SOME COMPUTATIONS WITH THE
GROTHENDIECK-TEICHMÜLLER GROUP
AND EQUIVARIANT DESSINS D’ENFANTS

PIERRE GUILLOT

ABSTRACT. For each finite group $G$, we define the Grothendieck-Teichmüller group of $G$, denoted $\mathcal{GT}(G)$, and explore its properties. The theory of dessins d’enfants shows that the inverse limit of $\mathcal{GT}(G)$ as $G$ varies can be identified with a group defined by Drinfeld and containing $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

We give in particular an identification of $\mathcal{GT}(G)$, in the case when $G$ is simple and non-abelian, with a certain very explicit group of permutations that can be analyzed easily. With the help of a computer, we obtain precise information for $G = \text{PSL}_2(\mathbb{F}_q)$ when $q \in \{4, 7, 8, 9, 11, 13, 17, 19\}$, and we treat $A_7$, $\text{PSL}_3(\mathbb{F}_3)$ and $M_{11}$.

In the rest of the paper we give a conceptual explanation for the technique which we use in our calculations. It turns out that the classical action of the Grothendieck-Teichmüller group on dessins d’enfants can be refined to an action on equivariant dessins, which we define, and this elucidates much of the first part.

1. Introduction

Suppose that $\Gamma$ is a finite group, generated by two distinguished elements $x$ and $y$, and such that

(i) $\Gamma$ has an automorphism $\theta$ such that $\theta(x) = y$ and $\theta(y) = x$,
(ii) $\Gamma$ has an automorphism $\delta$ such that $\delta(x) = z$ and $\delta(y) = y$, where $z$ is the element such that $xyz = 1$.

In this situation we define a subgroup $A(\Gamma) \subset \text{Aut}(\Gamma)$ as follows: an element $\varphi \in \text{Aut}(\Gamma)$ belongs to $A(\Gamma)$, by definition, when

1. $\varphi(x)$ is a conjugate of $x^k$ for some $k$ prime to the order of $\Gamma$,
2. $\varphi$ commutes with $\theta$ and $\delta$ in $\text{Out}(\Gamma)$.

(It follows that $\varphi(y)$ is a conjugate of $y^k$, and likewise for $z$.) The image of $A(\Gamma)$ in $\text{Out}(\Gamma)$ will be denoted by $A'(\Gamma)$.

For any finite group $G$ at all, we shall see that there is a way to construct a group $\mathcal{G}$ with the above properties, so that it can play the role of $\Gamma$ (and moreover $\mathcal{G} = \mathcal{G}$). Thus it makes sense to define $\mathcal{GT}(G) := A'(\mathcal{G})$. We call it the Grothendieck-Teichmüller group of $G$, and the present paper is dedicated to the study of its properties. We start with a few words of motivation and background.

How $\mathcal{GT}(G)$ varies with $G$ is a discussion which we postpone; for the time being, we take it for granted that it is possible to form the inverse limit

$$\mathcal{GT} := \lim_{G} \mathcal{GT}(G).$$

In [Gui] we proved the central (for us) result that there is a monomorphism

$$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathcal{GT}.$$ 

Thus $\mathcal{GT}$, with its very brief definition, gives a group-theoretic angle to the study of the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of the field $\mathbb{Q}$. A very first step towards
understanding $\mathcal{G}T$ is to provide information on $\mathcal{G}T(G)$ for some individual choices of $G$, and this is what we propose to do here.

As an aside, the reader will probably find it useful to know that
\[
\lim_{\overline{G}} \text{Out}(\overline{G}) \cong \text{Out}(\hat{F}_2),
\]
where $\hat{F}_2$ is the profinite completion of the free group $F_2$ on two generators. Thus $\mathcal{G}T$ can be seen as a certain subgroup of $\text{Out}(\hat{F}_2)$, and one can show that it can be lifted to a subgroup of $\text{Aut}(\hat{F}_2)$. Also, let us indicate that $\mathcal{G}T$ coincides with the group denoted $\mathcal{G}T_0$ by Drinfeld in [Dri90] (we shall have nothing to say about the subgroup $\mathcal{G}T \subset \mathcal{G}T_0$, also considered by Drinfeld). All this, and more, is proved in [Gui].

A good deal of the present paper will in fact pertain to $\mathcal{G}T_1(G)$, which is the subgroup of $\mathcal{G}T(G)$ obtained by restricting condition (1) above to $k = 1$ only. One can show that there is a monomorphism
\[
\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})' \longrightarrow \mathcal{G}T_1 := \lim_{\overline{G}} \mathcal{G}T_1(G),
\]
where $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})'$ is the derived subgroup of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. So $\mathcal{G}T_1$ can potentially give us information on $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})'$ just like $\mathcal{G}T$ can give us information on $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and of course the abelianization $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})' \cong \hat{\mathbb{Z}}^\times$ is well-understood. Here $\hat{\mathbb{Z}}^\times$ is the group of units in the profinite completion of $\mathbb{Z}$.

Before describing the results of the paper, we can give a straightforward example. When $G = C_n$, the cyclic group of order $n$, it is easy to see that $C_n / N \cong C_n \times C_n$ with its canonical pair of generators. Then $\mathcal{G}T(C_n) \cong (\mathbb{Z}/n)^\times$, directly from the definition, while $\mathcal{G}T_1(C_n)$ is trivial. Letting $n$ vary, we can take the inverse limit and obtain
\[
\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \lim_n \mathcal{G}T_1(C_n) \cong \hat{\mathbb{Z}}^\times.
\]
In turn, this homomorphism can be identified with the celebrated cyclotomic character, whose kernel is $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})'$. In a sense, consideration of cyclic groups accounts for what is abelian in $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and we must turn to non-abelian groups and their $\mathcal{G}T_1$ to proceed further.

Let us describe now the contents of the paper. It is in Section 2 that, after expanding on the definitions above, we prove that properties of $G$ are reflected in properties of $\mathcal{G}T_1$ (but not $\mathcal{G}T$). For example we establish:

**Theorem 1.1** – When $G$ is a $p$-group for some prime $p$, so is $\mathcal{G}T_1(G)$; when $G$ is nilpotent, so is $\mathcal{G}T_1(G)$.

The group $\mathcal{G}T(G)/\mathcal{G}T_1(G)$ is abelian, with exponent dividing that of $(\mathbb{Z}/N)^\times$, where $N$ is the order of $x$ or $y$ in $\overline{G}$ (in particular, this exponent may not be a power of $p$ when $G$ is a $p$-group).

In Section 3 we define a new group $\mathcal{S}(G)$. We hasten to add that when $G$ is non-abelian and simple we shall prove that there is an isomorphism $\mathcal{G}T_1(G) \cong \mathcal{S}(G)$, so the material in that section can be seen at least as a study of the “simple case”. However $\mathcal{S}(G)$ is defined for all $G$, and it is a much easier group to deal with than $\mathcal{G}T_1(G)$. It is described as the intersection, in a permutation group, of a Young subgroup and the centralizer of a few explicit permutations. The first virtue of $\mathcal{S}(G)$ is that it is easy to reason with, leading for example to the next result:

**Theorem 1.2** – Let $G$ be a finite, simple, non-abelian group. A simple factor occurring in $\mathcal{G}T_1(G)$ must be isomorphic to either:

- $C_2$,
- $C_3$, 

• a subquotient of $\text{Out}(G)$,
• an alternating group $A_s$ where $s \leq \frac{m^2}{207}$.

Here $m$ is the size of the largest conjugacy class in $G$.

(We stress that the theorem mentions $\text{Out}(G)$, not $\text{Out}(G)$ which is much bigger and would make for a tautological statement.)

It is also easy to compute explicitly with $\mathcal{S}(G)$. The reader should keep in mind that a computer, unleashed after $G\mathcal{T}_1(G)$ by a direct, brute force approach, will not be able to finish its task within a day or without exceeding the memory on a group $G$ whose order is much bigger than 32. Relying only on naive calculations, the author has yet to see a completed example for which the order of $G\mathcal{T}_1(G)$ is anything but 1, 2, 3, 4, 5, 6, 7. By contrast, the machinery of $\mathcal{S}(G)$ has allowed us to treat, for example, the case of the Mathieu group $M_{11}$ of order 7920, yielding:

**Theorem 1.3** – The direct product of the simple factors of $G\mathcal{T}_1(M_{11})$ is

$$C_2^{465} \times C_3^{46} \times A_5^{10} \times A_6^9 \times A_7^{10} \times A_8^9 \times A_9^5 \times A_{10}^5 \times A_{11}^5 \times A_{12}^4 \times A_{13}^4 \times A_{16}^4 \times A_{17}^3 \times A_{18}^2 \times A_{19} \times A_{20}^2 \times A_{23} \times A_{28} \times A_{31} \times A_{34}^3 \times A_{35}^2 .$$

Accordingly, the order of $G\mathcal{T}_1(M_{11})$ is

$$2^{21141} \cdot 3^{407} \cdot 5^{165} \cdot 7^{98} \cdot 11^{43} \cdot 13^{34} \cdot 17^{23} \cdot 19^{8} \cdot 23^{3} \cdot 29^{3} \cdot 31^{3} = 564,410,820,378,566,604,254,871,259,271,279,028,761,351,862,824.$$

To move on with our outline, let $\mathcal{P}$ be the set of pairs $(g,h) \in G$ such that $(g,h) = G$. We will see that there is a very natural action of $\text{GT}(G)$ on the set $\mathcal{P}/\text{Aut}(G)$. However, the development of the isomorphism between $G\mathcal{T}_1(G)$ and $\mathcal{S}(G)$ relies on the existence of an action of $G\mathcal{T}(G)$ on $\mathcal{P}$, the set of orbits in $\mathcal{P}$ under the action of the inner automorphisms only (the letter $c$ is for “conjugation”). At first sight this appears rather mysterious, and the arguments are ad hoc. In section 5 we give a conceptual explanation.

The key is to bring dessins d’enfants into the picture, perhaps unsurprisingly as these objects are at the roots of the construction of $G\mathcal{T}$. Recall that a dessin is essentially a bipartite graph drawn on a compact, oriented surface in such a way that the complement of the graph is a union of topological discs. The (isomorphism classes of) dessins d’enfants are in bijection with many other sets of (isomorphism classes of) objects, notably algebraic curves over $\mathbb{Q}$ with a certain ramification.
property, or étale algebras over $\overline{\mathbb{Q}}(x)$, again with a ramification property. The group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts naturally on étale algebras, and this is turned into an action on dessins via the said bijection.

