Galois Groups and Fundamental Groups
MSRI Publications
Volume **41**, 2003

Introduction

This volume is the outcome of the MSRI special semester on *Galois Groups and Fundamental Groups*, held in the fall of 1999. Respecting the famous Greek requirements of unity of place, time, and action, the semester was an unforgettable, four-month-long occasion for all mathematicians interested in and responsible for the developments of the connections between Galois theory and the theory of fundamental groups of curves, varieties, schemes and stacks to interact, via a multitude of conferences, lectures and conversations.

Classical Galois theory has developed a number of extensions and ramifications into more specific theories, which combine it with other areas of mathematics or restate its main problems in different situations. Three of the most important of these extensions are *geometric Galois theory*, *differential Galois theory*, and *Lie Galois theory*, all of which have undergone very rapid development in recent years. Each of these theories can be developed in characteristic zero, over the field $\mathbb{C}$ of complex numbers, over number fields or p-adic fields, or in characteristic $p > 0$; various versions of the classical and inverse Galois problems can be posed in each situation. The purpose of this introduction is to give a brief overview of these three themes, which form the framework for all the articles contained in this book.

The main focus of study of **geometric Galois theory** is the theory of *curves* and the many objects associated to them: curves with marked points, their fields of moduli and their fundamental groups, covers of curves with their ramification information and their fields of moduli, and the finite quotients of the fundamental group which are the Galois groups of the covers, as well as the moduli spaces and Hurwitz spaces which parametrize all these objects.

To consider a curve X topologically is tantamount to considering it over the field of complex numbers $\mathbb{C}$. As an abstract group, the *topological fundamental group* of the curve depends only on the genus g and the number n of marked points chosen on the curve; it can be identified with the group of homotopy classes of loops on the curve based at a fixed (not marked) base point, and is presented by standard generators $a_1, \ldots, a_g, b_1, \ldots, b_g, c_1, \ldots, c_n$ subject to the unique relation

$$[a_1, b_1] \cdots [a_g, b_g] c_1 \cdots c_n = 1. \qquad (*)$$

Note that when $n \geq 1$, this group is actually free. The Galois covers of the curve correspond to the finite quotients of this group, which are exactly the finite groups generated by generators a_i, b_i and c_j satisfying $(*)$, so they are perfectly understood. The *algebraic fundamental group* of the curve is the Galois group of the compositum of all function fields of finite étale covers of the curve over the function field of the curve itself; in fact, it is exactly the profinite limit of the finite quotients of the topological fundamental group.

This simple situation leads or generalizes very naturally into new regions that contain all kinds of very difficult problems. We sketch some of them:

1. Fundamental groups in characteristic p. When a curve X is defined over a field in characteristic p, all relations between its fundamental group and any topological notion of 'loops' must be forgotten. Over an algebraically closed field, one defines the algebraic fundamental group directly, exactly as above; it is the profinite limit of the Galois groups (monodromy groups) of finite étale covers of the curve. However, in this situation, for (g, n) different from $(0, 0)$ and $(1, 0)$, it is extremely difficult to determine the structure of the fundamental group, or even the weaker question of which finite groups can occur as its quotients. Indeed, this is one of the fundamental problems of geometric Galois theory in characteristic p. In the affine case ($n \geq 1$), the complete solution to the weaker problem was conjectured by Abhyankar; this conjecture was proved over the affine line by M. Raynaud, and the proof extended to all curves by D. Harbater. However, the situation remains completely mysterious in the case of complete curves ($n = 0$, $g > 1$).

Things are better if one considers only the quotients of order prime to p; then a result due to Grothendieck states that the groups of order prime to p which can occur are exactly the finite quotients of order prime to p of the topological fundamental group of type (g, n) defined in $(*)$, and that in fact the prime-to-p quotients of the fundamental groups over $\mathbb{C}$ and in characteristic p are isomorphic. In characteristic p, this group is a quotient of the *tame fundamental group*, which is the largest quotient of the fundamental group having inertia subgroups of order prime to p; this group (which is equal to the fundamental group when $n = 0$) is easier to work with than the full group for various purposes. But the structure of the tame fundamental group and the set of its finite quotients are absolutely unknown, except in the non-hyperbolic cases $(g, n) = (0, 0)$, $(0, 1)$, $(0, 2)$ and $(1, 0)$.

