THE GROTHENDIECK-TEICHMÜLLER GROUP OF $\text{PSL}(2,q)$

PIERRE GUILLOT

Abstract. We show that the Grothendieck-Teichmüller group of $\text{PSL}(2,q)$, or more precisely the group $\mathcal{GT}(\text{PSL}(2,q))$ as previously defined by the author, is the product of an elementary abelian 2-group and several copies of the dihedral group of order 8. Moreover, when $q$ is even, we show that it is trivial.

We explain how it follows that the moduli field of any “dessin d’enfant” whose monodromy group is $\text{PSL}(2,q)$ has derived length $\leq 3$.

This paper can serve as an introduction to the general results on the Grothendieck-Teichmüller group of finite groups obtained by the author.

1. Introduction & Statement of results

In [Gui], we have introduced the Grothendieck-Teichmüller group of a finite group $G$, denoted $\mathcal{GT}(G)$. Motivation for the study of this group stems from the theory of dessins d’enfants. Recall that a dessin is essentially a bipartite graph embedded on a compact, oriented surface (without boundary), and that the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on (isomorphism classes of) dessins. As explained in loc. cit., there is an action of $\mathcal{GT}(G)$ on those dessins whose monodromy group is $G$, and the Galois action on the same objects factors via a map $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathcal{GT}(G)$.

Motivation for the study of all groups $\mathcal{GT}(G)$, for all groups $G$, is increased by the fact that the combined map $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathcal{GT} := \lim_{G} \mathcal{GT}(G)$ is injective.

The group $\mathcal{GT}(G)$ possesses a normal subgroup $\mathcal{GT}_{1}(G)$, which is such that the quotient $\mathcal{GT}(G)/\mathcal{GT}_{1}(G)$ is abelian. It follows that the commutator subgroup of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ maps into $\mathcal{GT}_{1}(G)$, and injects into the inverse limit $\mathcal{GT}_{1}$ formed by these as $G$ varies. There is little mystery left in $\mathcal{GT}(G)/\mathcal{GT}_{1}(G)$ (see [Gui] again), and the challenge is in the computation of $\mathcal{GT}_{1}(G)$.

In this paper we treat the case of $G = \text{PSL}(2,q)$. We obtain the following result.

Theorem 1.1 – The group $\mathcal{GT}_{1}(\text{PSL}(2,2^{s}))$ is trivial for all $s \geq 1$.

The group $\mathcal{GT}_{1}(\text{PSL}(2,q))$, when $q$ is odd, is isomorphic to a product

$$C_{2}^{n_{1}} \times D_{8}^{n_{2}}.$$ 

Here $D_{8}$ is the dihedral group of order 8. Note that this result was observed experimentally for small values of $q$ in [Gui].

This theorem depends crucially on the work of MacBeath in [Mac69], which classifies the triples $(x,y,z)$ in $\text{PSL}(2,q)$ in various ways. Indeed, we feel that the group $\mathcal{GT}_{1}(\text{PSL}(2,q))$ encapsulates part of this information neatly.

Let us give an application to dessins d’enfants. The first part of the next theorem was implicit in [Gui], and indeed it hardly deserves a proof once the statement is properly explained. However, it seems worth spelling it out for emphasis.

Theorem 1.2 – Let $G$ be a finite group. There exists a number field $K$, Galois over $\mathbb{Q}$, such that $\text{Gal}(K/\mathbb{Q})$ is a subgroup of $\mathcal{GT}(G)$, and containing the moduli field of any dessin whose monodromy group is $G$. 

1
For example, suppose that $X$ is a dessin whose monodromy group is $PSL(2, q)$. If $q$ is even, then the moduli field of $X$ is an abelian extension of $\mathbb{Q}$. If $q$ is odd, then the Galois closure $\tilde{F}$ of the moduli field $F$ of $X$ is such that $\text{Gal}(\tilde{F}/\mathbb{Q})$ has derived length $\leq 3$.

