Introduction to anabelian geometry

Columbia Undergrad Math Society Talk, 10/13/21

Caleb Ji

Contents

1 Galois groups

1.1 Field extensions

Even if you don't know the definition of a field, you surely know many examples of them. For example, here are some commonly used ones.

$$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt[3]{2}, i), \overline{\mathbb{Q}}, \mathbb{C}(t), \mathbb{F}_p, \mathbb{F}_{p^k}$$

Essentially, what makes these sets fields is the fact that there are two operations $+, \cdot$ which satisfy commutativity, associativity, and distributivity, which also have inverses – with the important exception of 0 not having a multiplicative inverse.

Let's consider the basic case of $\mathbb{R} \subset \mathbb{C}$. The way we get from $\mathbb{R}$ to $\mathbb{C}$ is by defining a number i to satisfy $i^2 = -1$, and constructing all numbers of the form $a + bi; a, b \in \mathbb{R}$. But once we have constructed $\mathbb{C}$, we note that we could have just as easily have chosen $-i$ in place of i to use to construct $\mathbb{C}$ from $\mathbb{R}$. This ambiguity is described by the **automorphism group** $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.

Definition 1.1. *A field automorphism $\sigma \in \mathrm{Aut}(K)$ is a surjective field endomorphism. The group $\mathrm{Aut}(L/K)$ denotes the subgroup of $\mathrm{Aut}(L)$ that fixes K.*

Exercise 1.1. Show that all field homomorphisms are injective.

There is another basic property of field extensions: the degree. If L/K is a field extension, then the degree $[L : K]$ is given by the dimension of L when considered as a vector space over K. For instance, $[\mathbb{C} : \mathbb{R}] = 2$.

Example 1.2. $\mathbb{Q}(\sqrt[3]{2}, i)/\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(i)/\mathbb{Q}$. $\mathbb{F}_{p^k}/\mathbb{F}_p$.

1.2 Galois extensions

This process of taking a field and 'adjoining' a new element that is prescribed to fulfill some polynomial equation is a very common way of producing field extensions. Not all field extensions can be constructed in this way – that is, some field extensions are not **algebraic**. For example, consider the field extension $\mathbb{R}/\mathbb{Q}$. The element $\pi \in \mathbb{R}$ is transcendental over $\mathbb{Q}$, meaning it is not the root of any polynomial with coefficients in $\mathbb{Q}$. Here we will be interested only in algebraic extensions.

Given any field extension L/K, we may consider its automorphism group $\mathrm{Aut}(L/K)$. For any subgroup $G \subset \mathrm{Aut}(L/K)$, we may also consider the subset of L fixed by G, denoted L^G. For example, $L^{\{e\}} = L$ and $K \subset L^{\mathrm{Aut}(L/K)}$.

Definition 1.3. *Let L/K be an algebraic field extension. We say it is a **Galois extension** if $L^{\mathrm{Aut}(L/K)} = K$. In this case, we write $\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K)$.*

For example, $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ is **not** Galois. A more field-theoretic definition is as follows: L/K is Galois if it is normal and separable. This essentially means that every irreducible polynomial of degree n with coefficients in K and a root in L has all n roots in L (normality) which are all distinct (separability). For **finite** Galois extensions, another criterion is that $|\mathrm{Aut}(L/K)| = [L : K]$.

Exercise 1.2. If L/K is finite, show that $|\mathrm{Aut}(L/K)| \leq [L : K]$.

The general theory of finite Galois extensions is summarized by the **fundamental theorem of Galois theory**, which state that subgroups of a Galois group L/K correspond bijectively to sub-extensions $L \subset E \subset K$, under the maps

$$G \mapsto L^G, \qquad E \mapsto \mathrm{Gal}(L/E).$$

Moreover, normal subgroups correspond to Galois subextensions E/K.

Remark. There is still a very interesting sort of Galois theory in the case of some transcendental equations, but it is much more difficult and mysterious. Some keywords are **Grothendieck's period conjecture** and the **motivic Galois group**, yet more contributions of Grothendieck that are far outside the scope of this talk.

1.3 Infinite Galois theory

Things start to get even more interesting when we consider infinite Galois extensions. Because Galois extensions are by definition algebraic, an infinite Galois extension is a union of finite Galois extensions. Two key examples are the field extensions $\overline{\mathbb{F}_p}/\mathbb{F}_p$ and $\overline{\mathbb{Q}}/\mathbb{Q}$. We have

$$\overline{\mathbb{F}_p} = \bigcup_{n\geq 1} \mathbb{F}_{p^n}, \qquad \overline{\mathbb{Q}} = \bigcup_{K/\mathbb{Q}\text{ finite Galois}} K$$

and

$$\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \varprojlim_{n\geq 1} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \widehat{\mathbb{Z}}, \qquad \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_{K\text{ finite Galois}} \mathrm{Gal}(K/\mathbb{Q}) \cong ???$$

Let's explain the first one. First, $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ if and only if $m|n$. In particular, if $m|n$, then each element of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ restricts to an element of $\mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p)$. Each individual group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$, generated by the **Frobenius automorphism** $x \mapsto x^p$. Now to give an element $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ is to give an automorphism $\sigma_n \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ for each n. Moreover, these σ_n must be compatible, which in this case means that the reduction of $[\sigma_n] \in \mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$ must coincide with $[\sigma_m] \in \mathbb{Z}/m\mathbb{Z}$.

The fundamental theorem of Galois theory does not hold as stated in the finite case. Indeed, consider the fixed field of the subgroup $\langle\phi\rangle$ generated by the Frobenius automorphism. This is simply $\mathbb{F}_p$, so under the supposed inverse bijections $\langle\phi\rangle$ would correspond to the entire group $\widehat{\mathbb{Z}}$. THis is saying that the natural inclusion $\mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}}$ is surjective, which is false!

Exercise 1.3. Construct an element $x \in \widehat{\mathbb{Z}}\backslash\mathbb{Z}$.

