The Grothendieck–Teichmüller Group and Galois Theory of the Rational Numbers

— European Network GTEM —

Jakob Stix, Mathematisches Institut der Universität Bonn

September 27, 2004

Abstract — GTEM is an acronym for Galois Theory and Explicit Methods. A selection from the activities within the network is presented. We focus on nonabelian Galois action, Grothendieck–Teichmüller theory and anabelian geometry. The style is expository and proofs are omitted.

1 The network

The network is based on nodes from eight European countries. Geographically ordered, the participating Universities are located in Nottingham, Leiden, Essen, Lille, Bonn, Paris 6, Heidelberg, Besançon, Bordeaux, Lausanne, Barcelona, Rom, and Tel Aviv. They joined under the acronym GTEM, read je t’aime, which abbreviates the common interest of these various different research groups: Galois Theory and Explicit Methods. More precisely, research within the network centers around many interesting topics of arithmetic related with \( \text{Gal}_\mathbb{Q} \), the absolute Galois group of the rational numbers, as follows:

1. (Explicit) finite Galois groups over \( \mathbb{Q} \).
2. The Inverse Galois Problem (IGP).
3. Dessins d’êtres.
4. Grothendieck–Teichmüller Theory: \( \text{Gal}_\mathbb{Q} \) and GT.
5. Arithmetic of elliptic curves over number fields.
6. Algorithms in number theory, in particular class field theory.
8. Arithmetic of covers, arithmetic fundamental groups.
9. (Birational) anabelian geometry.

The research so far was very vivid and produced many results. The following list of network related achievements mentions a few with no claim on completeness at all. Any omission, is due to mainly the ignorance of the author for which he offers his apologies. In the sequel, membies of the GTEM network are typeset in SMALLCAPS.

1. Realization of Galois groups by ‘middle convolution’ and ‘parabolic cohomology’ (Dettweiler–Reiter [DR00], Völklein [Vö01], Dettweiler–Wewers [DW03]).
2. Realization of Galois groups via Galois representations (Dieulefait, Vila, Crespo, see [GTEM]).
3. A combinatorial description of \( \text{Gal}_{\mathbb{Q}_p} \) in \( \text{Gal}_\mathbb{Q} \) using \( p \)-adic GT (André [An03]).
(4) New GT variants (Harbater–Schneps [HS00], Hatcher–Lochak–Schneps [HLS00], Nakamura–Schneps [NS00]).

(5) Proof of the generalized Kotchevakov conjecture (Zapponi [Za00]).

(6) Advances in the absolute Inverse Galois Problem (IGP) (Haran–Jarden–Pop [HJP04]).

(7) Construction of Hurwitz moduli schemes and applications to IGP (Dèbes, Deschamps, Emsalem, Flon, Romagny, see [GTEM]).

(8) Explicit 2– and 3–descent (Cremona–Stoll [CS02])

(9) Proof of the differential Abhyankar Conjecture, treatment of the differential IGP (Bertrand, Matzat–van der Put [MvdP03a] [MvdP03b], Hartmann [Ha02])

(10) Unraveling a connection between the Lamé operator and dessins d’enfant (Litcanu [Li03], Zapponi [Za04]).

(11) Results in birational (pro-ℓ) anabelian geometry (Pop [Po03], Efrat [Ef00], Efrat–Fešenko [EF99], Koenigsmann [Ko03]),

(12) Proof of anabelian geometry for nonconstant curves in characteristic p (Stix [Sx02]).

(13) A proof of finiteness of isomorphism classes of smooth proper curves over $\mathbb{F}_p$ with given $\pi_1$ (Raynaud [Ra02], Pop–Saidi [PS03] [Sa03], Tamagawa [Ta04]).

(14) Description of the stable reduction of $X(p^n)$ (Bouw–Wewers [BW04]).

(15) Results about reduction/lifting of curves (Green, Lehr–Matignon, Henrio, Mezard, Wewers, Bouw–Wewers, see [GTEM]).

(16) Determination of the asymptotics for certain Galois groups over $\mathbb{Q}$, database of Galois extensions of polynomials over $\mathbb{Q}$ up to degree 15 (Malle [Ma02, Ma04], Klüners–Malle [KM01]).

It is obvious that from the abundance of mathematics contained in this list, in the sequel, we will have to select a small portion and elaborate on these particular results and questions. Namely, the rest of this article will be devoted to the GT-geometric aspect of GTEM research, unfortunately leaving aside such exciting areas as differential Galois theory in which great strides have been made (see articles above, especially [MvdP03a]). Again, of course, the choice reflects a personal bias.

We will stick to the ground field of the rational numbers because the knowledgeable reader will anyway easily transfer what will be said to more general settings or may have a look at the references.

2 Galois action and $\mathbb{P}^1 - \{0, 1, \infty\}$

In his ‘Esquisse d’un programme’ [Gr84], Grothendieck suggests – among other things – that one should try to give a description of the absolute Galois group $\text{Gal}_\mathbb{Q} = \text{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$ of the rational numbers, by studying its action on the geometry (more precisely: algebraic invariants) of $\mathbb{Q}$-varieties. As good candidates he proposes the geometric fundamental group of (categories of) moduli spaces of curves with marked points. Special attention should be paid to the moduli space of the Riemann sphere with $n \geq 4$ marked points. The Grothendieck–Teichmüller group GT, that will be discussed in Section 3, is the simplest incarnation of this idea. By enlarging and modifying the category of $\mathbb{Q}$-varieties under discussion, one gets variants of GT (which might be equal to GT) reflecting more and more arithmetic of the rational numbers.
2.1 abelian actions

Let us first explain what we mean by action on geometry by means of an example. We clearly don’t have in mind the natural action by definition of $\text{Gal}_Q$ on the algebraic closure $Q^{\text{alg}}$ of $Q$. This action is tautological and cannot serve to clarify the structure of $\text{Gal}_Q$.

