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* $\rho_C : \pi_1(X, x) \to \operatorname{Aut}(p^{-1}(x))$.

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

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 $\rho : G \to \operatorname{Out}(\pi)$. For $g \in G$, put $\rho(g)(x) = \widetilde{g} x \widetilde{g}^{-1}$. It is essentially trivial that the class of $\rho(g)$ in $\operatorname{Out}(\pi)$ does not depend on the choice of a lift $\widetilde{g}$ of g to H.

2 Some Galois theory

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

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

3 Algebraic fundamental groups

Now let X be a variety over $\mathbf{Q}$. I won't define this precisely, but you should think of subsets of $\mathbf{A}^n$ or $\mathbf{P}^n$ cut out by polynomials with coefficients in $\mathbf{Q}$. It makes sense to ask for complex solutions to these polynomial equations, and $X(\mathbf{C})$ is naturally a topological space. If X is smooth, then $X(\mathbf{C})$ 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 $\mathbf{Q}$ (that means that the polynomials defining p have coefficients in $\mathbf{Q}$) is a *cover* if the induced map $f : X(\mathbf{C}) \to Y(\mathbf{C})$ is a cover in the sense of differential geometry (a local analytic diffeomorphism). Choose a point $x \in X(\mathbf{Q})$ and let $F_x(C) = p^{-1}(x)$. Since everything is algebraic, $F_x(C)$ is a finite set. Put $\pi_1(X) = \mathrm{Aut}(F_x)$; 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 $\mathbf{Q}$, let $X_{\overline{\mathbf{Q}}}$ 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 $\overline{\mathbf{Q}}$. We can define a category of covers of $X_{\overline{\mathbf{Q}}}$ in the same way, and get a fundamental group $\pi_1(X_{\overline{\mathbf{Q}}})$. There is a canonical short exact sequence

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

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

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

$$\begin{aligned}
\pi_1(\mathbf{P}^1_{\overline{\mathbf{Q}}} \smallsetminus \{0,\infty\}) &= \widehat{\mathbf{Z}} \\
\pi_1(\mathbf{P}^1_{\overline{\mathbf{Q}}} \smallsetminus \{0,1,\infty\}) &= \widehat{F_2} \\
&\cdots \\
\pi_1(\mathbf{P}^1_{\overline{\mathbf{Q}}} \smallsetminus \{x_0,\dots,x_n\}) &= \widehat{F_n}.
\end{aligned}$$

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

4 Teichmüller tower

Let $\mathbf{P}^1(\mathbf{C}) = \mathbf{C} \cup \{\infty\}$ be the Riemann sphere. Recall that if $\{x_1, x_2, x_3\}$ are three distinct points in $\mathbf{P}^1$, 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 $\mathrm{PGL}_2(\mathbf{C})$ be the group of fractional linear transformations. We can rephrase this by saying that $\mathrm{PGL}_2(\mathbf{C})$ acts simply transitively on $\mathbf{P}^1(\mathbf{C})$.

Let $n \geqslant 1$ be an integer. Let $\Delta \subset (\mathbf{P}^1)^n$ be the "weak diagonal" consisting of all tuples $(x_1, \dots, x_n)$ with some $x_i = x_j$. Put

$$\mathcal{M}_{0,n} = \left((\mathbf{P}^1(\mathbf{C}))^n \smallsetminus \Delta\right) / \mathrm{PGL}_2(\mathbf{C}).$$

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

$$\mathcal{M}_{0,n} = \left((\mathbf{P}^1)^n \smallsetminus \Delta\right) / \mathrm{PGL}(2),$$

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

$$\begin{aligned}
\mathcal{M}_{0,4} &= \mathbf{P}^1 \smallsetminus \{0,1,\infty\} \\
\mathcal{M}_{0,5} &= (\mathcal{M}_{0,4})^2 \smallsetminus \Delta.
\end{aligned}$$

There are obvious maps $\mathcal{M}_{0,n+1} \to \mathcal{M}_{0,n}$ given by "forget a point." Denote by $\mathcal{M}_{0,\bullet}$ 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 $3g - 3 + n \geqslant 0$, 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 $(X, \boldsymbol{x}, \phi)$ where X is a genus g curve, $\boldsymbol{x} = (x_1, \dots, x_n)$ is a tuple of n distinct points in X, and $\phi : S_{g,n} \xrightarrow{\sim} X$ is a diffeomorphism. The space $\mathcal{T}_{g,n}$ is simply connected. Let $\boldsymbol{\Gamma}_{g,n} = \pi_0\left(\mathrm{Diff}^+(S_{g,n})\right)$, 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 $\mathbf{Q}$. We will only need $\mathcal{M}_{0,n}$. Note that the geometric fundamental group $\pi_1((\mathcal{M}_{g,n})_{\overline{\mathbf{Q}}}) = \boldsymbol{\Gamma}_{g,n}$, where we write $\boldsymbol{\Gamma}_{g,n}$ for the profinite completion of $\Gamma_{g,n}$. Since $\mathcal{M}_{0,4} = \mathbf{P}^1 \smallsetminus \{0, 1, \infty\}$, we have $\boldsymbol{\Gamma}_{0,4} = \widehat{F_2}$.