Thus, the structure involved here is more subtle. Infinite Galois groups are **profinite groups** – projective (inverse) limits of finite groups. Such groups naturally come with a **profinite topology**. Namely, we equip each G_i with the discrete topology, give $\prod_i G_i$ the product topology, and give $G = \varprojlim_i G_i \subset \prod_i G_i$ the subspace topology. Equivalently in the case of a Galois group $\mathrm{Gal}(\Omega/K)$, one may take a open neighborhood of id to be the subgroups $\mathrm{Gal}(\Omega/L)$ where L/K is finite. Then the fundamental theorem of Galois theory gives a bijection between subfields $K \subset L \subset \Omega$ and **closed subgroups** of $\mathrm{Gal}(\Omega/L)$.

For example, in the case of $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$, the closed subgroups are given by $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_{p^k})$, which correspond to the elements of $\widehat{\mathbb{Z}}$ that are divisible by k. The case of $\mathrm{Gal}(\overline{Q}/\mathbb{Q})$ is significantly more complicated, and lies at the heart of arithmetic geometry and number theory.

2 Fundamental groups

2.1 Path description

Let X be a topological space. In algebraic topology, one assigns algebraic invariants – such as groups – to topological spaces. We would like them to be invariant on homeomorphism classes, and even stronger, on homotopy classes. This means that they should be defined on the (naïve) homotopy category, where morphisms between spaces are given by homotopy classes of continuous maps. This means that two spaces X and Y are homotopy equivalent if there are maps $f : X \to Y$ and $g : Y \to X$ such that $g \circ f$ and $f \circ g$ are homotopic to id_X and id_Y, respectively.

For example, homeomorphic spaces are always homotopy equivalent. $\mathbb{R}^2 - \{*\}$ is homotopy equivalent to S^1, and $\mathbb{R}^2 - \{2 \text{ points}\}$ is homotopy equivalent to $S^1 \vee S^1$.

Now take two paths $f, g : I \to X$ with the same beginning and endpoints. We say that f and g are **path homotopic** if there is a continuous map $H : I \times I \to X$ with $H(0,t) = f(t), H(1,t) = g(t)$, and $H(s,0) = f(0) = g(0), H(s,1) = f(1) = g(1)$.

Definition 2.1. *Take a point in a topological space $x \in X$. Then $\pi_1(X,x)$ is defined to be the group of paths in X beginning and ending at x modulo homotopy of paths, with composition of paths as the group operation.*

We are generally interested in the case when X is path-connected, in which case different basepoints will give isomorphic fundamental groups by 'conjugating' via a path between x and y. The fundamental group is a functor in a natural way, and it is easily seen to be a homotopy invariant. In this case we can speak of $\pi_1(X)$ as an isomorphism class of groups. One of the most fundamental computations is that

$$\pi_1(S^1) \cong \mathbb{Z}, \qquad \pi_1\Big(\bigvee_n S^1\Big) \cong F_n,$$

where F_n is the free group on n generators. Because fundamental groups are homotopy invariant, this means that

$$\pi_1(\mathbb{R}^2 - \{*\}) \cong \mathbb{Z}, \qquad \pi_1(\mathbb{R}^2 - \{2 \text{ points}\}) \cong F_2.$$

2.2 Covering spaces

The previous approach to fundamental groups is fine, but there is another powerful perspective which is more important for our purposes. This is the theory of covering spaces.

Definition 2.2. *A **covering space** $p : Y \to X$ of X is a topological space Y equipped with a surjective projection to X such that for all $x \in X$, there is a neighborhood $U \ni x$ such that $p : p^{-1}(U) \to U$ is a projection of disjoint isomorphic copies of of U down to U.*

Covering spaces are analogous to field extensions, with the degree of a covering space being the magnitude of the preimage of a single point of the base – this is well-defined if the base is connected. We may also try to define their homomorphisms and automorphism groups. Indeed, a morphism of covering spaces is just a continuous map between them that commutes with their projections to X. In this way, we can define the automorphism group of a covering space $\mathrm{Aut}_X(Y)$. One might also hope for there to be an 'absolute' covering space, similar to an algebraic closure. This exists under some mild conditions, and is known as the **universal covering space**.

Proposition 2.3. *Let X be a path-connected, locally path-connected, and semilocally simply connected topological space. (This includes connected manifolds and connected CW-complexes.) Then there exists a unique simply connected covering space $\tilde{X}$ of X up to isomorphism, known as the **universal covering space** of X.*

The construction of $\tilde{X}$ essentially proceeds by letting each point of $\tilde{X}$ be a homotopy class of a path in X beginning at a basepoint $x \in X$. The conditions on X allow us to topologize this set naturally and appropriately. Fix X as above. It is useful to fix a universal cover and basepoints: $p : (\tilde{X}, \tilde{x}) \to (X, x)$. Now we can state the classification of covering spaces and explain how it relates to the fundamental group.

Proposition 2.4. *(a) $\pi_1(X) \cong \mathrm{Aut}_X \tilde{X}$.*

(b) The isomorphism classes of covering spaces $q : (Y,y) \to (X,x)$ are in bijection with the subgroups of $\pi_1(X,x)$ by the map

$$Y \mapsto q_*(\pi_1(Y,y)) \subset \pi_1(X,x).$$

Part b is the analogue of the fundamental theorem of Galois theory: we have a bijection between coverings and subgroups of the automorphism group. Moreover, normal subgroups correspond to Galois covering spaces, which are ones whose automorphism group acts transitively on fibers. This is the analog of the condition that $|\operatorname{Aut}(L/K)| = [L : K]$. Let us look at some covers of our examples S^1 and $S^1 \vee S^1$.

Remark. The theory of covering spaces is clarified significantly by considering the fiber functor F_x : **Cov**$/X \to$ **Set**. This perspective is also important in many generalizations, such as to schemes. It only uses basic category theory and is not too complicated, but unfortunately we will not discuss it here for lack of time.

3 The étale fundamental group

3.1 Étale morphisms

Our present goal is to, following Grothendieck, define a fundamental group for schemes that encapsulates both the Galois theory of fields and the topological fundamental group. First, we will define the analogue of a covering space: an étale cover. These are supposed to be local isomorphisms (in a way that will be made precise later). For this, we need the notions of flat and unramified morphisms. These notions (flat, unramified) are *local*.