But $\text{Gal}_Q$ also acts on the multiplicative group $G_m$, a $Q$-variety, and moreover respects the group structure. Consequently, the tower of ‘multiplication by $n$ maps’

$\xymatrix{ G_m \ar[d] \ar[r] & \langle \zeta_n \rangle \ar[d] \\
G_m \ar[r] & \mathbb{Z}^*}$

yields a compatible action of $\text{Gal}_Q$ on the kernels, the groups $\mu_n = \langle \zeta_n \rangle$ of $n$th roots of unity. At first sight, roots of unity might belong to the world of $Q^{\text{alg}}$ that we just have rejected, but we may also canonically identify $\mu_n$ with a group of covering automorphisms, which is clearly a geometric group. We deduce an abelian representation $\text{Gal}_Q \rightarrow \text{Aut}(\mu_n)$; altogether we have a geometric description of the cyclotomic character $\chi_{\text{cycl}} : \text{Gal}_Q \rightarrow \mathbb{Z}^*$.

We understand the abelian part of $\text{Gal}_Q$ by Class Field Theory, which is the main achievement of abelian mathematics in number theory. The result concerning the tower of $G_m$ is the following:

**Theorem 1 (Kronecker–Weber).** The cyclotomic character identifies the maximal abelian quotient $(\text{Gal}_Q)^{\text{ab}}$ of the absolute Galois group of the rationals with $\mathbb{Z}^*$. The corresponding maximal abelian extension $Q^{\text{ab}}$ coincides with the maximal cyclotomic extension $Q(\bigcup_n \zeta_n)$.

2.2 nonabelian actions

We called the cyclotomic character an abelian representation. Here the nonabelian counterparts are not the representations of higher rank, i.e., $\ell$-adic representations $\text{Gal}_Q \rightarrow \text{GL}_n(\mathbb{Z}_\ell)$, which generalize the example with the multiplicative group to other (systems of finite) abelian group schemes and still exploit the group structure of the geometric object. For us the nonabelian representations are Galois actions on nonabelian groups.

Due to the absence of real paths in the context of algebraic varieties (over $Q^{\text{alg}}$) Grothendieck generalized the concept of a fundamental group by the algebraic equivalent of the theory of covers. The (étale) fundamental group $\pi_1^{\text{alg}}$ of a connected variety is defined as the pro-finite group of automorphisms of the tower of all finite étale covers, see [SGA 1] Exp. V.

Thus a variety $X/Q$ defined over the rationals leads to a $\text{Gal}_Q$-action on the fundamental group $\pi_1^{\text{alg}}(X \otimes Q^{\text{alg}})$ of the corresponding geometric variety, the base change $X \otimes Q^{\text{alg}}$, just because the Galois group acts on the latter and $\pi_1^{\text{alg}}$ is a functor. Note that although $X$ is defined with equations using coefficients from $Q$, the action however will most likely be non trivial as the definition of covers may require non-rational algebraic numbers.

The tower of $G_m$‘s discussed above can be identified with the tower of unramified covers of $G_m \otimes Q^{\text{alg}}$ and as $\pi_1^{\text{alg}}(G_m \otimes Q^{\text{alg}}) = \mathbb{Z}$ we recover again the cyclotomic character

$\chi_{\text{cycl}} : \text{Gal}_Q \rightarrow \text{Aut}(\pi_1^{\text{alg}}(G_m \otimes Q^{\text{alg}})) = \mathbb{Z}^*$.

In the nonabelian case we need to be more precise. The functor $\pi_1^{\text{alg}}$ actually depends on a pair of a space together with a base point. If we want to neglect the base point we pay the price by knowing everything only up to inner automorphisms. We deduce as nonabelian actions homomorphisms

$\text{Gal}_Q \rightarrow \text{Out}(\pi_1^{\text{alg}}(X \otimes Q^{\text{alg}})),$
where $\text{Out} = \text{Aut}/\text{Inn}$ is the group of outer automorphisms. We call such a map an exterior representation. The first example of a curve with nonabelian fundamental group is certainly

$$\mathbb{P}^1 - \{0, 1, \infty\}.$$  

Its collection of étale covers was proven to be very rich.

**Theorem 2 (Belyi [Be79]).** (a) A proper smooth curve $X/\mathbb{C}$, i.e., a compact Riemann surface, is defined over $\mathbb{Q}^{\text{alg}}$ if and only if there exists a map $\beta : X \to \mathbb{P}^1_k$ with ramification at most above $0, 1, \infty$. (b) The exterior representation $\text{Gal}_{\mathbb{Q}} \hookrightarrow \text{Out}(\pi_1^{\text{alg}}(\mathbb{P}^1_{\mathbb{Q}^{\text{alg}}}/\{0, 1, \infty\}))$ is faithful (meaning the homomorphism is injective).