A word of explanation. First, when $\Gamma$ is a group we write $\Gamma'$ for the derived (commutator) subgroup, and we say that $\Gamma$ has derived length $\leq 3$ when $\Gamma''$ is trivial. Also, the moduli field of a dessin is the extension $F$ of $\mathbb{Q}$ such that $\text{Gal}(\mathbb{Q}/F)$ is the stabilizer of the isomorphism class of $X$ under the Galois action. Note that if we can write down explicit equations for $X$ with coefficients in the number field $L$, then certainly the moduli field $F$ is a subfield of $L$. While there are subtle counterexamples of dessins for which there are no equations over $F$, it is still intuitively helpful to think of $F$ as the smallest field over which the dessin is defined.

For example in [Gui14], Example 4.6 and Example 4.13, we have examined a certain dessin $X$ (a planar tree), whose monodromy group is the simple group of order 168, that is $PSL(2, 7)$ (or $PSL(3, 2)$, as it is written in loc. cit.). We found explicit equations with coefficients in a field of the form $\mathbb{Q}(\alpha)$ with the minimal polynomial of $\alpha$ having degree 4 (though not all details are provided); if $L$ is the Galois closure of $\mathbb{Q}(\alpha)$, then $\text{Gal}(L/\mathbb{Q})$ is a subgroup of $S_4$, which has derived length 3, confirming the prediction. However, there is even an easier way to see that the moduli field is very simple: there are only two dessins in the Galois orbit of $X$, so the moduli field is in fact a quadratic extension of $\mathbb{Q}$.

It is an open problem to explicitly exhibit a dessin such that $\text{Gal}(\tilde{F}/\mathbb{Q})$ is non-abelian.

The examples treated in this paper are a less technical illustration of the ideas discussed in [Gui], and may serve as an introduction to the latter. Note that, motivation and background aside, it is not necessary to be familiar with [Gui] in order to follow the arguments we present, leading to the computation of $\mathcal{G}T_1(PSL(2, q))$.

2. Definitions

We take a definition of $\mathcal{G}T_1(G)$ which is only suitable when $G$ is non-abelian and simple, such as $G = PSL(2, q)$; see [Gui] for the more general definition.

So let $G$ be such a finite group, and let $\mathcal{T}$ denote the set of triples $(x, y, z) \in G^3$ such that $xyz = 1$ and $(x, y, z) = G$. Further, we let $\mathcal{T}/G$ denote the set of orbits in $\mathcal{T}$ under simultaneous conjugation by an element of $G$. We write $[x, y, z]$ for the class of $(x, y, z)$. (In [Gui] we write $\mathcal{P}$ instead of $\mathcal{T}$, thinking of these elements as pairs $(x, y)$.)

There is a free action of $\text{Out}(G)$, the group of outer automorphisms of $G$, on $\mathcal{T}/G$. Moreover, there is also an action of $S_3$, the symmetric group of degree 3. This is essentially a permutation of the coordinates, but to be more precise, one usually introduces the permutation $\theta$ of $\mathcal{T}/G$ defined by $\theta \cdot [x, y, z] = [y, x, z^x]$, and the permutation $\delta$ defined by $\delta \cdot [x, y, z] = [z, y, x^y]$. These are both well-defined, and square to the identity operation of $\mathcal{T}/G$. There is a homomorphism $S_3 \to S(\mathcal{T}/G)$, where $S(\mathcal{T}/G)$ is the symmetric group of the set $\mathcal{T}/G$, mapping (12) to $\theta$ and (13) to $\delta$.

The two actions described commute, and together define an action of $H := \text{Out}(G) \times S_3$ on $\mathcal{T}/G$.

Let us write $[x, y, z] \equiv [x', y', z']$ when $x$ is a conjugate of $x'$, while $y$ is a conjugate of $y'$, and $z$ is a conjugate of $z'$. This is an equivalence relation on $\mathcal{T}/G$.

The group $\mathcal{G}T_1(G)$ is defined, in this context, to be the subgroup of the symmetric group $S(\mathcal{T}/G)$ comprised by those permutations $\varphi$ which:
• commute with the action of $H$; in other words, if $h \in H$, $t \in \mathcal{I}/G$ then $\varphi(h \cdot t) = h \cdot \varphi(t)$.

• are compatible with $\equiv$; that is, $t \equiv t'$ implies $\varphi(t) \equiv \varphi(t')$, if $t, t' \in \mathcal{I}/G$.

