Proceedings of Symposia in Pure Mathematics

Prelude: Arithmetic Fundamental Groups and Noncommutative Algebra

Michael D. Fried

Abstract. From number theory to string theory, analyzing algebraic relations in two variables still dominates how we view laws governing relations between quantities. An algebraic relation between two variables defines a nonsingular projective curve. Our understanding starts with moduli of curves. From, however, cryptography to Hamiltonian mechanics, we command complicated data through a key data variable. We're human; we come to complicated issues through specific compelling interests. That data variable eventually drags us into deeper, less personal territory. Abel, Galois and Riemann knew that; though some versions of algebraic geometry from the late 1970s lost it. A choice data variable (function to the Riemann sphere) to extract information brings the tool of finite group theory. Giving such relations structure, and calling for advanced tools and interpretations, is the study of their moduli — the main goal of the papers of this volume. Applications in this volume are to analyzing properties of the absolute Galois group $G_{\mathbb{Q}}$ (Part I) and to describing systems of relations over a finite field (Part II). Such applications have us looking at finite group theory and related algebra (Parts III and IV) in a new way.

§1 reminds of classical problems that motivated those authors whose papers appear in this volume. We dramatize research events around the 1995 Seattle Conference, Recent Developments in the Inverse Galois Problem, in the Contemporary Math series of AMS, in §2. This also has reader aids for connecting that 1995 volume to this volume's papers. In this one sees how group theory applies to modern applications. Conversely, when we see the effect of studying moduli of algebraic relations, it changes how we perceive group theory classification results. §3 points to applications addressed by particular papers in this volume. This is inadequate to explain either the motivations of the authors or the connections between the papers. To get the results out to the public, the author of this prelude has added some necessary background to the Part I papers in §2. He will, however, reference this volume, in a later paper that ties the finite group theory, Lie theory and Tannakian viewpoints together.

2000 *Mathematics Subject Classification.* Primary 11F32, 11G18, 11R58 14G32; Secondary 20B05, 20C25, 20D25, 20E18, 20F34.

Author support from MSRI, NSF #DMS-9970676 and a senior research Alexander von Humboldt award.

1. Algebraic relations, moduli and $G_{\mathbb{Q}}$

We use the word *moduli* to mean working smartly with gobs of algebraic relations. As in our abstract we intend that the relations (algebraic curves) come with a data variable (function). An elliptic curve described by the equation $y^2 = x^3+ax+b$ with x as its data variable is an appropriate example. So too is the w-sphere with a choice of rational function $f(w) = z$. Applications demand understanding more than one relation at a time. We often must pick special equations from a mass of candidates. Typical is the quest for a good chunk of specific relations to have a chosen definition field ($\mathbb{Q}$ or a p-adic field). The j and λ lines of classical complex variables inform the wise investigator of algebraic relations daily. Was there ever a greater joining of group theory to complex variables than when Galois applied his famous solvability criteria to modular curves [**Ri96**, last pages]? This extends that tradition where classical modular functions help us understand new relations. We closely relate to quotients of Siegel upper half space, significant moduli spaces. Taking advantage of data from a function on a curve immensely increases applications. Further, we see from a different view problems that plague progress on Siegel modular functions.

Relations with a data variable have more discrete invariants than the genus of a curve. Riemann called his favorite example half-canonical classes. These helped him pick the right theta function for his monumental solution to Jacobi's inversion problem. Serre connected Schur multipliers of alternating groups to half-canonical classes. His results hastened investigations of algebraic relations with groups having a nontrivial center. The most mysterious of perfect groups appear as extensions of simple groups with a nilpotent tail. Serre posed problems that embed in this situation. In Part I, we find how modular representations help solve and generalize this. Some papers march from Riemann's abelian functions into the domain of nilpotent functions. These tie moduli generalizing modular curves to the whole Inverse Galois Problem. Relations with a data variable: Connecting, demanding and inspiring in what it tells us of the effectiveness of mathematics.

1.1. Each element of $G_{\mathbb{Q}}$ gives a motion on algebraic points. We use the notation $\bar{\mathbb{Q}}$ for the algebraic numbers and $G_{\mathbb{Q}}$ for its automorphism (or Galois) group. Similar notation works for any other field. Example: The Galois group of the algebraic closure $\bar{\mathbb{F}}_p$ of the finite field $\mathbb{F}_p$ is $G_{\mathbb{F}_p}$. The basic question of arithmetic geometry: With what groups are we to compare $G_{\mathbb{Q}}$ and what are its significant subgroups and quotient groups? Other fields K (for example, $\mathbb{Q}(z)$ with z an indeterminate) replace $\mathbb{Q}$ in natural problems and they receive great attention. For example, that every finite group is a quotient of $G_{\mathbb{Q}}$ is the conjecture we call *The Inverse Galois Problem* (IGP: Hilbert's version). Any homomorphism $\varphi : G_{\mathbb{Q}(z)} \to G$ gives a map $G_{\mathbb{Q}} \to G$ by restricting elements of $G_{\mathbb{Q}(z)}$ to $\bar{\mathbb{Q}}$. The IGP has a variant: Each finite group G is the range of a map $\varphi : G_{\mathbb{Q}(z)} \to G$ that factors trivially through $G_{\mathbb{Q}}$. We call such quotient a *regular* realization of G. By running over z in $\mathbb{Q}$ we produce infinitely many disjoint ordinary realizations of G. So the *regular* version of the Inverse Galois Problem is much stronger than Hilbert's version. Suppose, for example, G is a simple group, presented as a quotient of $G_{\mathbb{Q}(z)}$. Then this is either a regular realization or it presents G as a quotient of $G_{\mathbb{Q}}$. Excluding Shafarevich's result on nilpotent groups, aiming for the regular version is also more successful.

Any $\sigma \in G_{\mathbb{Q}}$ permutes algebraic points on algebraic sets having equations with coefficients in $\mathbb{Q}$. We can view $G_{\mathbb{Q}}$ as a set of motions on algebraic sets over $\mathbb{Q}$. Still, there are topological peculiarities. First: Algebraic points have many topologies. Each is equally natural. Further, $G_{\mathbb{Q}}$ also has a natural topology. Its basic open sets are translates of subgroups G_F with F a finite extension of $\mathbb{Q}$. Though $G_{\mathbb{Q}}$ is huge, we have the advantage that this topology is compact. Each topology on $\bar{\mathbb{Q}}$ has, up to isometry, an attached prime P. A Cauchy completion of $\bar{\mathbb{Q}}$ then restricts to a completion of $\mathbb{Q}$ that is either the real numbers (archimedean) or the p-adic numbers (nonarchimedian) with p a prime. We say P *lies over* p. For a given P, elements in $G_{\mathbb{Q}}$ continuous in this topology comprise the *decomposition group* D_P of P. Concretely, P is an ideal in the subring $\mathcal{O}_{\bar{\mathbb{Q}}}$ of $\bar{\mathbb{Q}}$ whose elements satisfy a monic polynomial over $\mathbb{Z}$. Then, D_P is the collection $\{\sigma \in G_{\mathbb{Q}} | \sigma(P) = P\}$. This is a complicated group. Its action on $\mathcal{O}_{\bar{\mathbb{Q}}}/P$ has the *inertia* group I_P as kernel. The quotient D_P/I_P identifies with the pro-cyclic group $G_{\mathbb{F}_p}$. This has a classical generator Fr_p, the pth power homomorphism of $\bar{\mathbb{F}}_p$.

Decomposition groups for all primes over one p comprise a conjugacy class of groups in $G_{\mathbb{Q}}$. An overriding theme of a 200 year old study seeks collections of related objects $\{A_i\}_{i \in I}$ having a $G_{\mathbb{Q}}$ action respecting the relations and the following property. For any $i \in I$, all but finitely many of the conjugacy classes of groups I_P act trivially on A_i: The action is unramified at almost all p. There is no intention of forgetting about I_P. Rather, we scrutinize carefully for each i the exceptions to I_P acting trivially. There is a natural filtration on I_P. Its kth element is $I_{P^{k+1}}$, the elements acting trivially on the quotients P/P^{k+1}, $k = 1, 2, \ldots$. A *tame* action on an A_i is one for which I_{P^2} acts trivially.

1.2. A classical event in the history of $G_{\mathbb{Q}}$. We understand most groups through their representations. So $G_{\mathbb{Q}}$ should be no exception. Any family of projective nonsingular varieties provides a $G_{\mathbb{Q}}$ action attached to the ℓ-adic (ℓ a prime) cohomology of a $\mathbb{Q}$ fiber of the family. Restriction to D_P factors through D_P/I_P for all but a finite number of primes $p(P)$. Part I papers use families of curves, though the action of $G_{\mathbb{Q}}$ is not on the cohomology of the curves. Rather, the study is of an action on particular profinite quotients of the fundamental group of curves. This fiber action has another goal. Ultimate information on $G_{\mathbb{Q}}$ comes from its action on a quotient of the parameter variety fundamental group. I'll give preliminaries on this, and how the parameter variety becomes the center of attention.

Any (finite) cover of $\mathbb{Q}$ varieties gives us a test for the action of $G_{\mathbb{Q}}$. The test has fascinated many mathematicians. At its source is how to understand values of algebraic functions. For example, let $f(z)$ be a (nonconstant) algebraic function. That means for some nonzero $m(z, w)$ in the polynomial ring $\mathbb{Q}[z, w]$, $m(z, f(z))$ is identically 0. Then, f defines a ramified cover $\varphi_f : X_f \to \mathbb{P}^1_z$ of the z-line with X_f a projective nonsingular curve. Exclude z' from being in the branch set $\boldsymbol{z}$ of f. For the remaining z', points on X_f over z' come from evaluating analytic continuations of $f(z)$ along paths in $U_{\boldsymbol{z}} = \mathbb{P}^1_z \setminus \boldsymbol{z}$ at z'. Let $V_{f,z'}$ be that complete set of values. As we vary z' over $\mathbb{Q} \cup \{\infty\}$ minus $\boldsymbol{z}$, these values $V_{f,z'}$ vary strikingly with no apparent continuity in z'. Here is why.

Values in $V_{f,z'}$ generate a field. We call this $\Omega_{f,z'}$. Similarly, denote the set of analytic continuations of f to z', following closed paths in $U_{\boldsymbol{z}}$, by V_f. Then V_f generates a field, Ω_f. The constants of Ω_f form a field we call $\hat{\mathbb{Q}}_f$. As a splitting field, $\Omega_f/\mathbb{Q}(z)$ is a Galois extension with group G_f. Similarly, $\Omega_{f,z'}$ is a Galois

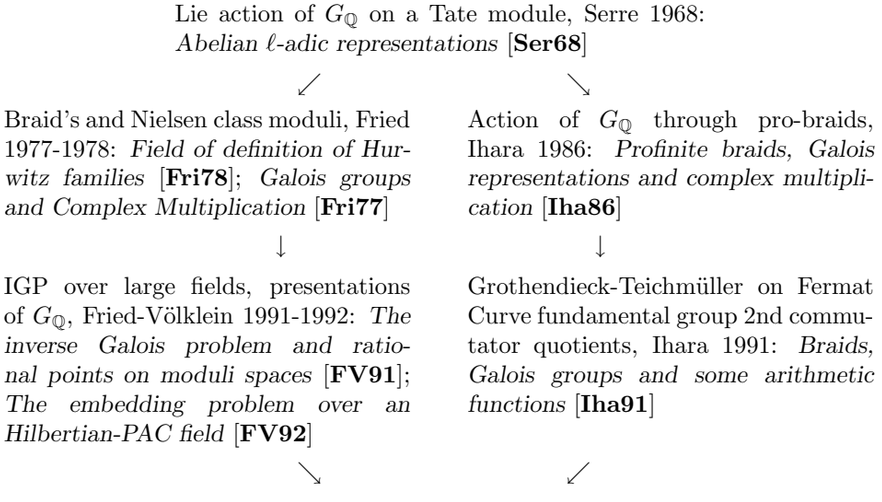
extension of $\mathbb{Q}$ with group $G_{f,z'} \leq G_f$. Hilbert's irreducibility theorem produces an infinite set S_f of z' with $G_{f,z'} = G_f$ and $\Omega_{f,z'} \cap \Omega_{f,z''} = \hat{\mathbb{Q}}_f$ for any two distinct elements $z', z'' \in S_f$.