In [Gui] (which is our reference for dessins), we prove that dessins form a category $\text{Dessins}$, and that the aforementioned bijections can be refined into equivalences of categories. Such a refinement may not seem to bring much new information at first sight, but it is not so. Indeed, with this formalism it is completely straightforward to define the category $G\text{Dessins}$ of equivariant dessins, that is, dessins equipped with an action of a fixed group $G$; and we prove the following:

**Theorem 1.4** – The group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the set of isomorphism classes of objects in $G\text{Dessins}$, for any group $G$.

Moreover, suppose we consider the regular $G$-dessins $X$ in $G\text{Dessins}$ such that the action gives an isomorphism $G \rightarrow \text{Aut}(X)$. Then the set of isomorphism classes of such objects is naturally in bijection with $\mathcal{P}_c$, and the latter is endowed with an action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

(The word regular will be explain in the text.) It is now much more believable that $G\mathcal{T}$ should act on $\mathcal{P}_c$; given that the action of $G\mathcal{T}$ on dessins, when restricted to those dessins $X$ such that $\text{Aut}(X) \cong G$, factors via $G\mathcal{T}(G)$, we should not be overly surprised by the discovery made in Section 3 that $G\mathcal{T}(G)$ does act on $\mathcal{P}_c$.

### 2. Generalities

We start by expanding on the definitions given in the Introduction. We define $\overline{\mathcal{G}}$, the group $G\mathcal{T}(G)$ as a subgroup of $\text{Out}(\overline{\mathcal{G}})$, explain the relationship with $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and prove the most basic properties.

#### 2.1. The group $\overline{\mathcal{G}}$

Let $G$ be a finite group. Whenever $N$ is a subgroup of a group $\Gamma$, it will be convenient to say that $N$ has index $G$ in $\Gamma$ when (i) $N$ is normal in $\Gamma$ and (ii) there is an isomorphism $\Gamma/N \cong G$.

Writing $F_2 = \langle x, y \rangle$ for the free group on two generators $x$ and $y$, we call $N_G$ the intersection of all the subgroups of $F_2$ having index $G$. There are finitely many of these, so the group $\overline{\mathcal{G}} := F_2/N_G$ is finite. We usually write $x$ and $y$ for the images of the generators of $F_2$ in $\overline{\mathcal{G}}$, since no confusion should arise.

The following lemma is almost trivial.

**Lemma 2.1** – $\overline{\mathcal{G}}$ has the following properties:

1. The intersection of all the subgroups of $\overline{\mathcal{G}}$ having index $G$ is trivial.
2. If $\Gamma$ is any group such that the intersection of all its subgroups of index $G$ is trivial, and if $x'$ and $y'$ are generators of $\Gamma$, then there is a homomorphism $\overline{\mathcal{G}} \rightarrow \Gamma$ mapping $x$ to $x'$ and $y$ to $y'$.
3. If $x'$ and $y'$ are generators for $\overline{\mathcal{G}}$, then there is an automorphism of $\overline{\mathcal{G}}$ mapping $x$ to $x'$ and $y$ to $y'$.

We turn to the description of a concrete “model” for $\overline{\mathcal{G}}$. The key observation is that subgroups of $F_2$ of index $G$ are in bijection with the orbits of $\text{Aut}(G)$ on the set $\mathcal{P}$ of pairs of generators for $G$; the bijection sends a pair $(x', y')$ to the kernel of the map $F_2 \rightarrow G$ sending $x$ to $x'$ and $y$ to $y'$.

Based on this, we select pairs $(x_1, y_1), \ldots, (x_r, y_r)$ forming a system of representatives for the orbits of $\text{Aut}(G)$, that is, with just one pair out of each orbit. (The number $r = r(G)$ was much studied in [Jon].) Consider then the subgroup $\tilde{G}$ of $G^r$ generated by $x = (x_1, x_2, \ldots, x_r)$ and $y = (y_1, y_2, \ldots, y_r)$. Then it is straightforward to show that $\tilde{G}$ satisfies (2) of lemma 2.1 (since the group $\Gamma$ mentioned there embeds into $G^r$). This property clearly characterizes $\overline{\mathcal{G}}$ as a group with distinguished generators, so there must be an isomorphism $\overline{\mathcal{G}} \cong \tilde{G}$ identifying the two
elements which we have both called $x$, and likewise for $y$. For most of this paper we will consider $\overline{G}$ to be the subgroup of $G''$ just defined.

Let $p_i$ be the projection onto the $i$-th factor of $G''$, restricted to $\overline{G}$. It send $x$ to $x_i$ and $y$ to $y_i$, so it is surjective and its kernel $K_i$ has index $G$. The various $K_i$’s are distinct (by choice of the pairs $(x_i, y_i)$), so they must constitute the $r$ different subgroups of index $G$ in $\overline{G}$. In particular they form a characteristic family of subgroups, that is, for any $\varphi \in Aut(\overline{G})$ we must have $\varphi(K_i) = K_{\varphi(i)}$ for some permutation $\sigma \in S_r$.

Finally we note that $\overline{G} = G$. Indeed, if we try to construct the model for $\overline{G}$ as we have just done with $\overline{G}$, then property (3) of lemma 2.1 leaves us only one pair to consider; in other words, $r(\overline{G}) = 1$.

2.2. The group $\mathcal{G}T(G)$. By (3) of lemma 2.1, the group $\overline{G}$ has an automorphism $\theta$ with $\theta(x) = y$ and $\theta(y) = x$; likewise, $\overline{G}$ possesses an automorphism $\delta$ with $\delta(x) = y^{-1}x^{-1}$ and $\delta(y) = y$.

Consider now the elements $\varphi \in Aut(\overline{G})$ satisfying

1. $\varphi(x)$ is a conjugate of $x^k$ for some $k$ prime to the order of $\overline{G}$,
2. $\varphi$ commutes with $\theta$ and $\delta$ in $Out(\overline{G})$.

(It follows that $\varphi(y)$ is a conjugate of $y^k$, and likewise $xy$ is a conjugate of $(xy)^k$.)

These form a subgroup of $Aut(\overline{G})$, and its image in $Out(\overline{G})$ we call $\mathcal{G}T(G)$.

Likewise, we can consider those automorphisms satisfying (1) for $k = 1$ only, as well as (2); they induce a normal subgroup $\mathcal{G}T_1(G)$ of $\mathcal{G}T(G)$.

A complication to keep in mind is that there is no well-defined map on $\mathcal{G}T(G)$ that would associate to $\varphi$ the number $k$ as above; the latter is not unique, and not even unique modulo the order of $x$, for some powers of $x$ may well be conjugated to one another. In other words an element of $\mathcal{G}T_1(G)$ may have the property that $\varphi(x)$ is a conjugate of $x^k$ for many values of $k \neq 1$.

It is however true that when $\varphi(x)$ is a conjugate of $x^k$ and $\psi(x)$ is a conjugate of $x^l$, then $\psi \circ \varphi(x)$ is a conjugate of $x^{kl}$; also $\varphi^{-1}(x)$ is a conjugate of $x^{-k}$. These simple observations suffice to show that all commutators in $\mathcal{G}T(G)$ must belong to $\mathcal{G}T_1(G)$. Thus we have

**Lemma 2.2** – The group $\mathcal{G}T(G)/\mathcal{G}T_1(G)$ is an abelian group, of exponent dividing that of $(\mathbb{Z}/N\mathbb{Z})^\times$, where $N$ is the order of $x$ (or $y$) in $\overline{G}$.

2.3. Inverse limits. When $N$ is a normal subgroup of $F_2$ of finite index, we can always find a $G$ such that $N_G \subset N$: indeed it suffices to take $G = F_2/N$. From this one can show that

$$\lim\ F_2/N_G \cong \hat{F}_2,$$

where $\hat{F}_2$ is the profinite completion of $F_2$. Here the inverse limit is over the directed set of all the subgroups of the form $N_G$ (with their inclusions). Details for this, and everything else in the next few paragraphs, are provided in [Gui].

When $N_G \subset N_H$, we have a map $\overline{G} \to \overline{H}$, whose kernel is the intersection of all the subgroups of $\overline{G}$ having index $H$. In particular, this kernel is a characteristic subgroup, and as a result we have an induced map

$$\mathcal{G}T(G) \longrightarrow \mathcal{G}T(H).$$

Thus it makes sense to talk about the inverse limit $\lim\mathcal{G}T(G)$. Again the indexing set for the limit is the set of the various subgroups $N_G$, but we prefer to write more suggestively

$$\lim\mathcal{G}T(G)$$
which we call $\mathcal{GT}$. We also put
\[
\mathcal{GT}_{1} := \varprojlim \mathcal{GT}_{1}(G).
\]

2.4. The Galois group of $\mathbb{Q}$. In [Gui] we prove the existence of a monomorphism
\[
\Phi : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathcal{GT}
\]
which is the motivation for the study of $\mathcal{GT}$. Moreover, if $\lambda \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and if $\varphi = \Phi(\lambda)$, then we can compute for any $G$ an integer $k$ such that $\varphi(x)$ and $x^k$ are conjugate in $\overline{G}$: namely, let $N$ be the order of $x$, let $\zeta = e \frac{2i\pi}{N}$, and pick $k$ such that $\lambda(\zeta) = \zeta^k$.

We write $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})'$ for the derived subgroup of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (the closed subgroup generated by the commutators). A celebrated result in number theory asserts that $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})'$ is precisely the subgroup of elements acting trivially on all the roots of unity. As a result there is also a monomorphism
\[
\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})' \rightarrow \mathcal{GT}_{1}.
\]

It is surprising that the lemma below seems hard to prove without appealing to $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. It is never used on the sequel.

Lemma 2.3 – Let $N$ be the order of $x$ (or $y$) in $\overline{G}$. Then for any integer $k$ prime to $N$, there is $\varphi \in \mathcal{GT}(G)$ such that $\varphi(x)$ is a conjugate of $x^k$.

Proof. Simply take $\varphi = \Phi(\lambda)$ where $\lambda \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ has the appropriate effect on roots of unity. $\square$

2.5. $p$-groups and nilpotent groups.

Proposition 2.4 – When $G$ is a $p$-group, so is $\mathcal{GT}_{1}(G)$.

Proof. First note that $\overline{G}$ is itself a $p$-group, being a subgroup of $G^\prime$. Let $A'(\overline{G})$ denote the preimage of $\mathcal{GT}_{1}(\overline{G})$ in $A\text{ut}(\overline{G})$. If $A'(\overline{G})$ is not a $p$-group, then it contains an element $\varphi$ whose order is a prime $\ell \neq p$.