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

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

Define $\widehat{\mathrm{GT}} = \mathrm{Aut}(\boldsymbol{\Gamma}_{\bullet,\bullet})$. By the theory of "base points at infinity" we have a representation $\rho : G_{\mathbf{Q}} \to \widehat{\mathrm{GT}}$. A fundamental theorem of Belyĭ is that ρ is an injection. The *Grothendieck-Teichmüller conjecture* states that $G_{\mathbf{Q}} \xrightarrow{\sim} \widehat{\mathrm{GT}}$. Even if this were proved, it wouldn't a priori be especially helpful if we couldn't determine $\widehat{\mathrm{GT}}$. Fortunately, it is possible to pin down $\widehat{\mathrm{GT}}$ as a subgroup of $\mathrm{Aut}(\widehat{F_2})$. First, it is known that $\mathrm{Aut}(\boldsymbol{\Gamma}_{\bullet,\bullet}) = \mathrm{Aut}(\boldsymbol{\Gamma}_{0,\leqslant 5})$, i.e. an automorphism of the Teichmüller tower is determined by its restriction to $\boldsymbol{\Gamma}_{0,4}$ and $\boldsymbol{\Gamma}_{0,5}$. Moreover, it is shown in [Sch97] that this restriction has an explicit description.

To be precise, for $(\lambda, f) \in \widehat{\mathbf{Z}}^\times \times [\widehat{F_2}, \widehat{F_2}]$, consider the map $\phi_{\lambda,f} : \widehat{F_2} \to \widehat{F_2}$ given by

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

Here we have chosen generators $F_2 = \langle x, y \rangle$. Let

$$\begin{aligned}P_5 = \langle \sigma_1, \dots, \sigma_4 :& \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \\ & \sigma_i \sigma_j = \sigma_j \sigma_i \\ & \sigma_4 \sigma_3 \sigma_2 \sigma_1^2 \sigma_2 \sigma_3 \sigma_4 = 1 \\ & (\sigma_1 \sigma_2 \sigma_3 \sigma_4)^5 = 1 \rangle\end{aligned}$$

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

Let $\theta \in \mathrm{Aut}(\widehat{\mathbf{F}_2})$ 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 $\boldsymbol{\Gamma}_{0,5}$ if and only if

$$f(x,y) f(y,x) = 1 \tag{I}$$

$$f(z,x) z^m f(y,z) y^m f(x,y) x^m = 1 \text{ if } xyz = 1 \text{ and } m = \frac{1}{2}(\lambda - 1) \tag{II}$$

$$f(x_{1,2}, x_{2,3}) f(x_{3,4}, x_{4,0}) f(x_{0,1}, x_{1,2}) f(x_{2,3}, x_{3,4}) f(x_{4,0}, x_{0,1}) = 1 \tag{III}$$

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 $G_{\mathbf{Q}}$ is isomorphic to the subgroup of $\mathrm{Aut}(\widehat{F_2})$ consisting of $\phi_{\lambda,f}$ satisfying (I), (II), and (III).

Finally. If $p : C \to \mathbf{P}^1_{\overline{\mathbf{Q}}} \smallsetminus \{0, 1, \infty\}$ is a Belyĭ 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

[Gro97] Alexandre Grothendieck. Esquisse d'un programme. In *Geometric Galois actions, 1*, volume 242 of *London Math. Soc. Lecture Note Ser.*, pages 5–48. Cambridge Univ. Press, 1997. With an English translation on pp. 243–283.

[Iha91] Yasutaka Ihara. Braids, Galois groups, and some arithmetic functions. In *Proceedings of the International Congress of Mathematicians, Vol. I, I (Kyoto, 1990)*, pages 99–120, Tokyo, 1991. Math. Soc. Japan.

[Loc97] Pierre Lochak. The fundamental groups at infinity of the moduli spaces of curves. In *Geometric Galois actions, 1*, volume 242 of *London Math. Soc. Lecture Note Ser.*, pages 139–158. Cambridge Univ. Press, 1997.

[Sch97] Leila Schneps. The Grothendieck-Teichmüller group $\widehat{\mathrm{GT}}$: a survey. In *Geometric Galois actions, 1*, volume 242 of *London Math. Soc. Lecture Note Ser.*, pages 183–203. Cambridge Univ. Press, 1997.