A map $\beta$ as in (a) is called a Belyi map. Let us deduce (b) from (a). By (a) the elliptic curve $E_j$ with $j$-invariant $j \in \mathbb{Q}^{\text{alg}}$ is the (canonical) smooth compactification of a finite étale cover of the three punctured projective line. If $\sigma \in \text{Gal}_{\mathbb{Q}}$ belongs to the kernel of the map in (b) then $E_{\sigma(j)}$ is isomorphic to $E_j$, whence $\sigma(j) = j$ for all $j$ and so (b) follows from (a).

Because the nonabelian Galois action on $\pi_1^{\text{alg}}(\mathbb{P}^1_{\mathbb{Q}^{\text{alg}}}/\{0, 1, \infty\})$ is faithful we consequently want to know the structure of the latter group. The structure is determined in two steps. First, by a result of Grauert–Remmert/Grothendieck [SGA 1] Exp. XII Thm 5.1, namely GAGA for finite étale covers, finite analytic étale covers of an algebraic variety over $\mathbb{C}$ is faithful (meaning the homomorphism is injective). Thus the algebraic fundamental group coincides via analytification $(X \to X^{\text{an}})$ with the pro-finite completion of the traditional topological fundamental group.

Secondly, at least in characteristic 0, the algebraic fundamental group behaves geometrically and does not change under base change of algebraically closed fields, see [SGA 1] Exp. X Cor 1.8 (the proof for the proper case given there works also in general if the characteristic is 0). Both isomorphisms taken together imply isomorphisms

$$\pi_1^{\text{top}}(X^{\text{an}}) \cong \pi_1^{\text{alg}}(X \otimes \mathbb{C}) \cong \pi_1^{\text{alg}}(X \otimes \mathbb{Q}^{\text{alg}}).$$

Hence, $\pi_1^{\text{alg}}(\mathbb{P}^1_{\mathbb{Q}^{\text{alg}}}/\{0, 1, \infty\})$ is a free pro-finite group $\hat{F}_2$ on two generators $x, y$, or more symmetrically, three generators $x, y, z$ modulo the relation $xyz = 1$. The elements $x, y, z$ are loops/inertia generators at 0, 1, $\infty$ respectively. Therefore Belyi’s Theorem above states that $\text{Gal}_{\mathbb{Q}}$ acts faithfully on a group as ‘easy’ as $\hat{F}_2$.

### 2.3 dessin d’enfant — children’s drawings

The part of Belyi’s Theorem that we proved above actually only exploits the action of $\text{Gal}_{\mathbb{Q}}$ on the set of isomorphy classes of finite étale covers of the three punctured projective line. A combinatorial description of these isomorphy classes is obtained through the notion of a dessin d’enfant, see [Gr84].

**Definition 3.** A dessin d’enfant is a CW-structure on a compact, oriented, topological surface together with a bipartite structure, such that attaching maps of 2-cells are covering maps over the interior of 1-cells. A bipartite structure here means that the set of vertices (the 0-skeleton) is labeled with labels from $\{0, 1\}$ such that each attaching map of a 1-cell hits vertices of both labels. Isomorphisms of dessins are defined as cellular homeomorphisms of the underlying surface.

The name dessin d’enfant, or dessin for short, stems from the fact that such an object is encoded in the graph on the surface formed by the 1-skeleton: its shape may happen to resemble the masterpieces of our childhood. The picture on the right gives an example of a dessin on the Riemann sphere with black and white vertices corresponding to those labeled 0 and 1 respectively.

To a Belyi map $\beta : X \to \mathbb{P}^1$ we associate the dessin formed by the graph $\beta^{-1}(\{0, 1, \infty\})$ on the topological surface underlying $X^{\text{an}}$. The bipartite structure is given by labeling a vertex $v \in \beta^{-1}(\{0, 1\})$ by $\beta(v)$. One easily checks that this construction identifies isomorphism classes of étale covers of $\mathbb{P}^1 - \{0, 1, \infty\}$ with isomorphism classes of dessins.
The combinatorial description of covers by dessins allows for a more combinatorial analysis of the respective Galois action. The Galois action preserves certain invariants of the dessin: the genus of the surface, the degree = number of 1-cells, the valency list = ramification indices above 0, 1 and ∞ respectively. At least conjecturally this is only the tip of an iceberg of combinatorial invariants that describe Galois orbits of Gal$_Q$ acting on isomorphy classes of dessins.

At least we know that Gal$_Q$ acts continuously on the finite sets of isomorphy classes of dessins with fixed genus, degree and valency list. Thus there are number fields corresponding to the stabilizers of this action that are mysteriously attached to the combinatorial data of each dessin d’enfant. A nontrivial result in the spirit of the above discussion is the following (see [Za00] for the definition of the dessin called ‘Leila flowers’).

**Theorem 4 (Zapponi [Za00]).** A generalization of the Kochetkov Conjecture is true, in particular: The 24 ‘Leila flowers’ of type $a < b < c < d < e$ form at least two Galois orbits if $abcde(a + b + c + d + e)$ is a square $\in \mathbb{Q}$.

The proof uses Strebel differentials (quadratic differentials) and a stratification of the decorated moduli space following Kontsevich and Penner. Recently, in his Diplomarbeit, Ronkine obtained the following higher dimensional analogue of Belyi’s Theorem.