We apply the *Chebotarev density theorem* for a version of *Hilbert's irreducibility theorem* [**FJ86**, Thm. 12.7]. Consider any algebraic function $f(z)$. For all but finitely many primes p (the exceptional set is dependent on f) there is an infinite set $S'_{f,p} \subset S_f$ of $z' \in \mathbb{Q}$ so the action of D_P factors through D_P/I_P. Restrict the element giving the Frobenius map Fr_p to $\Omega_{f,z'}$. Call this $\sigma_{p,z'}$; we know it up to conjugacy in $\hat{G}_f$. Further restriction of $\sigma_{p,z'}$ to $\hat{\mathbb{Q}}_f$ will be independent of z'. Call this σ_p. The Chebotarev result says we can choose $S'_{f,p}$ (even as an explicit arithmetic progression of integers) so the following holds. As z' varies, $\sigma_{p,z'}$ runs over all elements of $G(\Omega_f/\mathbb{Q}(z)) = \hat{G}_f$ that restrict as $\hat{\mathbb{Q}}_f$ is σ_p.

Frobenius elements of $\bar{\mathbb{Q}}$, running over primes p are dense in $G_{\mathbb{Q}}$. Conclusion: For most elements $\sigma \in G_{\mathbb{Q}}$ their action on fibers of any nontrivial cover depends greatly on which fiber. There is no way to recognize anything special about most elements of $G_{\mathbb{Q}}$ from one cover alone. Even worse, the action is completely chaotic if we expect to understand the action for all points $z' \in \mathbb{Q}$.

2. Research Events 1988-1995 and the Seattle Volume

Complex multiplication, especially that we call *Serre's Open Image Theorem*, guided many investigations. We separate developments closely allied with moduli of curves from more constructive aspects of the Seattle conference. Both Fried and Ihara fastened their attentions on the role of moduli, the braid group and the use of geometry to understand the effect of $G_{\mathbb{Q}}$ on algebraic relations. Influences on subsequent research events up to the Seattle Conference, 1995 appear below.



2.1. Other events in the 1995 Seattle volume. I especially mention developments that came to a satisfactory conclusion near the 1995 volume. Each subarea went from a resonant defining problem into a new territory after 1995. New approaches came with higher practical expectations and they brought more advanced techniques, as we see in §3. A synopsis of the Inverse Galois Problem (IGP) not using the full power of braid rigidity from before the 1995 volume pervades [**Ser92**]. [**Fri94**] (or [**Fri95b**]) gives an inkling of what was to happen during and after production of the 1995 volume.

2.1.1. *Abhyankar's Conjecture.* Extending Grothendieck's tame ramification theorems is behind much of this volume's Part II [**Gr71**]. [**Ab57**] inspired both Grothendieck and these authors. So, its influence spans many decades. Let G be a finite group with $\mathbf{C} = (\mathrm{C}_1, \dots, \mathrm{C}_r)$ a set of r conjugacy classes in G. In characteristic 0, Riemann's Existence Theorem says there is a simple condition guaranteeing a (ramified) cover of the z-sphere (or z-line; $\mathbb{P}^1_z$) with Galois (monodromy) group G, r branch points $z_1, \dots, z_r = \boldsymbol{z}$ and local monodromy at these respective points in $\mathbf{C}$. It is this. Some elements $g_i \in \mathrm{C}_i$, $i = 1, \dots, r$, satisfy two conditions:

(2.1a) Product-one: $\prod_{i=1}^r g_i = 1$; and
(2.1b) Generation: $\langle g_1, \dots, g_r \rangle = G$.

Further, such covers (up to covering equivalence) correspond to such choices, up to a permutation equivalence on r-tuples in G. [**Gr71**] showed this works the same in characteristic p if p is prime to $|G|$. The gist of Abhyankar's conjecture: We can drop the product-one relation if p does not divide the local inertia orders.

How is that possible? How can it be, in characteristic 2, that a cover of the z-line ramified only over ∞ can have as monodromy group the simple group we know as the Monster? ([**Ser92**,] reproduces Thompson's argument for a Monster cover over $\mathbb{Q}$; it has the minimal number of branch points, three, in characteristic 0.) It helps that local field extensions with wild ramification have possibly large inertia groups. Still, in this explanatory case, such groups are 2-groups. So, it doesn't explain how to get the Monster. While all places in the cover ramified over ∞ have inertia groups in one conjugacy class, unlike over $\mathbb{C}$, they may not have isomorphic local field extensions. Such a cover creates a collection of conjugate 2-groups in the Monster that generate it. Abhyankar's conjecture is that any group with generating p-Sylows is the group of a $\bar{\mathbb{F}}_p$ cover of the z-sphere ramified only over ∞. Raynaud [**Ra94**] proved this using Harbater patching and some serious analysis of the stable compactification theorem in positive characteristic. [**Ha94**] then generalized this to arbitrary affine curves. Though an achievement, this result left serious questions. We use the phrase, p' by p group, to mean a group that is the semi-direct product of a cyclic group of order prime to p acting on some p group. Inertia groups of points on curves in characteristic p are always p' by p groups.

(2.2a) What can we expect of the specific inertia groups and of monodromy groups of covers of the z-sphere ramified only over ∞? Specifically, for a given group can we bound the Herbrand upper numbering of the corresponding inertia groups?
(2.2b) Does Riemann's existence theorem in characteristic p extend so as allowing attaching extensions of cyclic p' groups by p groups to each ramified place?

(2.2c) Anabelian problem: Can we expect to determine any curve from its profinite (geometric) fundamental group up to conjugacy by the Frobenius? (If yes, is it possible to describe those profinite groups?)

There is a known case of the anabelian problem: For a finite set $\boldsymbol{z}$ over $\bar{\mathbb{F}}_p$ on the z-line, the (profinite) fundamental group of $U_{\boldsymbol{z}}$, $\pi_1(U_{\boldsymbol{z}})$ determines $\boldsymbol{z}$ up to $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ and $G_{\mathbb{F}_p}$ action ([**Ta99**], §3.2.1). Harbater's patching method has become a standard on its own. [**D95**] and [**Des95**] used it to find p-adic points on Hurwitz spaces corresponding to Nielsen classes containing *Harbater-Mumford representatives* (see [BF] §3.1).

2.1.2. *The genus 0 problem.* Suppose $f(w)$ is rational function in w. It maps points on the w-sphere to the z-sphere. The Galois closure group of the splitting field of $f(w) - z$ over $\mathbb{C}(z)$ (monodromy group of f) is special. That is the gist of the genus 0 problem over $\mathbb{C}$. (The same qualitative statement holds for any fixed genus.) Guralnick and Thompson's original version is this. With finitely many exceptions, the simple composition factors of the monodromy group of such a map must be alternating or cyclic groups. The solution of this left three big problems.

(2.3a) What are the precise monodromy groups, with finitely many exceptions, of *indecomposable* rational functions? Guralnick's 0-Conjecture: We only get alternating groups, symmetric groups, cyclic and dihedral groups. These should come only with special degree representations.

(2.3b) What groups must one add for rational functions over fields of positive characteristic? Guralnick's p-Conjecture: In characteristic p add Chevalley groups over extensions of $\mathbb{F}_p$ to alternating and cyclic groups.

(2.3c) Mumford's Question: What function fields in one variable over $\mathbb{C}$ have uniformizations by the Galois closure field of a rational map?

[**Fri99**] discusses all of these and the history from the Davenport Problem motivations to the complete resolution of the genus 0 problem. Further, Davenport's problem in positive characteristic corroborates Guralnick's inspired p-conjecture. So does the voluminous work of Abhyankar toward his exponent mantra for producing Chevalley groups over $\mathbb{F}_p$ from genus 0 covers. A gem from 1995 is Müller's listing of the monodromy groups of polynomials [**Mül95**].

Like the genus 0 problem, Mumford's question has several forms. For example: Any curve defined by a separated variables equation $f(w) - g(u)$ would have its function field in the composite of splitting fields over $\mathbb{C}(z)$ of functions $f(w)-z$ and $g(u)-z$. That includes all hyperelliptic curves. Directly, the description of modular curves as moduli of genus 0 curves [**Fri78**] produces elliptic curves from systems of rational function Galois closures, no composite required. Mumford's question has no representation in this volume. It remains untouched in that no function field has been excluded from the genus 0 closure field.

2.1.3. *Shafarevich's Conjecture.* Let $\mathbb{Q}^{\mathrm{cyc}}$ be the minimal extension of $\mathbb{Q}$ containing all roots of one. Shafarevich's Conjecture: The kernel of the cyclotomic map $G_{\mathbb{Q}} \xrightarrow{G} (\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q})$ is a pro-free group. There were two very different approaches to this still unsolved problem. Two properties put $\mathbb{Q}^{\mathrm{cyc}}$ in a context. First: Its absolute Galois is projective (in the category of profinite groups). Second: It is an Hilbertian field. [**FV92**] proposed a general conjecture: All subfields K of $\bar{\mathbb{Q}}$ with these properties would have pro-free absolute Galois groups. It proved this conjecture under a weakening of projective to K being P(seudo)A(lgebraically)C(losed).

For example, adjoin any complex number to the field of algebraic totally real numbers. Such a field is PAC field and its absolute Galois group is pro-free.

Matzat-Malle (MM) used *GAR* realizations over $\mathbb{Q}^{\rm cyc}$. From the inception of braid rigidity [**Fri77**], cyclotomic fields played a special role. This was from the appearance of characters of finite groups. Using generators of the classical groups that satisfy Belyi's criterion [**Be79**], having one common large eigenspace, MM applied Chevalley simple groups and the rigidity technique alone. Since $G(\mathbb{Q}^{\rm cyc}/\mathbb{Q})$ is projective, a technical result reduces this conjecture to proving every single finite simple group has a GAR realization over $\mathbf{Q}_{\rm cyc}$. You can't leave out even one simple group. Thus, [**MM99**, Chap. II] runs parallel to aspects of the classification of finite simple groups. They get all sporadic simple groups. As expected, exceptional Lie-type groups are a big problem. Groups they got, and those they did not, appear in a list in [**MM99**, §10].

