A brief tour of Grothendieck-Teichmüller theory

Daniel Miller

September 2, 2014

Everything in this brief note is inspired by Grothendieck’s revolutionary letter [Gro97].

1 Motivation from topology

Let’s start with a slightly unorthodox take on the (standard) fundamental group of a topological space. Let $X$ be a “nice” space (e.g. a manifold) and let $x \in X$ be a chosen basepoint. Let $p : C \to X$ be a cover. If $\gamma \in \pi_1(X, x)$ is a path, it induces a permutation of the set $p^{-1}(x)$ in the usual way [draw picture]. We get in this way the monodromy representation $\rho_C : \pi_1(X, x) \to \text{Aut}(p^{-1}(x))$.

Introduce a bit of notation and write $F_q(C) = p^{-1}(x)$ if $C \to X$ is a cover. The monodromy representation is functorial in the sense that it gives us a representation $\rho : \pi_1(X, x) \to \text{Aut}(F_q)$. In fact, this “universal” monodromy representation is an isomorphism, i.e. $\pi_1(X, x) \cong \text{Aut}(F_q)$. Our general heuristic towards fundamental groups will be that there is a category $\mathcal{C}$ of “covers” and a functor $F : \mathcal{C} \to \text{set}$. One puts $\pi_1(C) = \text{Aut}(F)$. This is naturally a topological group, and if everything is sufficiently nice, induces an equivalence $\mathcal{C} \cong \text{set}(\pi)$.

Finally, recall a bit of group theory. If $1 \to \pi \to H \to G \to 1$ is a short exact sequence of groups, then there is a natural representation $\rho : G \to \text{Out}(\pi)$. For $g \in G$, put $\rho(g)(x) = \bar{g}x\bar{g}^{-1}$. It is essentially trivial that the class of $\rho(g)$ in $\text{Out}(\pi)$ does not depend on the choice of a lift $\tilde{g}$ of $g$ to $H$.

2 Some Galois theory

Let $q = p^f$ be a prime power, and let $F_q$ be the finite field with $q$ elements. Let $\overline{F}_q$ be an algebraic closure of $F_q$. Let’s compute $G_{F_q} = \text{Gal}(\overline{F}_q/F_q)$. Let $f(r)(x) = x^q$; this gives an element $f_r \in G_{F_q}$. So then $f_r^q \subset G_{F_q}$. But we haven’t exhausted $G_{F_q}$. Choose a sequence of numbers $a_n \in \mathbb{Z}/n!$ such that $a_{n+1} \equiv a_n (\text{mod } n!)$. Then $f_r^a$ makes sense as an element of $G_{F_q}$. For $x \in F_q^a$, choose $n$ such that $x \in F_q^a$ and put $f(r)^a(x) = f(r)^a(x)$; it is easy to see that this is a well-defined element of $G_{F_q}$. Let $\widehat{\mathbb{Z}}$ be the group of sequences $a = (a_n) \in \prod_n \mathbb{Z}/n!$ such that $a_{n+1} \equiv a_n (\text{mod } n!)$. This is naturally a compact topological group, and $a \mapsto f_r^a$ is an isomorphism $\widehat{\mathbb{Z}} \cong G_{F_q}$.

It seems that Galois groups are naturally topological groups. Let $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. For $x \in \overline{\mathbb{Q}}$, put $G_{\mathbb{Q}}(x) = \text{Stab}_{G_{\mathbb{Q}}}(x)$. The $G_{\mathbb{Q}}(x)$ form the basis for a topology (the Krull topology), with which $G_{\mathbb{Q}}$ is a compact, totally disconnected topological group with a basis of open normal subgroups of finite index. Such groups are called profinite. Understanding $G_{\mathbb{Q}}$ is the central object of algebraic number theory. Unfortunately, studying $G_{\mathbb{Q}}$ directly has not been very fruitful. The best approach up till now has been to study $G_{\mathbb{Q}}$ via its representations. A good source of these representations are the fundamental groups of varieties over $\mathbb{Q}$.