**Theorem 5 (Ronkine [Ro03]).** Let $X/\mathbb{C}$ be a smooth, proper surface of general type. Then the birational class of $X$ is defined over $\mathbb{Q}_{\text{alg}}$ if and only if there exists an $X’$ birational to $X$ and a map $\gamma : X’ \to \mathbb{P}^1$ of relative dimension 1 with singular locus at most over $\{0, 1, \infty\}$ and either $\gamma$ truly varying or all nonsingular fibres of $\gamma$ are defined over $\mathbb{Q}_{\text{alg}}$.

From Ronkine’s Theorem we deduce that Gal$_Q$ acts continuously on the finite set (Geometric Shafarevich Conjecture) of truly varying, smooth, proper curves of genus $g \geq 2$ parametrized by $\mathbb{P}^1_{\mathbb{C}} - \{0, 1, \infty\}$. To have a higher dimensional analogue of dessins would be desirable.

### 3 Grothendieck–Teichmüller theory

So far we have neglected that the category of covers is governed by a group, the algebraic fundamental group. Instead of only exploiting the action on isomorphy classes we now study what the Galois action does with the group structure.

#### 3.1 the group $\hat{\Gamma}_T$

In some sense the Galois action is local. It respects inertia groups of boundary components (cusps) and, moreover, acts cyclotomically on inertia generators up to conjugation. Recall that we identified $\pi^\text{alg}_1(\mathbb{P}^1 - \{0, 1, \infty\})$ with the pro-finite free group $\hat{\mathbb{F}}_2$ on generators $x, y$. For $f \in \hat{\mathbb{Z}}$ and $f \in \hat{\mathbb{F}}_2$ let $\varphi_{\lambda, f}$ be the following endomorphism of $\hat{\mathbb{F}}_2$:

$$
\varphi_{\lambda, f} : = \left\{ \begin{array}{c}
x \mapsto x^\lambda \\
y \mapsto f^{-1}y^\lambda f.
\end{array} \right.
$$

Deligne’s method of tangential base points (see [De89]) lifts the exterior Galois representation from Belyi’s theorem to an injective homomorphism

$$
\text{Gal}_Q \hookrightarrow \text{Aut}(\hat{\mathbb{F}}_2)
$$

mapping $\sigma$ to $\varphi_{\lambda, f_\sigma}$ where $\lambda(\sigma) = \chi^{\text{cycl}}(\sigma)$ is the cyclotomic character and $f_\sigma$ is a uniquely determined element from the commutator subgroup $\hat{\mathbb{F}}'_2$ of $\hat{\mathbb{F}}_2$. Following Drinfel’d [Dr90] and Ihara [Ih90], and in fact using results of Lochak–Schneeps [LS97], we define the pro-finite Grothendieck–Teichmüller group (unhistorically) as

$$
\hat{\Gamma}_T = \left\{ (\lambda, f) \in \hat{\mathbb{Z}}^* \times \hat{\mathbb{F}}'_2 \mid \text{I, II, III and } \varphi_{\lambda, f} \in \text{Aut}(\hat{\mathbb{F}}_2) \right\}
$$
Here \( \theta \) and \( \omega \) (resp. \( \rho \)) are certain automorphisms of \( \hat{\mathbb{F}}_2 \) (resp. \( \hat{\mathbb{F}}_{0.5} \)), see [LS97]. The original defining equations differ but are equivalent to the above I, II, III. Note that the group structure on \( \hat{GT} \) is not induced from the product \( \hat{\mathbb{Z}}^* \times \hat{\mathbb{F}}_2 \) but stems from composition of \( \varphi_{\lambda,f} \) within \( \text{Aut}(\hat{\mathbb{F}}_2) \). Let us mention that it is by no means obvious but nevertheless true that \( \hat{GT} \) is actually a pro-finite group.

The theme of GT was discovered by different people from different perspectives. For example Drinfel’d was led to consider a pro-algebraic version of GT over a field \( k \) when studying the universal way to deform associativity and braiding in a quasi-associative, quasi-braided tensor category, see [Dr90]. To summarize the above we note the following theorem.

**Theorem 6 (Drinfel’d [Dr90], Ihara [Ih90]; Deligne [De89]).** We have injective group homomorphisms \( \text{Gal}_\mathbb{Q} \hookrightarrow \hat{GT} \subset \text{Aut}(\hat{\mathbb{F}}_2) \) that map \( \sigma \) to \( (\lambda_\sigma,f_\sigma) \) and thus yield a parametrization of the set of elements of \( \text{Gal}_\mathbb{Q} \) by an invertible element of \( \hat{\mathbb{Z}} \) and a pro-word in the letters \( x,y \) from the commutator subgroup \( \hat{\mathbb{F}}_2 \).

### 3.2 moduli of curves

Let \( \mathcal{M}_{g,n} \) be the moduli space of smooth proper curves of genus \( g \) with \( n \) ordered marked points. The double ratio defines an isomorphism \( \mathcal{M}_{0,4} = \mathbb{P}^1 \setminus \{0,1,\infty\} \) that ultimately will lead us to a change in perspective. First of all note that \( \pi_1^{\text{alg}}(\mathcal{M}_{g,n} \otimes \mathbb{Q}^{\text{alg}}) = \hat{\Gamma}_{g,n} \) is the pro-finite completion of the mapping class group. Here \( \pi_1^{\text{alg}}(\mathcal{M}_{g,n}) \) is the fundamental group in the sense of algebraic stacks (orbifold-\( \pi_1 \)). The group \( \hat{\Gamma}_{g,n} \) inherits a nonabelian action by \( \text{Gal}_\mathbb{Q} \) in the usual way by functoriality.