Consider the elementary abelian $p$-group $E = \overline{G}/\Phi(\overline{G})$, where $\Phi(\overline{G})$ is the Fraternal subgroup of $\overline{G}$, generated by the images $\overline{x}$ and $\overline{y}$ of $x$ and $y$. The induced action of $\varphi$ on $E$ is then trivial. It follows from [Isa08], Corollary 3.29, that the action of $\varphi$ on $\overline{G}$ is trivial, violating the assumption that the order of $\varphi$ is $\ell$. This contradiction shows that $A'(\overline{G})$ is a $p$-group, and so also is $\mathcal{GT}_{1}(G)$. $\square$

Proposition 2.5 – When $G$ and $H$ have coprime orders, we have $\overline{G} \times \overline{H} \cong \overline{G} \times \overline{H}$ and $\mathcal{GT}(G \times H) \cong \mathcal{GT}(G) \times \mathcal{GT}(H)$, as well as $\mathcal{GT}_{1}(G \times H) \cong \mathcal{GT}_{1}(G) \times \mathcal{GT}_{1}(H)$.

Proof. We start with a remark. Whenever a group $N$ has index $G \times H$ in a group $\Gamma$, then we can write $N = N' \cap N''$ where $N'$ has index $G$ and $N''$ has index $H$, clearly. Now suppose the orders of $G$ and $H$ are coprime, and let us prove the converse. If $N = N' \cap N''$ for such $N'$ and $N''$, then $\Gamma/N$ injects in $\Gamma/N' \times \Gamma/N'' \cong G \times H$, and its image surjects onto both $G$ and $H$. Thus the order of $\Gamma/N$ is divisible by both $|G|$ and $|H|$ and so by their product, so that $\Gamma/N \cong G \times H$, as we wished to show.

Applying this remark to the subgroups of the free group $F_2$, we deduce that

\[
N_{G \times H} = N_G \cap N_H.
\]

(Recall that $N_G$ is the intersection of the subgroups of index $G$, and likewise for $N_H$ and $N_{G \times H}$.)

What is more, $\overline{G}$ and $\overline{H}$ also have coprime orders since they are subgroups of $G^\prime$ and $H^\prime$ respectively. Thus we may apply the remark again, and deduce from (*)
that \( N_{G \times H} \) has index \( G \times H \) (being the intersection of a group of index \( G \) and a group of index \( H \)). This shows that there is an isomorphism \( G \times H \to \bar{G} \times \bar{H} \).

Next we note that an automorphism of \( G \times H \) must be of the form \( \alpha \times \beta \) where \( \alpha \in \text{Aut}(G) \) and \( \beta \in \text{Aut}(H) \). It follows easily that \( \mathcal{G}T(G \times H) \cong \mathcal{G}T(G) \times \mathcal{G}T(H) \). \( \Box \)

**Corollary 2.6** – When \( G \) is nilpotent, so is \( \mathcal{G}T_1(G) \).

**Proof.** A finite group is nilpotent precisely when it is a direct product of \( p \)-groups. \( \Box \)

### 3. The case of simple groups

For any finite group \( G \), we define a permutation group \( \mathcal{P}(G) \). When \( G \) is simple and non-abelian, we proceed to show that there is an isomorphism \( \mathcal{G}T_1(G) \cong \mathcal{P}(G) \). This is used to analyse the possible simple factors in \( \mathcal{G}T_1(G) \) in this case.

#### 3.1. Notation.

Let \( G \) be a finite group (shortly to be assumed simple and non-abelian below, but not for the moment). The following notation will be used throughout this section. Let us emphasize that we make some arbitrary choices at the same time.

Let \( \mathcal{P} \) denote the set of pairs of elements \((g, h)\) generating \( G \). The group \( \text{Aut}(G) \) acts on \( \mathcal{P} \), and the set \( \mathcal{P}/\text{Aut}(G) \) of orbits has cardinality \( r \). It will be useful to also work with \( \mathcal{P}_c \), the set of orbits under the sole action of the inner automorphisms. We see that \( \text{Out}(G) \) acts freely on \( \mathcal{P}_c \), and \( \mathcal{P}_c/\text{Out}(G) = \mathcal{P}/\text{Aut}(G) \). Thus the set \( \mathcal{P}_c \) has cardinality \( r|\text{Out}(G)| \). (Please note that the actions considered here are on the left.)

For each \( 1 \leq i \leq r \) we choose a representative \((x_i, y_i)\) in \( \mathcal{P}_c \) for the \( i \)-th orbit in \( \mathcal{P}/\text{Aut}(G) \), in some ordering.

The \( \text{Aut}(G) \)-orbit of \((g, h)\) in \( \mathcal{P}_c \) will be denoted \([g, h]_c\), while its orbit under \( \text{Inn}(G) \) will be written \([g, h]_e \) (the brackets will never denote commutators in this section). In this notation the action of \( \alpha \in \text{Out}(G) \) on \([g, h]_c \) is \( \alpha \cdot [g, h]_c = [\alpha(g), \alpha(h)]_c \). The elements of \( \mathcal{P}_c \) are precisely enumerated as \( \alpha \cdot [x_i, y_i]_c \) for \( \alpha \in \text{Out}(G) \) and \( 1 \leq i \leq r \). The following is immediate.

**Lemma 3.1** – There is a bijection of sets

\[ \mathcal{P}_c \longrightarrow \text{Out}(G) \times \mathcal{P}/\text{Aut}(G), \]

sending \( \alpha \cdot [x_i, y_i]_c \) to the pair \( (\alpha, [x_i, y_i]) \). It is equivariant with respect to the \( \text{Out}(G) \) actions, where on the right hand side the group \( \text{Out}(G) \) acts trivially on \( \mathcal{P}/\text{Aut}(G) \) and by left multiplication on itself.

Finally, each pair \((x_i, y_i)\) determines a unique homomorphism \( p_i : \bar{G} \to G \) sending \( x \) and \( y \) to \( x_i \) and \( y_i \) respectively (recall that \( x \) and \( y \) are the canonical generators of \( \bar{G} \)). The kernel of \( p_i \) will be written \( \text{K}_i \).

#### 3.2. An action of \( \text{Out}(\bar{G}) \) on \( \mathcal{P}_c \).

First recall that the \( \text{K}_i \)'s form a characteristic family of subgroups in \( \bar{G} \); in other words, for any \( \varphi \in \text{Aut}(\bar{G}) \) and any \( i \) there is a \( \sigma(i) \) such that \( \varphi(\text{K}_i) = \text{K}_{\sigma(i)} \). The permutation \( \sigma \in S_r \) thus obtained from \( \varphi \) may occasionally be written \( \sigma(\varphi) \).

Next, the composition \( \bar{G} \xrightarrow{\varphi} \bar{G} \xrightarrow{p_{\sigma(\varphi)}} G \) factors through \( p_i \), thus resulting in an automorphism \( G \to G \) which we write \( \varphi_i \). There is the composition formula

\[ (\psi \circ \varphi)_i = \psi_{\sigma(i)} \circ \varphi_i \quad \text{where} \quad \sigma = \sigma(\varphi). \]

We can now define an action of \( \text{Aut}(\bar{G}) \) on \( \text{Out}(G) \times \mathcal{P}/\text{Aut}(G) \) by setting

\[ \varphi \cdot (\alpha, [x_i, y_i]) = (\alpha \varphi_i^{-1}, [x_{\sigma(i)}, y_{\sigma(i)}]). \]
(On the second factor this is the natural action on $\mathcal{P}/\text{Aut}(G)$, which can be identified with the set of the $K_i$’s.) In this expression we have written $\varphi_i^{-1}$ for the class of this automorphism in $\text{Out}(G)$. It is clear that the action factors through $\text{Out}(\overline{G})$, and indeed that it is an action.

Crucially, we notice that the action just defined commutes with that of $\text{Out}(G)$ (by left multiplication on itself and trivially on $\mathcal{P}/\text{Aut}(G)$).

By lemma 3.1, we also have an action of $\text{Out}(\overline{G})$ on $\mathcal{P}_c$, which commutes with the natural action of $\text{Out}(G)$. We have in particular

$$\varphi \cdot [x, y]_c = \varphi_i^{-1} \cdot [x_{\sigma(i)}, y_{\sigma(i)}]_c,$$

which we will use more often than the general expression

$$\varphi \cdot (\alpha \cdot [x, y]_c) = \alpha \varphi_i^{-1} \cdot [x_{\sigma(i)}, y_{\sigma(i)}].$$

(Commuation with $\text{Out}(G)$ means that the first formula implies the second anyway.)

This discussion is summarized in the next proposition.

**Proposition 3.2** — There is a homomorphism

$$\text{Out}(\overline{G}) \longrightarrow C_S(\text{Out}(G)),$$

where $S = S(\mathcal{P}_c)$ is the symmetric group of the set $\mathcal{P}_c$, and $C_S(\text{Out}(G))$ is the centralizer of $\text{Out}(G)$ for the natural action. The corresponding action of $\text{Out}(\overline{G})$ on $\mathcal{P}_c$ satisfies in particular

$$\varphi \cdot [x, y]_c = \varphi_i^{-1} \cdot [x_{\sigma(i)}, y_{\sigma(i)}]_c.$$

(Note that when $\varphi \in \text{Out}(\overline{G})$, or $\varphi \in \text{Aut}(\overline{G})$, we simply write $\varphi \cdot [g, h]_c$ for the action.)

We need to identify the permutations of $\mathcal{P}_c$ induced by certain specific elements of $\text{Aut}(\overline{G})$. We start with the automorphism $\theta$ of $\overline{G}$ which exchanges $x$ and $y$. The next lemma is perhaps not surprising, but its proof requires some care.

**Lemma 3.3** — For all $g, h \in G$, we have

$$\theta \cdot [g, h]_c = [h, g]_c.$$

**Proof.** Consider the following commutative diagram:

$$\begin{array}{ccc}
\overline{G} & \xrightarrow{\theta} & \overline{G} \\
p_i \downarrow & & \downarrow p_{\sigma(i)} \\
G & \xrightarrow{\theta} & G
\end{array}$$

Recall that $\theta(x) = y$, $\theta(y) = x$, $p_i(x) = x_i$, $p_i(y) = y_i$, and likewise for $p_{\sigma(i)}$. Thus we see that $\theta_i(x_i) = y_{\sigma(i)}$ and $\theta_i(y_i) = x_{\sigma(i)}$, which we may profitably rewrite $\theta_i^{-1}(y_{\sigma(i)}) = x_i$ and $\theta_i^{-1}(x_{\sigma(i)}) = y_i$.