(Somewhat arbitrarily, we write $h \cdot t$ for the action of $h \in H$, and $\varphi(t)$ for the action of $\varphi \in \mathcal{G}_T_1(G)$, in order to set the elements of $\mathcal{G}_T_1(G)$ apart.)

3. Characteristic two

We start by assuming that $q$ is a power of 2, so that $\text{PSL}(2, q) = \text{SL}(2, q)$.

Following MacBeath [Mac69], we partition the set of triples $(x, y, z)$ of elements of $\text{SL}(2, q)$ satisfying $xyz = 1$ into the subsets $E(a, b, c)$, where $a, b, c \in \mathbb{F}_q$, by requiring $(x, y, z) \in E(a, b, c)$ when $\text{Tr}(x) = a$, $\text{Tr}(y) = b$, $\text{Tr}(z) = c$ (here Tr is the trace).

Since elements of $\mathcal{G}_T_1(\text{SL}(2, q))$ are assumed to be compatible with the relation $\equiv$, the following observation is trivially true.

**Lemma 3.1** — **Suppose** $(x, y, z) \in E(a, b, c)$, **with** $(x, y, z) = \text{SL}(2, q)$, **let** $\varphi \in \mathcal{G}_T_1(\text{SL}(2, q))$, **and suppose** that $x', y', z'$ satisfy

$$\varphi([x, y, z]) = [x', y', z']. \quad \Box$$

Then $(x', y', z') \in E(a, b, c)$.

Note that $\text{SL}(2, q)$ acts on $E(a, b, c)$ by simultaneous conjugation. The crucial point is this:

**Proposition 3.2** (after MacBeath) — **When** the set $E(a, b, c)$ **contains a triple** $(x, y, z)$ **such that** $(x, y, z) = \text{SL}(2, q)$, **it consists of just one conjugacy class.**

**Proof.** In [Mac69], the triples $(a, b, c)$ are divided into the “singular” ones and the “non-singular” ones; also, the type of $(x, y, z)$ is the type of $(\text{Tr}(x), \text{Tr}(y), \text{Tr}(z))$ by definition. Theorem 2 asserts that when $(x, y, z)$ is singular, the group $(x, y, z)$ is “affine”, and in particular it is not all of $\text{SL}(2, q)$. Our hypothesis guarantees thus that $(a, b, c)$ is non-singular.

We may then apply (ii) of Theorem 3 in loc. cit., giving the result. \(\Box\)

**Corollary 3.3** — **The group** $\mathcal{G}_T_1(\text{SL}(2, q))$ **is trivial.**

**Proof.** Let $\varphi \in \mathcal{G}_T_1(\text{SL}(2, q))$. Any $t \in \mathcal{I}/G$ is of the form $t = [x, y, z]$ with $(x, y, z) \in E(a, b, c)$ for some $a, b, c$, and $(x, y, z) = \text{SL}(2, q)$ by definition. The Lemma applies, showing that $\varphi(t) = [x', y', z']$ with $(x', y', z') \in E(a, b, c)$, while the Proposition proves that all triples in $E(a, b, c)$ are in fact conjugate. As a result $\varphi(t) = t$. \(\Box\)

4. Odd characteristics

Now we assume that $q = p^s$ is a power of the odd prime $p$, and we turn to the description of $\mathcal{G}_T_1(G)$ where $G = \text{PSL}(2, q)$.

4.1. Sets of triples. As in the previous section, we define $E(a, b, c)$ to be the set of triples $(x, y, z) \in \text{SL}(2, q)^3$ such that $xyz = 1$ and with $\text{Tr}(x) = a$, $\text{Tr}(y) = b$, $\text{Tr}(z) = c$. We also define $E(a, b, c)$ to be the subset of $E(a, b, c)$, which may well be empty, of triples generating $\text{SL}(2, q)$ (or equivalently, whose images generate $G$). Finally, we write $PE(a, b, c)$ for the image of $E(a, b, c)$ in $G^3$.

**Lemma 4.1** — **The notation behaves as follows.**

1. If $PE(a, b, c)$ and $PE(a', b', c')$ are not disjoint, then they are equal, and $(a', b', c') = (\pm a, \pm b, \pm c)$ for some choices of signs.
(2) We have
\[ PE(a, b, c) = PE(-a, -b, c) = PE(-a, b, -c) = PE(a, -b, -c). \]
In other words, the set \( PE(a, b, c) \) is not altered when an even number of signs are introduced.