It was observed by Lochak and Schneps that symmetries of the moduli spaces for small values of \( (g,n) \) explain the nature of the equations that define \( \hat{GT} \). More precisely, I and II is the shadow of the natural \( S_3 \) action permuting the cusps of \( \mathcal{M}_{0,4} \), and the cyclic permutation action of cusps of \( \mathcal{M}_{0,5} \) is responsible for equation III according to the following theorem.

**Theorem 7 (Lochak–Schneps [LS97]).** The equations I, II, III are nonabelian cocycle equations. The corresponding nonabelian cohomology classes have natural representatives that lead to parameterizations of pairs \( (\lambda,f) \) that belong to \( \hat{GT} \).

Underlying these efforts is the hope to arrive at a combinatorial description of \( \text{Gal}_\mathbb{Q} \), resp. its image in \( \hat{GT} \), from geometric Galois theory. By imposing correct additional constraints one desires to get hold of a variant of GT that actually coincides with \( \text{Gal}_\mathbb{Q} \).

### 3.3 actions on towers

Let \( \mathcal{V} \) be a category of smooth varieties over \( \mathbb{Q} \). We define a generalized Grothendieck–Teichmüller group to be the pro-finite group of local automorphisms of the functor \( \pi_1^{\text{alg}} \) restricted to \( \mathcal{V}_{\text{alg}} \) that is the category of base changes \( X \otimes \mathbb{Q}^{\text{alg}} \) of varieties from \( \mathcal{V} \) and maps defined over \( \mathbb{Q} \).

\[
\hat{\text{GT}}_{\mathcal{V}} := \text{Aut} \left( \pi_1^{\text{alg}} : \mathcal{V}_{\text{alg}} \to (\text{groups}) \right)
\]

Here automorphisms of the functor are invertible natural transformations up to inner automorphisms. Locality refers to cyclotomic action up to conjugation on inertia subgroups coming from boundary components of natural compactifications. The natural nonabelian action of \( \text{Gal}_\mathbb{Q} \) is compatible with \( \mathbb{Q} \)-rational maps of \( \mathbb{Q} \)-varieties and thus induces a natural homomorphism \( \text{Gal}_\mathbb{Q} \to \hat{\text{GT}}_{\mathcal{V}} \).
A particular choice of \( \mathcal{V} \) is the ‘genus 0 Teichmüller tower’ (together with the compactifications by stable curves)

\[
\mathcal{T}_0 := \left\{ \mathcal{M}_{0,n} \mid n \geq 4, \ S_n\text{-action on } \mathcal{M}_{0,n}, \text{ forgetful maps } \mathcal{M}_{0,n+1} \to \mathcal{M}_{0,n} \right\}.
\]

By the following theorem we recover the classical pro-finite Grothendieck–Teichmüller group in this generalized setting.

**Theorem 8 (Drinfel’d, Ihara, Harbater–Schneps [HS00]).** There exists a natural isomorphism

\[
\hat{\mathcal{GT}}_{\mathcal{T}_0} = \hat{\mathcal{GT}}.
\]

The full Teichmüller tower consists of

\[
\mathcal{T} := \left\{ \mathcal{M}_{g,n} \mid 2 - 2g - n < 0, \ \text{Aut}(\mathcal{M}_{g,n}), \text{ forgetful maps } \mathcal{M}_{g,n+1} \to \mathcal{M}_{g,n} \right\}
\]

(again with compactifications by stable curves). On the corresponding generalized \( \hat{\mathcal{GT}} \) we have the following theorem.

**Theorem 9 (Hatcher–Lochak–Schneps [HLS00], Nakamura–Schneps [NS00]).** There is an equation \( IV \) from \( \mathcal{M}_{1,2} \) that leads to the group \( \hat{\mathcal{GT}}_{\text{new}} \) of elements in \( \hat{\mathcal{GT}} \) that satisfy equation \( IV \).

The new group acts on the algebraic fundamental groups of the full Teichmüller tower \( \mathcal{T} \) in a natural way such that its image contains the Galois action:

\[
\text{Gal}_\mathbb{Q} \subseteq \hat{\mathcal{GT}}_{\text{new}} \subseteq \hat{\mathcal{GT}}_{\mathcal{T}}.
\]

It has been announced that \( \hat{\mathcal{GT}}_{\text{new}} \) equals \( \hat{\mathcal{GT}}_{\mathcal{T}} \), but it is not known whether the other inclusion in Theorem 9 is in fact an isomorphism or a strict inclusion. The proof uses the curve complex of Hatcher–Thurston. This complex being simply connected allows us to detect sets of equations that generate all equations that an action on the algebraic fundamental groups of the full Teichmüller tower have to verify.

What is more, the above theorem is in accordance with Grothendieck’s ‘first two level philosophy’. The ‘first two level philosophy’ predicts that generators for \( \hat{\mathcal{GT}}_{\mathcal{T}} \) come from cases of modular dimension \( 3g - 3 + n \) equal to 1, namely \( \mathcal{M}_{0,4} \) and \( \mathcal{M}_{1,1} \), whereas equations are generated by equations of origin in modular dimension 2, namely \( \mathcal{M}_{0,5} \) and \( \mathcal{M}_{1,2} \).

### 3.4 arithmetic in \( \hat{\mathcal{GT}} \)

Still the guiding question is the following. How close is actually \( \text{Gal}_\mathbb{Q} \) to \( \hat{\mathcal{GT}} \)? One way to decide whether both groups don’t coincide consists of disproving group-theoretic properties of \( \text{Gal}_\mathbb{Q} \) for \( \hat{\mathcal{GT}} \).

