Preface

E. Galois (1811–1832) would certainly be surprised to see how often his name is mentioned in the mathematical books and articles of the twentieth century, in topics which are so far from his original work.

Since antiquity, mathematicians have been able to solve polynomial equations of degree 1 or 2. Formulæ for solving the equations of degree 3 or 4 were found during the sixteenth century. But it was only during the nineteenth century that the problem of equations of higher degree reached a final answer: the impossibility of solving by radicals a general equation of degree at least 5, and some methods for finding some solutions by radicals when these exist. Galois and Abel certainly played a key role in the development of this theory. All these results can be found in almost every book on Galois theory ... and that's the reason why we considered it useless to present them once more in the present book.

A strong peculiarity of those developments about solving equations is that the methods used to reach the final goal proved to be much more interesting than the problem to be solved. Nobody uses the formulæ for solving cubic or quartic equations ... but their consideration forced the discovery of complex numbers. And the impossibility proof for equations of higher degree led to specifying the notion of group, on the interest of which it is unnecessary to comment.

Let us now sketch, in modern language, the central result used by Galois to prove his celebrated theorem. A field extension $K \subseteq L$ is a Galois extension when every element of L is the root of a polynomial $p(X) \in K[X]$ which factors in $L[X]$ into linear factors and all of whose roots are simple. The Galois group $\mathsf{Gal}\,[L : K]$ of this extension is the group of all field automorphisms of L which fix all the elements of K. The classical Galois theorem asserts that when $K \subseteq L$ is a finite dimensional Galois extension, the subgroups $G \subseteq \mathsf{Gal}\,[L:K]$ of the Galois group classify exactly the intermediate field extensions $K \subseteq M \subseteq L$. An elementary presentation of this classical Galois theory is given in chapter 1.

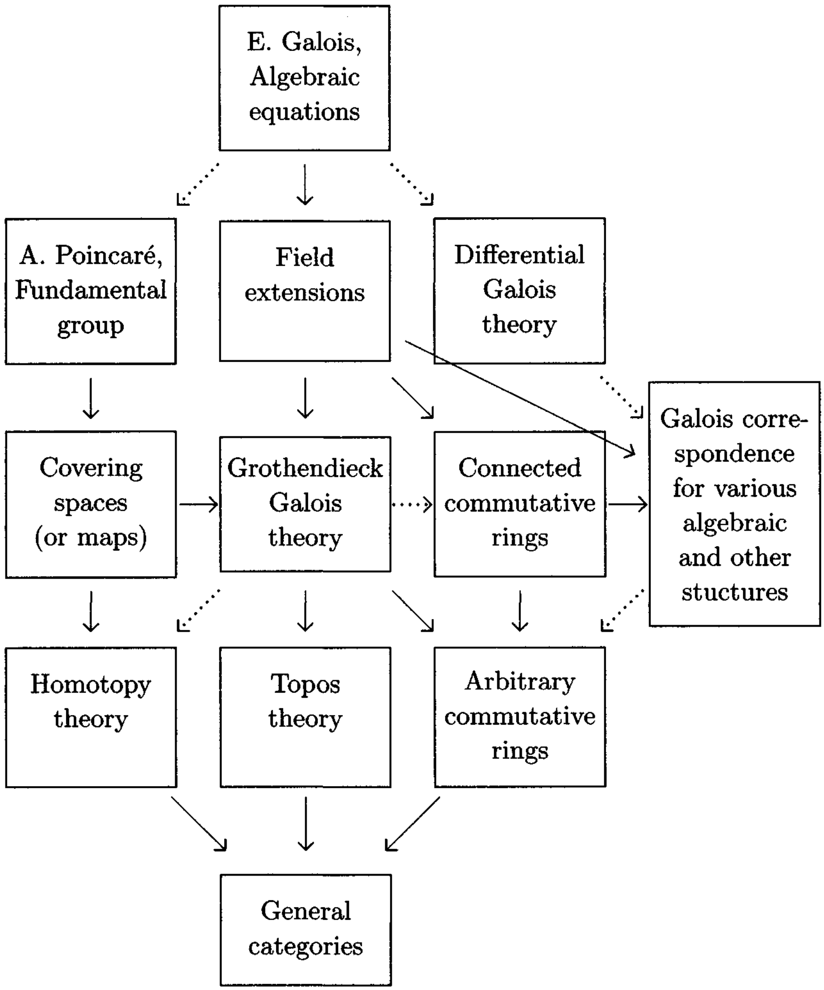
The environment for the theory named after Galois has been extended and changed many times, as displayed in the rough scheme of key words on page ix. Moreover, even this scheme would be incomplete if one tried to include the Galois descent and cohomology, Tannaka duality in connection with the Grothendieck motivic Galois theory, and some other closely related topics.