(3) When \( abc = 0 \), all choices of signs give the same set \( PE(\pm a, \pm b, \pm c) \).

(4) When \( abc \neq 0 \), the sets \( PE(a, b, c) \) and \( PE(a, b, -c) \) are disjoint.

**Proof.** (1) An element \((g, h, k) \in PE(a, b, c)\) is of the form \((\overline{x}, \overline{y}, \overline{z})\), where \(x, y, z \in SL(2, q)\) and the bar denotes the morphism to \(G\), where the traces of these elements are \(a, b, c\) respectively. If \((g, h, k)\) also belongs to \(PE(a', b', c')\), given that the possible lifts of \(g, h, k\) are \(\pm x, \pm y, \pm z\) respectively, we see that \(a' = \pm a, b' = \pm b, c' = \pm c\). The fact that \(PE(a, b, c) = PE(a', b', c')\) will follow from (2)-(3)-(4) (since these properties imply that \(PE(a, b, c)\) and \(PE(\pm a, \pm b, \pm c)\) are either equal or disjoint).

(2) If \((x, y, z) \in E(a, b, c)\), then \((-x, -y, z) \in E(-a, -b, c)\), and these two triples map to the same element in \(G^3\). This shows that an element of \(PE(a, b, c)\) also belongs to \(PE(-a, -b, c)\), and conversely. The other arguments are similar.

(3) If \(abc = 0\), then one of \(a, b, c\) is \(0\), say \(a = 0\), so that \(a = -a\). We are thus free to change the sign of \(a\), and an even number of other signs, which gives the result.

(4) If \(x' = \pm x, \) and \(\text{Tr}(x') = \text{Tr}(x) \neq 0\), then \(x' = x\). We see thus that, whenever two triples \((x, y, z) \in E(a, b, c)\) and \((x', y', z') \in E(a, b, -c)\) map to the same element of \(G^3\), we must have \(x' = x\) and \(y' = y\), so that \(z' = z\) since \(xyz = 1 = x'y'z'\). This is a contradiction since the traces of \(z\) and \(z'\) are \(c \neq 0\) and \(-c\). As a result, \(PE(a, b, c)\) and \(PE(a, b, -c)\) are disjoint in this case. \(\Box\)

**Example 4.2** – Trying the example of \(PSL(2, 5)\), one finds that \(PE(0, 2, 3)\) is non-empty, showing that the case \(abc = 0\) does occur non-trivially. The set \(PE(2, 2, 4)\) is also non-empty, as is \(PE(2, 2, -4)\), so the case \(abc \neq 0\) occurs and states here the disjointness of non-empty sets. However, \(PE(1, 2, 4)\) is non-empty, but \(PE(1, 2, -4)\) is empty, an instance where (4) still holds, but in a degenerate way.

We define finally
\[ \mathcal{T}(a, b, c) = \bigcup_{\text{signs}} PE(\pm a, \pm b, \pm c) = PE(a, b, c) \cup PE(a, b, -c). \]
This is a subset of \(\mathcal{T}\), and \(\mathcal{T}(a, b, c)/G\) is a subset of \(\mathcal{T}/G\). As \((a, b, c)\) varies, the subsets \(\mathcal{T}(a, b, c)/G\) are disjoint, and constitute an initial partition of \(\mathcal{T}/G\).

**Lemma 4.3** – The subset \(\mathcal{T}(a, b, c)/G\) is stable under the action of \(\mathcal{G}T_1(G)\).

**Proof.** Suppose \(\varphi \in \mathcal{G}T_1(G)\), and \(\varphi([g, h, k]) = [g', h', k']\), with \(g, h, k, g', h', k' \in G\). Since \(\varphi\) is compatible with \(\equiv\) by definition, we see that \(g'\) is conjugate to \(g\) within \(G\); writing \(g = \overline{x}\) for \(x \in SL(2, q)\), and similiary \(g' = \overline{x}^\prime\), we conclude that \(x'\) is a conjugate of \(x\), so \(\text{Tr}(x') = \pm \text{Tr}(x)\). Similar considerations apply to \(h\) and \(h'\), and to \(k\) and \(k'\).

