(Some) New Trends in Galois Theory and Arithmetic

by Florian Pop at Bonn

Introduction: Galois group / Fundamental group

Starting from the question about the solvability of equation by radicals, Galois had the genius idea of attaching to every polynomial equation

$$\mathcal{E}: \quad p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

in the unknown x with coefficients a_i in some "field" $K \subset \mathbb{C}$ (for the sake of simplicity), the field extension $K_{\mathcal{E}}|K$ generated over K by all the roots x_i of the equation under discussion. The point is that $K_{\mathcal{E}}|K$ is a kind of *invariant* of $\mathcal{E}$, which does not depend on the way we find the solutions x_i. The next step is –and this is the very genius idea of Galois– to go even further, and attach to $\mathcal{E}$ the automorphism group $G_{\mathcal{E}} = \mathrm{Aut}(K_{\mathcal{E}}|K)$, a group which we call today the *Galois group of the field extension* $K_{\mathcal{E}}|K$. It is a finite group, whose subgroups H *parameterize* canonically the fields in between $K \subseteq L \subseteq K_{\mathcal{E}}$ such that $(G_{\mathcal{E}} : H) = [L : K]$. As we all know, the very amazing fact about this is: solvability by (various) radicals of $\mathcal{E}$ is encoded in $G_{\mathcal{E}}$ by the fact that this finite group is solvable. In particular, the famous fact that the "general" polynomial equation $\mathcal{E}_n$ of degree n is not solvable by radicals for $n > 4$, follows from two more or less formal facts: (i) $G_{\mathcal{E}_n}$ is isomorphic to the symmetric group $\mathfrak{S}_n$ on n elements; (2) $\mathfrak{S}_n$ is not solvable for $n > 4$.

We are at the eve of one of the greatest developments in the modern mathematics, *The Galois Theory with its various aspects and applications,* arising from the ashes of the negative answer to the solvability by radicals question given by Abel and Ruffini...

We begin by recalling the definition of the *absolute Galois group* of K as follows: For every finite set of polynomials $p_j(X)$ over K, consider $p(X)$ their product, and $\mathcal{E} : p(x) = 0$ the corresponding polynomial equation over K. Taking larger and larger (finite) sets $p_j(X)$ of polynomials, we easily see that the field extensions $(K_{\mathcal{E}})_{\mathcal{E}}$ build an increasingly filtered family of subfields of $\mathbb{C}$, and that the corresponding automorphism groups $(G_{\mathcal{E}})_{\mathcal{E}}$ build an inverse filtered family (i.e., a projective surjective system) of finite groups. One has: $\overline{K} = \cup_{\mathcal{E}} K_{\mathcal{E}}$ is the algebraic closure of K inside

$\mathbb{C}$, and further $G_K := \varprojlim_{\mathcal{E}} G_{\mathcal{E}}$ is the automorphism group of $\overline{K}$ over K. By its construction, G_K is a profinite group, thus a topological compact and totally disconnected group. The family of all *closed* subgroups of G_K is in a canonical bijection with the family of all K-subfields of $\overline{K}$ (generalizing the corresponding assertion about $G_{\mathcal{E}}$ and $K_{\mathcal{E}}|K$ as indicated above). One could ask questions concerning Galois Theory as follows:

1) Give a description of G_K (different from the tautological one), at least in very "down to earth" cases, like $K = \mathbb{Q}$; and more generally, for fields K which are interesting from number theoretic point of view. For instance $K = \mathbb{Q}(z_1, \dots, z_n)$ finitely generated over $\mathbb{Q}$ (as a subfield of $\mathbb{C}$). We make here an *ad-hoc* definition, and call such fields primitive.

- Part of the problem here is to give a description of the set of all the finite quotients $\text{f.q.}(G_K) = \{G_{\mathcal{E}} \mid \text{all } \mathcal{E}\}$ of G_K.

- *N.B.,* to describe G_K itself is more than just giving the set of its finite quotients. Indeed, knowing the set $\{G_{\mathcal{E}} \mid \text{all } \mathcal{E}\}$, we do not know yet how the finite quotients $G_{\mathcal{E}}$ "fit" together to finally produce G_K.

- Here we come then to one of the most outstanding open questions concerning the Galois theory of fields, namely the

Inverse Galois Problem (IGP) *Show that for every finite group G there exists a polynomial equation $\mathcal{E}$ over the rationals $\mathbb{Q}$ such that $G_{\mathcal{E}} \cong G$. Equivalently,* $\text{f.q.}(G_{\mathbb{Q}})$ *is the set of all finite groups.*

2) Which (kind of) information about K is encoded in G_K?

- One may recall here the celebrated result of Artin–Schreier:

Theorem. *A field K is real closed iff G_K is finite and $\neq \{1\}$.*

Nevertheless, this assertion concerns rather algebra and arithmetic over K, as zeros of polynomials and/or rational points on varieties over K, and says little about the isomorphy type of K itself...