Definition 3.1 (flat morphism)**.** *We say f is flat at $x \in X$ if $f^\# : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ gives a flat $\mathcal{O}_{Y,f(x)}$-module structure on $\mathcal{O}_{X,x}$.*

Example 3.2. *Affine space is flat; i.e., $\mathbb{A}^n_A \to \operatorname{Spec} A$. However, $\operatorname{Spec} k[x,y]/(xy) \to \operatorname{Spec} k[x]$ is not flat. This illustrates the fact that fibers of flat morphisms are equidimensional.*

In general, we have free $\Rightarrow$ projective $\Rightarrow$ flat. For finitely generated modules over local rings, these are all equivalent.

Ramification is the phenomenon of multiplicity. Algebraically, we say that $\phi : A \to B$ is unramified if it is of finite type and $\Omega_{B/A} = 0$. Similarly, consider a morphism of schemes $f : X \to Y$.

Definition 3.3 (unramified morphism)**.** *We say f is unramified if f is locally of finite type and $\Omega_{X/Y} = 0$.*

There are other characterizations of unramified morphisms which may be more useful in various situations. For example, the first one is sometimes taken as the definition.

Proposition 3.4. *Let $f : X \to Y$ be a morphism of schemes that is locally of finite type. Then the following conditions are equivalent to f being unramified.*

1. *If $f(x) = y$, then $k(x)$ is a finite separable extension of $k(y)$ and $\mathfrak{m}_y \mathcal{O}_{X,x} = \mathfrak{m}_x$.*

2. *$\Omega_{X/Y} = 0$.*

3. *The diagonal map $\Delta : Y \to X \times_Y X$ is an open immersion.*

Definition 3.5. *An étale morphism is one that is flat and unramified.*

Intuitively, flat maps are those whose fibers have the same dimension, and unramified ones are those with no multiple points. As flat and ramified are both local conditions, so is étale, so we may speak of a morphism being étale at a point. An étale cover is a surjective étale morphism.

For example, the finite étale covers of $\operatorname{Spec} K$ are given by unions of finite separable extensions $\cup \operatorname{Spec} L$. As another example, the normalization of the nodal cubic: $\operatorname{Spec} k[t] \to \operatorname{Spec} k[x,y]/(y^2 - x^3 - x^2)$ given by $x \mapsto t^2 - 1, y \mapsto t^3 - t$ is unramified but not flat. On the other hand, flat maps that lower the dimension will not satisfy the finiteness condition of unramified morphisms.

A key example of étale morphisms is given by the standard ones.

Definition 3.6 (standard étale morphism)**.** *Take $b \in B = A[T]/P(T)$ such that $P'(T)$ is a unit in B_b. Then $\phi_b : \operatorname{Spec} B_b \to \operatorname{Spec} A$ is a standard étale morphism.*

For example, the map $\operatorname{Spec} k[x,y]/y - x^2 \to \operatorname{Spec} k[y]$ is a standard étale morphism if you take away the origin. In fact, every étale morphism is locally standard étale. A key input to the proof is Zariski's main theorem. This fact implies that dimension, normality, and regularity are preserved under étale morphisms. For details, again see [**?**], Section I.3.

Let us now briefly explain how this definition relates to the notion of being a local isomorphism. Let k be an algebraically closed field and let $f : X \to Y$ be a morphism of smooth varieties over k. In this context, we can define the tangent spaces as simply a space of solutions to linear equations, and we obtain the map $df : T_x X \to T_y Y$. If we wish to extend this idea to singular varieties, we can replace the tangent space with the tangent cone. One then shows that an isomorphism of tangent cones is equivalent to an isomorphism of completed local rings: $\widehat{f}_x : \widehat{\mathcal{O}_{Y,f(x)}} \to \widehat{\mathcal{O}_{X,x}}$. Using the standard étale characterization, one can prove that this is indeed equivalent to f being étale at x.

3.2 The étale fundamental group

In this section, we will define Galois covers, a class of finite étale covers that will pro-represent the fiber functors. We will use S to denote a connected scheme, which will be the base scheme.

Given a finite étale morphism $\phi : X \to S$, we can define the degree of ϕ to be the cardinality of $\phi^{-1}(\overline{s}) \subset X$, where $\overline{s}$ is a geometric point of S. In fact, let $\phi : X \to S$ be a finite étale morphism with X connected. Then one can show there is a positive integer n such that for all geometric points $\overline{s}$ of S, we have $|\phi^{-1}(\overline{s})| = n$.

In accordance with the topological situation, we have that if $p \in \operatorname{Aut}_S(X)$ has a fixed point, then it must be the identity. More generally, two morphisms from a connected S-scheme to a finite étale S-scheme that agree on a geometric point must be equal. This implies that $|\operatorname{Aut}_S(X)| \leq n$.

Definition 3.7 (Galois cover). *We call an étale cover $p : X \to S$ **Galois** if $|\operatorname{Aut}_S(X)| = n$, where n is the degree of p.*

Remark. One does not even need the notion of degree for all this, as one can just define Galois covers to be the ones for which the automorphism group acts transitively on geometric fibers.

In general, there does not exist a universal cover that we can use to define the étale fundamental group. However, taking inspiration from the fact that

$$\operatorname{Gal}(\overline{K}/K) \cong \varprojlim_{L/K \text{ finite Galois}} \operatorname{Gal}(L/K),$$

we can try to express $\pi_1^{et}(X)$ as a suitable inverse limit. We will precisely use the Galois covers in this inverse limit. In more detail, if $\{X_i\}_{i\in G}$ are the Galois covers of S, then first we order the X_i so that $X_i \le X_j$ if there is an S-morphism $\phi_{ij} : X_i \to X_j$. In this case, since X_i and X_j are Galois, there will be a surjective group homomorphism $\operatorname{Aut}_S X_i \to \operatorname{Aut}_S X_j$. This essentially comes by quotienting out $\operatorname{Aut}_{X_j} X_i$.

Definition 3.8. *Let S be a connected scheme and let X_i be the finite Galois covers of S as constructed above. Then the étale fundamental group of S is defined as*

$$\pi_1^{et}(S, \overline{s}) := \varprojlim \operatorname{Aut}_S(X_i).$$

3.3 Examples

Let us now justify why the étale fundamental group deserves its name by some examples. We have already essentially explained the following.