Following the definitions, we see that

$$\theta \cdot [x_i, y_i]_c = [y_i, x_i]_c.$$

Thus the proposed formula is true at least when $[g, h]_c = [x_i, y_i]_c$ for some $i$. However the map $[g, h]_c \mapsto [h, g]_c$ commutes with the action of $\text{Out}(G)$, as does $[g, h]_c \mapsto \theta \cdot [g, h]_c$, so these two maps have to agree.

In the exact same vein, we have

**Lemma 3.4** — For all $g, h \in G$, we have

$$\delta \cdot [g, h]_c = [h^{-1}g^{-1}, h]_c.$$
We leave the proof to the reader (recall that \( \delta(x) = y^{-1}x^{-1} \) and \( \delta(y) = y \)).

The next (and last) lemma involves the action of \( G \times G \) on \( \mathcal{P}_c \) by conjugation.

**Lemma 3.5** – Let \( \varphi \in \text{Aut}(G) \) be such that \( \varphi(x) \) is conjugated to \( x \), and \( \varphi(y) \) is conjugated to \( y \). Then the action of \( \varphi \) on \( \mathcal{P}_c \) preserves the orbits of \( G \times G \).

**Proof.** The action of \( \text{Out}(G) \) on \( \mathcal{P}_c \) preserves the \( G \times G \)-orbits, clearly, so it suffices to show that \( \varphi \cdot [x_i, y_i]_c \) is in the same \( G \times G \)-orbit as \( [x_i, y_i]_c \) for each index \( i \).

By assumption \( \varphi(x) = x^y \) so \( \varphi_i(x_i) = p_{\sigma(i)}(\varphi(x)) = x_i^{\sigma(i)} \) where \( g' = p_{\sigma(i)}(g) \). It follows that \( \varphi_i^{-1}(x_{\sigma(i)}) \) is conjugated to \( x_i \). Likewise, \( \varphi_i(y_{\sigma(i)}) \) is conjugated to \( y_i \), and in the end we have indeed shown that \( \varphi_i^{-1} \cdot [x_{\sigma(i)}, y_{\sigma(i)}]_c \) is in the \( G \times G \)-orbit of \( [x_i, y_i]_c \).

### 3.3. The group \( \mathcal{S}(G) \)

Let us use the notation \( \theta \) and \( \delta \) for the permutations induced on \( \mathcal{P}_c \) by the automorphisms of the same name in \( \text{Aut}(G) \). They generate a subgroup \( (\theta, \delta) \) in \( S(\mathcal{P}_c) \), the symmetric group of the set \( \mathcal{P}_c \). One checks the identities \( \theta^2 = 1, \delta^2 = 1, \delta \theta \delta = \theta \delta \theta \), and it follows that \( (\theta, \delta) \) is a homomorphic image of \( S_3 \).

We define \( \mathcal{S}(G) \) to be the subgroup of \( S(\mathcal{P}_c) \) of those permutations commuting with the action of \( \text{Out}(G) \times (\theta, \delta) \), and preserving the \( G \times G \)-orbits. Thus \( \mathcal{S}(G) \) is the intersection of the centralizer of a certain subgroup on the one hand, and a Young subgroup of \( S(\mathcal{P}_c) \) on the other hand.

For any group \( G \), we have a map \( \mathcal{S}(G) \to \mathcal{S}(G) \), by the lemmas just established. The rest of this section is dedicated to the proof of:

**Theorem 3.6** – When \( G \) is simple and non-abelian, the map

\[
\mathcal{S}(G) \to \mathcal{S}(G)
\]

is an isomorphism.

Recall that we have a model of \( G^r \) as the subgroup of the cartesian product \( G^r \) generated by \( x = (x_1, x_2, \ldots, x_r) \) and \( y = (y_1, y_2, \ldots, y_r) \). The map \( p_i \) is then just the projection onto the \( i \)-th factor. In [Jon] one finds a proof of the following

**Lemma 3.7** – Let \( G \) be a nonabelian, simple finite group. Then

1. The group \( G \) is all of \( G^r \).
2. The normal subgroups of \( G^r \) are those of the form \( \prod_{I \subseteq \{1, \ldots, r\}} G_i \) for some \( I \subset \{1, \ldots, r\} \) (where \( G_i \) is the \( i \)-th embedded copy of \( G \) in \( G^r \)).
3. As a result, the maximal, proper normal subgroups of \( G^r \) are those of the form \( \prod_{i \neq j} G_i \) for some \( j \). This is precisely \( K_j \).

In the rest of this section \( G \) will always be nonabelian and simple, as well as finite. Let us add:

**Lemma 3.8** – The automorphisms of \( G^r \) are as follows:

1. \( \text{Aut}(G^r) \cong \text{Aut}(G) \times S_r \).
2. \( \text{Out}(G^r) \cong \text{Out}(G) \times S_r \).
3. The action of \( \text{Out}(G) \) on \( \mathcal{P}_c \) is faithful.

**Proof.** Considering the action on the \( K_j \)’s, we obtain a map \( \text{Out}(G^r) \to S_r \) which is clearly split surjective. Now suppose \( \varphi \) is an automorphism of \( G^r \) preserving all the \( K_j \)’s. By taking intersections, we see that \( \varphi \) preserves all the normal subgroups of \( G^r \), including \( G_1 \) and \( K_1 \cong G^{r-1} \), these two satisfying \( G_1 \times K_1 = G^r \). By induction, it is immediate that \( \varphi \) is of the form \( \alpha_1 \times \cdots \times \alpha_r \). This proves (1).

An inner automorphism of \( G^r \) is the direct product of inner automorphisms of each \( G_i \), so we have also (2).
Now suppose \( \varphi \in \text{Aut}(G) \) acts trivially on \( \mathcal{R} \). Then it must also act trivially on \( \mathcal{R}/\text{Aut}(G) \) (the map \( \mathcal{R} \to \mathcal{R}/\text{Aut}(G) \) is equivariant for this action). It follows that \( \sigma(\varphi) \) is the trivial permutation of \( G/\mathcal{R} \). The map considered in (2) then sends \( \varphi \) to \( (\varphi_1, \varphi_2, \ldots, \varphi_r) \in \text{Out}(G)^r \), in our earlier notation. As the action on \( \mathcal{R} \) is trivial, we see that \( \varphi_r \) must be inner (that is, it represents the trivial element in \( \text{Out}(G) \)), so (2) implies that \( \varphi \) is itself inner. \( \square \)

If we combine (3) of the lemma with proposition 3.2, we see that \( \text{Out}(G) \) injects into \( C_{S}(\text{Out}(G)) \), the centralizer of \( \text{Out}(G) \) in \( S = S(\mathcal{R}) \). However since the action of \( \text{Out}(G) \) on \( \mathcal{R} \) is free with \( r \) orbits, its centralizer is itself a wreath product \( \text{Out}(G) \wr \mathcal{R} \). Comparing orders, we conclude that \( \text{Out}(G) \) maps isomorphically onto \( C_{S}(\text{Out}(G)) \) via the action on \( \mathcal{R} \).

It remains to check that the conditions defining \( \mathcal{G} \mathcal{T}_{1}(G) \) as a subgroup of \( \text{Out}(G) \) correspond to what is stated in the theorem. This is immediate for the commutation with \( \theta \) and \( \delta \). Lemma 3.5 does half the remaining work, by showing that the elements of \( \mathcal{G} \mathcal{T}_{1}(G) \) must preserve the \( G \times G \)-orbits in \( \mathcal{R} \). The proof will be concluded by establishing the converse.

Indeed, if the action of \( \varphi \in \text{Aut}(G) \) is such that \( \varphi_i^{-1}[x_{\sigma(i)},y_{\tau(i)}]_c \) is in the \( G \times G \)-orbits of \( [x_i,y_i]_c \) for all \( 1 \leq i \leq r \) then \( x_{\sigma(i)} \) and \( \varphi_i(x_i) \) are conjugate; in other words \( p_{\sigma(i)}(x) \) and \( p_{\tau(i)}(\varphi(x)) \) are conjugate. If we recall that \( \overline{G} = G^r \) and each \( p_j \) is just the projection onto the \( j \)-th factor, then we see immediately that \( x \) and \( \varphi(x) \) are conjugate in \( G^r \), so in \( \overline{G} \). Likewise for \( y \). This concludes the proof of theorem 3.6.

3.4. Properties of \( \mathcal{F}(G) \). We write \( S = S(\mathcal{R}) \) and \( H = \text{Out}(G) \times \langle \theta, \delta \rangle \), while \( Y \) is the Young subgroup of those permutations in \( S \) which preserve the \( G \times G \)-orbits on \( \mathcal{R} \). We have \( \mathcal{F}(G) = C_{S}(H) \cap Y \).

Proposition 3.9 – The group \( \mathcal{F}(G) \) is a product of wreath products \( E_k \wr S_{r_k} \) where \( \sum_k r_k = r \) and \( E_k \) is a quotient of \( H \).

Moreover each integer \( r_k \) verifies

\[
    r_k \leq \frac{|Z| m^2}{|G|}
\]

where \( m \) is the size of the largest conjugacy class in \( G \), and \( Z \) is the centre of \( G \).

Of course we will mostly use this proposition when \( G \) is simple and non-abelian, so that \( |Z| = 1 \). Note also that other bounds are possible for \( r_k \).

Proof. We number arbitrarily the \( G \times G \)-orbits \( P_1, P_2, \ldots \) on \( \mathcal{R} \). Every orbit \( X \) of \( H \) has an ordered “partition” into the subsets \( X^{(1)} = X \cap P_1, X^{(2)} = X \cap P_2, \ldots \) of some of which may be empty. Call two of these \( H \)-orbits \( X_1 \) and \( X_2 \) equivalent when there is an \( H \)-equivariant bijection \( X_1 \to X_2 \) mapping \( X^{(i)}_1 \) onto \( X^{(i)}_2 \) for each \( i \). Finally a block is a subset of \( \mathcal{R} \) obtained as the union of the \( H \)-orbits inside one equivalence class.

The image of an \( H \)-orbit under an element of \( \mathcal{F}(G) \) is another \( H \)-orbit which is equivalent to the original one. It follows that \( \mathcal{F}(G) \) preserves the blocks, as does \( H \). Moreover this affords a decomposition of \( \mathcal{F}(G) \) as a direct product of groups, one for each block: namely, if \( B \) is a block, define \( \mathcal{F}(G)_B = C_{S(B)}(H) \cap Y_B \) where \( Y_B \) is the Young subgroup corresponding to the partition of \( B \) by the subsets \( B \cap P_i \); then \( \mathcal{F}(G) \) is the direct product of the various groups \( \mathcal{F}(G)_B \).