The articles by R. Guralnick, A. Tamagawa, and F. Pop and M. Saïdi all work in the situation of curves defined over an algebraically closed field of characteristic p. Guralnick works on the problem of determining which groups can occur as Galois groups (or their composition factors) of finite separable covers $f : Y \to X$, where Y is of fixed genus g, and seeks groups which can specifically be excluded. Tamagawa shows that given the tame fundamental group, it is possible to recover the type (g, n) of the curve (if $(g, n) \neq (0, 0)$ or $(0, 1)$).

Results in this and other papers by Tamagawa even tend to imply that in some cases, the tame fundamental group may determine the isomorphism class of the curve completely. This shows how different the characteristic p case is from the characteristic 0 case, in which as we saw, curves of many different types may have isomorphic fundamental groups (for instance, the fundamental groups of curves of type $(2,2)$ and $(1,4)$ are both free of rank 5). Finally, Pop and Saïdi address similar questions, proving, under certain hypotheses on the Jacobians, that at most a finite number of curves can have isomorphic fundamental groups.

2. Anabelian theory. We saw above that the isomorphism class of the topological or the algebraic fundamental group is very far from determining even the most basic information about a curve in characteristic 0, such as its type (g,n), whereas in characteristic p it determines much more if not all of the information about the specific curve. However, one can also consider the algebraic fundamental group equipped with its canonical outer Galois action, which should provide more information. Indeed, any variety (scheme, stack) defined over an algebraically closed field can actually be considered as defined over a subfield K, given by the coefficients of the equations of a defining model, say, and which is finitely generated over the prime field and not algebraically closed. Then there is an exact sequence

$$1 \to \pi_1(X \otimes \bar{K}) \to \pi_1(X) \to \mathrm{Gal}(\bar{K}/K) \to 1, \qquad (**)$$

where $\pi_1(X \otimes \bar{K})$ denotes the algebraic fundamental group. The *anabelian problem*, which was posed by Grothendieck in his famous letter to G. Faltings, asks which varieties are entirely determined by the group $\pi_1(X \otimes \bar{K})$ together with the action $\mathrm{Gal}(\bar{K}/K) \to \mathrm{Out}(\pi_1(X \otimes \bar{K}))$. Grothendieck called varieties which are thus determined *anabelian varieties*, and explicitly stated that hyperbolic curves should be anabelian. This is related to the hitherto unproven *section conjecture* for a hyperbolic curve X, which states that the sections

$$\mathrm{Gal}(\bar{K}/K) \to \pi_1(X)$$

of $(**)$ are in bijection with the rational points of X if X is complete, and this set together with the tangential base points if X is not complete.

S. Mochizuki proved that hyperbolic curves defined over sub-p-adic fields, that is, fields which are subfields of fields finitely generated over the p-adics, are indeed anabelian. In his article in this volume, he discusses various results related to this theorem, including a partial generalization to characteristic p and a discussion of the section conjecture over the field of real numbers.

3. Galois action on fundamental groups. In his *Esquisse d'un Programme*, completing the letter to Faltings, Grothendieck suggested that not only hyperbolic curves, but also the moduli spaces $\mathcal{M}_{g,n}$ of curves of type (g,n) should be examples of anabelian varieties, and that explicitly investigating the Galois action on their fundamental groups should provide information of an entirely new