- Intuitively, the absolute Galois group G_K of a "primitive" field K is expected to encode a lot of information about the field. The usual real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ are at the other extreme in the class of all fields. For their "nice" topological/analytical properties they pay the price of loosing (almost all) Galois information...

3) How do we get, resp. can use the information encoded in G_K in solving concrete problems over K, like for instance behavior of roots of polynomials and rational points on varieties over K?

- A general point of view here is to study/look for objects on which the profinite group G_K canonically acts, thus find and study *representations of* G_K.

- Part of this question is the very famous and important problem concerning the description of the character group of G_K. In case K is a number field, i.e., K is a finite extension of $\mathbb{Q}$, the answer to this question is given by the *class field theory* of K, which originates in the work of KRONECKER and WEBER, followed by HILBERT, then coming into its classical period, the time of TAKAGI, ARTIN, HASSE, CHEVALLEY, TATE, and many others.

As a general comment, we should remark that the distinction between these aspects of Galois Theory above is though artificial, as a progress in one direction sheds new light in the other directions too...

Before going into details concerning some aspects of today's Galois Theory, we recall some facts about fundamental groups, facts which are relevant to what we want to say later on. Namely, parallel to considering finite field extensions $K \hookrightarrow L$ as above, one can consider finite, connected topological covers of "nice" topological spaces as follows.

Let X be a (for the sake of simplicity) smooth variety defined over the complex numbers $\mathbb{C}$. Then the analytification X^{an} of X is a complex manifold, whose underlying topological space we denote by $X(\mathbb{C})$.

Consider a finite, connected (topological) cover $f^{\mathrm{top}} : Y^{\mathrm{top}} \to X(\mathbb{C})$. It is well known, that Y^{top} caries a unique analytic structure Y^{an} such that f^{top} is a morphism f^{an} of complex manifolds. Moreover, using GAGA type results, it follows that Y^{an} is the analytification of some algebraic variety Y over the complex numbers, and that f^{an} is actually defined by a morphism of algebraic varieties $f : Y \to X$. The topological fact that f^{top} is a topological cover is equivalent to saying that f is an un-ramified cover. We have an equivalence of categories:

$$\Big(\text{Connect. topol. covers of } X(\mathbb{C})\Big) \longleftrightarrow \Big(\text{Connect. unram. covers of } X\Big)$$

The first relation of this with Galois extensions of fields is as follows: Let $\mathbb{C}(X)$ be the function field of X; thus $\mathbb{C}(X) = \mathfrak{M}_X$ the field of meromorphic functions on X^{an}. Then every un-ramified cover $Y \to X$ as above, gives rise to a field extension $\mathbb{C}(X) = \mathfrak{M}_X \hookrightarrow \mathfrak{M}_Y = \mathbb{C}(Y)$ in a canonical way. We will call such field extensions X-unramified extensions of $\mathbb{C}(X)$.

Now suppose that $Y(\mathbb{C}) \to X(\mathbb{C})$ is Galois (as a topological cover). Then its deck transformation group G becomes in a canonical way the X^{an}-automorphism group of Y^{an}, thus the X-automorphism group of Y. Moreover, $\mathbb{C}(X) = \mathfrak{M}_X$ is exactly the field of G-invariant functions in $\mathbb{C}(Y) = \mathfrak{M}_Y$. Thus $\mathbb{C}(X) \hookrightarrow \mathbb{C}(Y)$ is a Galois extension with Galois group (canonically) isomorphic to G.

There are two observation to make here: First, the equivalence of categories described above gives a method to construct (Galois) field extensions of function fields $\mathfrak{K} = \mathbb{C}(X)$ of given varieties X over the complex numbers, which moreover are X-unramified. Second, this is more or less the only "general" method to construct Galois extensions of fields with given Galois group G, at the provision that we first have realized G as the deck transformation group of some topological cover $Y^{\mathrm{top}} \to X(\mathbb{C})$ for some smooth complex variety X.

For the illustration of the procedure, let us consider the case $X = \mathbb{P}^1_t \backslash S$, where $S = \{s_0, \ldots, s_n\}$ is a finite set of points in the t-projective line (this means, t is the usual affine coordinate on $\mathbb{C}$). Then $X(\mathbb{C})$ is an $(n+1)$-punctured Riemann sphere, and its (finite) Galois covers are well known: They have as Galois groups the (finite) groups

$$G =< g_0, \ldots, g_n >$$

which are generated by $n+1$ elements g_i with $g_0 \ldots g_n = 1$. Taking into account that in this case $\mathbb{C}(X) = \mathbb{C}(t)$, we get: For every finite group G with n generators, there exists an unramified Galois cover $Y \to X$ such that the Galois group of the field extension $\mathbb{C}(t) = \mathbb{C}(X) \hookrightarrow \mathbb{C}(Y)$is isomorphic to G. One way to interpret this result is the following:

The Inverse Galois Problem **(IGP)** *has a positive solution over $K = \mathbb{C}(t)$, the field of rational functions over $\mathbb{C}$.*

It was the idea of Hilbert, to try to use this fact in order to solve the IGP over other fields (which we call nowadays *Hilbertian fields;* the "primitive" fields introduced above, in particular $\mathbb{Q}$ itself, are Hilbertian fields). We will say later more about this.