2.1.4. *Realizations of Chevalley group sequences.* There is a way to combine the regular version of the IGP with Hilbert's version. That technique was essential to [**FV92**] . Following that Völklein, using how [**Fri78**] examined complex multiplication to reformulate a Schur cover problem, made a spectacular jump in the IGP with refinements to braid rigidity. The constraint on the rigidity method is that it seemed to require two generators of the group with very special properties. Braid group ideas relaxed that to allow every group to have appropriate generators. The cost being you had to find rational points on a canonically defined variety to finish the process. There were but a handful of Chevalley groups of rank exceeding 1 with regular realizations over $\mathbb{Q}$ at the writing of [**Ser92**]. [**Vö95a**] and papers referenced in [**Vö96**], bring the method of [**FV92**] to produce regular realizations of infinite sequences of such groups. These papers establish the rubric toward the following goal of Thompson-Völklein: For each finite field $\mathbb{F}_q$, excluding finitely many exceptions, show each Chevalley group has a *large family* of regular realizations parametrized by a unirational Hurwitz space over $\mathbb{Q}$. Example case: The symplectic family of groups $\mathrm{Sp}_{2n}(\mathbb{F}_q)$, $n = 1, 2, \ldots$ with q a square and not a power of 2. §3.3 describes a competing development.

2.2. Moduli fundamental groups and sphere covers. Applications from our understanding of $G_{\mathbb{Q}}$ come through its acting on fundamental groups of curves. We need, however, to beef up the fundamental groups to get such an action since $G_{\mathbb{Q}}$ is a compact topological group and fundamental groups are discrete groups. Also, those accustomed to looking at a hyperbolic curve C uniformized by a disc might wonder why we don't just act by $G_{\mathbb{Q}}$ on the algebraic points of the disc and induce an action on the curve. Answer: The uniformization function is not algebraic, so it rarely takes algebraic points to algebraic points. By beefing up a fundamental group we mean to take its profinite completion with respect to subgroups of finite index [**FJ86**, Chap. 15]. This is the object whose finite index subgroups correspond to algebraic functions. By acting on coefficients of Puiseux expansions of algebraic functions around algebraic points, we develop formulas for that action, and some structure on $G_{\mathbb{Q}}$ (see §2.4). It is systems of covers from moduli problems that give both structure and applications.

From this point the phrase fundamental group will mean this profinite completion (or some quotient of it). Moduli problems define the quotients directly. Instead of saying a quotient of a fundamental group, we say we are looking at the

fundamental group of a moduli problem. Particular moduli problems define quotients of traditional fundamental groups of spaces. We will call this the *moduli fundamental group*. Another name, from classical examples, is the *mapping class group* on the moduli problem. More refined applications paradoxically relate to the oldest problems, those formed by masters from a century or more ago. These come from inspecting the action of $G_{\mathbb{Q}}$ on the moduli fundamental group.

Even so fundamental an object as the Tate module of an elliptic curve looks different from the viewpoint of sphere covers. This is the profinite completion of the following group [**Fri95a**, Intro]:

$$\langle \sigma_1, \dots, \sigma_4 \rangle / \langle \sigma_i^2 = 1, i = 1, \dots, 4, \prod_{i=1}^{4} \sigma_i = 1 \rangle. \tag{2.4}$$

The product-one relation (2.1) here appears as $\prod_{i=1}^{4} \sigma_i = 1$. (More precisely the p-adic Tate module is from the pro-p quotient of this group for some prime p.) It is an error to ignore the obvious. Genus 1 curves come from degree 2 covers of the sphere ramified at four points. An elliptic curve appears as the Picard group of degree 0 divisor classes on that covering curve. Sometimes this is like looking at such genus 1 curves up to the action of $\mathrm{PGL}_2(\mathbb{C})$ (Möbius transformations) on the branch points. Should the unordered set of branch points be over $\mathbb{Q}$, then $\mathbb{Q}$ acts on (profinite completion of) a group isomorphic to (2.4). So, if the Tate module and the $G_{\mathbb{Q}}$ action look so unfamiliar this way, why take this approach?

An easy historical answer: The same idea blesses the literature's preoccupation with hyperelliptic curves. As, however, in [**Fri95a**, Intro] there is compelling reason to find $\mu_{p^{k+1}}$ points on hyperelliptic jacobians rather than $\mathbb{Q}$ points of order p^{k+1}. Even for genus 1, practical cryptography applications have a voluminous literature on exceptional covers and Schur's problem [**Fri78**]. The study of genus 0 covers is still very much alive. Moduli of genus 0 covers includes the most used modular curves classically denoted $X_0(n)$ [**Fri78**].

Still, we can give a better answer to using (2.4). Many classical diophantine problems dramatically generalize when we see them as special cases of the regular Inverse Galois Problem (§3.1.1). With profit we view those modular curves classically denoted $X_1(n)$ as moduli spaces: Moduli of dihedral group involution realizations. Then, a statement about dihedral groups generalizes to every finite group in the program of Modular Towers. A Tate module appearing in (2.4), is the special case for dihedral groups of a general situation for all finite groups. Structures on Tate modules reappear gracefully at crucial steps in every case as a piece of the picture. The name Modular Towers appears jointly for its relation to modular curves and its reliance on modular representation theory.

Using moduli of curve covers generalizes mathematical applications over those for abelian varieties, without losing anything from our knowledge and delight with abelian varieties. It is algebraic relations in two variables that we understand best. These bring our literature and intuition about mysterious mathematical objects, like $G_{\mathbb{Q}}$. Abelian varieties that get intense scrutiny often are isogeny factors of curve Jacobian. Very often they are Schottky factors from a piece of the Galois theory of covers (§2.1.1).

Moduli of curve covers has this relation to the classical simple groups. The symplectic group $\mathrm{Sp}_{2g}(\mathbb{R})$ consists of $2g \times 2g$ matrices $T = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix} \right)$ over $\mathbb{R}$ that

preserve an alternating pairing. With $\mathcal{I}_g = \left(\begin{smallmatrix} 0_g & -I_g \\ I_g & 0_g \end{smallmatrix}\right)$, we write the pairing as $T^{\mathrm{t}}\mathcal{I}_g T = \mathcal{I}_g$. When $G_{\mathbb{Q}}$ acts on a $2g$ dimensional Tate module, its image is in $\mathrm{Sp}_{2g}(\mathbb{Z}_p)$ (rather than wandering all over the general linear group $\mathrm{GL}_{2g}(\mathbb{Z}_p)$). The constraint confining it is from the Weil pairing on the Tate module. While $\mathrm{Sp}_{2g}(\mathbb{R})$ doesn't have many open subgroups, $\mathrm{Sp}_{2g}(\mathbb{Z}_p)$ does. So it is still significant if the image of $G_{\mathbb{Q}}$ is an open subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z}_p)$.

Serre's Open Image program foundered when addressing higher dimensional abelian varieties. The problem is the practical likelihood in real applications – especially defined by curves – that other geometric reasons (correspondences) would limit the action of $G_{\mathbb{Q}}$ to appear in Zariski proper subgroups of $\mathrm{Sp}_{2g}(\mathbb{Z}_p)$.

2.3. Nilpotent functions and real sets of r points on $\mathbb{P}^1_z$. In acting on moduli fundamental groups there is no obvious classical group comparison. One can view the *Grothendieck-Teichmüller group* (GT; see (2.5)) as a nilpotent analog on curve moduli of the Weil pairing. There has been a switch in thinking from 1995. That switch persists even as this volume appears. The approach through identifying the image of $G_{\mathbb{Q}}$ in moduli mapping class groups holds great promise. Some papers of this volume give that meaning. Outside this volume we point specifically to the progress of [**HM01**] (based on [**Ma95**]). Now we discuss something more down-to-earth: The meaning of nilpotent functions.

Let $\boldsymbol{z}$ be a set of points in $\mathbb{P}^1_z$. Call a function f in a neighborhood of $z_0 \in U_{\boldsymbol{z}}$ *extensible* if it analytically continues along every path (not necessarily uniquely) from z_0 in $U_{\boldsymbol{z}}$. Should $f(z)$ be a branch of log on $U_{0,1}$, then f is extensible everywhere in $U_{0,1}$. Let α be a fractional transformation taking $z', z'' \in \boldsymbol{z}$ to $\{0,1\}$, so $f\circ\alpha(z)$ is extensible on $U_{z',z''}$. Abelian functions on $U_{\boldsymbol{z}}$ whose group have exponent n are rational functions in the likes of $e^{f\circ\alpha(z)/n}$.

Elements of $G_{\mathbb{Q}}$ act on roots of one. So, to every $\sigma \in G_{\mathbb{Q}}$ we associate a supernatural integer $n_\sigma \in \hat{\mathbb{N}}$. [**Iha86**] gives σ a deeper function recognition than the simple tag n_σ. That uses how σ acts on the pro-ℓ completion π of $\pi_1(U_{0,1,\infty})$. This attached a power series in two explicit generators of $\pi_1(U_{0,1,\infty})$ to σ. We explain this; it ties many topics together. Modular Towers has a different paradigm, yet it benefits from it. [**Fri77**] exploited n_σ by applying it where the branch set $\boldsymbol{z}$ has definition field $\mathbb{Q}$ though the points in $\boldsymbol{z}$ may not be in $\mathbb{Q}$. The *Branch Cycle Lemma* formula relates the cyclotomic behavior of the set $\boldsymbol{z}$ to the conjugacy classes $\mathbf{C}$ attached to a cover of $U_{\boldsymbol{z}}$ (as in (2.1)). A special case of this is the behavior of $\boldsymbol{z}$ under complex conjugation. It is a real set if complex conjugation fixes it. The λ-line is sets of four ordered points on $\mathbb{P}^1_z$ modulo the action of $\mathrm{PGL}_2(\mathbb{C})$. Ihara's real sets are those points $\boldsymbol{z}$ with all points in the set real, $r = 4$. Then, $\mathrm{PGL}_2(\mathbb{R})$ equivalence classes give the real points on the λ-line. Real sets in [SW] and [BF] (§3.1) may consist of complex conjugate pairs of points, and other configurations (as in determining all real points on Hurwitz spaces in [**DF90**]). When $r = 4$, these papers use the j-line as their base moduli space. [**IM95**] started bringing these viewpoints together and Part I papers of this volume exploit their joining.

In Ihara's approach, paths in the fundamental group get names by what they do to algebraic functions. So, the approach requires *well-known functions* with a calculable $G_{\mathbb{Q}}$ action. Nilpotent covers of $U_{\boldsymbol{z}}$ (covers with nilpotent Galois group) have such functions. They come from polylogarithms in the way abelian functions

on $U_{\boldsymbol{z}}$ come from logarithms. Each is a function extensible to all $U_{\boldsymbol{z}}$. Polylogarithms are complicated, yet we see how it works in §2.4 ([NW] from §3.1).

On $U_{0,1,\infty} = P^1_z \setminus \{0,1,\infty\}$ regard z as the variable λ. Deligne treated this as the line uniformized by the famous function $\lambda(\tau)$ of complex variables. As a moduli space, $U_{0,1,\infty}$ is then equivalence classes of elliptic curves with an order on their 2-division points. By contrast, Modular Towers ([BF] from §3.1) regards $U_{0,1,\infty}$ as the moduli for 4-branch point covers with ordered branch points. What Ihara's program has done with the open λ-line is our best model for expectations.

2.4. Algebraic paths, tangential base points and Lie groups. We now give aids to some Part I papers. Deligne introduced *tangential base points*. Traditional paths permute algebraic functions through analytic continuation. We describe a simple case of this on the path $\lambda_{\overline{0\,1}}$ and its conjugates under the action of $G_{\mathbb{Q}}$. More precisely, we give the effect of the base point $\overline{0\,1}$ on the λ-line in the direction from 0 to 1 and the path $\lambda_{\overline{0\,1}}$ attached to it ([**De89**] or [**Iha91**]).