Proposition 3.9. $\pi_1(\operatorname{Spec} K) = \operatorname{Gal}(\overline{K}/K)$.

Theorem 3.10. *Let X be a connected scheme of finite type over $\mathbb{C}$. The functor $X \mapsto X^{\mathrm{an}}$ is an equivalence of categories between finite étale covers of X and finite topological covers of X^{an}. Thus we obtain an isomorphism*

$$\pi_1(\widehat{X^{\mathrm{top}}, \overline{x}}) \cong \pi_1(X, \overline{x}).$$

For instance, $\pi_1^{et}(\mathbb{A}^1_{\mathbb{C}}) = 1$, $\pi_1^{et}(\operatorname{Spec} \mathbb{C}[x]_(x)) \cong \widehat{Z}$ and $\pi_1^{et}(\mathbb{P}^1_{\mathbb{C}} - \{0, 1, \infty\}) \cong \widehat{F_2}$.

Theorem 3.11. *Let $k \subset K$ be an extension of algebraically closed fields and let X be a proper integral scheme over k. Then the natural map*

$$\pi_1(X_K, \overline{x}_K) \to \pi_1(X, \overline{x})$$

is an isomorphism.

This is useful when we want to pass from, say, $\overline{\mathbb{Q}}$ to $\mathbb{C}$. In particular, $\pi_1^{et}(\mathbb{P}^1_{\overline{\mathbb{Q}}} - \{0, 1, \infty\}) \cong \widehat{F_2}$.

Next, Grothendieck showed the existence of a remarkable theorem which connects the arithmetic and geometry of étale fundamental groups.

Theorem 3.12. *Let X be a quasi-compact, quasi-separated, and geometrically integral scheme over a field K. Then we have the following short exact sequence:*

$$1 \to \pi_1^{et}(X_{\overline{K}}) \xrightarrow{i} \pi_1^{et}(X) \xrightarrow{j} \pi_1^{et}(\operatorname{Spec} K) \to 1.$$

What makes this so remarkable (e.g. when $K = \mathbb{Q}$) is that it splits up the middle étale fundamental group into something geometric on the left and something arithmetic: $\operatorname{Gal}(\overline{K}/K)$ on the right.

4 Regular polyhedra over finite fields and dessins d'enfants

4.1 A new perspective on polyhedra

Let's instead talk about something seemingly quite unrelated...

Take some graph G embedded on some real surface X. We call the resulting configuration (X, G) a **map**. A map has faces, edges, and vertices. Define a **flag** of (X, G) to be a choice of a face, an edge of that face, and a vertex of that edge. Now whatever (X, G) we take, there is going to be a transitive action on the set of flags by the **cartographic group**[1]

$$\underline{C}_2 = \langle \sigma_0, \sigma_1, \sigma_2 | \sigma_0^2 = \sigma_1^2 = \sigma_2^2 = (\sigma_0\sigma_2)^2 = 1 \rangle.$$

These operations $\sigma_0, \sigma_1, \sigma_2$ correspond to the reflection of the chosen vertex, edge, and face, respectively. There is also an action of the **oriented cartographic group**

$$\underline{C}_2^+ = \langle \rho_v, \rho_f, \rho_e | \rho_2\rho_0 = \rho_1, \rho_1^2 = 1 \rangle$$

where $\rho_0 = \sigma_1 \circ \sigma_2, \rho_1 = \sigma_0 \circ \sigma_2, \rho_2 = \sigma_0 \circ \sigma_1$. Thus, ρ_0, ρ_1, ρ_2 correspond to the rotation of the flag around the vertex, edge, and face, respectively. Draw a picture!

An alternate way of presenting this group is by the relations $\rho_0\rho_1\rho_2 = 1, \rho_1^2 = 1$.

Now when do we get a regular polyhedron? Precisely when its automorphism group acts transitively on its flags. We see that every pair of integers $p, q \geq 1$ gives rise to a unique connected map by imposing the additional relations

$$\rho_0^p = \rho_2^q = 1$$

on its automorphism group. We see that, after pinning down a flag, this automorphism group determines the polyhedron. In particular, p is the number of faces to a vertex and q is the number of edges to a face. Try some examples!

Immediately we see hat not all the regular polyhedra we get in this way are Platonic solids. Rather, only the compact ones are; i.e. those realizable on a sphere. These are the ones with finite automorphism group. The others give regular tilings of either the Euclidean plane or the hyperbolic plane. In fact, this approach leads to an easy classification of Platonic solids!

[1] Beware, my conventions differ slightly from Grothendieck's in the *Esquisse*; here I consider the elements as operators so I multiply in the opposite direction.

Exercise 4.1. Determine which p and q give rise to spherical (Platonic) maps, Euclidean tilings, and hyperbolic tilings. (Hint: Calculate some angles.)

This is a nice way of looking at things, and moreover it provides a framework for additional ideas to give some truly new phenomena! In particular, it allows us to consider regular polyhedra in characteristic p, or over any base ring! This comes through the following observation: **the formulas for the fundamental reflections σ_i can be written in terms of universal formulae in terms of the cosines of the angles of the polyhedron!**

Indeed, fixing a flag v_0, v_1, v_2, we have

$$\begin{aligned}
\sigma_0(v_0) &= 2v_1 - v_0,\\
\sigma_1(v_1) &= (1-\cos\theta)v_0 - v_1 + (1+\cos\theta)v_2,\\
\sigma_2(v_2) &= (1-\cos\gamma) - v_2.
\end{aligned}$$

The data of the polyhedron is completely contained in these values of $\cos\theta$ and $\cos\gamma$. Thus, taking any base field, we may substitute any pair of values for them and obtain a *regular polyhedron*! Note that there will be many of these which all correspond to $p = q = \infty$. In particular, we may *specialize* from the field $\mathbb{R}$ to finite fields! For instance, in the case of the octahedron, we have $\cos\theta = 1/2, \cos\gamma = -1/3$. For $6 \nmid q$, we see that we can specialize these values to $\mathbb{F}_q$, and therefore obtain an octahedron over $\mathbb{F}_q$! This has the same automorphism group as the ordinary octahedron[2].