We finish this Section by the fundamental remark, that there is a subtle connection between the **absolute Galois group** and the **fundamental group** as follows:

First, for a given algebraic complex variety X, let $\widetilde{X^{\mathrm{top}}} \to X(\mathbb{C})$ be a universal topological cover of $X(\mathbb{C})$. On the algebraic side, one also can define a kind of algebraic universal cover $\widetilde{X} \to X$, which nevertheless is not a variety, but a pro-algebraic space(...). One defines the *algebraic fundamental group* $\pi_1(X) = \mathrm{Aut}(\widetilde{X}|X)$. By the equivalence of categories mentioned above, it follows that $\pi_1(X)$ is isomorphic to the *profinite completion* of the topological group $\pi_1(X(\mathbb{C}))$.

The interpretation of this construction in terms of function field extensions is the following: The set of all X-unramified extensions of $\mathbb{C}(X)$, say in some fixed algebraic closure of this field, is increasingly filtered, and their union is an (usually infinite) Galois extension $\mathbb{C}(X) \hookrightarrow \mathfrak{K}_X$ with

$$\mathrm{Aut}\Big(\mathfrak{K}_X \mid \mathbb{C}(X)\Big) \cong \pi_1(X)$$

in a canonical way.

Second, suppose that the complex variety X is defined over some subfield $K \subset \mathbb{C}$, i.e., that there exists a variety X_K over K which becomes (canonically) isomorphic to X over the complex numbers $\mathbb{C}$. It is a basic fact concerning unramified covers of algebraic varieties (called after Grothendieck the *Specialization Theorem,* or maybe, *Invariance under geometric base change*), that every unramified algebraic cover $Y \to X$ is defined over some finite field extension L of K. In particular, if $\overline{K}$ is the algebraic closure of K, then every unramified cover $Y \to X$ of X is defined over $\overline{K}$; and it is not difficult to show that $\mathfrak{K}_X$ itself is defined over $\overline{K}$; this means that there exists an algebraic field extension $K(X) \hookrightarrow \mathfrak{K}_{X_K}$ such that $\overline{K}(X) \hookrightarrow \mathfrak{K}_{X_{\overline{K}}}$ becomes $\mathbb{C}(X) \hookrightarrow \mathfrak{K}_X$ when viewed over $\mathbb{C}$.

Finally, the whole field extension $K(X) \hookrightarrow \mathfrak{K}_{X_K}$ is a Galois extension (usually of infinite degree). Its Galois group is canonically isomorphic to the so called *étale fundamental group* $\pi_1(X_K)$ as introduced by Grothendieck. It is a profinite group whose open subgroups classify all finite étale connected covers of X_K. It fits in a natural way in the following exact sequence

$$1 \to \pi_1(X) \to \pi_1(X_K) \to G_K \to 1$$

It is the main object of interest in the modern Galois Theory and Arithmetic/algebraic Geometry. The absolute Galois group G_K, as a factor of $\pi_1(X_K)$, classifies the so called constant covers of X_K, wheres $\pi_1(X)$ as a subgroup of $\pi_1(X_K)$ classifies "geometric" covers of X_K (thus connected covers of X.

Further, it's interesting to remark that the first term in the above exact sequence is of geometric/combinatorial nature (coming from geometry and topology), wheres the right term is of arithmetic nature, coming from the field theory of the field K. This is of particular interest when we start with a primitive field K as field of definition for X, as in this case we expect that G_K encodes a lot of information about K. (*N.B.,* every complex variety X is defined over some primitive field.)

Example: Let $X = \mathbb{P}^1 \backslash \{0, \infty\}$, thus $X(\mathbb{C}) = \mathbb{C}^\times$ is homotopic to $\mathbb{S}^1$. The finite covers of $X(\mathbb{C})$ are all cyclic of the form $\mathbb{C}^\times \to \mathbb{C}^\times$, $w \mapsto z = w^n$. They correspond to algebraic morphisms $Y_n \cong X \to X$ defined by $x \mapsto y^n$ (where x and y are "canonical parameters on X and Y). Thus every X-automorphism σ of Y is defined by an n^{th} root of unity ζ_σ via $\sigma(y) = \zeta_\sigma y$, and $\mathrm{Aut}(Y_n|X) \cong \mu_n$, $\sigma \mapsto \zeta_\sigma$ is a canonical group isomorphism. By taking projective limits we get $\pi_1(X) \cong \widehat{\mu} = \varprojlim_n \mu_n$ canonically. Next we remark that X as well as all the Y_n are defined over $\mathbb{Q}$ (as they correspond to the affine rings homomorphisms $\mathbb{Q}[x] \hookrightarrow \mathbb{Q}[y]$, $x \mapsto y^n$). But <u>warning</u>: The deck transformation group is not defined over $\mathbb{Q}$, but over the corresponding cyclotomic extensions $\mathbb{Q}[\mu_n]$ of $\mathbb{Q}$. Moreover, the action of $G_\mathbb{Q}$ on $\pi_1(X) \cong \widehat{\mu}$ is given via the action of $G_\mathbb{Q}$ on every particular root of unity ζ_σ. The above canonical exact sequence becomes very explicit:

$$1 \to \widehat{\mu} \cong \pi_1(X) \longrightarrow \widehat{\mu} \rtimes G_\mathbb{Q} \cong \pi_1(X_\mathbb{Q}) \longrightarrow G_\mathbb{Q} \to 1$$