We conclude that if \((g, h, k) \in PE(a, b, c)\), then \((g', h', k') \in PE(\pm a, \pm b, \pm c)\), as we wanted. \(\square\)

**Remark 4.4.** Similar arguments show that \(\mathcal{T}(a, b, c)/G\) is a union of equivalence classes for \(\equiv\).

### 4.2. Number of conjugacy classes of triples.

The action of \(G\) on \(\mathcal{T}\) by (simultaneous) conjugation restricts to an action on each set \(PE(a, b, c)\), clearly. Moreover, let us introduce the automorphism \(\alpha\) of \(G\) induced by conjugation by
\[ \left( \begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right) \in GL(2, q) \setminus SL(2, q). \]
One verifies that $\alpha$ is not inner (below we recall the description of $\text{Out}(G)$). Moreover, since conjugate matrices have the same trace, we see that the action of $\alpha$ on the triples in $\mathcal{T}$ also preserves the sets $\mathcal{P}E(a, b, c)$.

**Proposition 4.5 (after MacBeath)** - When $\mathcal{P}E(a, b, c)$ is non-empty, it is made of precisely two conjugacy classes, which are exchanged by $\alpha$.

*Proof.* First we argue as in Proposition 3.2, relying on (i) of Theorem 3 in [MacBeath]. The conclusion is that when $E(a, b, c)$ is non-empty, then $E(a, b, c)$ contains a triple generating $\text{SL}(2, q)$, then $E(a, b, c)$ consists of two conjugacy classes exactly.

If $(x, y, z) \in E(a, b, c)$, then $(\alpha(x), \alpha(y), \alpha(z))$ cannot be in the conjugacy class of $(x, y, z)$, lest we should conclude that $\alpha$ is inner (here we view $\alpha$ as an automorphism of $\text{SL}(2, q)$, rather than $G$). However $\langle \alpha(x), \alpha(y), \alpha(z) \rangle \in E(a, b, c)$, showing that $E(a, b, c)$ intersects both conjugacy classes in $E(a, b, c)$, and that $E(a, b, c) = E(a, b, c)$.

When $\alpha$ is viewed as an automorphism of $G$, it is still non-inner. So the same reasoning applies, showing that there are triples in $\mathcal{P}E(a, b, c)$ which are not conjugate to one another, and more precisely that $(g, h, k)$ and $(\alpha(g), \alpha(h), \alpha(k))$ are never conjugate. The Proposition has been proved. \[\Box\]

The cardinality of $\mathcal{P}E(a, b, c)/G$ is thus 2, when it is not 0; and $\mathcal{T}(a, b, c)/G$ contains 2 or 4 elements (or 0). These sets are unions of orbits of $\alpha$ (recall that $\text{Out}(G)$ acts freely on $\mathcal{T}/G$).

**4.3. The action of $H$.** Recall that we write $H = \text{Out}(G) \times S_3$. According to [Wilson], Theorem 3.2, when $G = \text{PSL}(2, p^k)$ with $p$ odd, we have $\text{Out}(G) = \langle \alpha \rangle \times \text{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p) \cong C_2 \times C_2$. Here $\alpha$ is as above, and the Galois group acts on matrix entries in the obvious way. In particular, note that $\alpha$ is central in $H$.

Now suppose that $(a, b, c)$ is a fixed triple, and let $H_0$ denote the subgroup of $H$ leaving the subset $\mathcal{T}(a, b, c)/G$ stable, assuming the latter is non-empty. Note that $\alpha \in H_0$.

**Lemma 4.6** - The permutation group induced by $H_0$ on the set $\mathcal{T}(a, b, c)/G$ is isomorphic to either $C_2$ or $C_2^2$, or $D_8$. The same can be said of the centralizer of this permutation group in the symmetric group $S(\mathcal{T}(a, b, c)/G)$.

*Proof.* If $\mathcal{T}(a, b, c)/G$ has only 2 elements, there is nothing to prove, so we turn to the alternative, namely, we assume that this set has 4 elements. These are freely permuted by $\alpha$, which has order 2, so they may be numbered 1, 2, 3, 4 in such a way that $\alpha$ acts as $(1234)$.