However, as Grothendieck writes, the situation is entirely different if we start with an infinite (i.e. Euclidean/hyperbolic tilings) regular polyhedron! Then when we specialize it to $\mathbb{F}_q$, the fact that polyhedra over finite fields must necessarily be finite implies that we get an infinite number of finite regular polyhedra as q varies, whose automorphism group varies arithmetically with q!

The richness of this discovery leads in many directions. Grothendieck describes a certain (apparently) incredible phenomenon that occurs when specializing polyhedra under singular characteristics. I have not yet been able to decipher what he means by this. Another set of questions arises once we consider a **Galois action of** $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on these maps. This Galois action is extremely nontrivial and interesting, and we will now explain it.

4.2 Dessins d'enfants

Let us denote $\mathrm{Gal}(\overline{K}/K)$ by G_K. Recall that $G_{\mathbb{Q}}$ is this deep mysterious group at the center of number theory. On the other hand consider dessins d'enfants: bicolourable maps (X, G), where X is compact. The upshot is that there is a natural correspondence between

$$\{\text{dessins d'enfants}\}/\cong \quad \Leftrightarrow \quad \{\text{algebraic curves defined over } \overline{\mathbb{Q}}\}/\cong$$

It goes as follows. First, every flag (X, G) corresponds to a **clean dessin**; that is, one where every white vertex has degree 2, simply by placing a white vertex in the middle of every edge.

[2] Grothendieck seems to claim this; I haven't checked it.

Note that if we are considering oriented flags, every such flag is associated to a unique edge between a black and white vertex. Thus we can describe the action of the oriented cartographic group simply on these edges. We can extend this action to all dessins, not just the clean ones. Looking at the definition given before, in terms of edges we are rotating them around black and white vertices. These two operations generate a free group F_2 on two elements.

We will now see how to go from a dessin to an algebraic curve defined over $\overline{Q}$. First, note that since the dessin is finite, F_2 acts by a finite quotient, so we in fact have an action of $\widehat{F_2}$ on the edges. Fix an edge E of the dessin (X, G) and consider its stabilizer subgroup $H \subset \underline{C}_2^+$. This subgroup is well-defined up to conjugacy. Moreover, the dessin can be reconstructed from this stabilizer. Now note that $F_2 \cong \pi_1(\mathbb{P}^1_{\mathbb{C}} - \{0, 1, \infty\}$. By the correspondence between conjugacy classes of subgroups of the fundamental group and topological covers, we obtain a bijection from dessins to covers of $\mathbb{P}^1_{\mathbb{C}} - \{0, 1, \infty\}$. Then, by the Riemann existence theorem this corresponds to a unique algebraic curve X with a morphism $\beta : X \to \mathbb{P}^1_{\mathbb{C}}$ ramified only at the three points $\{0, 1, \infty\}$. Finally, by some nontrivial algebraic geometry, one shows that algebraic curves admitting such a map can be defined over $\overline{\mathbb{Q}}$. Thus, we have shown how to canonically get an algebraic curve defined over $\overline{\mathbb{Q}}$ from the combinatorial data of a dessin!

But there's even more: do we get *all* algebraic curves defined over $\overline{\mathbb{Q}}$ his way? The answer is yes, and is given by Belyi's theorem.

Theorem 4.1 (Belyi's theorem)**.** *Every complex algebraic curve definable over $\overline{\mathbb{Q}}$ admits a morphism to $\mathbb{P}^1_{\mathbb{C}}$ ramified only at $0, 1, \infty$.*

Finally, one sees that by composing β with the map $z \mapsto 4z(1-z)$, one obtains a map from X still ramified only over $\{0, 1, \infty\}$, but with ramification index exactly 2 over the point 1. In this way, we get a bijection between isomorphism classes of clean dessins and 'clean Belyi pairs' (X, β). In fact, it can be visualized in the following way. Given $\beta : X \to \mathbb{P}^1_{\mathbb{C}}$, the preimages of $0, 1, \infty$ are precisely the vertices, midpoints of edges, and centers of faces of the corresponding map.

4.3 The Galois action

What is the significance of all this? It comes from the fact that there is a natural action of $G_{\mathbb{Q}}$ on algebraic curves defined over $\overline{\mathbb{Q}}$! For example, in genus 0 the Belyi morphism β is given by some rational function with algebraic number coefficients, which $G_{\mathbb{Q}}$ acts on. The incredible thing is that $G_{\mathbb{Q}}$ acts faithfully on the set of dessins! This means that every element $\sigma \in G_{\mathbb{Q}}$ can be seen through its action on these graphs on surfaces! As a matter of fact, more is true – the Galois action is faithful on genus 0 dessins, and in fact even on trees![3].

The way one approaches this is by tracing out the action of $G_{\mathbb{Q}}$, and seeing that it comes from the fancy exact sequence from the previous section! Indeed, given the exact sequence

$$1 \to \pi_1^{et}(X_{\overline{\mathbb{Q}}}) \xrightarrow{i} \pi_1^{et}(X_{\mathbb{Q}}) \xrightarrow{j} G_{\mathbb{Q}} \to 1$$

we obtain an **outer automorphism**

$$G_{\mathbb{Q}} \to \mathrm{Out}(\pi_1^{et}(X_{\overline{\mathbb{Q}}})).$$

When we take $X = \mathbb{P}^1_{\mathbb{Q}} - \{0, 1, \infty\}$, we have that this homomorphism is injective.