Remark: One should remark that this example is maybe illustrative, but not very exciting... In the more general case, where we want to understand $\pi_1(X_K)$ with $X_K \subset \mathbb{P}^1$ the complement of $r > 2$ points, the situation is much more intricate.

The first non-trivial case, i.e., $X = \mathbb{P}^1 \backslash \{0, 1\, \infty\}$, for short $\mathbb{P}^1_{01\infty}$, was first studied by Ihara, Anderson–Ihara. The conclusion is that there exists a subtle *deep relation between the action of* $G_\mathbb{Q}$ *on* $\pi_1(\mathbb{P}^1_{01\infty})$ *and the arithmetic of cyclotomic fields* (Jacobi sums, Iwasawa theory, etc.).

1. Structure of absolute Galois / fundamental groups

On the Inverse Galois Problem

Probably the best result of a general nature concerning the IGP over number fields (until now) is the one by Shafarevich saying that *every finite solvable group G is a finite quotient of G_K for every "primitive" field K* (in particular also for $K = \mathbb{Q}$). The proof uses very deep number theory, and in spite of the efforts of several mathematicians, we do not have a significant simplification of SHAFAREVICH's original and very technical proof (but some improvements by SCHMIDT–WINGBERG)...

There is –on the other hand– in recent years a lot of progress concerning the IGP using "geometric methods". The first idea in this direction goes back to HILBERT, as already mentioned, and reads:

Let $X \subset \mathbb{P}^1_t$ be the complement of some finite set $S = \{s_0, \dots, s_n\}$ with s_i in a primitive field $K \subset \mathbb{C}$. Then X is an algebraic variety defined over K, and as remarked above, every non-ramified cover of algebraic varieties (viewed as complex varieties) $Y \to X$ together with all its X-automorphisms are defined over some (Galois) finite extension of K. This means that given a finite group $G =< g_0, \dots, g_n >$ with $g_0 \dots g_n = 1$, after replacing K by some finite (say Galois) extension L, we can find a non-ramified Galois cover $Y_L \to X_L$ with $\mathrm{Aut}(Y_L|X_L) \cong G$. Let's denote $L(t) = L(X_L) \hookrightarrow L(Y_L)$ the corresponding Galois field extension with Galois group G. Then we have $L(Y_L) = L(t, y)$, with y a root of some polynomial $p_t(y) \in L[t, y]$. The fundamental observation of HILBERT is that in this situation there are "many" specializations $t \mapsto a \in L$, such that the resulting polynomial equation $\mathcal{E} : p_a(y) = 0$ over L is irreducible, and the resulting Galois group over L is $G_{\mathcal{E}} \cong G$.

In particular, if in this context $K = L$, we then have $G \cong G_{\mathcal{E}}$ as Galois group over K.

We are then at core of the problem: *Under which circumstances, do we have that the Galois unramified cover $Y \to X$ with Galois group $\cong G$ from above is defined together with all its X-automorphisms over K?*

Well, this is the major open question in the IGP !...

There is a *group theoretic criterion* for this, the so called *rigidity criterion* of BELYI, MATZAT, THOMPSON. Using this criterion, one can show that for several finite simple groups the answer to the above question is positive, thus these groups are isomorphic to Galois groups over every "primitive" field.

Although it is dangerous/difficult to make predictions, I think that before we will be able to give a satisfactory (positive) answer to the above question in general, we have to discover some new essential facts about fields of definition of unramified covers of curves. Nevertheless, the specialists strongly believe, that the following form of the IGP has a positive answer:

Generalized IGP: *Every finite group is the Galois group of some finite Galois extension $K|k(t)$, where k is a fixed base field, and $k(t)$ the rational field in one variable over k.*

The above Generalized IGP is true for $k = \mathbb{C}$ and over many other "interesting" fields k. Second, it would imply the IGP over every primitive field (as they are Hilbertian).

On the structure of G_K

As remarked in the first section, even if we know all the finite quotients of an absolute Galois group G_K, we are still far away from understanding the Galois group G_K itself. We would be most interested in knowing/understanding the structure of G_K, in the case K is a "primitive" field.