3 Algebraic fundamental groups

Now let $X$ be a variety over $\mathbb{Q}$. We won’t define this precisely, but you should think of subsets of $\mathbb{A}^n$ or $\mathbb{P}^n$ cut out by polynomials with coefficients in $\mathbb{Q}$. It makes sense to ask for complex solutions to these polynomial
equations, and $X(\mathbb{C})$ is naturally a topological space. If $X$ is smooth, then $X(\mathbb{C})$ is a complex manifold.

We want a good category of covers of $X$. We will say that a morphism $p : C \to X$ of varieties over $\mathbb{Q}$ (that means that the polynomials defining $p$ have coefficients in $\mathbb{Q}$) is a cover if the induced map $f : X(\mathbb{C}) \to Y(\mathbb{C})$ is a cover in the sense of differential geometry (a local analytic diffeomorphism). Choose a point $x \in X(\mathbb{Q})$ and let $F_x(C) = p^{-1}(x)$. Since everything is algebraic, $F_x(C)$ is a finite set. Put $\pi_1(X) = \text{Aut}(F_x)$; this is naturally a profinite group. Indeed,

$$\pi_1(X) = \left\{ (\sigma_C) \in \prod_{p : C \to X} F_x(C) : f \circ \sigma_C = \sigma_D \circ f \text{ for all } f : C \to D \text{ between covers} \right\}.$$ 

The group $\prod_{C} F_x(C)$ is a product of finite (hence compact) groups, so it is compact.

If $X$ is a variety over $\mathbb{Q}$, let $X_{\mathbb{Q}}$ be $X$, except now that we allow maps $f : Y \to X$ where the equations defining $Y$ and the polynomials defining $f$ have coefficients in $\mathbb{Q}$. We can define a category of covers of $X_{\mathbb{Q}}$ in the same way, and get a fundamental group $\pi_1(X_{\mathbb{Q}})$. There is a canonical short exact sequence

$$1 \to \pi_1(X_{\mathbb{Q}}) \to \pi_1(X) \to G_\mathbb{Q} \to 1.$$ 

Basically, if $\gamma \in \pi_1(X)$, we need to define how $\gamma$ acts on finite Galois extensions $F/\mathbb{Q}$. The variety $X \times F$ is a cover of $X$, so $\gamma$ acts on $X \times F$. This action must come from one of $\gamma$ on $F$ itself.

There is a nice comparison theorem. If $X$ is a variety over $\mathbb{Q}$, then $\pi_1(X_{\mathbb{Q}})$ is the profinite completion of the topological fundamental group $\pi_1(X(\mathbb{C}))$. Thus:

$$\pi_1(P^1_{\mathbb{Q}} \setminus \{0, \infty\}) = \hat{\mathbb{Z}}$$
$$\pi_1(P^1_{\mathbb{Q}} \setminus \{0, 1, \infty\}) = \hat{\mathbb{F}}_2$$
$$\cdots$$
$$\pi_1(P^1_{\mathbb{Q}} \setminus \{x_0, \ldots, x_n\}) = \hat{\mathbb{F}}_n.$$ 

Note that if we choose $x \in X(\mathbb{Q})$, then the surjection $\pi_1(X) \to G_\mathbb{Q}$ has a section. This gives a representation $G_\mathbb{Q} \to \text{Aut}(\pi_1(X_{\mathbb{Q}}))$. We will be interested in a clever choice of $X$, to be described in the next section.

### 4 Teichmüller tower

Let $P^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ be the Riemann sphere. Recall that if $\{x_1, x_2, x_3\}$ are three distinct points in $P^1$, then there is a unique fractional linear transformation $\mu(z) = \frac{az + b}{cz + d}$ such that $\mu(x_1) = 0$, $\mu(x_2) = 1$ and $\mu(x_3) = \infty$. Let $\text{PGL}_2(\mathbb{C})$ be the group of fractional linear transformations. We can rephrase this by saying that $\text{PGL}_2(\mathbb{C})$ acts simply transitively on $P^1(\mathbb{C})$.