Theorem 4.2. *The outer representation $\rho : \mathrm{Gal}(\mathbb{Q}) \to \mathrm{Out}(\pi_1(\mathbb{P}^1_{\overline{\mathbb{Q}}} - \{0, 1, \infty\})) \cong \mathrm{Out}(\widehat{F_2})$ is injective.*

[3]A proof may be found in Leila Schenps's *Dessins d'enfants on the Riemann sphere*

Proof. If ρ has nontrivial kernel, then say it fixes $L \subset \overline{\mathbb{Q}}$. Then $\mathrm{Gal}(L)$ must act trivially on $\widehat{F_2}$. This action comes from conjugation in the sequence

$$1 \to \widehat{F_2} \to \pi_1(\mathbb{P}^1_L - \{0, 1, \infty\}).$$

Triviality means that the image of $\widehat{F_2}$ and its centralizer must generate $\pi_1(\mathbb{P}^1_L - \{0, 1, \infty\})$. But since $\widehat{F_2}$ has trivial center, this implies that $\pi_1(\mathbb{P}^1_L - \{0, 1, \infty\})$ is their direct product. Now recall that the finite continuous left $\widehat{F_2}$ sets correspond to the finite étale covers of $\mathbb{P}^1_{\overline{Q}} - \{0, 1, \infty\}$. The natural inclusion of $\pi_1(\mathbb{P}^1_{\overline{\mathbb{Q}}} - \{0, 1, \infty\})$ into $\pi_1(\mathbb{P}^1_L - \{0, 1, \infty\})$ corresponds to the base change of curves over L to curves over $\overline{\mathbb{Q}}$. Now that there is a section to this map, we get that every curve over $\overline{\mathbb{Q}}$ can be defined over L. But this is not the case; e.g. take an elliptic curve with j-invariant outside L. □

But there's more! The existence of a rational point in $\mathbb{P}^1_{\overline{\mathbb{Q}}} - \{0, 1, \infty\})$ gives by functoriality a section in the exact sequence, which means that we may in fact lift this to an actual action of $G_{\mathbb{Q}}$ on $\widehat{F_2}$. Thus there is an embedding

$$G_{\mathbb{Q}} \hookrightarrow \mathrm{Aut}(\widehat{F_2})$$

well-defined up to conjugacy. The fact this is an embedding means that $G_{\mathbb{Q}}$ acts faithfully on dessins. This is the birth of anabelian geometry.

5 Anabelian geometry and Grothendieck-Teichmüller theory

The basic idea of anabelian geometry is to study varieties through their fundamental groups, especially in the presence of a rich action of the absolute Galois group on them. The term anabelian refers to being very far away from being abelian, such as a free group. This is in contrast to usual cohomological methods where the action of the Galois group is linear. The unexpected richness of the original case of $X = \mathbb{P}^1_{\mathbb{Q}} - \{0, 1, \infty\}$ suggests that there are a lot of new things to discover. In fact, even in this special case there has been an incredible amount of great work, especially by Deligne, even without using the full structure of the fundamental group...

5.1 Anabelian varieties

The structure of étale fundamental groups is deep enough in some cases to reconstruct the original variety. That is, given knowing the map $\pi_1^{et}(X_K) \to G_K$ for K a global field, one should be able to reconstruct X_K. Varieties for which this is true are called **anabelian varieties**. Grothendieck had a clear idea[4] that hyperbolic curves are abelian; namely does for which $\chi = 2 - 2g - \nu < 0$, where g is the genus and ν is the number of marked points. Mochizuki proved this, and in fact proved more.

Theorem 5.1. *Hyperbolic curves over finitely generated fields of characteristic zero are anabelian.*

In particular, Mochizuki proved this over p-adic fields, whereas previously people had not considered this extension. His proof is very complex and, among other things, uses Faltings's p-adic Hodge theory.

[4]Though we do not have any written proof by him

5.2 The section conjecture

The study of rational points on varieties has been a major topic in mathematics since antiquity. The section conjecture provides a way to associate rational points to sections of the homotopy exact sequence, which correspond to 'path torsors.' Indeed, we have an injective map

$$X(\mathbb{Q}) \to H^1(G_{\mathbb{Q}}, \pi_1^{et}(\overline{X}, b)) \qquad \text{where} \qquad s \mapsto [\pi_1^{et}(X, b, s)],$$

and the section conjecture states that this map is surjective.

We quote from *The Grothendieck Conjecture on the Fundamental Groups of Algebraic Curves* by Hiroaki Nakamura, Akio Tamagawa, and Shinichi Mochizuki.

> "Among those mathematicians who were involved with the anabelian philosophy in its early years, the Grothendieck Conjecture appears to have been thought of as a new approach to Diophantine Geometry, i.e., to the study of rational points on varieties over global fields. The following argument is representative of this approach. Suppose that we wish to show that a certain algebraic variety has only finitely many rational points. We then assume that there are infinitely many and attempt to derive a contradiction by showing that any rational point arising as a "limit" of this infinite set of rational points has various properties that are "too good to be true." In order to carry out this argument, however, one needs to know that the "limit" exists. Since a field like a number field is not complete with respect to any nontrivial topology, the existence of such a limit is by no means clear. On the other hand, since Galois representations (as in (1.2)) are, in some sense, analytic objects, it is comparatively easy to show that a sequence of such Galois representations always has a convergent subsequence (i.e., a subsequence whose limit exists, as a Galois representation). Thus, if one knows, as is asserted in the Section Conjecture (GC3), that rational points and Galois representations (which satisfy certain conditions) are, in fact, equivalent objects, then one can conclude the existence of a limit of a sequence of rational points from the existence of the limit of the corresponding sequence of Galois representations. If one refines this argument somewhat, then the possibility arises of deriving a new proof of the "Mordell Conjecture"14) for algebraic curves of high genus from the Section Conjecture (GC3)."

5.3 Moduli spaces of curves and the Teichmüller tower

Next, Grothendieck had the intuition that the **moduli stacks of curves** $\mathcal{M}_{g,n}$ should be anabelian. Note that the case $\mathcal{M}_{0,4}$ is precisely the case $\mathbb{P}^1_{\mathbb{C}} - \{0, 1, \infty\}$. Grothendieck considered all these moduli spaces together, linked by the operations of erasing marked points and gluing. As he writes in the *Esquisse*:

> "Indeed, it is more the system of all the multiplicities $\mathcal{M}_{g,\nu}$ for variable g, ν, linked together by a certain number of fundamental operations (such as the operations of "plugging holes", i.e. "erasing" marked points, and of "glueing", and the inverse operations), which are the reflection in absolute algebraic geometry in characteristic zero (for the moment) of geometric operations familiar from the point of view of topological or conformal "surgery" of surfaces. Doubtless the principal reason of this fascination is that this very rich geometric structure on the system of "open" modular multiplicities $\mathcal{M}_{g,\nu}$ is reflected in an analogous structure on the corresponding fundamental groupoids, the "Teichmüller groupoids" b $\hat{T}_{g,\nu}$, and that these operations on the level of the $\hat{T}_{g,\nu}$ are sufficiently intrinsic for the Galois group Γ of $\overline{\mathbb{Q}}/\mathbb{Q}$ to act on this whole "tower" of Teichmüller groupoids, respecting all these structures."