At the beginning of the Eighties, Grothendieck proposed in his *Esquisse d'un Programme* a *geometric/combinatoric* way to describe the absolute Galois group of $\mathbb{Q}$ along the following lines: Let us fix a subfield $K \subset \mathbb{C}$. For every complex variety X which is defined over K consider the canonical exact sequence defined above

$$1 \to \pi_1(X) \to \pi_1(X_K) \to G_K \to 1.$$

It is just easy group theory to see that the above exact sequence gives rise to a canonical <u>representation</u> $\rho_X : G_K \to \mathrm{Out}(\pi_1(X))$, where Out $=$ Aut/Inn denotes the group of outer isomorphisms. In words:

- *The absolute Galois group G_K acts canonically on the geometric fundamental group $\pi_1(X)$ via outer isomorphisms.*

Moreover, this action is functorial in the following way: If $f : X \to X'$ is a morphism of varieties, then the canonical homomorphism of profinite groups $\pi_1(f) : \pi_1(X) \to \pi_1(X')$ is a G_K-homomorphism. In words:

- *Every $\sigma \in G_K$ is in canonical way an automorphism of the geometric fundamental group functor π_1.*

Let us fix a category of complex varieties $\mathcal{V}$ which are defined over $\mathbb{Q}$, and let $\pi_{\mathcal{V}} : \mathcal{V} \longrightarrow \mathcal{G}$ be the geometric fundamental group functor (here $\mathcal{G}$ is the category of profinite groups and <u>outer</u> morphisms). Finally let $\mathrm{Aut}(\pi_{\mathcal{V}})$ be the automorphism group of the geometric fundamental group functor on $\mathcal{V}$. By the discussion above we have a group homomorphism

$$\imath_{\mathcal{V}} : G_K \to \mathrm{Aut}(\pi_{\mathcal{V}})$$

Following GROTHENDIECK, we can ask the following questions:

1) Find examples of such "interesting" categories $\mathcal{V}$, for which one can describe $\mathrm{Aut}(\pi_{\mathcal{V}})$ concretely, say using geometric/combinatorial/purely group theoretical objects/ways.

We would have a concrete description of G_K, which might prove useful in dealing with concrete questions concerning the arithmetic of $\mathbb{Q}$ (and more generally, of primitive fields), like for instance the IGP, rational points on varieties, etc..

2) Find some "interesting" categories of varieties $\mathcal{V}$ such that the representation $\imath_{\mathcal{V}} : G_K \to \mathrm{Aut}(\pi_{\mathcal{V}})$ is an isomorphism.

Comment: Via such categories we would have a description of G_K of a completely new nature, namely a geometric/combinatoric one; N.B., the objects on the right side are defined only in geometric terms, as they are varieties over $\mathbb{C}$.

GROTHENDIECK himself proposed as an "interesting" category the so called *Teichmüller modular tower* $\mathcal{T}$, which consists of all moduli spaces $M_{g,n}$ which classify compact Riemann surfaces of genus g with n punctures, and "connecting" morphisms. Every $M_{g,n}$ is a variety defined over $\mathbb{Q}$.

A special sub-category of $\mathcal{T}$ is the so called *genus* 0 *modular tower* $\mathcal{T}_0$*,* i.e., the sub-category consisting of all M_{0n}, thus the moduli spaces classifying the Riemann sphere with n punctures. One has:

- $M_{04} \cong \mathbb{P}^1 \backslash \{0, 1, \infty\}$, for short denoted $\mathbb{P}^1_{01\infty}$.
- In general, $M_{0n} = {M_{04}}^{n-3} \setminus \{\text{weak diagonal}\}$.

A special role is played here by the "mini"-sub-categories $\mathcal{M}_1 = \{M_{04}, M_{05}\}$ and $\mathcal{M}_2 = \{M_{04}, M_{05}, M_{11}, M_{12}\}$ called the first two levels in $\mathcal{T}$.

The automorphism group of $\pi_{\mathcal{M}_1}$ is the famous "Grothendieck–Teichmüller group" $\widehat{GT}$, which was intensively studied at a first instance by DRINFELD, IHARA, DELIGNE, and since then by several other people: MATSUMOTO, NAKAMURA, LOCHAK, SCHNEPS, HAIN, HARBATER, WOHLFAHRT, and many others. A first remark here is that $\mathbb{P}^1_{01\infty}$ has an "easy" geometric fundamental group, namely the profinite free group on two generators $\widehat{F}_2 = \pi_1(\mathbb{P}^1_{01\infty}) =< g_0, g_1, g_\infty \mid g_0\, g_1\, g_\infty = 1 >$ with the generators $x = g_0, y = g_1$. Second, using a (so called) tangential base point at $t = 0$, one can replace the outer action of $G_{\mathbb{Q}}$ on $\widehat{F}_2 = \pi_1(\mathbb{P}^1_{01\infty})$ by a "true" $G_{\mathbb{Q}}$-action which is then defined as follows: For $\sigma \in G_{\mathbb{Q}}$, let $\lambda = \chi(\sigma) \in \widehat{\mathbb{Z}}^\times$ be the value of the cyclotomic character at σ. Then

$$\sigma(x) = x^{\lambda}, \quad \sigma(y) = f_{\sigma}^{-1} y^{\lambda} f_{\sigma}, \qquad \text{for some } f_{\sigma} \in [\widehat{F}_2, \widehat{F}_2]$$

Thus the action is completely defined by f_σ; and understanding what f_σ is/does, is equivalent to understanding σ. These elements f_σ satisfy the so called *relations I, II, III,* introduced/studied by DRINFELD and IHARA.