Suppose that the \( H \)-orbits in the block \( B \) are \( X_1, \ldots, X_s \). These are permuted by \( \mathcal{F}(G) \), or \( \mathcal{F}(G)_B \), yielding a homomorphism \( \mathcal{F}(G)_B \to S_k \) which is easily seen to be split surjective. The kernel of this homomorphism is a direct product of \( s \) copies of the group \( E \) of self-equivalences of \( X_1 \) (in the above sense). The latter is a subgroup of the automorphism group of \( X_1 \) as an \( H \)-set; if \( X_1 \cong H/K \) for some...
subgroup $K$ of $H$, then this automorphism group is $N_H(K)/K$. This completes the description of $\mathcal{F}(G)_B$ as a wreath product $E \wr S_e$ where $E$ is a subquotient of $H$.

There remains to prove the bound on $r_k$. If $X_1$ is an $H$-orbit, then an $H$-equivariant bijection $X_1 \to X_2$ is entirely determined by the image of a single point $p \in X_1$; if this bijection is to afford an equivalence between $X_1$ and $X_2$, then this image must be taken in the $G \times G$-orbit of $p$. As a result, there are fewer orbits equivalent to $X_1$ than elements in the largest $G \times G$-orbit. As $G/Z$ acts freely on $\mathcal{P}$, and a $G \times G$-orbit on $\mathcal{P}$ has size $\leq m^2$, we see that a $G \times G$-orbit on $\mathcal{P}_c$ has size $\leq |Z|/m^2|G|$. □

Keeping in mind that $(\theta, \delta)$ is a homomorphic image of $S_3$, we draw:

**COROLLARY 3.10** – A simple factor occurring in $\mathcal{F}(G)$ must be isomorphic to either:

- $C_2$,
- $C_3$,
- a subquotient of $Out(G)$,
- an alternating group $A_s$ where $s \leq |Z|m^2/|G|$.

Combining this with theorem 3.6 yields a description of the possible simple factors in $\mathcal{T}_G^1$ when $G$ is non-abelian and simple (namely, those in the corollary). Also using that $\mathcal{T}(G)/\mathcal{T}_1(G)$ is abelian (lemma 2.2), we draw:

**COROLLARY 3.11** – Let $G$ be non-abelian and simple. Then a simple factor occurring in $\mathcal{T}(G)$ must be isomorphic to either:

- a cyclic group,
- a subquotient of $Out(G)$,
- an alternating group $A_s$ where $s \leq m^2/|G|$.

Note that the classification of finite simple groups implies by inspection that the group $Out(G)$ is always solvable, so if one accepts this result then we conclude that the list of simple factors reduces to cyclic and alternating groups.

In any case, we can consider those non-abelian simple groups such that $Out(G)$ has order 1, 2 or 4: this includes the alternating groups for $n \geq 5$, almost all Chevalley groups over fields of prime order, and all 26 sporadic groups. The results above show that $\mathcal{T}_1(G)$ can only have, as simple factors, the groups $C_2$ and $C_3$ as well as some alternating groups. In $\mathcal{T}(G)$ one may encounter further cyclic groups.

### 3.5. A complete example

Take $G = PSL_3(F_2)$, a simple group of order 168 with $Out(G) = C_2 = \langle a \rangle$. The following information is obtained with GAP.

There are 114 elements in $\mathcal{P}$; in the following some arbitrary numbering is used for them. Looking at the action of $G \times G$ we obtain the following partition of $\{1, \ldots, 114\}$:

\[
\{1, 10, 27, 28, 96, 106\}, \{2, 11, 52, 57, 82, 86\}, \{3, 12\}, \{62, 63\}, \{107, 109\}, \{4, 13, 29, 49, 51, 54, 56, 70, 101, 102\}, \{5, 6, 31, 32, 71, 72\}, \{7, 34, 75\}, \{8, 84, 97\}, \{9, 36, 53, 73, 83, 85\}, \{14, 16, 38, 60, 91, 114\}, \{15, 61, 76\}, \{17, 98, 110\}, \{18, 40, 58, 59, 78, 99\}, \{19, 21\}, \{20, 41, 43\}, \{22, 42, 64\}, \{39, 77, 90\}, \{23, 25, 44, 48, 67, 79, 87, 103, 108, 111\}, \{24, 45, 68, 94, 105, 112\}, \{33, 35, 74\}, \{26, 46, 69, 89, 93, 104\}, \{30, 37, 50, 55, 100, 113\}, \{47, 65, 66, 80, 81, 88, 92, 95\}.
\]

There are 4 of size 2; 8 of size 3; 9 of size 6; one of size 8 and two of size 10. Thus $Y \cong C_2^4 \times S_6^8 \times S_6^8 \times S_8 \times S_{10}$.

Then we compute
• the permutation induced by $\alpha$: (1,11) (2,10) (3,12) (4,101) (5,16) (6,14) (7,15) (8,17) (9,18) (13,102) (19,21) (20,22) (23,48) (24,26) (25,103) (27,52) (28,57) (29,70) (30,100) (31,60) (32,38) (33,77) (34,61) (35,39) (36,59) (37,113) (40,85) (41,42) (43,64) (44,87) (45,104) (46,94) (47,88) (49,56) (50,55) (51,54) (53,58) (62,63) (65,80) (66,95) (67,111) (68,93) (69,105) (71,114) (72,91) (73,78) (74,90) (75,76) (79,108) (81,92) (82,96) (83,99) (84,110) (86,106) (89,112) (97,98) (107,109).

• the permutation induced by $\theta$: (1,5) (2,14) (3,19) (4,23) (6,10) (7,15) (8,20) (9,24) (11,16) (12,21) (13,25) (17,22) (18,26) (27,31) (28,72) (29,67) (30,100) (32,96) (34,61) (36,68) (38,82) (40,69) (41,97) (42,98) (43,84) (44,49) (45,53) (46,99) (47,88) (48,101) (50,55) (51,79) (52,60) (54,108) (56,87) (57,91) (58,104) (59,93) (62,107) (63,109) (64,110) (66,95) (70,111) (71,106) (73,112) (75,76) (78,89) (81,92) (83,94) (85,105) (86,114) (102,103).

• the permutation induced by $\delta$: (2,3) (4,106) (5,35) (6,8) (7,85) (10,12) (13,100) (14,17) (15,40) (16,39) (19,22) (20,21) (23,68) (24,65) (25,103) (26,80) (27,52) (28,70) (29,57) (30,102) (31,75) (34,73) (36,71) (37,96) (41,63) (42,62) (44,87) (45,111) (46,107) (47,88) (48,93) (49,55) (50,56) (51,54) (53,72) (58,91) (59,114) (60,76) (61,78) (66,108) (67,104) (69,105) (74,84) (79,95) (81,92) (82,113) (83,97) (86,101) (89,112) (90,110) (94,109) (98,99).

We can then ask GAP to compute $\mathcal{G}\mathcal{T}_1(G)$ as the intersection of $Y$ and the centralizer of the three permutations above. We find that $\mathcal{G}\mathcal{T}_1(G)$ has order 512; its centre $Z$ is elementary abelian of order 32; and $\mathcal{G}\mathcal{T}_1(G)/Z$ is elementary abelian of order 16. In fact, finer use of GAP as described below allows us to improve this very last step of the computation, showing that $\mathcal{G}\mathcal{T}_1(G) \cong C_2^2 \times D_8^2$, where $D_8$ is the dihedral group of order 8.

4. Computing explicitly

In this Section we provide details on the use of the computer algebra system GAP in order to apply our results about $\mathcal{S}(G)$. No doubt many readers who are not computer enclined will wish to skip most of this, and we encourage them to browse the results themselves in §4.3 and §4.4.

We have chosen to give the explanation in a mathematical discourse interspersed with GAP commands, for several reasons. First we feel that the readers having little familiarity with computational group theory will be able to understand what follows, while an opportunity is given to get a sense of “what is feasible with just one command” (and by contrast, what requires more effort). On the other hand, we find it useful to indicate some relevant GAP commands to those readers who will wish to implement their own calculations. Finally, we point out that writing this Section in this fashion has been very natural.

4.1. Computing $\mathcal{G}\mathcal{T}_1(G)$. The first task is to construct $\bar{G}$ given $G$, and it is straightforward. We provide some details solely with the purpose of indicating some GAP functions to the reader. One builds the automorphism group of $G$ using \texttt{AutomorphismGroup(G)}, then converts its generators into automorphisms of $G \times G$, see \texttt{DirectProduct(G, G)} and also the function \texttt{GroupHomomorphismByImages}.

Having thus constructed the group $A$ of these automorphisms of $G \times G$, one appeals to \texttt{OrbitsDomain(A, GG)} (where $GG$ is $G \times G$) to find the orbits. For each orbit \texttt{orb}, pick a representative \texttt{orb[1]} (which is an element of $G \times G$), extract the two elements $x$ and $y$ comprising the pair, and check whether we have the equality \texttt{Subgroup(G, [x, y]) = G}. If not, discard the orbit.
Picking representatives in the $r$ remaining orbits, one constructs $\mathcal{G}$ as a subgroup of $G^r$, using \texttt{DirectProduct} again.

As for $\mathcal{G}_T(G)$, we will rely on the next lemma.

\textbf{Lemma 4.1} – Let $C_x$ and $C_y$ be the centralizers of the canonical generators $x$ and $y$ of $\mathcal{G}$, respectively. To each element $\varphi \in \mathcal{G}_T(G)$ we may associate a unique double coset $D \in C_x \backslash \mathcal{G} / C_y$. In fact, if $\varphi$ is induced by the automorphism $\tilde{\varphi}$ of $\mathcal{G}$ satisfying $x \mapsto x^f$ and $y \mapsto y$, then $D$ is the double coset of $f$.

Moreover, we have $1 \in C_x f \theta (f) C_y^{\theta(f)}$, in the same notation. Conversely if $\tilde{\varphi} \in \text{Aut}(\mathcal{G})$ satisfies $x \mapsto x^f$ and $y \mapsto y$ for some $f$ such that $1 \in C_x f \theta (f) C_y^{\theta(f)}$, then the induced $\varphi \in \text{Out}(\mathcal{G})$ commutes with $\theta$.