What is more, \( \text{Gal}_\mathbb{Q} \) is not just a group, it is the group of arithmetic of integers. As arithmetic content of \( \text{Gal}_\mathbb{Q} \) itself we can consider the family of (conjugacy classes of) decomposition subgroups \( \text{Gal}_\mathbb{Q}_p \) (resp. \( \text{Gal}_\mathbb{Q} \)) of \( \text{Gal}_\mathbb{Q} \) that are parametrized by the finite (resp. infinite) places of \( \mathbb{Q} \). These decomposition subgroups are canonically isomorphic to the absolute Galois groups of the completion of \( \mathbb{Q} \) at the respective places. It is an important result of F.K. Schmidt and Neukirch, that these decomposition subgroups are group-theoretically characteristic among the set of all closed subgroups. Now, if \( \hat{\mathcal{GT}} \) coincides or at least is close to \( \text{Gal}_\mathbb{Q} \), then we should be able to describe arithmetic in \( \hat{\mathcal{GT}} \) by geometric Galois theory.

Here arithmetic in \( \hat{\mathcal{GT}} \) means conjugacy classes of subgroups related to a place of \( \mathbb{Q} \).

Let us reconsider how we received our knowledge of the group theoretic structure of \( \pi_1^{\text{alg}}(\mathbb{P}^1_{\mathbb{Q}\text{alg}} - \{0,1,\infty\}) \). We used \( \mathcal{C} \)-analytic methods and knowledge about the topological fundamental group, which could as well be considered as the \( \mathcal{C} \)-analytic \( \pi_1 \). This kind of geometry is certainly related to the infinite place of \( \mathbb{Q} \). So we are led to think that the various places of \( \mathbb{Q} \) should lead to arithmetic within \( \hat{\mathcal{GT}} \) through the different ways to complete \( \mathbb{Q} \) and then do analysis.
Let us check for the infinite place whether we can detect arithmetic in $\hat{\Gamma}$. We have inclusions
$$\Gamma_{0,4}^{\text{top}} := \pi_{1}^{\text{top}}(\mathcal{M}_{0,4}) \subset \pi_{1}^{\text{alg}}(\mathcal{M}_{0,4}) = \hat{\Gamma}_{0,4},$$
and a compatible nonabelian action
$$\text{Gal}_{k} \to \text{Out}(\Gamma_{0,4}^{\text{top}})$$
of the subgroup $\text{Gal}_{k} \subset \text{Gal}_{\mathbb{Q}}$. Let $\text{Out}(\Gamma_{0,4}^{\text{top}})$ be the closure of the image under the canonical map $\text{Out}(\Gamma_{0,4}^{\text{top}}) \to \text{Out}(\hat{\Gamma}_{0,4})$ induced by pro-finite completion. Then we have the following theorem.

**Theorem 10 (André [An03] Thm 3.3.1).**

The intersection $\text{Out}(\Gamma_{0,4}^{\text{top}}) \cap \text{Gal}_{\mathbb{Q}}$ inside $\text{Out}(\hat{\Gamma}_{0,4})$ coincides with $\text{Gal}_{k}$.

The theorem suggests that under the canonical map $\hat{\Gamma} \to \text{Out}(\hat{\Gamma}_{0,4})$ the preimage of $\text{Out}(\Gamma_{0,4}^{\text{top}})$ reflects the arithmetic at the infinite place.

For analysis at $p$ we chose to do $\mathbb{C}_{p}$-analytic geometry in the sense of Berkovich. But what is the right fundamental group here to replace the question mark in the following table:

- infinite place: completion $\mathbb{R} \leftrightarrow \mathbb{C}$-analytic: $\pi_{1}^{\text{top}}$
- finite place $p$: completion $\mathbb{Q}_{p} \leftrightarrow \mathbb{C}_{p}$-analytic (Berkovich): ?

### 3.5 the tempered fundamental group

Let $X$ be a variety over $\mathbb{Q}$. For a fixed isomorphism of fields $\mathbb{C} \cong \mathbb{C}_{p}$, André defines the **tempered** $\pi_{1}$ of the Berkovich-$\mathbb{C}_{p}$-analytic space $X \otimes \mathbb{C}_{p}$, a topological group together with a homomorphism
$$\pi_{1}^{\text{temp}}(X \otimes \mathbb{C}_{p}) \to \pi_{1}^{\text{alg}}(X \otimes \mathbb{Q}_{p}),$$
that identifies $\pi_{1}^{\text{alg}}$ with the pro-finite completion of $\pi_{1}^{\text{temp}}$. The tempered fundamental group classifies ‘topological by étale’ $\mathbb{C}_{p}$-analytic covers. In a sense, it catches reduction behaviour of covers mod $p$. Namely for an elliptic curve $E/\mathbb{Q}$ we can compute the tempered fundamental group of the underlying $\mathbb{C}_{p}$-analytic space as follows.

$$\pi_{1}^{\text{temp}}(E \otimes \mathbb{C}_{p}) = \begin{cases} \hat{\mathbb{Z}} \times \hat{\mathbb{Z}} & E \text{ good at } p \\ \mathbb{Z} \times \hat{\mathbb{Z}} & E \text{ bad at } p \end{cases}$$

The definition of the tempered fundamental group arose from the study of $p$-adic differential equations. But it also serves for the following analogue of Theorem 10. Let $\text{Out}(\Gamma_{0,4}^{\text{temp}})$ be the closure of the image under the canonical map $\text{Out}(\Gamma_{0,4}^{\text{temp}}) \to \text{Out}(\hat{\Gamma}_{0,4})$ induced by pro-finite completion.