A major result of the very last time here was proved by NAKAMURA–SCHNEPS, who confirmed GROTHENDIECK's philosophy that the information carried in the representation $\imath_{\mathcal{T}} : G_{\mathbb{Q}} \to \mathrm{Aut}(\pi_{\mathcal{T}})$ is actually already encoded in the much simpler representation $\imath_{\mathcal{M}_2} : G_{\mathbb{Q}} \to \mathrm{Aut}(\pi_{\mathcal{M}_2})$; and very important, that $\mathrm{Aut}(\pi_{\mathcal{M}_2})$ can be explicitly given...

Concerning question 2) above, we know very little about the nature of the representation $\imath_{\mathcal{V}} : G_K \to \mathrm{Aut}(\pi_{\mathcal{V}})$; more precisely, under which conditions $\imath_{\mathcal{V}}$ is an isomorphism. First, it is part of a famous result of BELYI (describing the compact Riemann surfaces defined over $\overline{\mathbb{Q}}$ in purely combinatorial way), that $\imath_{\mathcal{V}} : G_K \to \mathrm{Aut}(\pi_{\mathcal{V}})$ is injective if $\mathbb{P}^1_{01\infty}$ is an element of $\mathcal{V}$. But it is unclear under which hypothesis $\imath_{\mathcal{V}}$ is surjective. Intuitively, the larger the category $\mathcal{V}$ is, the better chances we have for the surjectivity (as every variety in $\mathcal{V}$ produces new obstructions for automorphisms of $\pi_{\mathcal{V}}$). By POP we know that $\imath_{\mathcal{V}}$ is an isomorphism in case $\mathcal{V}$ is the category of all complex varieties which are defined over $\mathbb{Q}$ (this question was asked by IHARA, ODA–MATSUMOTO, maybe others too).

Galois / fundamental groups in positive characteristic

Until now we discussed only Galois groups of subfields $K \subset \mathbb{C}$ and étale fundamental groups of varieties defined over such fields.

On the other hand, it is clear how one can/could proceed in order to define Galois extensions and absolute Galois groups of arbitrary fields K, thus also of fields of positive characteristic, like for instance finite fields...

It is less obvious to say what the right generalization of the geometric fundamental group should be, but this problem was solved very successfully by GROTHENDIECK via his definition of the étale fundamental group. Namely, for a given variety X_K over an arbitrary field K, one shows that the category of all non-ramified finite covers $Y \to X_K$ is a *Galois category,* thus it has a "fundamental group", which we denote $\pi_1(X_K)$ and call the fundamental group of X_K. This construction generalizes the construction of the fundamental group described previously, and coincides with it in the case $K \subset \mathbb{C}$. In particular, as in the complex case, there exists an exact sequence

$$1 \to \pi_1(X) \to \pi_1(X_K) \to G_K \to 1$$

with X the variety X_K viewed as variety over the algebraic closure of K.

But there are major differences between the situation in characteristic 0 and the situation in positive characteristic $p > 0$. Even very familiar assertions cannot be immediately transfered from characteristic zero to positive characteristic $p > 0$. For instance, let $\mathbb{A}^1_K$ be the affine t-line over the base field K. Then:

1) If $\mathrm{char}(K) = 0$, then $\mathbb{A}^1_K$ has only "constant" unramified covers. This is nothing but the fact that $\mathbb{A}^1(\mathbb{C}) \cong \mathbb{C}$ is simply connected !

2) But this is not true if $\mathrm{char}(K) = p > 0$. Indeed, $y^p - y = at$ defines an unramified cover of $\mathbb{A}^1_K$ for all $a \in K^\times$; such covers are called *Artin–Schreier covers.* In other words, the affine line has many unramified covers in positive characteristic !...

In contrast to the characteristic zero case, in positive characteristic we do not know unfortunately $\pi_1(X)$ in any single case of interest !... GROTHENDIECK proposed an ingenious way to tackle problems concerning fundamental groups in char $= p > 0$, by using *formal geometry* in order to "specialize" from characteristic zero. I think, it's better not to go into details here, but roughly speaking, the situation is as follows:

Suppose that k is an algebraically closed field of positive characteristic $p > 0$, and that X_k is a projective variety over k. Then there exists a projective variety over $\mathbb{C}$ (which is closely related to X_k), such that one has a *surjective "specialization" homomorphism*

$$\pi_1(X) \to \pi_1(X_k)$$

In particular, the geometric fundamental group of projective varieties is finitely generated as a topological group.