2.4.1. *Comparing algebraic functions over branch points.* Let C_0^+ be a small circle tangent to 0 centered on the positive real line. Take f in $\bar{\mathbb{Q}}((z^{1/e}))$, with $e \geq 1$ any integer, whose restriction to the positive real axis in C_0^+ converges by regarding $z^{1/e}$ as positive. Assigning a positive value to $z^{1/e}$ on the positive real axis between 0 and 1 gives the notation $\overline{0\,1}$. Now add that f is algebraic (significantly given by its Puiseux expansion in $z^{1/e}$), and extensible in $U_{0,1,\infty}$ (§2.3). Denote all such functions by $\mathcal{F}_0$.

By analytic continuation along $\lambda_{\overline{0\,1}}$ we mean this. Restrict $g \in \mathcal{F}_0$ to the right of 0 (in C_0^+), then analytically continue along the z-axis to a similar circle C_1^- tangent on the left of 1.

Similarly, we denote extensible algebraic functions in $\cup_{e=1}^{\infty}\bar{\mathbb{Q}}(((1-z)^{1/e}))$, by $\mathcal{F}_1$. Continue $f \in \mathcal{F}_1$ to the left of 1 along the real axis by having it take the positive eth root of $1-z$. Apply $\sigma \in G_{\mathbb{Q}}$ to the coefficients, fixing the functions $(1-z)^{1/e}$. Then, the symbol $\sigma \circ \lambda_{\overline{0\,1}} \circ \sigma^{-1}$ gives a map on functions $\mathcal{F}_1 \to \mathcal{F}_0$ by this formula:

$$g \in \mathcal{F}_1 \mapsto (g)\sigma \circ \lambda_{\overline{0\,1}}^{-1} \circ \sigma^{-1}.$$

(We've taken all actions on the right.) The product of the two,

$$\mathfrak{f}_{\sigma}^{\overline{1\,0}} = \lambda_{\overline{0\,1}} \circ \sigma \circ (\lambda_{\overline{0\,1}})^{-1} \circ \sigma^{-1},$$

is not a topological path. We see it is a profinite (closed) path giving an automorphism of $\mathcal{F}_0$ that acts trivially on $\bar{\mathbb{Q}}$. It is in the algebraic fundamental group $\pi_1(U_{0,1,\infty}, \overline{0\,1})$.

Fields of Puiseux expansions around 0, 1 and ∞, $\mathcal{F}_0$, $\mathcal{F}_1$ and $\mathcal{F}_\infty$ give three copies of the meromorphic algebraic functions M extensible on $U_{0,1,\infty}$. These three copies of M are all isomorphic, by analytic continuations around paths.

2.4.2. *Encoding $G_{\mathbb{Q}}$, some relations and a connection to the j-line.* The goal of [**Iha86**], [**De89**] and, in increasingly more general situations, of §3.1 [YI], [RS] and [NW] is to compare the action of $G_{\mathbb{Q}}$ on these three copies of M, by acting on their puiseux expansions using explicit paths that identify of these copies. At least for those functions defining nilpotent extensions, we can hope to understand this action. That is the gist of Ihara's program: Explicitly find the action of $G_{\mathbb{Q}}$ on the nilpotent quotient of significant fundamental groups.

Compute that each $\mathfrak{f}_{\sigma}^{\overline{i\,i'}}$, $i, i' \in \{0,1,\infty\}$ fixes $z^{1/e}$ and $(1-z)^{1/e}$. So it fixes extensible abelian functions on $U_{0,1,\infty}$. Conclude: $\mathfrak{f}_{\sigma}^{\overline{i\,i'}}$ is in the commutator group

of $\pi_1(U_{0,1,\infty})$. Attaching to $\sigma \in G_{\mathbb{Q}}$ the pair $(n_\sigma, \mathfrak{f}_\sigma^{\overline{01}})$ gives an encoding of $G_{\mathbb{Q}}$ in paths. The trick is to regard $\mathfrak{f}_\sigma^{\overline{01}}$ as a word $\mathfrak{f}_\sigma(x,y)$ in the generators x and y. The automorphism $\alpha : \lambda \mapsto 1-\lambda$ (with which any $\sigma \in G_{\mathbb{Q}}$ commutes) of the λ-line permutes the profinite generators x and y. It also takes the path $\lambda_{\overline{01}}$ to its inverse $\lambda_{\overline{01}}^{-1}$. Conjugate $\lambda_{\overline{01}}\lambda_{\overline{01}}^{-1} = 1$ (in its effect by analytic continuation) by $\sigma \in G_{\mathbb{Q}}$. Combine this with the statement on α to conclude $f_\sigma(x,y)f_\sigma(y,x) = 1$.

Use $\alpha_{0,1,\infty} : \lambda \mapsto 1/(1-\lambda)$ to write another path is trivial on extensible functions on $U_{0,1,\infty}$. Let r be the upper half (clockwise) circle of the path for x and let λ_0 be r times $\lambda_{\overline{01}}$. That is a path from the real axis on the left of 0 to the real axis on the left of 1. The transform of λ_0 by $\alpha_{0,1,\infty}$ gives λ_1 from the end point of λ_0 to the left of ∞. Transform λ_1 by $\alpha_{0,1,\infty}$ to give λ_∞. As previously, on extensible functions we have the relation $\lambda_0\lambda_1\lambda_\infty = 1$. Write $z = (xy)^{-1}$. Conjugate everything by σ and combine to find a relation in $f_\sigma(x,y)$ having the form $f_\sigma(z,x)z^{u_\sigma}f_\sigma(y,z)y^{u_\sigma}f_\sigma(x,y)x^{u_\sigma} = 1$ with $u_\sigma = \frac{n_\sigma - 1}{2}$. We call this Ihara's 3-cycle relation (there is also a 5-cycle relation in [**Iha91**, p. 106]). We have given this detail for two reasons.

(2.5a) These three types of relations define the group GT (§2.3) of pairs $(n, f(x,y)) \in \hat{\mathbb{Z}} \times (\pi_1, \pi_1)$.

(2.5b) In Modular Towers (§3.1 [BF]), the image of the path $\lambda_0\lambda_1\lambda_\infty$ in the j-line is called the *shift* for its effect on reduced Nielsen classes.

As the moduli space of 4 branch point covers, the moduli fundamental group of the j-line has two generators. This shift (of order 2) and the circle around $j = \infty$ that gives the monodromy around cusps of covers of the j-line.

2.4.3. *Power series expressions for the effect of $\sigma \in G_{\mathbb{Q}}$.* For any rational point $z' \in (0,1)$, §3.1, [NW] checks how $\sigma \in G_{\mathbb{Q}}$ acts on the analogous path $\mathfrak{f}_\sigma^{z'}$ extending from $\overline{1\,0}$ along the positive real axis to z'. This is great practice. View x and y as generators of the pro-free pro-p group $\pi(p)$. Denote the commutator subgroup of $\pi(p) = \pi$ by $\pi(p)'$ and $(\pi(p)')'$ by $\pi(p)''$. We take $\mathfrak{f}_\sigma^{z'}$ to be a profinite word in paths x (resp. y) counterclockwise from $\overline{1\,0}$ going around 0 (resp. 1).

The 1-cocycle $\rho_{z'}(\sigma)$ for the action of $G_{\mathbb{Q}}$ appears in this formula:

$$\sigma((z')^{1/e}) = \zeta_e^{\rho_{z'}(\sigma)}(z')^{1/e}$$

for $e \geq 1$. There is a similar 1-cocycle $\rho_{1-z'}(\sigma)$ by $\sigma((1-z')^{1/e}) = \zeta_e^{\rho_{1-z'}(\sigma)}(1-z')^{1/e}$. We compute (as in §2.4.2) that $\mathfrak{f}_\sigma^{z'}$ is $x^{-\rho_{z'}(\sigma)}y^{-\rho_{1-z'}(\sigma)}$ modulo the commutator group $\pi' = (\pi,\pi)$. So, $\mathfrak{h}_\sigma^{z'} = y^{\rho_{1-z'}(\sigma)}x^{\rho_{z'}(\sigma)}\mathfrak{f}_\sigma^{z'}$ is in π'. [NW] investigates this modulo π''.

Denote the completed group algebra of $\pi(p)$ over $\mathbb{Z}_p$ by $\mathbb{Z}_p[\![\pi(p)]\!]$. To see that $\pi(p)'/\pi(p)''$ is a 1-dimensional $\mathbb{Z}_p[\![\pi(p)/\pi(p)']\!]$ module do an induction on the length of expressions $h(x,y)h^{-1}$ (with $(x,y) = xyx^{-1}y^{-1}$) with h running over π/π'. Conclude that (x,y) generates.

Identify $\mathbb{Z}_p[\![\pi(p)/\pi(p)']\!]$ with $\mathbb{Z}_p\langle\langle u,v\rangle\rangle$, the ring of noncommutative power series in two variables $u = x-1$ and $v = y-1$. (By contrast, write the quotient ring in which u and v commute is $\mathbb{Z}_p[\![u,v]\!]$.) Any p-group P defines a Lie algebra. This is from the graded module on the lower central series using the $(\ ,\ )$ product, from [**Se64**, Chap. II]. Further, the corresponding Lie algebra $\mathcal{L}$ generates a *universal enveloping algebra* of formal finite tensors, modulo the Lie relations $[u,v] - u\otimes v + v\otimes u$ for $u, v \in \mathcal{L}$. The Campbell-Hausdorff formula identifies the

Lie-like elements in the case when the (pro)-p group is (pro)-free. As we are in a completed group ring, likewise complete the formal sums to power series.

Conjugating $M = \pi(p)'/\pi(p)''$ by $\pi(p)/\pi(p)'$ extends to make M a rank one $\mathbb{Z}_p[\![\pi(p)/\pi(p)']\!]$ module. Ihara uses his relations to compute how the automorphism $x \mapsto x$ and $y \mapsto fyf^{-1}$ with $f \in \pi(p)'/\pi(p)''$ (so it acts trivially on $\pi(p)/\pi(p)'$) acts in this module setup. Decompose $f \in (\pi(p), \pi(p))$ uniquely as $1 + \partial_x(f)u + \partial_y(f)v$, so defining the free differentials $\partial_x(f), \partial_y(f) \in \mathbb{Z}_p\langle\langle u, v\rangle\rangle$.

Drop the partial $\partial_x(f)u$ related to x and consider the image $F(u, v)$ of $1+\partial_y(f)v$ in $\mathbb{Z}_p[\![u, v]\!]$; an abelianization of $1 + \partial_y(f)v$. Then, multiplication by $F(u, v)$ gives the desired effect on $\pi(p)'/\pi(p)''$. Generalizing this is the goal of [NW].

3. The papers in this volume

3.1. Part I: $G_{\mathbb{Q}}$ action on moduli spaces of covers.

PD: Pierre Debes: Descent Theory for Algebraic Covers

JE: Jordan Ellenberg: Galois invariants of dessins d'enfants

HN: Hiroaki Nakamura: Limits of Galois representations in fundamental groups along maximal degeneration of marked curves, II

BF: Paul Bailey and Michael Fried: Hurwitz monodromy, spin separation and higher levels of a Modular Tower

SW: Stefan Wewers: Field of moduli and field of definition of Galois covers

YI: Yasutaka Ihara: Galois actions on the pro-p fundamental group

RS: Romyar Sharifi: Relationships between conjectures on the structure of pro-p Galois groups unramified outside p

NW: Hiroaki Nakamura and Zdzisław Wojtkowiak: On explicit formulae for l-adic polylogarithms

We can organize many from these papers by asking what covers and applications they consider. Definitions of italicized items are in the referenced papers.