**Theorem 11 (André [An03] Thm 7.2.1).**

The intersection $\text{Out}(\Gamma_{0,4}^{\text{temp}}) \cap \text{Gal}_{\mathbb{Q}}$ inside $\text{Out}(\hat{\Gamma}_{0,4})$ coincides with $\text{Gal}_{\mathbb{Q}_{p}}$.

If we moreover define tempered analogues of the generalized Grothendieck–Teichmüller groups associated to a category $\mathcal{V}$ of $\mathbb{Q}$-varieties by

$$\text{GT}_{\mathcal{V}}^{\text{temp}} := \text{Aut} \left( \pi_{1}^{\text{alg}} : \mathcal{V}_{p} \to \text{(groups)} \right) \text{ preserving inertia}$$

and let $\hat{\text{GT}}_{p}$ be the closure of image of $\text{GT}_{\mathcal{V}}^{\text{temp}} \to \hat{\text{GT}}_{\mathcal{V}}$, then we obtain more precisely the following result.

**Theorem 12 (André [An03] Thm 8.7.1).** $\text{Gal}_{\mathbb{Q}_{p}} = \hat{\text{GT}}_{p} \cap \text{Gal}_{\mathbb{Q}} \subset \hat{\text{GT}}.$

Hence, we are also able to detect arithmetic at a finite prime within the Grothendieck–Teichmüller group.
4 Anabelian geometry

Anabelian geometry deals with the geometry encoded in the algebraic fundamental group of a variety, as well as the arithmetic encoded in the corresponding outer Galois representations. To my knowledge, the following conjecture of anabelian nature was first raised as a question by Ihara and later given the status of a conjecture by Oda–Matsumoto. It is now a theorem by Pop which relies on birational anabelian results, but remains unpublished to date.

**Theorem 13 (Pop).** The Ihara/Oda–Matsumoto Conjecture holds. Namely, let $\mathcal{V}$ be the category of all smooth varieties over $\mathbb{Q}$. Then $\text{Gal}_{\mathbb{Q}} \to \hat{\text{GT}}_{\mathcal{V}}$ is an isomorphism.

A direct consequence of Andrè’s studies of the tempered fundamental group leads to the following local version of the conjecture.

**Theorem 14 (Andrè [An03] thm 9.2.2).** Let $\mathcal{V}$ be the category of all smooth varieties over $\mathbb{Q}$ as above. Then $\text{Gal}_{\mathbb{Q}_p} \to \text{GT}^\text{temp}_{\mathcal{V}}$ is an isomorphism.

One may think of these two theorems as astonishing facts because they claim to give an alternative, non tautological description of the absolute Galois group of the rationals together with its arithmetic. However, first of all the category $\mathcal{V}$ above is too large to lead to anything manageable. And secondly, to give the list of varieties in $\mathcal{V}$ one still needs to write down equations with rational numbers. Nevertheless, the results guides us to look for interesting $\mathcal{V}$ that allow for a concrete combinatorial/geometric/group theoretical description of $\text{GT}_{\mathcal{V}}$ and thus $\text{Gal}_{\mathbb{Q}}$. According to Pop, in his approach it is even possible to work with complements of rational hyperplane arrangements on $\mathbb{P}^2$. He then uses Ronkine’s theorem (Theorem 5) combined with a clever covering trick to give, in principle, a complex analytic description of the corresponding $\hat{\text{GT}}_{\mathcal{V}}$. The use of rational numbers to describe $\text{Gal}_{\mathbb{Q}}$ has disappeared!

The anabelian methods of Pop yield even stronger results: it is sufficient to work with pro-$\ell$ completions for a fixed prime $\ell$.

4.1 birational pro-$\ell$ anabelian geometry

In birational anabelian geometry one deals with absolute Galois groups of function fields. A major breakthrough in anabelian geometry towards Grothendieck’s conjectures in the field was achieved by Pop in the ‘90s. Let $K^{\text{ins}}$ denote the pure inseparable closures of a field (in particular $K^{\text{ins}} = K$ if the characteristic is 0), and let $\text{Isom}^i$ denote isomorphisms of perfect fields up to powers of the Frobenius automorphism (again, if the characteristic is 0 disregard the $^i$).

**Theorem 15 (Pop [Po94]).** Let $K, L$ be infinite, finitely generated fields. Then the natural map

$$\text{Isom}^i(L^{\text{ins}}, K^{\text{ins}}) \to \text{Isom}^\text{out}(\text{Gal}_K, \text{Gal}_L)$$

is a bijection.

The birational pro-$\ell$ anabelian conjecture asks for a stronger and more geometric result about pro-$\ell$ completed absolute Galois groups $\text{Gal}_K^\wedge\ell$. Let $k$ be an algebraically closed field and $\ell$ a prime different from the characteristic. Then the conjecture claims the following.

**Conjecture 16.** Let $K/k, L/k$ be function fields of transcendence degree exceeding 1. Then the natural map

$$\text{Isom}^i(L^{\text{ins}}, K^{\text{ins}}) \to \text{Isom}^\text{out}(\text{Gal}_K^\wedge\ell, \text{Gal}_L^\wedge\ell)$$

is a bijection.