The situation is completely different, if we consider affine varieties, like for instance the affine line $\mathbb{A}^1_k$. Here, the geometric fundamental group is "huge"; and one of the reasons for this fact are the Artin–Schreier covers mentioned above, covers which are specific to positive characteristic. Some of the major results proved here in recent years are as follows.

Abhyankar type Conjectures

Studying finite unramified covers of the affine line $X_k \to \mathbb{A}^1_k$ over an algebraically closed field of characteristic $p > 0$, Abhyankar conjectured that the only obstruction for a finite group G to be isomorphic to the Galois group of such a cover is that G should be a *quasi-p group,* i.e., it should be generated by its Sylow p-subgroups. Equivalently, this means conjecturally that $\text{f.q.}(\pi_1(\mathbb{A}^1_k)) = \{\text{all finite quasi-}p \text{ groups}\}$. He went on and generalized this conjecture in more directions, which we call "Abhyankar type conjectures" (AC). They describe conjecturally the set of finite quotients of the geometric fundamental group of some specific affine varieties X_k over k, and could be viewed as an Inverse Galois Problem for the geometric fundamental group. First, for a finite group G, let $p(G)$ be the normal subgroup of G generated by all Sylow p-groups. Further set:

- $\Gamma_{g,n} \cong < a_1, b_1, \dots, a_g, b_g, c_1, \dots c_n \mid [a_1 b_1] \dots [a_g b_g] c_1 \dots c_r = 1 >$ the (isomorphy type of the) topological fundamental group of any compact Riemann surface of genus g with r punctures.

- $\Delta_d \cong < c_1, \dots, c_d \mid c_1 \dots c_d = 1 >^{\text{ab}}$ the (isomorphy type of the) topological fundamental group of the complement of d complex hyperplanes in $\mathbb{P}^n$ meeting transversally. Thus Δ_d is the free Abelian group on d generators on one relation.

The (AC) we want to recall are:

1) (AC) *for the complement X_k of $r \geq 1$ points in a complete smooth genus g curve:* $G \in \text{f.q.}(\pi_1(X_k)) \iff G/p(G) \in \text{f.q.}(\Gamma_{g,r})$
2) (AC) *for the complement X_k of d hyperplanes in $\mathbb{P}^n_k$ meeting transversally:* $G \in \text{f.q.}(\pi_1(X_k)) \iff G/p(G) \in \text{f.q.}(\Delta_d)$

This means that the prime to p-quotient of the geometric fundamental group which we know very well, as it looks like in characteristic zero. And on the top of it, there are covers which *have to do with the positive characteristic $p > 0$,* covers which we do not understand...

The status of the art with this problem is as follows:

1) First, the (AC) for affine curves is proved: After partial results by Abhyankar, Mori, Serre using several/different methods, Raynaud proved the conjecture in the case $X_k = \mathbb{A}^1_k$ using formal/rigid geometry; and based on this Harbater proved the conjecture in general.

2) The higher dimensional (AC) conjecture is out of reach. One should nevertheless remark that the (AC) as made by Abhyankar and explained

above is not correct (HARBATER–VAN DER PUT). Unfortunately, we do not know yet –even conjecturally– what the "true" conjecture might be...

Thus we could say that at least in the case of affine curves X_k, we have a satisfactory solution to the Inverse Galois Problem for the geometric fundamental group $\pi_1(X_k)$. On the other hand, we would be most interested in knowing the *full structure* of the geometric fundamental group.

Fundamental groups of complete curves

In contrast to the affine case, for complete curves X_k, the geometric fundamental group is (topologically) finitely generated. Such groups are *Pfaffian,* i.e., the set of their finite quotients determines the isomorphy type of the group in discussion. Thus f.q.$(\pi_1(X_k))$ completely determines the fundamental group. By Grothendieck's Specialization Theorem, if g is the geometric genus of X_k, then there exists a surjective group homomorphism

$$pr_X : \Gamma_g \to \pi_1(X_k)$$

And by the Pfaffian property, to determine $\pi_1(X_k)$, is equivalent to describing f.q.$(\pi_1(X_k))$ as a subset of f.q.(Γ_g).

There are several attempts/results in this direction, starting with the classical ones by HASSE–WITT, SHAFAREVICH, and then in later times by NAKAJIMA, RAYNAUD, STEVENSON, SAIDI, and many others, but we are far from understanding what the complete picture is...

2. What is encoded in the absolute Galois group

It was in the Seventies when NEUKIRCH and (after some partial results by KOMATSU and IKEDA) finally UCHIDA showed that for every number field (even for every global field) K, the *field structure is completely encoded in* G_K in a functorial way. This is indeed a very surprising fact !...

At the beginning of the Eighties, GROTHENDIECK made the "programmatic" conjecture that *arithmetic and geometry are group theoretically encoded in Galois theory and étale fundamental groups,* if some specific hypotheses (which he calls anabelian) are satisfied. This point of view sheds a new light on the NEUKIRCH–UCHIDA result, and puts it into a much broader picture. In a few words, the idea of GROTHENDIECK is the following:

Anabelian Objects:

1) First, all *"primitive" fields should be anabelian* (anabelian birational conjecture).