Sources

Sections 1 and 2 are standard – see any book on abstract algebra and algebraic topology. The material in Section 3 was developed by Grothendieck in SGA 1. Sections 4 and 5 come from Grothendieck's *Esquisse d'un Programme*. The most detailed basic explanation of dessins can be found in Leila Schneps's article *Dessins d'enfants on the Riemann Sphere*. I also suggest reading *The Grothendieck Conjecture on the Fundamental Groups of Algebraic Curves* by Hiroaki Nakamura, Akio Tamagawa, and Shinichi Mochizuki.

Grothendieck and anabelian geometry

The 1958 ICM address

THE COHOMOLOGY THEORY OF ABSTRACT ALGEBRAIC VARIETIES

By ALEXANDER GROTHENDIECK

It is less than four years since cohomological methods (i.e. methods of Homological Algebra) were introduced into Algebraic Geometry in Serre's fundamental paper[11], and it seems already certain that they are to overflow this part of mathematics in the coming years, from the foundations up to the most advanced parts. All we can do here is to sketch briefly some of the ideas and results. None of these have been published in their final form, but most of them originated in or were suggested by Serre's paper.

Schemes

Definition (affine scheme)

Given any commutative ring A, define the affine scheme $\operatorname{Spec} A$ to be the locally ringed space consisting of the prime ideals of A equipped with the Zariski topology. The structure sheaf is defined by $O_{\operatorname{Spec} A}(D(f)) = A_f$ on distinguished open sets $D(f)$. A scheme is a locally ringed space where every point has a neighborhood isomorphic to an affine scheme.

Schemes

Definition (affine scheme)

Given any commutative ring A, define the affine scheme $\operatorname{Spec} A$ to be the locally ringed space consisting of the prime ideals of A equipped with the Zariski topology. The structure sheaf is defined by $O_{\operatorname{Spec} A}(D(f)) = A_f$ on distinguished open sets $D(f)$. A scheme is a locally ringed space where every point has a neighborhood isomorphic to an affine scheme.

"The very notion of a scheme has a childlike simplicity - so simple, so humble in fact that no one before me had the audacity to take it seriously." – Alexander Grothendieck

Grothendieck at the IHES (1958–1970)

Grothendieck's EGA and SGA

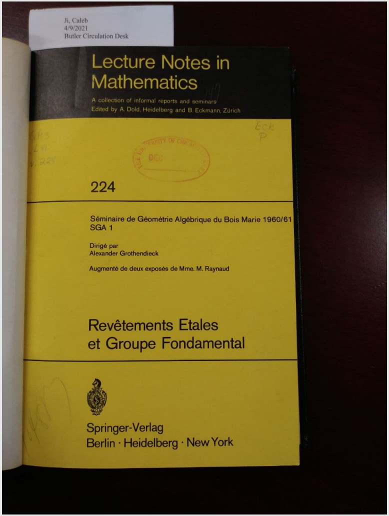
EGA

1. Le langage des schémas
2. Étude globale élémentaire de quelques classes de morphismes
3. Étude cohomologique des faisceaux cohérents
4. Étude locale des schémas et des morphismes de schémas

SGA

1. Revêtements étales et groupe fondamental
2. Cohomologie locale des faisceaux cohérents et théorèmes de Lefschetz locaux et globaux
3. Schémas en groupes
4. Théorie des topos et cohomologie étale des schémas
5. Cohomologie l-adique et fonctions L
6. Théorie des intersections et théorème de Riemann-Roch
7. Groupes de monodromie en géométrie algébrique

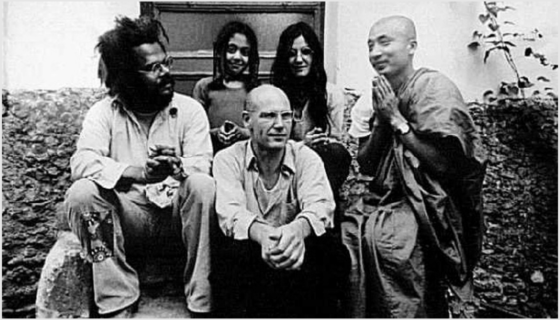
SGA 1: Revêtements étales et groupe fondamental



Develops the theory of étale morphisms, the étale fundamental group, fibered categories, descent, ...

The great turning point, 1970

"Yes, it was a liberation. *And, for the first time in my life I believe, it was then given to me to know the amazed joy and the fullness of one who feels heavy obstacles detaching from him whose existence he had not hitherto even foreseen, and who sees an unsuspected world opening up in front of him, calling him to discover it." – AG, La Clef des Songes*



After

- Founding *Survivre et vivre*
- Boxing police officers
- Being jailed for housing a Japanese Buddhist monk
- Going barefoot in the Canadian winter
- Founding communes, funding agrarian movements
- Awakening his Yin
- Asked to be the leader of Nipponzan Myohoji Buddhism
- Getting his drivers license after nine failures
- Beginning a relationship with a Buddhist nun
- ...

He settles down as a professor at the University of Montpellier.

Polyhedra

- Begins to teach undergraduate math, c. 1975
- 1977, 1978: teaches a course on the cube, another on the icosahedron

The mathematical thought of a child (in so far as it actually leads to a "discovery") could be more "valuable" than a published work (inasmuch as it is mindless and joyless, a routine publication). Or rather, the one is valuable, and the other is spiritual and psychological "junk". ... Polyhedra (take just the cube or even the icosahedron) are an equally inexhaustible source of mathematical reflection and insight on every "level".

A mysterious principle...