This conjecture goes back to Bogomolov and there are already some articles devoted to it. The claim of the conjecture includes in particular the case of $k = \mathbb{C}$, hence a question of complex analysis rather than arithmetic geometry!
4.2 anabelian phenomena over $\mathbb{F}_p^{\text{alg}}$

So far there has been progress on the conjecture above only in the case of $k$ being the algebraic closure of a finite field. In this case, recently there have been given proofs by Bogomolov–Tschinkel for the case of transcendence degree 2 and some further assumptions, and by Pop in the general case (again $k = \mathbb{F}_p^{\text{alg}}$).

**Theorem 17 (Bogomolov–Tschinkel [BT03]; Pop [Po03]).** Let $k$ be the algebraic closure of a finite field of characteristic different from $\ell$. Let $K/k, L/k$ be function fields of transcendence degree exceeding 1. Then the natural map

$$\text{Isom}^i(L^{\text{ins}}, K^{\text{ins}}) \to \text{Isom}^{\text{out}}(\text{Gal}_K^{\text{pr}}), \text{Gal}_L^{\text{pr}})$$

is a bijection.

For a detailed and carefully written survey see the Bourbaki talk by Szamuely [Sz03]. An important step in the proof consists in the treatment of the local theory. Here one also has results by Ware, Efrat, Efrat-Fesenko, and Koenigsmann.

Let us now turn to more geometric anabelian phenomena. If we replace the absolute Galois group of the function field of a variety by the algebraic fundamental group of the variety itself, then we get a relatively small quotient that nevertheless still contains room for anabelian geometry.

Let us consider smooth proper curves over an algebraically closed field. In characteristic 0 the respective fundamental group is isomorphic to the pro-finite completion of the topological fundamental group of the corresponding Riemann surface. Hence it does not vary in geometric fibres of a connected family. However, when the characteristic is positive, some covers cease to exist and it turns out that the fundamental group is a very subtle invariant.

**Theorem 18 (Raynaud [Ra02], Pop/Saïdi [PS03], Tamagawa [Ta04]).** Let $\pi$ be a pro-finite group not isomorphic to $\hat{\mathbb{Z}}_p \times \prod_{\ell \neq p} \hat{\mathbb{Z}}_{\ell^2}$ for any prime $p$. Then there are only finitely many isomorphy classes of smooth projective curves of genus $g$ over the algebraic closure of a finite field whose algebraic fundamental group is isomorphic to the given $\pi$.

The exceptions correspond to the infinity of ordinary elliptic curves over the algebraic closure of $\mathbb{F}_p$.

All three articles cited above for this theorem contain an abundant wealth of beautiful mathematics. They first of all exploit Raynaud’s $\Theta$-divisor in the Jacobian of the curve and how this divisor behaves in families. The central idea is to compare the number of elementary abelian $p$ covers of cyclic prime to $p$ covers of the curve. This number is encoded in the group theory of the fundamental group. When this number is maximal we call the cyclic cover new-ordinary and this property is obstructed by torsion points on $\Theta$. This leads to general questions of torsion points on divisors of abelian varieties and thus to other ingredients: a generalized Anderson-Indik theorem and Hrushovski’s theorem on relative Mordell-Lang. To get this setup up and running in the general case, delicate studies of families of abelian varieties are necessary. Among the interesting things proven along the way there is a ‘new-Torelli theorem’ (Tamagawa [Ta04]) stating that a family of curves is trivial if and only if a certain family of generalized Prym-varieties is trivial.

4.3 anabelian curves: with Galois action

Of course, we conjecture not only finiteness in Theorem 18 but that the sets of $\mathbb{F}_p^{\text{alg}}$ points of $\mathcal{M}_g$ with fixed prescribed fundamental group coincide with the orbits under Frobenius. This is obviously the strongest form possible. So far, to get uniqueness up to Frobenius we have to exploit arithmetic of Galois action and, unfortunately, also restrict to non-constant curves.

Following earlier results due to Tamagawa for affine, hyperbolic curves over finite fields, and fields finitely generated over $\mathbb{Q}$, see [Ta97], and then soon afterwards by Mochizuki for hyperbolic curves over sub-$p$-adic fields, see [Mz99a], we have also the following theorem.
Theorem 19 (Stix [Sx02]). Let $k$ be an infinite but finitely generated field of positive characteristic $p$. Let $X$ and $X'$ be smooth, hyperbolic (i.e., with negative Euler characteristic) curves over $k$, such that and $X \otimes k_{alg}$ is not defined over $F_p$. Then the following holds.

1. $X$ and $X'$ have isomorphic exterior Galois representations on $\pi_{1, alg}$ if and only if there is a purely inseparable map $X' \rightarrow X$ (or vice versa).

2. The canonical map $\text{Aut}_k(X) \rightarrow \text{Out}_{\text{Gal}_k(\pi_{1, alg}(X \otimes k_{alg}))}$ is an isomorphism of finite groups.

References


[De89] Deligne, P., Le groupe fondamental de la droite projective moins trois points, in: Galois groups over $\mathbb{Q}$, Publ. MSRI 16 (1989), 79–298.


Grothendieck–Teichmüller Theory and Galois Theory over $\mathbb{Q}$


Grothendieck–Teichmüller Theory and Galois Theory over $\mathbb{Q}$


