. The subgroup of $\mathrm{Aut}(\hat{F}_2)$ for which all of these obstructions vanish should contain $\widehat{GT}$. What is the subgroup arising from the family of all Tate modules of generalized Jacobians?

3. Grunewald, Larsen, Lubotzky and Malestein used the ideas involved in their construction of representations of $\mathrm{Aut}(F_d)$ to construct representations of $\mathrm{Aut}(\pi_1(\Sigma_g))$ when Σ_g is a closed Riemann surface of genus g. Here $\pi_1(\Sigma_g)$ is the quotient of a free group by one relation. This relation makes it more difficult to lift automorphisms of finite quotients of the profinite completion $\widehat{\pi_1(\Sigma_g)}$ of $\pi_1(\Sigma_g)$. So it remains to construct in this way large linear representations of $\mathrm{Aut}(\widehat{\pi_1(\Sigma_g)})$.

4. We can realize the principal congruence modular curve $X = X(N)$ of positive even level $N > 2$ as a Galois cover of $\mathbb{P}^1_{\mathbb{Q}}$ that is unramified outside of $\{0, 1, \infty\}$, with the cusps X being the inverse image of $\{0, 1, \infty\}$. For every prime ℓ, the Galois representation associated to the weight two cusp forms of level N is $\mathrm{Hom}(T_{X,S}, \mathbb{Q}_\ell)$. This is why our results pertain to weight two cusp forms when X is a modular curve.

5. It's natural to ask how to lift the action of finite index subgroups of $G_{\mathbb{Q}}$ on forms of weight $k \geq 2$ to large subgroups of $\mathrm{Aut}(\hat{F}_2)$. Let $f : E \to X(N) - \{\mathrm{cusps}\}$ be the universal family of elliptic curves with level N structure. Let $T_\ell(E^{un})$ be the rational ℓ-adic Tate module of the base change E^{un} to $\overline{\mathbb{Q}}(t)_{0,1,\infty}$ of the universal family E. Let $\Gamma = \mathrm{Gal}(\overline{\mathbb{Q}}(t)_{0,1,\infty}/\overline{\mathbb{Q}}(X(N)))$. Work of Deligne shows the ℓ-adic Galois representation associated to weight $k \geq 2$ forms on X is

$$V_{k,\ell} = H^1(\Gamma, \mathrm{Sym}^{k-2} T_\ell(E^{un})).$$

When $k = 2$, this gives

$$V_{2,\ell} = H^1(\Gamma, \mathbb{Q}_\ell) = \mathrm{Hom}(\Gamma^{ab}, \mathbb{Q}_\ell) = \mathrm{Hom}(T_{X(N),S}, \mathbb{Q}_\ell).$$

For $k > 2$ one approach is to define (infinite index) subgroups of $\mathrm{Aut}(\hat{F}_2)$ that act compatibly on Γ and on $\mathrm{Sym}^{k-2} T_\ell(E^{un})$. (The latter action is automatic when $k = 2$.)

How to view $T_\ell(E^{un})$ mod the action of ± 1 using the group theory of $\Gamma = \mathrm{Gal}(\overline{\mathbb{Q}}(t)_{0,1,\infty}/\overline{\mathbb{Q}}(X(N)))$

Assume ℓ does not divide N. Let $\overline{\mathbb{Q}}(X(N))^{mod,\ell}$ be the subfield of $\overline{\mathbb{Q}}(t)_{0,1,\infty}$ that is the union of $\overline{\mathbb{Q}}(X(N\ell^n))$ over all integers n. Then $\mathrm{Gal}(\overline{\mathbb{Q}}(X(N))^{mod,\ell}/\overline{\mathbb{Q}}(X(N)))$ is canonically isomorphic to $\mathrm{PSL}_2(\mathbb{Z}_\ell)$. Let $U^{mod,\ell}$ be the upper triangular unipotent subgroup of $\mathrm{PSL}_2(\mathbb{Z}_\ell)$. We can identify $T_\ell(E^{un})$ with $\mathbb{Z}_\ell^2$ in such way that the following is true. Let $\tilde{T}_\ell(E^{un})$ be the set of equivalence classes in $T_\ell(E^{un})$ under the multiplication action of $\{\pm 1\}$. Then there is a map from the cosets $\mathrm{PSL}_2(\mathbb{Z}_\ell)/U^{mod,\ell}$ to $\tilde{T}_\ell(E^{un})$ that sends the coset

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot U^{mod,\ell}$$

to the equivalence class $[(a,c)]$ of (a,c). The image $\mathcal{I}$ of this map consists of the equivalence classes $[(a,c)]$ of all pairs $(a,c) \in \mathbb{Z}_\ell^2$ such that at least one of a or c is a unit.

The upshot for extending Galois actions on modular forms of weight $k > 2$ to actions of subgroups of $\mathrm{Aut}(\hat{F}_2)$.

We can lift the action of a finite index subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $V_{k,\ell}$ to a subgroup $\tilde{H} \subset \mathrm{Aut}(\pi_1^{et}(\mathbb{P}^1_{\overline{\mathbb{Q}}} - \{0,1,\infty\})) = \mathrm{Aut}(\hat{F}_2)$ provided $\tilde{H}$ has the following properties:

(1) $\tilde{H}$ takes $\mathrm{Gal}(\overline{\mathbb{Q}}(t)_{0,1,\infty}/\overline{\mathbb{Q}}(X(N))^{mod,\ell})$ to itself.

(2) The action of $\tilde{H}$ on $\mathrm{Gal}(\overline{\mathbb{Q}}(X(N))^{mod,\ell}/\overline{\mathbb{Q}}(X(N))) = \mathrm{PSL}_2(\mathbb{Z}_\ell)$ that is induced by condition (1) takes the unipotent subgroup $U^{mod,\ell}$ to itelf.

(3) The action of $\tilde{H}$ on the cosets $\mathrm{PSL}_2(\mathbb{Z}_\ell)/U^{mod,\ell}$ that is induced by conditions (1) and (2) lifts to a $\mathbb{Z}_\ell$ linear action of $\tilde{H}$ on $T_\ell(E^{un})$. When such a lift exists, it is unique up to multiplication by a quadratic character of $\tilde{H}$.

Note that if $k-2$ is even, then the quadratic character in step (3) will not affect the action of $\tilde{H}$ on $V_{k,\ell}$ since the quadratic character will not affect the action of $\tilde{H}$ on $\mathrm{Sym}^{k-2} T_\ell(E^{un})$.