3.1.1. [BF], [PD] *and* [SW]*: Cusps and modular curve-like moduli.* Let p be an odd prime and $k \geq 0$. The Mazur-Merel Theorem is well-known. It says, for any number field K, there is an explicit bound C_K on p^{k+1} so that for $p^{k+1} > C_K$, there are no non-cusp rational points on the modular curve $X_1(p^{k+1})$. This has a Modular Tower [BF] interpretation: There are but finitely many four branch point, dihedral group involution realizations [**Fri95b**].

We show how Modular Towers formulates a generalization. Let G be any finite group acting irreducibly on a (possibly trivial) lattice L. Take conjugacy classes $\mathbf{C}$ in G having generators $g_1, \dots, g_r$ satisfying (2.1). Let $P_{\mathbf{C}}$ be those primes dividing orders of elements in $\mathbf{C}$. For any $p \notin P_{\mathbf{C}}$ (it may divide $|G|$) for which $L/pL \times^s G$ is *p-perfect*, consider the set U_p of characteristic p-Frattini covers of $L/pL \times^s G$. As we run over such p, the Merel-Mazur analog would be that only be finitely many such U_ps having a $\mathbf{C}$ realization. Falting's Theorem says for any one prime that $X_1(p^{k+1})$ has no rational points for k large. The analog for Modular Towers is the Main Conjecture for Modular Towers. It is still unknown even if $\mathbf{C}$ has just four conjugacy classes. We now allude to a fancy part of [BF]. For a given prime p the result would follow if G_F ($[F : \mathbb{Q}] < \infty$) has no fixed points on the Frattini flags of an attached *nilpotent version of a Tate Grassmanian.*

Modular Towers with $r = 4$ conjugacy classes of G have levels that are upper half plane quotients and covers of the j-line. Their description as moduli spaces

means that one does readily give the sequence of finite index subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ defining them. A Riemann-Hurwitz formula, from actions of a mapping class group on reduced Nielsen classes, gives a formula for the genus of their components. This uses data from modular representation theory (for the prime p in their definition) of the kth level characteristic group defining the tower level. We would complete the Main Conjecture for a particular tower by showing high level tower components have genus exceeding one. We don't know this generally, though our present cases show how the Frattini covering property interprets where cusps fall into components. [**Fri95a**] introduced Modular Towers to test for the GT relations at level of covers. Ihara's use in (2.5), at the Lie group level, gives information only on projective systems of covers.

Focusing on cusps in the Modular Towers that have p-adic and real definition fields gives challenging problems at all levels of many Modular Towers. These generalize Serre's Stiefel-Whitney class approach to spin cover realizations. Work in [PD] and [SW] motivates cases that will help analyze general tower levels. [SW] uses a version of the Ihara-Matsumoto action on a tangential base point. The specific Deligne Tangential base points of §2.4 are not suitable here. One must refine the approach of [**IM95**] for formulas proper for some details of the group G that enters in the Modular Tower. Specifically, [BF] applies this program on a Modular Tower where the group G is A_5. There have been several stages to detecting the moduli field along an algebraic subset of a Hurwitz space that may not be a fine moduli space. Following on [**Fri77**, §4] based on an early version of gerbes reported by Grothendieck, Debes and his cowriters [PD] produced an explicit obstruction to moduli field being a field of definition.

[SW] computes this Débes obstruction in cases. One step is to show the vanishing of a residue obstruction of Serre. This is at level 0 of an A_5 Modular Tower. The second step applies a new version of [**IM95**] using tangential base points attached to sequences of A_5 Modular Tower cusps. One projective system of tangential base points attaches to cusps for *H-M* representatives, which we understand using Harbater patching. The other associates to *near H-M* reps. Between them we are computing a Débes obstruction. [BF] shows how this generalizes part of Serre's Open Image Theorem from modular curves to Modular Towers.

3.1.2. [BF] *and* [JE]*: connected component applications.* Modular Towers have reduced Hurwitz spaces as their levels. Recall *Nielsen classes*: r tuples in a group G defined by the conditions of (2.1). A description of Modular Towers levels comes from computing an action of the Hurwitz monodromy group of degree r on Nielsen classes. [BF] denotes the standard generators of the braid group by $Q_1, \dots, Q_{r-1}$. To get the Hurwitz monodromy group add one relation to the usual braid relations:

$$Q_1Q_2\cdots Q_{r-1}Q_{r-1}\cdots Q_1. \tag{3.1}$$

When $r = 4$, reduced Hurwitz spaces cover the j-line have branch cycle description given by adding an extra relation $Q_1 = Q_3$. The image of $Q_1Q_2Q_3$, the shift (order 2) and the image of Q_2, called γ_∞, give generators of the resulting quotient group. Use $Q_1Q_1 = \gamma_0$, the shift, denoted γ_1, and γ_∞ with (3.1). This gives the product one relation $\gamma_0\gamma_1\gamma_\infty = 1$ and it shows γ_0 and γ_1 have orders 3 and 2. So $\langle \gamma_0, \gamma_1\rangle$ is naturally isomorphic to $\mathrm{PSL}_2(\mathbb{Z})$.

[BF] (and [**Fri95a**, Part III]) identifies orbits of these elements on Nielsen classes in many examples, using variants on [**Ser90**]. The *shift-incidence matrix* in

[BF] (works for all r) composed from the action of the shift on γ_∞ orbits in reduced Nielsen classes is an efficient tool to compute Hurwitz space components.

By contrast much attention on components has occurred for *dessins d'enfants*. This name applies to any cover of the sphere branched at 0, 1 and ∞, not necessarily with any given moduli properties. Of course, it includes pullbacks to the λ-line of modular curves or levels of a Modular Tower for families of four branch point covers. Belyi's theorem showing that all curves over $\bar{\mathbb{Q}}$ have such maps to the λ-line generated great interest. Now, however, it seems more a topic on covers with numerically interesting branch cycle patterns. [JE] gives suggestions for distinguishing such covers (up to the usual equivalence) with specified branch cycles. This makes use of the Galois group S_3 of the λ-line to the j-line to transport a dessins d'enfants by S_3. He gives examples where this *cartographic* group distinguishes dessins d'enfants in the same Nielsen class. The first examples we know of this type are in [**BF82**]. To date the [BF] and [JE] techniques don't have a generalization that specializes to both. [JE] detects inequivalent covers in the Nielsen class using $G_{\mathbb{Q}}$ invariants. In several cases, he proves these are actually GT-invariants, and so they are $G_{\mathbb{Q}}$ invariants (from the embedding of the latter in the former; for [BF] invariants in [**Fri95a**, Part III]).

3.1.3. *Ihara-Nakamura-Sharifi-Woitkoviak applications.* §2.4.3 discussed [NW]. Ihara used his version of the power series at the end of the section to affect complex multiplications on Fermat curves. Here is an elementary point. He is acting by $G_{\mathbb{Q}}$ on the pro-p second commutator of the λ-line fundamental group. The degree p^t Fermat curve is a cyclic cover (with group $\mathbb{Z}/p^t$) of the λ-line. So, a quotient by that second commutator would map to a group U_p that surjects to $\mathbb{Z}/p^t$ and has as its tail the Tate module of the degree n Fermat curve. We can look upon [NW] as developing similar formulas for curves they call *Heisenberg covers* of the λ-line.

Let $K((t))$ be Laurent series in a variable t over a field K. A K tangential base point on a moduli space $\mathcal{M}$ is a map $\mathrm{Spec}(K((t))) \to \mathcal{M}$. Such a point probes objects in $\mathcal{M}$ as t goes to 0. An excellent tangential base locates exceptional degeneration of moduli objects. Such degeneration helps us study how the group G_K acts on projective systems of points over the tangential base point.

Denote the moduli of genus g curves with n punctures by $\mathcal{M}_{g,n}$. Dehn twists generate the moduli fundamental group of $\mathcal{M}_{g,n}$. [**NS00**] finds a GT action on these Dehn twists. [HN] then creates a special tangential base point, where $G_{\mathbb{Q}}$ on the fibers over it in the Teichmüller tower. As this action is compatible with how $G_{\mathbb{Q}}$ embeds in GT, this is an analog of [**IM95**] on a comparable Hurwitz space situation. The result returns to using the Ihara-Drinfeld relations on $U_{0,1,\infty}$ (§2.4.2). Chains of copies of such $U_{0,1,\infty}$ define the [HN] tangential base point. [HN] stitches these together according to the Harbater-Stevenson rubric (allowing several variables of patching at a time). So the degenerate object placed over the special point of $\mathrm{Spec}(K((t)))$ deforms into general points in $\mathcal{M}_{g,n}$. Two examples work especially well, $\mathcal{M}_{g,1}$ and $\mathcal{M}_{g,2}$, by comparing this choice of tangential base point with that from previous works. Another viewpoint on GT appears in [**HaS00**], referring to it as the profinite group of outer automorphisms of the fundamental group of $\mathcal{M}_{0,n}$, $n \geq 5$, commuting with the action of S_n (on the branch points) and raising inertia generators to powers. I'm not yet competent on its relation to [**IM95**].

[YI] contains a welcome survey of many topics joining the special p-adic function theory from the topics in §2.4.3. This program appears in print over several hard

papers. Particularly, this includes results of [**HM01**], the weights of the Tate twists and the appearance of Soulé characters for the action of $G_{\mathbb{Q}}$ on the weight filtration of the pro-p completion of $\pi_1(U_{0,1,\infty})$. [RS] continues [YI] with, depending on a conjecture of Greenberg and the proof of [**HM01**], up-to-date information on how the pro-p extension of $\mathbb{Q}(\zeta_{p^\infty})$ unramified outside p acts on that graded filtration.

3.2. Part II: Curve covers in positive characteristic.

AT: Akio Tamagawa: Fundamental Groups and Geometry of Curves in Positive Characteristic

MR: Michel Raynaud: Sur le groupe fondamental d'une courbe complète en caractéristique $p > 0$

FM: Michael Fried and Ariane Mezard: Configuration spaces for wildly ramified covers

MG: Marco Garuti: Linear systems attached to cyclic inertia

GS: Bob Guralnick and Kate Stevenson: Prescribing Ramification

3.2.1. [AT] *and* [MR]*: anabelian expectations.* §2.1.1 discusses Grothendieck's anabelian problem. Tamagawa proved a version for the arithmetic fundamental group of affine curves over finite fields [**Ta97**]. There is, however, no reason to doubt it for complete curves. These authors bet it holds with the geometric fundamental group replacing the arithmetic fundamental group. [AT] includes some neat conjectures.

Let X be an n punctured curve of genus g, with $\bar{X}$ its the projective nonsingular completion. [**Gr71**] says the maximal prime to p quotient of the geometric fundamental group tells nothing more than what we already knew. The tame fundamental group refers to the projective limit of groups from covers of $\bar{X}$ that tamely ramify over $\bar{X} \setminus X$. [AT] explores two possibilities. First: $\pi_1(\bar{X})$ might determine $\bar{X}$ up to conjugacy (by the Frobenius). This case stands out since $\pi_1(\bar{X})$ is finitely generated. (This comes from it being a quotient of the fundamental group of its lift $\bar{X}^*$ to characteristic 0.) The finite quotients of a finitely generated profinite group determine the group. This follows from a statement about any finitely generated profinite group P: A surjective homomorphism $\psi : P \to P$ is an isomorphism. Morally: It is true for finite groups, so it should be true for profinite groups. The standard proof, however, requires something weaker than, but akin to, the finite generation property [**FJ86**, Prop. 15.3]. A not necessarily finitely generated group with this property is *Hopfian*. In 0 characteristic, fundamental groups of algebraic varieties are (topologically) finitely generated (because they have the structure of a finite CW complex).