Let $n \geq 1$ be an integer. Let $\Delta \subset (P^1)^n$ be the “weak diagonal” consisting of all tuples $(x_1, \ldots, x_n)$ with some $x_i = x_j$. Put

$$\mathcal{M}_{0,n} = \frac{(P^1(\mathbb{C}))^n \setminus \Delta}{\text{PGL}_2(\mathbb{C})}.$$ 

A priori, this is just a topological space. However, we could have repeated the definition with varieties:

$$\mathcal{M}_{0,n} = \frac{(P^1)^n \setminus \Delta}{\text{PGL}(2)},$$

and gotten a variety over $\mathbb{Q}$. As a set, $\mathcal{M}_{0,n}$ is the space of isomorphism classes of $n$ marked points on $P^1(\mathbb{C})$. Thus

$$\mathcal{M}_{0,4} = P^1 \setminus \{0, 1, \infty\}$$
$$\mathcal{M}_{0,5} = (\mathcal{M}_{0,4})^2 \setminus \Delta.$$
There are obvious maps $\mathcal{M}_{0,n+1} \to \mathcal{M}_{0,n}$ given by “forget a point.” Denote by $\mathcal{M}_{0,*}$ the whole collection of the $\mathcal{M}_{0,n}$ with these maps. Note that $\dim(\mathcal{M}_{0,n}) = \max\{0, n - 3\}$.

More generally, if $3g - 3 + n \geq 0$, let $\mathcal{M}_{g,n}$ be the “moduli space of genus $g$ curves with $n$ marked points. As a topological space, this has an easy description. Let $S_{g,n}$ be a genus $g$ surface with $n$ marked points, let $\mathcal{T}_{g,n}$ be the space of triples $(X, x, \phi)$ where $X$ is a genus $g$ curve, $x = (x_1, \ldots, x_n)$ is a tuple of $n$ distinct points in $X$, and $\phi : S_{g,n} \to X$ is a diffeomorphism. The space $\mathcal{T}_{g,n}$ is simply connected. Let $\Gamma_{g,n} = \pi_0\left(\text{Diff}^+(S_{g,n})\right)$, the space of connected components in the group of orientation-preserving, boundary fixing diffeomorphisms of $S_{g,n}$. This is the mapping class group of $S_{g,n}$. The group $\Gamma_{g,n}$ acts freely on $\mathcal{T}_{g,n}$ and (topologically) we have $\mathcal{M}_{g,n} = \mathcal{T}_{g,n}/\Gamma_{g,n}$. The space $\mathcal{M}_{g,n}$ exists as a variety of dimension $3g - 3 + n$ over $\mathbb{Q}$. We will only need $\mathcal{M}_{0,n}$. Note that the geometric fundamental group $\pi_1((\mathcal{M}_{g,n})^{\mathbb{Q}}) = \hat{\Gamma}_{g,n}$, where we write $\Gamma_{g,n}$ for the profinite completion of $\Gamma_{g,n}$. Since $\mathcal{M}_{0,4} = \mathbb{P}^1 \setminus \{0, 1, \infty\}$, we have $\Gamma_{0,4} = \hat{\mathbb{F}}_2$.

By [Loc97], there is a coherent way of choosing basepoints for the $\mathcal{M}_{g,n}$ in such a way that the actions of $G_{\mathbb{Q}}$ on $\Gamma_{g,n}$ are compatible with the degeneracy maps $\Gamma_{g,n+1} \to \Gamma_{g,n}$. We write $\mathcal{M}_{*,*}$ for the whole collection of the $\mathcal{M}_{g,n}$'s, and $\rho : G_{\mathbb{Q}} \to \text{Aut}(\Gamma_{*,*})$ for the induced action.