\textit{Proof.} By definition $\varphi$ can be induced by such an automorphism. If $f_1$ and $f_2$ are both possible choices for $f$, yielding $\tilde{\varphi}_1$ and $\tilde{\varphi}_2$ both inducing $\varphi$, then we see that $\tilde{\varphi}_2 = c_2 \circ \tilde{\varphi}_1$ where $c_2$ is conjugation by $t$. It follows that $y^t = y$ so $t \in C_y$, and that $x^{f_2} = x^{f_1}$ so $s := f_1 t f_2^{-1} \in C_x$. In the end $f_1 = s f_2 t^{-1}$ so $f_1$ and $f_2$ are in the same double coset. The converse is obvious.

We turn to the last statement, which follows from the fact that $\tilde{\varphi} \circ \theta$ and $\theta \circ \tilde{\varphi}$ must differ by an inner automorphism, by definition of $\mathcal{G}_T(G)$. So there must exist an element $t$ such that $y^t = y$ and $x^t = x$. We see that $s = f t \in C_x$ and $u = t \theta (f)^{-1} \in C_y$, so that $1 = s^{-1} f u \theta (f) \in C_x f G y \theta (f) = C_x f \theta (f) C_y^{\theta(f)}$. Again the converse is left to the reader. \hfill $\Box$

This suggest the following method to compute $\mathcal{G}_T(G)$. First, compute the centralizers $C_x := \text{Centralizer}(G, x)$ and $C_y := \text{Centralizer}(G, y)$, where $G$ is $\mathcal{G}$. Then compute $\text{DoubleCosets}(G, C_x, C_y)$ (which is an optimized process in GAP). Now filter the double cosets, by excluding $C_x f G y$ if the unit of $\mathcal{G}$ is not in $\text{DoubleCoset}(C_x, f \ast f k, C_y \ast f k)$, where $f k$ is $\theta (f)$. Also exclude $f$ if $x^f$ and $y$ generate a proper subgroup of $\mathcal{G}$.

The next step is to go through the remaining double cosets, and with each representative $f$ define $\tilde{\varphi}$ with $\text{GroupHomomorphismByImages}(G, G, [x, y], [x^f, y])$ (this is automatically well-defined by (3) of lemma 2.1: however the construction of $\tilde{\varphi}$ by GAP is surprisingly time-consuming, which is the reason for filtering out as many candidates for $f$ as possible before reaching this stage).

Finally, keep only those homomorphisms commuting with $\delta$ in $\text{Out}(\mathcal{G})$, which may be checked with $\text{IsInnerAutomorphism}(\phi \ast \delta \ast \phi^{-1} \ast \delta^{-1})$.

At this point, we have a list of automorphisms of $\mathcal{G}$ representing the elements of $\mathcal{G}_T(G)$ with no repetition; the number of these automorphisms is the order of $\mathcal{G}_T(G)$. Finding the group structure of $\mathcal{G}_T(G)$ can be achieved, rather slowly, with the help of the commands

\begin{verbatim}
A := AutomorphismGroup(GB);
int := InnerAutomorphismsAutomorphismGroup(A);
quo := NaturalHomomorphismByNormalSubgroup(A, int);
\end{verbatim}

One can then create the list of all the elements quo(phi) where phi is taken from our list of automorphisms, and ask GAP to describe the group they generate.

4.2. Computing $\mathcal{P}(G)$. This is several orders of magnitude faster than computing $\mathcal{G}_T(G)$.

The first step is to construct $\mathcal{P}_c$. For this, one builds $G \times G$ and the embedded diagonal copy of $G$ in $G \times G$, and one appeals to $\text{OrbitsDomain}(\text{diagG}, G)$. As above, one filters out an orbit if a representative pair $(x, y)$ fails to generate all of $G$. We obtain $\mathcal{P}_c$, as a GAP list, say $\text{pairsconj}$. Its length is $\ell = r |\text{Out}(G)|$.

Then one must build the orbits of $G \times G$ on $\mathcal{P}_c$, say stored as a list of lists of indices, those indices referring to $\text{pairsconj}$. It does not seem straightforward to rely
on OrbitsDomain for this; instead, for each pairorbit taken in pairsconj, we take
the representative pair:= pairorbit[1], then get its C:= ConjugacyClass(GG, pair) where GG is G × G. Then we run through all the indices, and those corre-
sponding to elements of P which happen to be in C we group together. After this
has been done for each pairorbit, we have a list of lists of indices partitioning the
set {1, . . . , ℓ}; for example in §3.5 we gave the corresponding partition of {1 . . . 114}
when G = PSL3(F2). The corresponding Young subgroup Y may be constructed
easily, but we will argue that it is not the best way to go.

Before turning to this though, we mention that we must construct two further
permutations of {1, . . . , ℓ} corresponding to θ and δ, and for this we follow lemma 3.3
and lemma 3.4. We then do the same for each generator of Out(G) which is not
inner, and compute the corresponding permutations. We let GAP know that we
call H the subgroup of St generated by all these elements.

It is possible at this stage to ask GAP to compute

\[ \text{Intersection( Centralizer(SymmetricGroup(ell), H), Y);} \]

but except in very small examples, the calculation will simply take too long (and
likely exhausts the available memory).

Instead, we partially implement the ideas of proposition 3.9 and its proof. Let
us use the notation introduced in that proof. First we compute the orbits of
H with OrbitsDomain(H, [1..ell]). Then we group these orbits according to a
looser equivalence relation than the one used in the proof of 3.9: we call two or-
bits X1 and X2 equivalent if (i) they are isomorphic as H-sets, which in practice is
checked by verifying whether the corresponding stabilizers are conjugate in
H, cf Stabilizer(H, orbit[1]) and ConjugacyClassesSubgroups(H) which together
allow to associate to each orbit the position of the conjugacy class of the stabilizer
in some numbering; and (ii) the cardinality of X1 ∩ Pi is equal to the cardinality
of X2 ∩ Pi, for each index i. The union of the orbits in one equivalence class we
call a packet, and each packet is a union of “blocks”.

Now each packet is H-invariant, and H(G) splits as a direct product corre-
sponding to the packets, which we see by arguing as we did in the proof of 3.9 with
blocks. We can compute the image H′ of H in the symmetric group of each packet
by applying RestrictedPermNC(g, packet) to each generator g of H. Also, the
Young subgroup Y′ corresponding to the intersections of the Pi’s with the packet
is readily created in GAP.

It is now possible to ask directly for the computation of the centralizer of H′,
and its intersection with Y′. The product of all the resulting groups, for all packets,
is H(G). For each factor in this product, we can prompt GAP for the composition
series, see for example DisplayCompositionSeries(factor). (Finer information,
such as StructureDescription(factor), can still take a very long time).

4.3. Simple groups of small order. We shall give information on GT_i(G) for 12
simple groups of small size. We start with the PSL2 family (recall that PSL2(F_4) ≃ PSL2(F_5) ≃ A_5, PSL2(F_7) ≃ PSL3(F_2) and PSL2(F_9) ≃ A_6):

**Theorem 4.2.** Write D_8 for the dihedral group of order 8.

- (Order 60) GT_1(PSL2(F_4)) is trivial.
- (Order 168) GT_1(PSL2(F_7)) ≃ C_4^3 × D_8.
- (Order 360) GT_1(PSL2(F_9)) ≃ C_4^12 × D_8.
- (Order 504) GT_1(PSL2(F_8)) is trivial.
- (Order 660) GT_1(PSL2(F_11)) ≃ C_2^27 × D_8.
- (Order 1092) GT_1(PSL2(F_13)) ≃ C_2^24 × D_8^17.
- (Order 2448) GT_1(PSL2(F_17)) ≃ C_2^204 × D_8^20.
- (Order 3420) GT_1(PSL2(F_19)) ≃ C_2^33 × D_8^24.
• (Order 4080) $\mathcal{G}T_1(PSL_2(\mathbb{F}_{16}))$ is trivial.

It seems tempting to conjecture that $\mathcal{G}T_1(PSL_2(\mathbb{F}_q)) \cong C_2^a \times D_8^b$, with $a = b = 0$ when $q$ is a power of 2. Let us now turn to the simple group of order 5616:

**Theorem 4.3** – The group $\mathcal{G}T_1(PSL_3(\mathbb{F}_3))$ is isomorphic to

$$C_2^{26} \times D_8^8 \times S_3^4 \times S_6^2 \times S_9^2 \times S_5^2 \times S_8^2 \times S_9^2 \times A_3^3 \times B^8 \times C^5$$

where

$$A = (((C_2 \times C_2 \times C_2 \times C_2) \times A_6) \times C_2) \times C_2,$$

and

$$B = (((C_2 \times D_8) \times C_2) \times C_3) \times C_2,$$

and

$$C = (((C_2 \times C_2 \times C_2) \times A_5) \times C_2).$$

Two more simple groups remain. It has not been possible to obtain a complete description of $\mathcal{G}T_1(G)$ for these (in a reasonable amount of time), no doubt because of the appearance of simple factors of the form $A_s$ for $s$ large (18 and above). At least we have been able to find those simple factors.

**Theorem 4.4** – The direct product of the simple factors of $\mathcal{G}T_1(A_7)$ is

$$C_2^{152} \times C_3^{15} \times A_5^3 \times A_6^3 \times A_7^2 \times A_8 \times A_{10} \times A_{18}.$$  

**Theorem 4.5** – The direct product of the simple factors of $\mathcal{G}T_1(M_{11})$ is

$$C_2^{465} \times C_3^{46} \times A_5^{10} \times A_6^9 \times A_{11}^{10} \times A_3^4 \times A_5^4 \times A_{10} \times A_{11}^2 \times A_{12} \times A_{14} \times A_{15} \times A_{16} \times A_{18}^2 \times A_{19} \times A_{20} \times A_{23} \times A_{28} \times A_{31} \times A_{33}^2.$$  

### 4.4. $p$-groups.

We are going to give information on the orders of $\mathcal{G}T_1(G)$ and $\mathcal{S}(G)$ for a few 2-groups. We offer the following table:

| $n$ | number of groups | $\max |\mathcal{G}T_1(G)|$ | $\max |\mathcal{S}(G)|$ | same order (prime) |
|-----|------------------|--------------------------|------------------------|-------------------|
| 3   | 2                | 1                        | 1                      | 2 (2)             |
| 4   | 6                | 1                        | 1                      | 6 (6)             |
| 5   | 17               | 2                        | 1                      | 14 (14)           |
| 6   | 50               | 4                        | 2                      | 40 (40)           |
| 7   | 159              | 4                        | 16                     | 111 (109)         |

The first column contains a number $n$, indicating that the row is about groups of order $2^n$. Among all these, we select those which can be generated by 2 elements, and which are non-abelian (otherwise $\mathcal{G}T_1(G)$ is not interesting). The next column gives the number of groups which we have kept. The largest order for $\mathcal{G}T_1(G)$, when $G$ runs among those groups, is recorded in the next column, followed by the maximum for $|\mathcal{S}(G)|$. Finally, we give the number of groups for which $|\mathcal{G}T_1(G)| = |\mathcal{S}(G)|$ followed in parenthesis by the number of groups for which this common order is prime (so that $\mathcal{G}T_1(G)$ and $\mathcal{S}(G)$ are at least abstractly isomorphic in these cases).