Also significant is that profinite fundamental groups of projective curves are p-projective. So, if G is a quotient of $\pi_1(\bar{X})$, then so is any p-Frattini cover of G (see §3.3.1). Based on [AT], the author later shows (generalizing work of Pop-Saidi and [MR]) there are only finitely many complete curves $\bar{X}$ with the same fundamental group quotients as a given curve. Still, we don't know if this set of curves is precisely a Frobenius orbit of one curve.

Second: [AT] explores that groups of X covers that extend to tamely ramified $\bar{X}$ covers also might determine X up to conjugacy. Again, since the tame fundamental group is finitely generated, group quotients of $\pi_1(X)$ from tame covers determine its maximal (profinite) tame quotient. [AT] reviews the known case, $g = 0$, and

then shows more generally for n punctured X of genus g, that one may recover n and g from the tame fundamental group.

Now suppose X has definition field $\bar{\mathbb{F}}_p$, $\bar{X} \setminus X$ has cardinality at least 1 and the genus of $\bar{X}$ is at least 1. Then, [AT] has a general conjecture that in this case implies $\pi_1(X)$ is Hopfian. Know any good (not finitely generated) Hopfian groups? For this one, keep your eye on the projectivity of $\pi_1(X)$.

[MR] also concentrates on anabelian expectations for a curve X over $\bar{\mathbb{F}}_p$. (Assume in the previous notation $\bar{X} = X$.) Riemann invented the classical θ function to put coordinates on constructing abelian covers of curves. The Schottky approach to differentiating Jacobians from all abelian varieties used small nonabelian covers of curves: dihedral group covers. That is, take a degree 2 unramified cover $\psi : Y \to X$ and consider cyclic unramified covers $Z \to Y$ of degree n for which $Z \to X$ is a dihedral group. The only other possibility for the Galois group is that it is abelian. The involution τ for the cover ψ decomposes the Jacobian $\mathrm{Pic}^{(0)}(Y)$ of Y up to isogeny as $P \times \mathrm{Pic}^{(0)}(X)$, with P being the piece on which τ acts nontrivially. So, the dihedral assumption means that Z is pullback from a cyclic isogeny $P' \to P$ of degree n. This is compatible with §2.2 to show how significant even dihedral groups can be.

The Main Result of [MR] is that the fundamental group of X does determine it among finitely many curves (not yet up to Frobenius conjugacy) when X has genus 2. This uses just meta-abelian groups of form $N \times^s M$: M is an elementary abelian prime to p group; and N is an elementary abelian p group. In the diagram above M is the Galois group of a cover $\psi' : Y' \to X$ and N is the Galois group of the maximal exponent p unramified cover $Z' \to Y'$. Even if you start with an ordinary curve (p rank of its Jacobian is half the genus), a cover of degree prime to p may not be ordinary. (Note: An unramified cover $Y' \to X$ with X ordinary, and with Galois closure a p group, *will* have Y' ordinary.) The key tool is a θ divisor defined by the Frobenius map on X. Detailed analysis extracts from this θ information on the size of N as we vary over possibilities for ψ'.

3.2.2. [FM], [MG] *and* [GS]*: constructive results using configuration spaces.* Take k an algebraically closed field of characteristic p. Recall what comes from [**Gr71**] on tame ramification. Suppose in a tame family of curve covers with exactly r branch points, the branch points don't move. Then the family is essentially trivial. Topics in [FM] include *ramification data* $\mathcal{R}$ attached to a local (perhaps not Galois) field extension, *regular ramification data* attached to the local field extension, the *$\mathcal{R}$-configuration space* and families of $\cup_{ij}\mathcal{R}_{ij}$ covers. Assume given a family of (not necessary Galois) covers of the projective line. [FM] produces a versal deformation space $\mathcal{P}(\mathcal{R})$ for local extensions $k((y))/k((x))$ having given ramification type $\mathcal{R}$. Then $\mathcal{P}(\mathcal{R})$ is an explicit open subspace of some affine space. Each extension $k((y))/k((x))$ of type $\mathcal{R}$ corresponds to finitely many (rarely one) points in $\mathcal{P}(\mathcal{R})$.

Assume a given family's members have a fixed number, r, of branch points and its ramified points fall in a fixed set of ramification data: $\cup_{ij}\mathcal{R}_{ij}$. Locally in the finite topology the $\cup_{ij}\mathcal{R}_{ij}$ configuration space $\mathcal{P}(\cup_{ij}\mathcal{R}_{ij})$ is a natural target for the parameter space of any family having type $\cup_{ij}\mathcal{R}_{ij}$. Further, any family of this type is the pullback of this configuration map from a family over a finite cover of the parameter space image in the configuration space. This generalizes the tame version of [**Gr71**]. A special case is an iso-triviality result: If a family has a constant map to the configuration space, after finite pullback it is a trivial

family. This uses a generalization of a Garuti theorem. There is a lift of any (wildly ramified) cover to characteristic 0 so the special fiber has only cusps as singularities, and its normalization is the covering curve we started with.

[MG] also constructs a type of configuration space. For a function field K of a variety of characteristic $p > 0$ over k, Artin-Schreier-Witt theory describes all separable cyclic extension of degree p^n of K. Such an extension is a generically étale cover of X with function field K. [MG] describes geometrically what happens at isolated points x_0 at which the cover is not étale. The goal is to extend the map given by the Witt vectors in a neighborhood of such a point x_0, to recover some information about the ramification at x_0. The paper produces a configuration space for such covers. The main result is a precise version of the following rough statement. For every positive integer n, there is a smooth projective rational variety $\bar{\mathbb{W}}_n$ over $\mathbb{F}_p$, equipped with a tautological line bundle $\mathcal{O}_{\bar{\mathbb{W}}_n}(1)$. The bundle has a section whose zero locus B_n (the complement of $\mathbb{W}_n$) has normal crossings.

Suppose a ramified a curve cover $\psi : Y \to X$ has a totally ramified place $x_0 \in X$ and the following hold. The cover ψ is cyclic of degree p^n, and a Witt vector of rational functions with poles of order prime to p on X defines the function field extension $k(Y)/k(X)$. Then, the Witt vector of rational functions gives a map of X into $\bar{\mathbb{W}}_n$ with Y the normalization of the pullback. Further, we have good control of the conductor of x_0 from our knowledge of the divisor B_n. The construction is local in x_0. So, there are variants for Galois covers $Y \to X$ with a place of Y that has a cyclic p^n inertia group.

The topic of [GS] is prescribing ramification groups of some covers of a projective curve X. [**Ha94**] determines exactly which finite groups occur as Galois groups for some cover of X with a given nonempty branch locus Δ. For a given such group, it actually occurs so that, excluding at most one point in Δ, the ramification is tame. Suppose G has any particular set of cyclic-by-p subgroups H_i, $i = 1, .., t$. The main result of [GS] is that there is a cover with group G so that the H_i s occur among the inertia groups of the cover. [GS] applies this to produce specific arithmetic/geometric monodromy group pairs. That is, suppose G is a normal subgroup of a group A with A/G cyclic. [GS] shows under general circumstances there is a finite field $\mathbb{F}_q \leq k$ and a cover $Y' \to X'$ over $\mathbb{F}_q$ so the Galois closure group of the cover over $\mathbb{F}_q$ is A and over k it is G. Precise results along this line are important for finite field applications. For example, if G is the subgroup of A generated by the p-Sylows of A, [GS] shows it is possible to take $X = \mathbb{P}^1$ with ramification at only one point. They contrast this with a result of Fried giving realization of arbitrary arithmetic/monodromy pairs with $X = \mathbb{P}^1$ over *all* finite fields of characteristic suitably large (excluding any prime dividing $|G|$). At this date [GS] has no control over the degree of $\mathbb{F}_q$ over the prime field.

3.3. Part III: Special groups for covers of the punctured sphere.

RA: Ram Abhyankar: Desingularization and Modular Galois Theory

GFM: Dan Frohardt, Bob Guralnick and Kay Maagard: Genus 0 actions of groups of Lie rank 1

HV: Helmut Völklein: Galois realizations of profinite projective linear groups

3.3.1. [RA]*: Fundamental groups of normal crossing complements.* For algebraic surfaces in positive characteristic one method to investigate their singularities

is to project the surface to a plane. Then, study the locus above the branch locus of the projection. [RA] looks back at the story behind the Abhyankar Conjecture and considers the most natural normal crossings version of it. What are the groups for Galois extensions of the local field $\bar{\mathbb{F}}_p((X_1,\dots,X_d))$ (formal Laurent series) which ramify only over the primes $X_1,\dots,X_d$ of $\bar{\mathbb{F}}_p[[X_1,\dots,X_d]]$? Similarly, what groups appear as Galois extensions of the field $\bar{\mathbb{F}}_p(X_1,\dots,X_d)$ of rational functions, which ramify only over primes $X_1,\dots,X_d$ of $\bar{\mathbb{F}}_p[X_1,\dots,X_d]$? These are questions about fundamental groups of complements, local and global, with normal crossings. Let G be a finite group, $p(G)$ be its minimal subgroup containing all p-Sylows of G. Call G a (p,t)-group if $G/p(G)$ is abelian with t generators.

For example, for Galois extensions, [RA] conjectures for $d>1$ in the local case that for $t>0$ all (p,t)-groups appear and for the global case the same holds even with $t=0$. Further, [RA] returns to refined versions of the Abhyankar Conjecture even for plane curves and their relation to the higher dimensional results.

We comment on an appendix by Harbater. This shows the conjectures above are not correct. The appendix reasons like this. The proof of Abhyankar's Conjecture for affine curves over an algebraically closed field [**Ha94**] uses that, given the prime to p group $G/p(G)$ in these situations there is a prime to p group H in G mapping surjectively to $G/p(G)$. Providing such a group under the hypotheses of the Abhyankar Conjecture was automatic using [**Gr71**]. This he calls a supplement to $p(G)$. [**Ha94**] notes one can pick a supplement to $p(G)$ that normalizes a p-Sylow of G (from the Schur-Zassenhaus Theorem). Even the local higher dimensional case would fail on group theoretic grounds, as this condition would require an abelian rank t supplement. The Appendix references examples and adjusts the conjectures of the first author's part. We quote a statement in the Appendix:

> Moreover, results of R. Guralnick (appendix to [**HaP00**]) essentially show that under some reasonable hypotheses, the three assertions [two made by Abhyankar and that amendment by Harbater] are equivalent if and only if the class of prime-to-p groups of unramified covers of X is closed under Frattini extensions.

Reminder: If $\pi_1(X)$ is projective, then for any group G that is a quotient of $\pi_1(X)$, any Frattini extension $\psi: H\to G$ will also be a quotient of $\pi_1(X)$. This is because the map of $\pi_1(X)$ to G will factor through ψ. Since ψ is a Frattini cover, the image of the factoring map must generate H. Also, an affine curve (though not a projective curve) in characteristic p does have a projective fundamental group. The fundamental group of a projective (complete) curve is p-projective, though not p'-projective for any prime p' different from p. Harbater did not reflect on the projectivity properties of the fundamental groups of higher dimensional varieties.