From Grothendieck's *Esquisse d'un Programme*:

> *Whether it happens that such a principle really exists, and even that we succeed in uncovering it from its cloak of fog, or that it recedes as we pursue it and ends up vanishing like a Fata Morgana, I find in it for my part a force of motivation, a rare fascination, perhaps similar to that of dreams. No doubt that following such an unformulated call, the unformulated seeking form, from an elusive glimpse which seems to take pleasure in simultaneously hiding and revealing itself – can only lead far, although no one could predict where...*

Grothendieck's challenge

From Grothendieck's *Esquisse d'un Programme*:

The moment seems ripe to rewrite a new version, in modern style, of Klein's classic book on the icosahedron and the other Pythagorean polyhedra. Writing such an exposé on regular 2-polyhedra would be a magnificent opportunity for a young researcher to familiarise himself with the geometry of polyhedra as well as their connections with spherical, Euclidean and hyperbolic geometry and with algebraic curves, and with the language and the basic techniques of modern algebraic geometry. Will there be found one, some day, who will seize this opportunity?

Caleb Ji

From Grothendieck's *Esquisse d'un Programme*:

In the form in which Bielyi states it, his result essentially says that every algebraic curve defined over a number field can be obtained as a covering of the projective line ramified only over the points 0, 1 and ∞. This result seems to have remained more or less unobserved. Yet it appears to me to have considerable importance. To me, its essential message is that there is a profound identity between the combinatorics of finite maps on the one hand, and the geometry of algebraic curves defined over number fields on the other. This deep result, together with the algebraic-geometric interpretation of maps, opens the door onto a new, unexplored world – within reach of all, who pass by without seeing it.

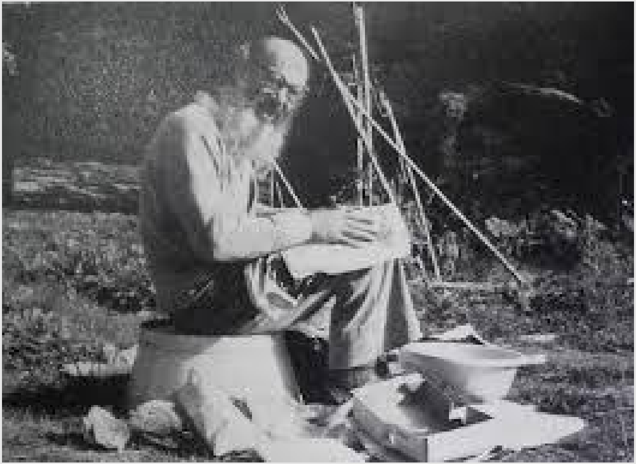
The birth of anabelian geometry

From Grothendieck's *Esquisse d'un Programme*:

ture of this action of $\mathbb{\Gamma}$. One sees immediately that roughly speaking, this action is expressed by a certain "outer" action of $\mathbb{\Gamma}$ on the profinite compactification of the oriented cartographic group $\underline{C}_2^+$, and this action in its turn is deduced by passage to the quotient of the canonical outer action of $\mathbb{\Gamma}$ on the profinite fundamental group $\hat{\pi}_{0,3}$ of $(U_{0,3})_{\overline{\mathbb{Q}}}$, where $U_{0,3}$ denotes the typical curve of genus 0 over the prime field $\mathbb{Q}$, with three points removed. This is how my attention was drawn to what I have since termed "anabelian algebraic geometry", whose starting point was exactly a study (limited for the moment to characteristic zero) of the action of "absolute" Galois groups (particularly the groups $\mathrm{Gal}(\overline{K}/K)$, where K is an extension of finite type of the prime field) on (profinite) geometric fundamental groups of algebraic varieties (defined over K), and more particularly (breaking with a well-established tradition) fundamental groups which are very far from abelian groups (and which for this reason I call "anabelian"). Among

La Gardette

- Spent a year in total solitude at La Gardette, 1979–1980



- Written in 1981
- The following quote about it from *Pursuing Stacks*

I thought it was going to take me a week or two to tour it and kind of recense resources. It took me five months instead of intensive work, and two impressive heaps of notes (baptized "La Longue Marche à travers la théorie de Galois"), to get a first, approximative grasp of some of the main structures and relationships involved. The main emphasis was (still is) on an understanding of the action of profinite Galois-groups (foremost among which $\mathrm{Gal}_{\overline{\mathbb{Q}}/\mathbb{Q}}$ and the subgroups of finite index) on non-commutative profinite fundamental groups, and primarily on fundamental groups of algebraic curves – increasingly too on those of modular varieties (more accurately, modular *multiplicities*) for such curves – the profinite completions of the Teichmüller group. The voyage was the most rewarding and exciting I had in mathematics so far – and still it became very clear that it was just like a first glimpse upon a wholly new landscape – one landscape surely among countless others of a continent unknown, eager to be discovered.

Grothendieck's letter to Faltings

- Anabelian question: How much information about the isomorphism class of the variety X is contained in the knowledge of the étale fundamental group?
- Conjecture (proven by Mochizuki): $\pi_1^{et}(C)$ determines C where C is an appropriate hyperbolic curve.

Gerd Faltings

Shinichi Mochizuki

From Grothendieck's *Esquisse*

a) Combinatorial construction of the Teichmüller tower.

b) Description of the automorphism group of the profinite compactification of this tower, and reflection on a characterisation of $\mathbb{\Gamma} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ as a subgroup of the latter.

c) The "motive machine" $\mathrm{Sl}(2, \mathbb{Z})$ and its variations.

d) The anabelian dictionary, and the fundamental conjecture (which is perhaps not so "out of reach" as all that!). Among the crucial points of this dictionary, I foresee the "profinite paradigm" for the fields $\mathbb{Q}$ (cf. b)), $\mathbb{R}$ and $\mathbb{C}$, for which a plausible formalism remains to be uncovered, as well as a description of the inertia subgroups of $\mathbb{\Gamma}$, via which the passage from characteristic zero to characteristic $p > 0$ begins, and to the absolute ring $\mathbb{Z}$.

e) Fermat's problem.

Why did he stop?

A partial answer, from Grothendieck's *Pursuing Stacks*:

"Doubtless, the very strongest attraction, the greatest fascination goes with the "new world" of anabelian algebraic geometry. It may seem strange that instead, I am indulging in this lengthy digression on homotopical algebra, which is almost wholly irrelevant I feel for the Galois-Teichmüller story. The reason is surely an inner reluctance, an unreadiness to embark upon a long-term voyage, well knowing that it is so enticing that I may well be caught in this game for a number of years – not doing anything else day and night than making love with mathematics, and maybe sleeping and eating now and then."

Questions?