The centraliser of $\alpha$ in $S_4$ is isomorphic to $D_8$, generated, say, by (12) and (13)(24). Since $\alpha$ is central in $H$, we have a map $H_0 \to D_8$, and the first part of the Lemma is about its image. The non-trivial subgroups of $D_8$ are all of the form indicated, except for the presence of cyclic groups of order 4.

So we assume that $h = \alpha i \sigma \pi \in \langle \alpha \rangle \times \text{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p) \times S_3 = H$ belongs to $H_0$ and acts as a 4-cycle on $\mathcal{T}(a, b, c)/G$, and work towards a contradiction.

First, we may replace $h$ by $\alpha h$ if necessary, and assume that $i = 0$, that is $h = \sigma \pi$. The element $\pi \in S_3$ has order 1, 2 or 3; if it has order 3, we replace $h$ by $h^3 = \sigma^2 \pi^2 = \sigma^2$ and we are reduced to the case when $\pi = 1$. So we assume that the order of $\pi$ divides 2.

Elements of order 4 in $D_8$, when squared, give the non-trivial central element, here (12)(34). Thus $h^2 = \sigma^2$ acts as $\alpha$ does. However, this is a contradiction,
since $\alpha$ and $\sigma$ belong to $Out(G)$, which acts freely on $\mathcal{T}/G$, while $\alpha = \sigma^2$ does not hold.

This proves the first part. For the second part, since $\alpha \in H_0$, we note that the centralizer in question must centralize $(12)(34)$, so it is a subgroup of the $D_8$ under consideration. The centralizer, in $D_8$, of a subgroup which is not cyclic of order 4 is again not cyclic of order 4, as is readily checked. □

4.4. The partition of $\mathcal{T}/G$. We now let

$$X(a, b, c) = \bigcup_{h \in H} h \cdot \mathcal{T}(a, b, c)/G.$$ 

As $a, b, c$ vary, the subsets $X(a, b, c)$ provide a partition of $\mathcal{T}/G$. Note that, given the description of $H$ (and $Out(G)$), we certainly have, for any $h \in H$,

$$h \cdot \mathcal{T}(a, b, c)/G = \mathcal{T}(a', b', c')/G$$

for some $a', b', c'$.

**Lemma 4.7** – Let $\mathcal{GT}_1(G)_{abc}$ be the permutation group on $X(a, b, c)$, consisting of those permutations commuting with the action of $H$, and compatible with the relation $\equiv$. Then $\mathcal{GT}_1(G)$ is the direct product of the various groups $\mathcal{GT}_1(G)_{abc}$.

**Proof.** This is a completely general fact: when $\mathcal{T}/G$ is partitioned into subsets which are stable under the action of $H$, and which are unions of equivalence classes for $\equiv$, then $\mathcal{GT}_1(G)$ splits as a corresponding direct product, as one sees from the definition. □

Now suppose $a, b, c$ are fixed, and resume the notation $H_0$ from the previous section.

**Lemma 4.8** – The permutation group $\mathcal{GT}_1(G)_{abc}$ is isomorphic to one of $\{1\}, C_2, C_2^2$, or $D_8$.

**Proof.** Since the action of $\mathcal{GT}_1(G)_{abc}$ commutes with that of $H$, it is determined by its restriction to $\mathcal{T}(a, b, c)/G$. In other words, the map $\mathcal{GT}_1(G)_{abc} \to S(\mathcal{T}(a, b, c)/G)$, which is well-defined since $\mathcal{T}(a, b, c)/G$ is stable under $\mathcal{GT}_1(G)$, is injective.

The image $\Gamma$ of that map is a permutation group which commutes with the action of $H_0$, and so by Lemma 4.6 it is a subgroup of either $C_2, C_2^2$ or $D_8$. Thus it remains to prove that $\Gamma$ is not cyclic of order 4, which potentially could happen when the centralizer $C$ of $H_0$ is isomorphic to $D_8$.