3.3.2. [GFM], *the classification of finite simple groups and the genus 0 problem.* Several pieces of the classification of finite simple groups (we call it just the classification) are valuable to algebraic and arithmetic geometry. This volume concentrates on problems having a phrasing as an algebraic relation in two variables with a select data variable. Formally, this gives a curve cover $\varphi: X\to\mathbb{P}^1_z$. Properties we expect of φ depend on the problem.

For someone who has never seen how this works, [**Fri99**] and references therein have many problems whose solutions came through the following rubric. (The references I make to group theory also appear there.) Suppose that if φ factors as

$\varphi_2 \circ \varphi_1 : X \to Y \to \mathbb{P}^1_z$, then the cover $\varphi_2 : Y \to \mathbb{P}^1_z$ inherits properties from φ that profitably revert the analysis from φ to φ_2. Then, we may reduce to considering covers that don't factor this way. These are *primitive* covers, so-named because their monodromy groups are primitive groups.

The genus 0 problem works this way (§2.1.2). In the best of cases such covers have the stronger property doubly transitivity property. One success of the classification is a fine description of all finite groups having doubly transitive permutation representations. The work for a general primitive representation is harder, though it breaks into five cases. Four obtain immediate benefit from the classification. The fifth (called the affine case) is where the monodromy group is a semidirect product of the form $V \times^s H$ with $V = \mathbb{F}_p^n$ for some n and H is a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ that acts irreducibly on V. This precise description of primitive group representations is the Aschbacher-O'Nan-Scott Theorem. A layman (to group theory) can often complete much of the analysis for covers from double transitivity (as in [**Fri99**, §9], based on the literature quoted there). Yet, it still requires a dedicated group theorist to deal with primitive, not doubly transitive, groups. For the genus 0 problem over $\mathbb{C}$, Guralnick-Neubauer treated the affine case early. They made a complete list of genus 0 primitive affine groups available. The affine case doesn't always fair so well, as we recall from the classification of exceptional polynomials with affine group [**Fri99**] .

[GMF] lay out their their reduction to the one case from primitive groups that needs serious extra analysis to decide what primitive groups actually occur. In this paper, among the possibilities for that case, they complete the description of those Chevalley groups having rank one. Perusal of the paper shows there are many genus 0 groups that are rank one. The value of this and related work is this. There are exceptions where special groups arise. Such exceptions allow an expert in the application to grab an appropriate group at random, a group that may be an anomaly for the problem. As in [**Fri99**, §5], such anomalies in characteristic 0 tend to blossom into general cases in positive characteristic (over a finite field), where most applications are these days. Not only does this work, it adds to the evidence for the genus 0 problem in positive characteristic (§2.1.2).

3.3.3. [HV] *and the BC Functor. Linear rigidity* arises for $\mathrm{GL}_n(\mathbb{C})$ as an aid to classifying flat bundles on the r punctured sphere [**Ka96**]. Its set up starts with an r-tuple of conjugacy classes $\mathbf{C}$ in $\mathrm{GL}_n(\mathbb{C})$. The desired conclusion that we call linear rigidity is that $\mathrm{GL}_n(\mathbb{C})$ is transitive on all r-tuples $g_1, \ldots, g_r$ from conjugacy classes that satisfy (2.1). This is like simple rigidity in the Inverse Galois problem. A translation between them replaces the group $\mathrm{GL}_n(\mathbb{C})$ by a finite group, and doesn't allow anything outside this group for the conjugations. (This simplest rigidity statement gives a regular realization of a group as a Galois group, as in [**Ser92**, Chap. 7].) A linear algebra version of the Riemann-Hurwitz formula gives a necessary condition for linear rigidity (due to Scott). The problem is to classify all linearly rigid tuples. Katz uses an operation, the BC functor, to produce from any rigid tuple, an r-tuple in a lower rank GL group. Reversing the process produces all rigid tuples. Further, the BC functor is useful even if the tuples are not rigid, though some close relative is valuable.

Dettweiler, Reitter and Völklein adopted Katz's definition, for Chevalley groups over finite fields. This generalized Katz's results. They made efficient use of a

natural pairing built into the Hurwitz monodromy group from (3.1) that is effective and replaces Katz's BC functor. For applications, Völklein identifies how the Belyi and Thompson tuples come from an r-tuple $\langle g_1, \dots, g_r \rangle$ in $\mathrm{GL}_1(\mathbb{F}_q)$ using his $\mathfrak{g}$-operation. He considers Nielsen classes for a particular Chevalley group as extending to Nielsen classes in GL_n. That the braid action commutes with the $\mathfrak{g}$-operation is a new feature. He analyzed the Symplectic group case this way to see that $\mathfrak{g}$ associates to linearly rigid Symplectic group Nielsen classes with Nielsen classes for the 2-dimensional rotation group. This is a conceptual explanation of the Thompson-Völklein papers referred to in §2.1.4.

[HV] shows the $\mathfrak{g}$ operator respects a natural Henselization attached to Chevellay groups. That is, one can work with the Witt vectors R_q (p-adic local ring) with residue class field $\mathbb{F}_q$. So, the $\mathfrak{g}$-operation takes the Henselization of one Chevalley group with corresponding conjugacy classes to the Henselization of another Chevalley group. The natural map $\psi_q : \mathrm{GL}_n(R_q) \to \mathrm{GL}_n(\mathbb{F}_q)$, for p odd, is a Frattini cover exactly when p does not divide n. We know ψ_q is only a small quotient of the universal p-Frattini cover of $\mathrm{GL}_n(\mathbb{F}_q)$. As, however, in [**Fri95a**, Part II], making comparison it with the full universal p-Frattini cover gives important applications.

3.4. Part IV: Fundamental groupoids and Tannakian categories.

SG: Shlomo Gelaki: Semisimple Triangular Hopf Algebras and Tannakian Categories

HP: Ho Hai Phung: On a Theorem of Deligne on Characterization of Tannakian Categories

SM: Shinichi Mochizuki: Hodge-Arakalov theory for elliptic curves I

3.4.1. [SG] *and* [HP] *and Tannakian interpretations of family structures.* Early papers of Grothendieck dealt with tensor products. For finite dimensional vector spaces V and W over a field K we have the standard isomorphism of $V^* \otimes W$ to $\mathrm{Hom}(V, W)$. Grothendieck's thesis considered Banach spaces V and those endomorphisms (trace class) in the range of $V^* \otimes V$. Later, his algebraic geometry results stated relative versions for a map $Y \to X$ with interpretations of the results along a fiber. This stemmed from recognizing fibers and fiber products of varieties as translating tensor products of algebras. Tannakian categories are tensor categories that resemble Kronecker's example, the category of representations of a group. We recognize two natural categories of modules for associative algebras stem from this example. Foremost is $\mathcal{M}_G$: Modules for the group ring $K[G]$ with K a field and G a group. Second: The universal enveloping algebra of any Lie algebra (as in §2.4.2).

Hopf algebras generalize both. If A is a Hopf algebra (over K) then it has a comultiplication $\Delta : A \to A \otimes A$ with which to define an action on the tensor $V \otimes W$ for any A modules V and W: For $a \in A$ on $v \otimes w$, with $\Delta(a) = \sum_i a_i \otimes b_i$ the action gives $\sum_i a_i(v) \otimes b_i(w)$. Tensor product has a natural switch map π: $\sum_i a_i \otimes b_i \mapsto \sum_i b_i \otimes a_i$. Comultiplication diagrams are multiplication diagrams with arrows reversed, Δ replacing multiplication and a co-unit replacing the map of K into the algebra. Further, to be a Hopf algebra it has an antihomomorphism (antipode) $\gamma : A \to A$ that connects multiplication and comultiplication. Thus, it allows an action on the dual space in the expected way. The two background examples are cocommutative: Comultiplication Δ' defined by $\Delta'(a) = pi \circ \Delta(a)$ is the same as Δ.

Let A^* be the units of A. [**Iha91**, p. 109] gives a less precise version of the following definitions. A *quasi-triangular* Hopf algebra —weakening of cocommutitivity —has an element $u \in (A \otimes A)^*$ where u conjugates Δ to Δ' (and some other natural compatibility relations [**Fu92**, p. 253]). It is triangular if $\pi(u) = u^{-1}$. Then, [**Iha91**, p. 109] discusses a quasi-triangular quasi-Hopf algebra as one in which the coassociativity is from conjugation by an element c (this time in $(A \otimes A \otimes A)^*$). That leads to a complicated diagram of isomorphisms between the various tensor products that associate from $V_1 \otimes V_2 \otimes V_3 \otimes V_4$ [**Iha91**, p. 110]. (The reference [**Dr90**] may be better than the preprint reference in Russian here.) This is where Drinfeld got his version of the 5-cycle Drinfeld-Ihara relation.

Our second, more pressing, motivation for Hopf algebras is from [**De89**]. Let k be an algebraically closed field of characteristic 0. Those mapping class groups of §2.2 will be fundamental groups attached to a representation category in the style of [**De89**]. The papers here will help those (like me) with mapping class investigations. The primal object is a fundamental groupoid attached to an abelian tensor category with an exact functor to quasicoherent sheaves over a scheme S. That is a Tannakian category. The essence is that various kinds of local systems give *realizations* (Deligne likes that name) of a classical fundamental group of a moduli space. Such realizations Deligne views as specializatoins of a motivic fundamental groupoid. So, while this has resemblance to studying a group ring or universal enveloping algebra, there is serious abstraction. [HP] gives an exposition of Deligne's Criterion that a tensor category be Tannakian. It includes valuable reinterpretations of Deligne's result. Example: How to embed a semisimple tensor category over $\mathbb{C}$, satisfying certain Deligne conditions, in the category of vector spaces over $\mathbb{C}$. [SG] uses this result to classify semisimple triangular Hopf algebras over k. They all come from a group algebra $k[G]$, of a unique (up to isomorphism) finite group, by a Drinfeld twist of its usual comultiplication [**Dr90**]. [**EG02**], however, drops the semisimple condition based on a strengthening of Deligne's result [**De01**]. [SG] mentions that with quasitriangular replacing triangular, we get more than twists of group algebras, though there is no classification yet.

3.4.2. [SM]: *An arithmetic fundamental groupoid.* [SM] attempts an arithmetic notion of analytic continuation. Given a smooth family of curves over a complex analytic base S, we can analyze the motion of the fibers of the family by differentiating differentials of the second kind (mod exact differentials). This way a motion in the base space induces a motion in the Hodge filtration of the fibers. The goal is to measure how differentiation moves the holomorphic differentials outside the holomorphic differentials. I imagine Riemann understood the Gauss-Manin connection and Kodaira-Spencer infinitesimal deformation this way. [SM] has as a goal to find an analog of the Kodaira-Spencer map when S is $\mathrm{Spec}(R)$ with R the ring of integers of a number field K.

The upper half plane $\mathbb{H}$ is contractible. Start with the universal elliptic curve $\mathcal{E} \to \mathbb{H}$ over $\mathbb{H}$. So, the Gauss-Manin connection parallel translates the line defining the Hodge filtration of the base fiber along $\mathbb{H}$. With no loss consider that as a map from $\mathbb{H} \to \mathbb{P}^1$ by removing the origin of the copy of H^1 and projectivizing. Since $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathbb{H}$, we induce a map $\psi : \mathrm{SL}_2(\mathbb{R}) \to \mathbb{P}^1$ from transport of the base point $z_0 \in \mathbb{H}$. [SM] calls this the group(-theoretic) Kodaira-Spencer map. From its differential you recover the Kodaira-Spencer map. Acting with $\mathrm{SL}_2(\mathbb{R})$ directly on the tangent space at the origin of the base elliptic curve induces the natural

action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{P}^1$. This shows the Kodaira-Spencer map is equivalent to the de Rham isomorphism. This little discussion near the end of the paper was helpful in grasping the author's vision.