This means, that there should exist a group theoretical recipe such that given any such field K (thus a field K which is generated as a field by finitely many elements over $\mathbb{Q}$), after checking/applying the recipe to G_K one gets as a result the isomorphy type of K. Naturally, this should happen in a functorial way.

2) Thinking about fields as 0-dimensional varieties, Grothendieck conjectures that the *smooth hyperbolic connected curves, when viewed as varieties defined over some "primitive" base fields* are anabelian 1-dimensional varieties (anabelian curve conjecture)

As above, this means that there should be a group theoretical recipe such that given such a curve X_K, its isomorphy type (as a curve over K) should come out from its étale fundamental group $\pi_1(X)$ in a functorial way.

- Unfortunately, it is difficult to say what higher dimensional anabelian varieties should be. There are meanwhile several attempts to find the right conjecture, but we are not yet successful.

Anabelian points

Finally, Grothendieck makes conjectures concerning "points" on anabelian objects. The starting observation here is that given a smooth variety X_K, every K-rational point $x \in X_K(K)$ gives rise to (a conjugacy class of) a section s_x of the canonical projection

$$pr : \pi_1(X_K) \;\to\; G_K$$

Moreover, in the case X_K is not a complete variety, the K-rational points $\tilde{x}$ "at infinity" of X_K give rise to (a bunch of conjugacy classes of) sections $s_{\tilde{x}}$ of pr.

Now Grothendieck conjectures that in the case of anabelian curves, this is the *only way sections of* pr *arise.* A positive answer to this conjecture would have deep consequences for the arithmetic of rational points.

Results / Comments

The status of the results concerning the above anabelian conjectures is quite satisfactory. First, Pop showed that the "primitive" fields are all anabelian, thus giving a natural generalization of the Neukirch–Uchida result. Concerning anabelian curves, after some partial results by Nakamura, the full answers where given, first, by A. Tamagawa in the case of affine anabelian curves, and then in general by Mochizuki (all in characteristic zero).

But there is a **very important remark** one has to make here: for Grothendieck at least, it seems that the "anabelian" is/was intimately related to "defined over primitive fields"... Well, the last developments show that the reasons for "anabelian" are of a much more subtle nature, which we do not yet understand. The status of the art is actually the following:

a) First, for function fields $K|k$ of transcendence degree > 1 over *algebraically closed base fields k*, there is a satisfactory "local theory", by Bogomolov, Koenigsmann, Pop, and this even in a pro-ℓ setting.

Thus one should/could hope that in spite of the total lack of arithmetic (as k is alg. closed), we will have here some anabelian type results.

b) Let $k = \overline{\mathbb{F}}_p$. It was shown by A. Tamagawa, that there do exist anabelian phenomena of *tame type* for affine smooth curves over k. Further, "weak" anabelian phenomena are present for a large class of complete smooth curves over k, as shown by Raynaud and Pop–Saidi.

The only "arithmetic" here is the fact that $k = \overline{\mathbb{F}}_p$.

c) Last but not least, we have the very deep result by Mochizuki: *The category of all hyperbolic curves and dominant morphisms over a sub-p-adic field is anabelian.* This is an incredible result, which goes far <u>beyond</u> Grothendieck's conjectures concerning anabelian curves...

- All these results contradict the "finitely generated base" canon!...

3) A short list of Questions/Problems

– Give a geometric proof of Shafarevich's result that every solvable group is a Galois group of a (regular) cover the line over $\mathbb{Q}$.

– Find the right higher dimensional "Abhyankar Conjecture", and prove it.

– Find an "algebraic proof" for the structure theorem of the fundamental group of complete curves in characteristic zero.

– Give a geometric/combinatorial description of the geometric fundamental group of curves in positive characteristic (e.g. for $\mathbb{A}^1$ or complete curves, genus > 1).

– Prove or disprove: $\widehat{GT} \cong G_{\mathbb{Q}}$. If NO, what is the precise description of $G_{\mathbb{Q}}$ inside $\widehat{GT}$?

– Solve the problem of determining/describing the Galois orbits of "dessins d'enfants".

– Find the “right” higher dimensional Belyi Theorem and “dessins d’enfants”.

– Prove the Hom-form of the birational anabelian conjecture in all characteristics.

– What are the “right” higher dimensional anabelian objects?

– Prove “Bogomolov’s claim” that the pro-ℓ birational conjecture is true in the geometric situation.

– Prove/disprove that complete curves in positive characteristic are (weak) anabelian. Is there a Hom-form?

– Prove or disprove Grothendieck’s section conjecture, respectively its p-adic variant(s).

– Prove the Shafarevich Conjecture saying that the kernel of the cyclotomic character of a global field is profinite free (geometric case known by HARBATER, POP).

– Prove or disprove: $\mathbb{Q}^{\mathrm{ab}}$ *is a large field.*

...and here is:

The $*****-$**Problem:** *Solve the generalized IGP over* $\mathbb{Q}$.