It may be difficult to comment sensibly on this small-scale analysis. We venture to say that $\mathcal{S}(G)$ is “quite often” abstractly isomorphic to $\mathcal{G}T_1(G)$ (though not always), and that the order of $\mathcal{G}T_1(G)$ seem to grow very slowly with that of $G$ (attempts to prove theoretical bounds on the order of $\mathcal{G}T_1(G)$ have produced very bad results, and there seems to be a phenomenon to understand here).
5. Dessins d’enfants

Keeping the notation as above, we have seen that there is a natural action of $\mathcal{GT}(G)$ on the set $\mathcal{P}/\text{Aut}(G)$. However, in the process of constructing a map from $\mathcal{GT}(G)$ to $\mathcal{P}(G)$, we have also defined an action of $\mathcal{GT}(G)$ (in fact, of $\text{Out}(\mathcal{C})$) on $\mathcal{P}$, the set of pairs in $\mathcal{P}$ up to conjugation. This seems a little ad hoc. In this section we provide a partial “explanation”, showing that at least for $\text{Gal}(\mathcal{C}/\mathbb{Q})$ (a close cousin of $\mathcal{GT}(G)$) there are very good reasons for an action to exist on $\mathcal{P}$.

5.1. The category of dessins. Dessins d’enfants are essentially bipartite graphs drawn on compact, oriented surfaces, forming the 1-skeleton of a CW-complex structure (in particular, the complement of the graph is homeomorphic to a disjoint union of open discs). For precise definitions, and for all statements about dessins to follow, we refer to [Gui].

Dessins form a category $\text{Dessins}$, and the first striking results of the theory are equivalences between $\text{Dessins}$ and various other categories. To name but the most important one: algebraic curves over $\mathbb{C}$ with appropriate ramification, étale algebras over $\mathbb{C}(x)$ with a ramification condition, the other two categories obtained by replacing $\mathbb{C}$ by $\mathcal{C}$, and the category of finite sets with a right action of $F_2$, to be denoted simply by $\text{Sets}_{xy}$ (our usual notation for the generators of $F_2$ being $x, y$).

Some dessins are called regular. Many definitions are possible; in $\text{Sets}_{xy}$, an object is regular if and only it is isomorphic to one of the following particular form: take a finite group $G$ with two distinguished generators $x$ and $y$, and let $F_2$ act on $G$ on the right via the canonical homomorphism $F_2 \rightarrow G$, using right multiplication. The regular dessins $(G, x, y)$ and $(G', x', y')$ (as we will denote them) are isomorphic in $\text{Sets}_{xy}$ if and only if there is a group isomorphism $G \rightarrow G'$ with $x \mapsto x'$, $y \mapsto y'$, as the reader may check.

The automorphism group of the regular dessin $(G, x, y)$ is then $G$ itself, acting on itself by left multiplication. As a result of this discussion, we see that the set of isomorphism classes of regular dessins with automorphism group isomorphic to a fixed group $G$ is in bijection with $\mathcal{P}/\text{Aut}(G)$, the set of pairs of elements generating $G$ under the action of $\text{Aut}(G)$.

Thus we can rephrase the fact that $\mathcal{GT}(G)$ acts on $\mathcal{P}/\text{Aut}(G)$ by saying that $\mathcal{GT}(G)$ acts on the isomorphism classes of regular dessins with automorphism group $G$. What is more, one can define an action of $\mathcal{GT} = \varinjlim G \mathcal{GT}(G)$ on the isomorphism classes of all dessins, regular or not (loc cit).

The other fundamental result is the fact that there is also a natural action of $\text{Gal}(\mathcal{C}/\mathbb{Q})$ on isomorphism classes of dessins. This action factorizes through the map $\Phi: \text{Gal}(\mathcal{C}/\mathbb{Q}) \rightarrow \mathcal{GT}$ (and is indeed instrumental in the very definition of $\Phi$); the classical result due to Belyi and Grothendieck that the action of $\text{Gal}(\mathcal{C}/\mathbb{Q})$ is faithful implies then the injectivity of this homomorphism. In turn one can show that $\mathcal{GT}$ also acts faithfully, and even that the action on regular dessins is already faithful (theorem 5.7 in [Gui]).

5.2. Equivariant dessins. In [Gui] we have defined a certain category $\text{Etale}(\mathcal{C}(x))$, whose objects are étale algebras over $\mathcal{C}(x)$ satisfying a certain ramification property, and we have built an equivalence of categories between $\text{Dessins}$ and $\text{Etale}(\mathcal{C}(x))$. The category $\text{Etale}(\mathcal{C}(x))$ is the one to use in order to define the action of $\text{Gal}(\mathcal{C}/\mathbb{Q})$ on isomorphism classes of dessins.

What is more, we proved in loc cit that each $\lambda \in \text{Gal}(\mathcal{C}/\mathbb{Q})$ actually defines a functor $F_\lambda: \text{Etale}(\mathcal{C}(x)) \rightarrow \text{Etale}(\mathcal{C}(x))$. This gives more precise information on the action, as we proceed to show. We shall work in a very general context, not for the sheer pleasure of writing abstract nonsense, but out of necessity: the equivalence between $\text{Dessins}$ (or the very practical $\text{Sets}_{xy}$) and $\text{Etale}(\mathcal{C}(x))$ is given
by a zig-zag of explicit functors, whose inverses we know very little about beyond the fact that their existence is guaranteed by the axiom of choice.

So let $\mathcal{C}$ be any category at all. Given a group $\Gamma$, we can define the category $\Gamma \mathcal{C}$ whose objects are the pairs $(X, \rho)$ where $X$ is an object of $\mathcal{C}$ and $\rho: \Gamma \to Aut\mathcal{C}(X)$ is a group homomorphism. (In the sequel we shall write $Aut(X)$ rather than $Aut\mathcal{C}(X)$ when no confusion can arise.) The morphisms $(X, \rho) \to (Y, \rho')$ in $\Gamma \mathcal{C}$ are those morphisms $f: X \to Y$ in $\mathcal{C}$ which are equivariant in the sense that the following diagram commutes, for any $g \in \Gamma$:

$$
\begin{array}{ccc}
X & \xrightarrow{\rho(g)} & X \\
\downarrow f & & \downarrow f \\
Y & \xrightarrow{\rho'(g)} & Y
\end{array}
$$

Now let $F$ be a self-equivalence of $\mathcal{C}$. The operation $[X] \mapsto [F(X)]$ gives a permutation of the set of equivalence classes of objects in $\mathcal{C}$, where we have written $[X]$ for the class of $X$.

However, more is true. Simply assuming that $F$ is a functor from $\mathcal{C}$ to itself, there is an induced homomorphism $\alpha_X: Aut(X) \to Aut(F(X))$, and we can employ it to construct a self-functor $\tilde{F}$ of $\Gamma \mathcal{C}$. On objects this is defined as $\tilde{F}(X, \rho) = (F(X), \alpha_X \circ \rho)$, while on morphisms $\tilde{F}$ is simply the restriction of $F$. One checks readily that $\tilde{F}$ is indeed a functor, that $\tilde{F} \circ G = \tilde{F} \circ \tilde{G}$, and that $\tilde{F}$ is the identity of $\Gamma \mathcal{C}$ if $F$ is the identity of $\mathcal{C}$. In particular, if $F$ is a self-equivalence of $\mathcal{C}$, then $\tilde{F}$ is a self-equivalence of $\Gamma \mathcal{C}$.

The comments we have made about $F$ then apply to $\tilde{F}$: there is an induced permutation of the set of isomorphism classes of objects in $\Gamma \mathcal{C}$. Since this discussion was conducted purely in the language of categories, it is clear that $\mathcal{C}$ can be replaced by any category equivalent to it.

We also point out that the group $Aut(\Gamma)$ acts on the isomorphism classes of objects, by the rule $\alpha \cdot (X, \rho) = (X, \rho \circ \alpha)$ (for $\alpha \in Aut(\Gamma)$). When $\alpha$ is inner, we see readily that this action is trivial (in fact if $\alpha$ is conjugation by $t$, then $\rho(t): X \to X$ is an isomorphism in $\Gamma \mathcal{C}$ between $(X, \rho)$ and $(X, \rho \circ \alpha$)). Thus we have an induced action of $Out(\Gamma)$, and it commutes visibly with the permutation induced by $\tilde{F}$.

Coming back to $\mathcal{Etal}(\overline{\mathbb{Q}}/\mathbb{Q})$, where we know that the action of $\lambda \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ is via some functor $F_{\lambda}$, we conclude:

**Proposition 5.1** – There is an action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on the set of isomorphism classes of equivariant dessins in $\Gamma \mathcal{Dessins}$, for any group $\Gamma$. The same holds with $\mathcal{Dessins}$ replaced by any equivalent category, such as $\mathcal{Sets}_{xy}$.

There is also an action of $Out(\Gamma)$, and the two actions commute.

Moreover, the forgetful functor $\Gamma \mathcal{Dessins} \to \mathcal{Dessins}$ induces a $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant map between the sets of isomorphism classes.

Finally, these actions restrict to the set of isomorphism classes of faithful, equivariant dessins.

The last sentence mentions faithful equivariant dessins, that is, those objects $(X, \rho)$ in $\Gamma \mathcal{Dessins}$ such that $\rho$ is injective. The statement holds obviously.

The reader may wish to skip ahead to §5.4 where two concrete examples of equivariant dessins are presented. However a little result is required in order to prove that they are not isomorphic to one another, and we turn to this easy point now.

### 5.3. Equivariant objects in $\mathcal{Sets}_{xy}$

As happens with many other concepts, the category $\mathcal{Sets}_{xy}$ provides the most clean-cut statements about equivariant dessins.
where \(\langle g,h \rangle\) is a group, and \(\varphi : \Gamma \to G\) is a homomorphism, modulo the relation
\[
(g,h,\varphi_1) \sim (g',h',\varphi_2)
\]
which holds (by definition) if and only if there is an automorphism \(\alpha \in \text{Aut}(G)\) and \(t \in G\) such that \(\alpha(g) = g', \alpha(h) = h', \) and \(\alpha(\varphi_1(\gamma)) = t^{-1}\varphi_2(\gamma)t, \) for all \(\gamma \in \Gamma.\)

**Proof.** It is clear from the definitions that a triple \((g,h,\varphi)\) defines a regular object in \(\Gamma \text{-Sets}\), and that each such object can be obtained in this way. What needs to be checked is the condition expressing that \((g,h,\varphi_1)\) and \((g',h',\varphi_2)\) yield isomorphic objects in \(\Gamma \text{-Sets}\).