Indeed, suppose $\Gamma$ contains a 4-cycle. We infer that $\mathcal{GT}_1(G)$ acts transitively on $\mathcal{T}(a, b, c)/G$. It follows that the equivalence relation $\equiv$, preserved by $\mathcal{GT}_1(G)$, is trivial, in the sense that it has just one class in this set: all the triples in $\mathcal{T}(a, b, c)$ are "coordinate-wise conjugate". Thus the same can be said of $\equiv$ on all the translates $h \cdot \mathcal{T}(a, b, c)/G$, easily. As a result, these translates are precisely the equivalence classes of $\equiv$ on $X(a, b, c)$ (see Remark 4.4).

However, let us now consider the action of the full centralizer $C \equiv D_8$, extended to all of $X(a, b, c)$ by requiring commutation with the action of $H$. Given the description of the classes of $\equiv$, it is clear that $C$ is compatible with this equivalence relation. We conclude that $\mathcal{GT}_1(G)_{abc}$ contains a copy of $D_8$, and in particular it is not cyclic of order 4. □

The last two lemmas establish that, as announced:

**Theorem 4.9** – When $q$ is a power of an odd prime, there exist integers $n_1, n_2$ such that

$$\mathcal{GT}_1(\text{PSL}(2, q)) \cong C_2^{n_1} \times D_8^{n_2}.$$
In [Gui], explicit examples have been computed (with the help of the GAP software). We found the following table.

| $q$ | $n_1$ | $n_2$ |
|-----|-------|-------|
| 5   | 0     | 0     |
| 7   | 3     | 2     |
| 9   | 12    | 1     |
| 11  | 27    | 7     |
| 13  | 54    | 17    |
| 17  | 104   | 50    |
| 19  | 133   | 74    |

The first line is in accordance with the isomorphism $\text{PSL}(2,5) \cong \text{PSL}(2,4)$.

5. Application to dessins

We will conclude the paper with a proof of Theorem 1.1. Recall that $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the isomorphism classes of dessins, and that the action on those dessins with monodromy group $G$ factors via a certain map

$$\lambda_G: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathcal{G}(G).$$

If $K$ is that field such that $\text{Gal}(\overline{\mathbb{Q}}/K) = \ker(\lambda_G)$, then $K/\mathbb{Q}$ is Galois and $\text{Gal}(K/\mathbb{Q})$ is identified with a subgroup of $\mathcal{G}(G)$.

The moduli field of the dessin $X$ is that field $F$ such that $\text{Gal}(\overline{\mathbb{Q}}/F)$ is the subgroup of elements stabilizing $X$ (up to isomorphism). This subgroup contains $\ker(\lambda_G)$ if the monodromy group of $X$ is $G$, so that $F \subset K$. This proves the first part of the theorem.

Now we specialize to $G = \text{PSL}(2,q)$. If $q$ is even, then $\mathcal{G}(G) = 1$, so that $\mathcal{G}(G)$ is abelian (since the commutators belong to $\mathcal{G}(G)$). In this case $K/\mathbb{Q}$ is an abelian extension of $\mathbb{Q}$, as is $F/\mathbb{Q}$ in the notation above.

When $q$ is odd, we can at least state that $\mathcal{G}(G)$ is of derived length $\leq 2$. As a result, the derived length of $\mathcal{G}(G)$ is $\leq 3$. The same can be said of $\text{Gal}(K/\mathbb{Q})$ and of $\text{Gal}(\overline{F}/\mathbb{Q})$, where $\overline{F} \subset K$ is the Galois closure of $F$.

References

[Gui] Pierre Guillot, The Grothendieck-Teichmüller group of a finite group and $G$-dessins d'enfants, to appear in the proceedings volume Symmetry in Graphs, Maps and Polytopes 2014, arXiv 1407.3112.

[Gui14] ——— An elementary approach to dessins d’enfants and the Grothendieck-Teichmüller group, Enseign. Math. 60 (2014), no. 3-4, 293–375. MR 3342648

[Mac69] A. M. Macbeath, Generators of the linear fractional groups, Number Theory (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967), Amer. Math. Soc., Providence, R.I., 1969, pp. 14–32. MR 0262379

[Wil09] Robert A. Wilson, The finite simple groups, Graduate Texts in Mathematics, vol. 251, Springer-Verlag London, Ltd., London, 2009. MR 2562037

Université de Strasbourg & CNRS, Institut de Recherche Mathématique Avancée, 7 Rue René Descartes, 67084 Strasbourg, France

E-mail address: guillot@math.unistra.fr