type about the elements of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$; this is known as *Grothendieck-Teichmüller theory*. The first non-trivial moduli space $\mathcal{M}_{g,n}$ is the case $(g,n) = (0,4)$; we have $\mathcal{M}_{0,4} = \mathbb{P}^1 - \{0,1,\infty\}$. Following the direction initiated by Grothendieck, the Galois action on the fundamental group of this space (the profinite free group $\widehat{F}_2$ on two generators) has been studied in a theory known as *dessins d'enfants*. The study has focused on coding the conjugacy classes of finite index subgroups of $\widehat{\pi}_1(\mathbb{P}^1 - \{0,1,\infty\})$, corresponding to the finite étale covers of $\mathbb{P}^1 - \{0,1,\infty\}$, as combinatorial objects (the dessins d'enfants), and using the combinatorics to look for invariants identifying the Galois orbits of these covers.

The only other moduli space of dimension 1 is $\mathcal{M}_{1,1}$, the moduli space of elliptic curves (genus one curves with one distinguished point). This space is the quotient of the Poincaré upper half-plane by the proper and discontinuous (but not free) action of $\mathrm{SL}_2(\mathbb{Z})$. Finite-index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ correspond to covers of $\mathcal{M}_{1,1}$. As in the case of $\mathcal{M}_{0,4}$, many specific families of these subgroups have been studied in detail, most familiarly the modular subgroups $\Gamma(N)$. Using graphs in the spirit of the theory of dessins d'enfants, F. Bogomolov and Y. Tschinkel characterize another family of very special finite-index subgroups of $\mathrm{SL}_2(\mathbb{Z})$, namely those corresponding to elliptic fibrations.

Before passing from these two curves to what can be said in the case of general moduli spaces $\mathcal{M}_{g,n}$, let us make a brief foray out of the geometric situation into the domain of **Lie Galois theory**, a subject that originates in the geometric situation but has been linearized by focusing on graded Lie algebras associated to the profinite fundamental groups rather than the groups themselves. A great deal of work has been done in this subject, mainly by Y. Ihara and his school, but we restrict ourselves here to discussing one conjecture which is a paradigm for the manner in which the problems in the domain arise in geometry, but raise their own interesting arithmetic questions.

Since as above, we have $\pi_1(\mathbb{P}^1 - \{0,1,\infty\}) \simeq \widehat{F}_2$, the exact sequence $(**)$ gives a canonical homomorphism

$$G_{\mathbb{Q}} \to \mathrm{Out}(\widehat{F}_2). \qquad (***)$$

As an initial step, the passage from the geometric situation to the Lie situation involves replacing the profinite completions of fundamental groups by their pro-ℓ completions, that is, the completions with respect to all finite quotients which are ℓ-groups for a fixed prime ℓ. Denote the pro-ℓ completion of F_2 by $F_2^{(\ell)}$. This completion is a quotient of the profinite completion by a characteristic subgroup, so that $(***)$ yields a homomorphism $G_{\mathbb{Q}} \to \mathrm{Out}(F_2^{(\ell)})$. Following Ihara, define a filtration on $G_{\mathbb{Q}}$ by setting

$$I^m G_{\mathbb{Q}} = \mathrm{Ker}\{G_{\mathbb{Q}} \to \mathrm{Out}(F_2^{(\ell)}/L^{m+1})\}$$

where L^m denotes the m-th term of the lower central series of $F_2^{(\ell)}$, and set

$$\mathrm{Gr}^m G_{\mathbb{Q}} = I^m G_{\mathbb{Q}}/I^{m+1} G_{\mathbb{Q}}.$$

The following conjecture on the structure of the graded Lie algebra associated to the filtration $I^m G_{\mathbb{Q}}$ was stated (in fuller detail) by Ihara, who attributed it to Deligne.

CONJECTURE. *The Lie algebra*

$$\left[\bigoplus_{m>0} \mathrm{Gr}^m G_{\mathbb{Q}}\right] \otimes \mathbb{Q}_\ell$$

is freely generated by generators $s_3, s_5, s_7, \ldots$, *where* $s_m \in \mathrm{Gr}^m G_{\mathbb{Q}}$ *is the so-called Soulé element.*

Part of this conjecture, namely the fact that the Lie algebra is actually generated by the s_i, was proved by Hain and Matsumoto. In their contribution to this volume, they discuss the conjecture and show how to fit it into a motivic framework.