5 The Grothendieck-Teichmüller group $\hat{\Gamma}$

Define $\hat{\Gamma} = \text{Aut}(\Gamma_{*,*})$. By the theory of “base points at infinity” we have a representation $\rho : G_{\mathbb{Q}} \to \hat{\Gamma}$. A fundamental theorem of Belyï is that $\rho$ is an injection. The Grothendieck-Teichmüller conjecture states that $G_{\mathbb{Q}} \to \hat{\Gamma}$. Even if this were proved, it wouldn’t a priori be especially helpful if we couldn’t determine $\hat{\Gamma}$. Fortunately, it is possible to pin down $\hat{\Gamma}$ as a subgroup of $\text{Aut}(\hat{\mathbb{F}}_2)$. First, it is known that $\text{Aut}(\Gamma_{*,*}) = \text{Aut}(\Gamma_{0,\leq 5})$, i.e. an automorphism of the Teichmüller tower is determined by its restriction to $\Gamma_{0,4}$ and $\Gamma_{0,5}$. Moreover, it is shown in [Sch97] that this restriction has an explicit description.

To be precise, for $(\lambda, f) \in \hat{\mathbb{Z}}^\times \times [\hat{\mathbb{F}}_2^2]$, consider the map $\phi_{\lambda,f} : \hat{\mathbb{F}}_2 \to \hat{\mathbb{F}}_2$ given by

$$\phi_{\lambda,f}(x) = x^\lambda$$
$$\phi_{\lambda,f}(y) = f^{-1} \cdot y^\lambda \cdot f.$$

Here we have chosen generators $\hat{\mathbb{F}}_2 = \langle x, y \rangle$. Let

$$P_5 = \langle \sigma_1, \ldots, \sigma_4 : \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, \sigma_4 \sigma_3 \sigma_2 \sigma_1 \sigma_2 \sigma_3 \sigma_4 = 1, (\sigma_2 \sigma_3 \sigma_4^5)^{-1} = 1 \rangle$$

and, for $i \in \mathbb{Z}/5$, let $x_{i+1} = \sigma_{i-1} \cdots \sigma_{i+2} \sigma_{i+1}^{-1} \sigma_{i+3} \cdots \sigma_i$ (check that this is independent of the class of $i$). A good reference here is [Iha91].

Let $\theta \in \text{Aut}(\hat{\mathbb{F}}_2)$ be $\theta(x) = y$, $\theta(y) = x$, and $\omega(x) = y$, $\omega(y) = (xy)^{-1}$. Suppose $\phi_{\lambda,f}$ is invertible. Then $\phi_{\lambda,f}$ extends to an automorphism of $\Gamma_{0,5}$ if and only if

$$f(x,y) f(y,x) = 1 \quad (I)$$
$$f(x,z)^m f(y,z) y^m f(x,y) x^m = 1 \text{ if } xyz = 1 \text{ and } m = \frac{1}{2}(\lambda - 1) \quad (II)$$
$$f(x_{1,2}, x_{2,3}) f(x_{3,4}, x_{4,0}) f(x_{0,1}, x_{1,2}) f(x_{2,3}, x_{3,4}) f(x_{4,0}, x_{0,1}) = 1 \quad (III)$$

The last relation takes place in $P_5$, where we interpret $f(a,b)$ (for $a,b$ elements of any group) in the obvious way. So conjecturally $G_{\mathbb{Q}}$ is isomorphic to the subgroup of $\text{Aut}(\hat{\mathbb{F}}_2)$ consisting of $\phi_{\lambda,f}$ satisfying (I), (II), and (III).

Finally. If $p : C \to \mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\}$ is a Belyï cover, let $\Gamma = p^{-1}[0,1]$; this is a graph in $C$ with edges marked black and white for lying over 0 and 1. It is an example of a dessin d’enfant: a connected graph
with a two-coloring of the vertices, for which each edge has endpoints of different colors. See the AMS article *What is a Dessin d’Enfant* by Leonardo Zapponi for examples.

**References**