So assume that there is \(\alpha_1 : G \to G\) giving such an isomorphism; that is, \(\alpha\) is a map of sets which is equivariant with respect to both the \(F_2\)-actions on the right, and the \(\Gamma\)-actions on the left. Let \(t = \alpha_1(1)\) and define \(\alpha_2 : G \to G\) by \(\alpha_2(g) = t^{-1}g.\) Finally put \(\alpha = \alpha_2 \circ \alpha_1.\) We have \(\alpha(1) = 1,\) and as we know that \(\alpha\) commutes with the \(F_2\)-actions on the right, implying in particular that \(\alpha(x) = \alpha(1 \cdot x) = \alpha(1) \cdot x' = x'\) and \(\alpha(y) = y',\) it follows easily that \(\alpha\) is in fact a homomorphism. Moreover for \(\gamma \in \Gamma\) we have \(\alpha(\varphi_1(\gamma)) = \alpha_2(\alpha_1(\varphi_1(\gamma) \cdot 1)) = \alpha_2(\varphi_2(\gamma) \cdot \alpha_1(1)) = t^{-1}\varphi_2(\gamma)t.\)

It is straightforward to reverse this argument and prove, conversely, that whenever \(\alpha\) and \(t\) exist, the objects defined by \((g,h,\varphi_1)\) and \((g',h',\varphi_2)\) are indeed isomorphic in \(\Gamma \text{-Sets}\).

For \(\Gamma = 1\) we find, as we already know, that the set of isomorphism classes of regular dessins with \(G\) as automorphism group is in bijection with \(\mathcal{P}/\text{Aut}(G)\). More interesting is the following

**Corollary 5.3** – For \(\Gamma = G,\) we find that the set of isomorphism classes in \(G \text{-Sets}\) of faithful, regular objects, with \(G\) as automorphism group, is in bijection with \(\mathcal{P}_c.\)

In particular \(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\) acts on \(\mathcal{P}_c\) as well as \(\mathcal{P}/\text{Aut}(G)\), and the map 
\[
\mathcal{P}_c \longrightarrow \mathcal{P}/\text{Aut}(G)
\]
is \(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\)-equivariant.

**Proof.** Start with an object \((g,h,\varphi)\). Since we consider only faithful objects, and since \(\Gamma = G\) here, the map \(\varphi\) is an automorphism. Taking \(\alpha = \varphi^{-1}\), the proposition, we see that the same object is represented by \((g',h',id)\) where \(g' = \varphi^{-1}(g),\) \(h' = \varphi^{-1}(h)\) (and \(id\) is the identity map).

We conclude that the objects under consideration can be represented by triples of the form \((g,h,\varphi)\). By the proposition, \((g_1,h_1,\varphi)\) and \((g_2,h_2,\varphi)\) represent isomorphic objects precisely when there is an automorphism \(\alpha\) of the form \(\alpha(\gamma) = t^{-1}\gamma t,\) that is an inner automorphism, taking \(g_1\) to \(g_2\) and \(h_1\) to \(h_2\). In the end the set of isomorphism classes is precisely \(\mathcal{P}_c.\)

Of course this falls short of a proof that \(\mathcal{GT}\), let alone \(\mathcal{GT}(G)\) or \(\text{Out}(\overline{\mathbb{G}})\), acts on \(\mathcal{P}_c,\) but this corollary makes the result much less surprising and much more natural. Also note that our ad hoc arguments to the effect that \(\text{Out}(\overline{\mathbb{G}})\) does act on this set do not guarantee any compatibility with the action of the image of \(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Out}(\overline{\mathbb{G}}).\)
5.4. A complete example; cyclic dessins. We follow the usual workflow for dessins. We start with an informal picture:

The theory predicts that enough information is conveyed in the picture to define an object unambiguously. To proceed with this, we move to \( \mathcal{S}ets_{x,y} \). Having numbered the “darts”, we write down the two permutations \( x \) and \( y \) of the set \( \{1, \ldots, 12\} \) which take each dart to the next one in the positive rotation around the incident black, resp. white, vertex. These are

\[
x = (123)(456)(789)(10, 11, 12) \quad \text{and} \quad y = (14)(2, 10)(37)(59)(6, 11)(8, 12)
\]

Then \( X = \{1, \ldots, 12\} \) is our object in \( \mathcal{S}ets_{x,y} \). The subgroup \( G \) of \( S_{12} \) generated by \( x \) and \( y \) has order 12, and is in fact isomorphic to \( A_4 \); it acts freely and transitively, and it follows that \( X \) is regular. For the rest of the discussion, we identify \( G \) with the set \( \{1, \ldots, 12\} \), by identifying \( g \in G \) with the image of 1 under \( g \), and the natural action of \( G \) on this set is by right multiplication.

The automorphism group of \( X \) is given by all the multiplications by elements of \( G \) on the left on \( \{1, \ldots, 12\} = G \). Thus this group is (isomorphic to) \( G \) itself. For example the permutation \( \tilde{x} \) of the set \( \{1, \ldots, 12\} \) corresponding to the action of \( x \) by left multiplication is the unique automorphism of \( X \) taking 1 to 2; from the picture we know that this must be the rotation around the black vertex incident with the dart 1, that is

\[
\tilde{x} = (123)(4, 10, 7)(6, 12, 9)(11, 8, 5)
\]

(This can also be checked by computation.) A similar reasoning gives

\[
\tilde{y} = (14)(8, 12)(2, 5)(3, 6)(10, 9)(11, 7)
\]

See Example 3.8 in [Gui] for more details.

Let us define equivariant dessins with \( X \) as the underlying dessin. Let \( C_3 = \langle r \rangle \) be the cyclic group of order 3, and define two homomorphisms \( \varphi_1, \varphi_2 : C_3 \to G \) by \( \varphi_1(r) = x \) and \( \varphi_2(r) = x^{-1} \). Then \( X_1 = (G, x, y, \varphi_1) \) and \( (G, x, y, \varphi_2) \) are \( C_3 \)-dessins.

Let us show that they are not isomorphic. If they were, by proposition 5.2 there would exist \( \alpha \in \text{Aut}(G) \) and \( t \in G \) such that \( \alpha(x) = x \), \( \alpha(y) = y \) and \( \alpha(\varphi_1(r)) = t^{-1} \varphi_2(r)t \). The first two conditions impose \( \alpha = Id \) of course, and the last one reads \( x = t^{-1}x^{-1}t \). However \( x \) and \( x^{-1} \) are not conjugate in \( G \), so \( t \) cannot exist.

To explore the Galois action, we continue with the usual workflow, and compute a Belyi map. A possible choice is

\[
f(z) = -64\frac{(z^3 + 1)^3}{(z^3 - 8)^3z^3}
\]

(taken from [MZ00]). The simple fact that the coefficients of \( f \) are in \( \mathbb{Q} \) means that \( X \) is fixed by \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \). However, we shall see that \( X_1 \) and \( X_2 \) are not.

First we can ask a computer to produce a picture of \( f^{-1}([0, 1]) \).
Here the white vertex on the real axis is $w = -(1 + \sqrt{3})$, a root of $w^2 + 2w - 2 = 0$. The dart from $\infty$ to $w$ we number as 1, and we number all the others so that $x$ and $y$ are as above.

We know that there must exist Moebius transformations inducing the actions of $\tilde{x}$ and $\tilde{y}$ as above, and we find easily that they are

$$\mu_x : z \mapsto j^2 z \quad \text{and} \quad \mu_y : z \mapsto \frac{-z + 2}{z + 1}$$

respectively, where $j = e^{2\pi i}$. (The use of $j^2$ rather than $j$ mirrors the fact that we consider the positive rotation around $\infty$, which is also the clockwise rotation around 0.) We can now think of $X$ as the Belyi pair $(\mathbb{P}^1, f)$ and of $\text{Aut}(X)$ as the group generated by $\mu_x$ and $\mu_y$. The $C_3$-dessins $X_1$ and $X_2$ are obtained from $X$ by throwing in the homomorphism $C_3 \to \text{Aut}(X)$ mapping $r$ to $\mu_x$ or $\mu_x^{-1}$.

If $\lambda \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ satisfies $\lambda(j) = j^2$ (and there are such elements!), then the action of $\lambda$ exchanges $X_1$ and $X_2$. [In fact, since the dessin $X$ is fixed by $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have a homomorphism $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Out}(\text{Aut}(X))$. The non-trivial element of $\text{Out}(A_4) \cong C_2$ sends $x$ to $x^{-1}$ and $y$ to $y^{-1} = y$.]

In a nutshell: the tetrahedron can be made into a $C_3$-dessin in two non-isomorphic ways, by picking a rotation of order 3 whose axis carries a black vertex and the centre of the opposite face; the two choices are afforded by the two possibilities for the orientation; these are interchanged by the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

More generally, let us call a dessin cyclic when it is a $C_n$-equivariant dessin for some $n$. Starting with a regular dessin $(G, x, y)$, a cyclic structure on it is simply given by an element of $G$ of order dividing $n$; the non-isomorphic cyclic structures correspond to the conjugacy classes of such elements. If the dessin is fixed by the Galois group, then $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ permutes these conjugacy classes.

**References**

[Drin90] V. G. Drinfel’d, *On quasitriangular quasi-Hopf algebras and on a group that is closely connected with $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*, Algebra i Analiz 2 (1990), no. 4, 149–181. MR 1080203 (92f:16047)

[Gui] Pierre Guillot, *An elementary approach to dessins d’enfants and the Grothendieck-Teichmüller group*, to appear in L’enseignement Mathématique.

[Isa08] I. Martin Isaacs, *Finite group theory*, Graduate Studies in Mathematics, vol. 92, American Mathematical Society, Providence, RI, 2008. MR 2426855 (2009e:20029)

[Jon] Gareth Jones, *Regular dessins with a given automorphism group*, preprint.
[MZ00] Nicolas Magot and Alexander Zvonkin, \textit{Belyi functions for Archimedean solids}, Discrete Math. \textbf{217} (2000), no. 1-3, 249–271, Formal power series and algebraic combinatorics (Vienna, 1997). MR 1766270 (2001m:14043)