Now let's return to the situation of geometry and consider the (conjecturally anabelian) moduli spaces $\mathcal{M}_{g,n}$. The geometry of these spaces has been described by explicitly cutting them into simply connected regions called cells, enumerated by objects known as fatgraphs, which are in fact equivalent to dessins d'enfant. The *Hurwitz spaces* are similar to the moduli spaces, but they parametrize equivalence classes of ramified coverings of Riemann surfaces, where two such coverings $f : Y \to X$ and $f' : Y' \to X'$ are equivalent if a diagram

$$\begin{array}{ccc} Y & \xrightarrow{f} & X \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\psi} \\ Y' & \xrightarrow{f'} & X' \end{array}$$

commutes for two biholomorphisms ϕ and ψ. A cellulation of the compactification of these spaces, analogous to that of the moduli spaces, is defined and studied in the article by M. Imbert.

The Hurwitz spaces are closely related to *special loci* in the moduli spaces, namely the loci of points in the moduli spaces corresponding to marked Riemann surfaces admitting a particular group of automorphisms. The article by L. Schneps studies these loci, showing that under certain conditions (which are always fulfilled in genus zero), the special loci are themselves moduli spaces of smaller type. The morphisms mapping these smaller moduli spaces to the special loci of the larger ones are respected by the canonical Galois action on the fundamental groups of the moduli spaces, so that the addition of these morphisms to those previously studied in Grothendieck-Teichmüller theory adds new combinatorial information on the elements of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

4. Inverse Galois theory. One of the most fundamental problems of Galois theory is that of determining which finite groups can occur as Galois groups over a given field K. This problem has been studied in many different situations and

by many different methods; by various direct methods, by explicit computation and solution of obstructions to embedding problems, and by geometry. The geometry comes in when studying a field of the type $K(t)$ for an indeterminate t, and the main tools are curves, since the desired groups are exactly the Galois groups of covers of the projective line over K.

When $K = \mathbb{C}$, the inverse Galois problem is solved by Riemann's existence theorem; every finite group occurs. Although no completely general analog to Riemann's existence theorem exists over arbitrary fields, many partial analogs have been developed in different situations. The key notion is that of *patching*; covers are constructed locally over disks, and the pieces are patched together (agree) on the overlaps. Like the theories described above, the inverse Galois problem exists in characteristic 0 and $p > 0$, necessitating the use of different techniques. Patching techniques have been developed using formal schemes (formal patching) and non-archimedean disks (rigid patching) which yield partial or complete solutions to the inverse Galois problem over many different fields (large or algebraically closed fields of any characteristic, fraction fields of complete local rings other than fields, complete fields, henselian fields, and so on). In fact, one can obtain stronger results, such as specific information on the structure of the fundamental group for affine curves; in certain cases, it can even be shown that the fundamental group is free, or that it has the property that every split embedding problem has a proper solution. The contribution by D. Harbater contains a comprehensive account of all these methods and results.

The domain of **differential Galois theory** is an adaptation of the classical inverse Galois problem; instead of considering finite groups as Galois groups of Galois extensions of arbitrary fields, one considers linear algebraic groups as Galois groups of so-called Picard-Vessiot extensions of D-fields, which are fields F equipped with a derivation $\partial : F \to F$. Over algebraically closed fields of characteristic 0, this problem has been completely solved by the combined results of Ramis, Mitschi, Singer, van der Put and finally Hartmann; any linear algebraic group over such a field is the differential Galois group of a Picard-Vessiot extension. In their contribution to this volume, Matzat and van der Put develop a non-obvious analog of these results in the characteristic p situation; they introduce iterated differential fields and give a complete formulation and solution to the inverse Galois problem over them.

Leila Schneps
Paris, November 2002