The rest of [SM] constructs the Kodaira-Spencer morphism from the isomorphism between de Rham and étale cohomology (for all fibers of the family). So, an analogue of the Kodaira-Spencer morphism for an elliptic curve E over $\mathrm{Spec}(R)$ comes from constructing a comparison isomorphism between de Rham cohomology of E (a 2-dim vector space with a Hodge filtration, over K) and étale cohomology (a rank two module over the adeles, with an action of G_K). The group Kodaira-Spencer map suggests determining an isomorphism using spaces of functions on the two cohomology groups. Mumford's algebraic theta functions provides half of such an isomorphism. The universal cover of an elliptic curve (a quotient of the de Rham cohomology) supports the theta functions which evaluate to (discrete) functions on the set of torsion points (representing etale cohomology).

Each degree 0 divisor class $[D]$ on E has many representatives as a flat line bundle $\mathcal{L}$ on E and each flat bundle is given by $\varphi \in \mathrm{Hom}(\pi_1(E), \mathbb{C}^*)$. By removing the 0 section of $\mathcal{L}$ form †, a bundle over E with fiber $\mathbb{C}^*$ and constant transition functions. Among the flat bundle representatives for the divisor class, there is a unique one for which $\mathcal{L}^\dagger$ is a group extension of E with fiber $\mathbb{C}^*$. Such a group extension has no automorphisms trivial on the fiber over the origin. So, there is a universal extension of E (a group scheme characterized in characteristic 0 as the moduli space of line bundles on E with a connection: according to the author of [SM], see [**Me72**], [**Ka77**, App. C]). The universal cover of the universal extension is the full de Rham cohomology of E. [SM] generalizes Mumford's theta function theory from E to the *universal extension* of E.

This gives a nonlinear isomorphism of interesting, though far from algebraic, spaces of functions. The goal — heading toward an understanding of Szpiro's Conjecture — is ambitious. [SM] takes pains to explain difficult ideas, packing his analysis with beautiful moduli observations.

References

[Ab57] S. S. Abhyankar, *Coverings of algebraic curves*, AJM **79** (1955), 825-856.

[Be79] G.V. Belyi, *On Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), 267-276 (Russian) English Translation (1980) 247–256.

[BF82] R. Biggers and M. Fried, *Moduli spaces of covers and the Hurwitz monodromy group*, Crelles Journal **335** (1982), 87–121.

[D95] P. Dèbes, *Covers of $\mathbb{P}^1$ over the p-adics*, Proceedings of the Recent developments in the Inverse Galois Problem conference, vol. 186, 1995, AMS Cont. Math series, pp. 217–238.

[DF90] P. Dèbes and M. Fried, *Rigidity and real residue class fields*, Acta Arith. **56** (1990), 13–45.

[Des95] B. Deschamps, *Existence de points p-adiques sur un espace de Hurwitz*, Proceedings of the Recent developments in the Inverse Galois Problem conference, vol. 186, 1995, AMS Cont. Math series, pp. 239–248.

[DDes01] P. Dèbes et B. Deschamps, *Corps ψ-libres et théorie inverse de Galois infinie*, preprint as of October, 2001.

[De89] P. Deligne, *Le Groupe Fondamental de la Droite Proejctive Moins Trois Points* , in *Galois groups over $\mathbb{Q}$*, Mathematical Sciences REsearch Inst. Publications **16** (1989), edited by Y. Ihara, K. Ribet, J.P. Serre, 79–297.

[De90] P. Deligne, Categories Tannakiennes, In The Grothendick Festschrift, Vol. II, Prog. Math. **87** (1990), 111-195.

[De01] P. Deligne, *Catégories tensorielles*, www.math.ias.edu/~phares/deligne/deligne.html, February 2002.

[Dr90] V. Drinfeld, On Almost Cocommutative Hopf Algebras, *Leningrad Mathematics Journal* **1** (1990), 321-342.

[EG02] P. Etingof and S. Gelaki, *The classification of finite-dimensional triangular Hopf algebras over an algebraically closed field of characteristic* 0, math.QA/0202258, March 10, 2002.

[Fri77] M. Fried, *Fields of definition of function fields and Hurwitz families and groups as Galois groups*, Communications in Algebra **5** (1977), 17–82.

[Fri78] M. Fried, *Galois groups and Complex Multiplication*, Trans.A.M.S. **235** (1978) 141–162.

[FJ86] M. Fried and M. Jarden, *Field arithmetic*, Ergebnisse der Mathematik III, vol. 11, Springer Verlag, Heidelberg, 1986.

[Fri99] M. Fried, *Separated variables polynomials and moduli spaces*, Number Theory in Progress (Berlin-New York) (J. Urbanowicz K. Gyory, H. Iwaniec, ed.), Walter de Gruyter, Berlin-New York (Feb. 1999), Proceedings of the Schinzel Festschrift, Summer 1997, pp. 169–228, http://www.math.uci.edu/~mfried/#math.

[Fri94] M. Fried, *Review: Serre's* Topics in Galois Theory *– (1992) Bartlett and Jones Publishers*, BAMS **30 #1** (1994), 124–135.

[Fri95a] M. Fried, *Introduction to Modular Towers: Generalizing the relation between dihedral groups and modular curves*, Proceedings AMS-NSF Summer Conference, vol. 186, 1995, Cont. Math series, Recent Developments in the Inverse Galois Problem, pp. 111–171.

[Fri95b] M. Fried, *Enhanced review: Serre's* Topics in Galois Theory, Proceed. Recent developments in the Inverse Galois Problem conferenc, AMS Cont. Math. **186** (1995), 15–32.

[FV91] M. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli spaces* , Math. Annalen **290** (1991), 771–800.

[FV92] M. Fried and H. Völklein, *The embedding problem over an Hilbertian-PAC field*, Annals of Math **135** (1992), 469–481.

[Fu92] J. Fuchs, *Affine Lie algebras and quantum groups*, Cambridge Univ. Press, Monographs on Mathematics physics, 1992.

[Gr71] A. Grothendieck, Revêtements étales et groupe fonda mental (SGA I). Lecture notes in mathematics **224**, Springer-Verlag (1971).

[GN95] R. Guralnick and M. Neubauer, *Monodromy groups of branched covers; the generic case*, Proceedings AMS-NSF Summer Conference, vol. 186, 1995, Cont. Math series, Recent Developments in the Inverse Galois Problem, pp. 325–352.

[HM01] R. Hain and M. Matsumoto, *Weighted Completion of Galois Groups and Galois Actions on the Fundamental Group of* $\mathbb{P}^1 - \{0, 1, \infty\}$, preprint http://xxx.lanl.gov/abs/math.AG/0006158. An exposition titled *Tannakian Fundamental Groups Associated to Galois Groups* appears as http://xxx.lanl.gov/abs/math.AG/0010210.

[Ha94] D. Harbater, *Abhyankar's conjecture on Galois groups over curves*, Invent. Math. **117** (1994), 1–25.

[HaS00] D. Harbater and L. Schneps, *Fundamental groups of moduli and the Grothendieck-Teichmuller group*, TAMS **352** (2000), 3117–3148.

[HaP00] D. Harbater and M. van der Put, *Valued fields and covers in characteristic p*, preprint 2000, submitted for publication.

[Iha86] Y. Ihara, *Profinite braid groups*, Annals of Math. **123** (1986), 43–106.

[Iha91] Y. Ihara, *Braids, Galois groups and some arithmetic functions*, Proceedings of the International Congress, vol. Kyoto 1990, pp. 99–120, Springer-Verlag, Tokyo, 1991.

[IM95] Y. Ihara and M. Matsumoto, *On Galois actions on profinite completions of braid groups*, Proceedings AMS-NSF Summer Conference, vol. 186, 1995, Cont. Math series, Recent Developments in the Inverse Galois Problem, 173–200.

[Ka77] N. Katz, *The Eisenstein Measure and p-adic Interpolation*, Amer. Journ. of Math. **99**, No. 2 (1977), pp. 238-311.

[Ka96] N. Katz, *Rigid local systems*, Princeton University Press 1996.

[Ma95] M. Matsumoto, *On the Galois image of the derivation action on* π_1 *of the projective line minus 3 points*, Proceedings AMS-NSF Summer Conference, vol. 186, 1995, Cont. Math series, Recent Developments in the Inverse Galois Problem, 201–216.

[MM99] G. Malle and B.H. Matzat, *Inverse Galois Theory*, ISBN 3-540-62890-8, Monographs in Mathematics, Springer, 1999.

[Me72] W. Messing, *The Crystals Associated to Barsotti-Tate Groups; with Applications to Abelian Schemes*, Lecture Notes in Mathematics **264**, Springer-Verlag (1972).

[Mül95] P. Müller, *Primitive monodromy groups of polynomials*, Proceedings of the Recent developments in the Inverse Galois Problem conference, vol. 186, 1995, AMS Cont. Math series, pp. 385–401.

[NS00] H. Nakamura and L. Schneps, *On a subgroup of Grothendieck-Teichmüller group acting on the tower of the profinite Teichmüller modular groups*, Invent. Math. **141** (2000), 503–560.

[Ra94] M. Raynaud, *Revêtment de la droit affine en charactéristic $p > 0$ et conjecture d'Abhyankar*, Invent. Math. **116** (1994), 425–462.

[Ri96] L.T. Rigatelli, *Evariste Galois: 1811-1832*, Vol. **11**, translated from the Italian by John Denton, Vita Mathematica, Birkhäuser, 1996.

[Ser68] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, 1st ed., McGill University Lecture Notes, Benjamin, New York • Amsterdam, 1968, in collaboration with Willem Kuyk and John Labute.

[Se64] J.-P. Serre, *Lie Algebras and Lie Groups*, Lecture notes in math. **1500**, Springer-Verlag, 1991. Reissue of Serre's 1964 Harvard Notes (we use the numbering of the latest edition).

[Ser90] J.-P. Serre, *Relêvements dans $\tilde{A}_n$*, C. R. Acad. Sci. Paris **311** (1990), 477–482.

[Ser92] J.-P. Serre, *Topics in Galois theory*, no. ISBN #0-86720-210-6, Bartlett and Jones Publishers, notes taken by H. Darmon, 1992.

[Ta97] A. Tamagawa, *The Grothendieck conjecture for affine curves*, Compositio Mathematica **109** (1997), p. 135-194, .

[Ta99] A. Tamagawa, *On the fundamental groups of curves over algebraically closed fields of characteristic > 0*, Internat. Math. Res. Notices **16** (1999), 853–873.

[Vö95a] H. Völklein, *Cyclic covers of $\mathbb{P}^1$ and Galois action on their Division Points*, Proceedings AMS-NSF Summer Conference, vol. 186, 1995, Cont. Math series, Recent Developments in the Inverse Galois Problem, 91–107.

[Vö96] H. Völklein, *Groups as Galois Groups* **53**, Cambridge Studies in Advanced Mathematics, Camb. U. Press, Camb. England, 1996.

UC Irvine, Irvine, CA 92697, USA
E-mail address: mfried@math.uci.edu