The solid arrows in the scheme represent generalizations of various constructions and results, and the dotted arrows represent "inspirations". Probably each of those arrows would be a good subject for a whole book, and so no reasonable description of them in a few pages can be produced.

The first step of generalization of the classical Galois theory is to replace the intermediate field extensions $K \subseteq M \subseteq L$ by more general commutative algebras over the field K. Given a field extension $K \subseteq L$, a K-algebra A is split by L when each element of A is the root of a polynomial $p(X) \in K[X]$ which factors in $L[X]$ into distinct linear factors. Of course, when $K \subseteq L$ is a Galois extension, every intermediate field extension $K \subseteq M \subseteq L$ is a K-algebra split by L. Conversely every intermediate algebra $K \subseteq A \subseteq L$ is necessarily a field.

Chapter 2, inspired by the work of Grothendieck, proves that the classical Galois theorem of chapter 1 is a local segment of a more general equivalence of categories. Given a finite dimensional Galois field extension $K \subseteq L$, the Galois theorem asserts now that the category of finite dimensional K-algebras split by L is equivalent to the category of finite $\mathsf{Gal}\,[L:K]$-sets, that is, finite sets provided with an action of the Galois group. The classical Galois theorem of chapter 1 is recaptured by observing that the subgroups $G \subseteq \mathsf{Gal}\,[L:K]$ correspond bijectively with the quotients of the Galois group in the category of $\mathsf{Gal}\,[L:K]$-sets; via the equivalence of categories, these are in bijection with the split algebras $K \subseteq A \subseteq L$, which turn out to be the intermediate fields.

In chapter 3 we handle the case of an arbitrary Galois extension of fields $K \subseteq L$, not necessarily finite dimensional. In that case, the Galois group $\mathsf{Gal}\,[L:K]$ comes naturally equiped with a profinite topology, that is, the structure of a compact Hausdorff space whose topology admits a base of closed–open subsets. The classical version of the Galois theorem asserts now that the closed subgroups of the profinite Galois group



Scheme 1: The contexts of Galois theories

classify the intermediate extensions $K \subseteq M \subseteq L$. The Galois theorem of Grothendieck extends in an analogous way, yielding now an equivalence between the category of K-algebras split by L and the category of profinite $\mathsf{Gal}\,[L : K]$-spaces, with continuous action of the Galois group.

The next and very crucial generalization is to replace the ground field K by a commutative ring R and thus develop the Galois theory for rings. The notion of Galois extension of commutative rings was first defined (independently of A. Grothendieck) by M. Auslander and O. Goldman (see [3]), and the Galois theory of those extensions was developed by S.U. Chase, D.K. Harrison, and A. Rosenberg (see [21]) and G.J. Janusz (see [54]), and many others (see the references in [24]). A.R. Magid in [67] develops the Grothendieck Galois theory of commutative rings in full generality.

Passing from fields to rings requires introducing a new ingredient: the spectrum of the ring. The idempotent elements $e = e^2$ of a commutative ring S constitute a boolean algebra, for the operations $e \wedge e' = ee'$ and $e \vee e' = e + e' - ee'$. The spectrum of this boolean algebra, constituted of the set of its ultrafilters with the Stone topology, is called the *Pierce spectrum* of the ring S. It is a profinite space, that is, a compact Hausdorff space whose topology is generated by its closed-open subsets. Of course since a field K admits 0 and 1 as its only idempotents, its Pierce spectrum is a singleton, which explains why the spectrum of a field never appeared up to now. Nevertheless, given a Galois field extension $K \subseteq L$, the K-algebra $L \otimes_K L$ has non-trivial idempotents; the ring case will show evidence that these idempotents determine the Galois group of the extension.

Every morphism of fields is injective, thus mentioning a field extension is the same as mentioning a morphism of fields. The Galois theory of commutative rings will be developed for Galois morphisms of rings $\sigma \colon R \longrightarrow S$, also called morphisms of Galois descent. Here *descent* refers to σ being an effective descent morphism in the dual of the category of commutative rings, that is, pulling back along this morphism in the dual of the category of rings yields a monadic functor between the corresponding slice categories. In other words, tensoring along this morphism in the category of rings yields a comonadic situation. The definition of σ being of *Galois* descent, and also the definition of being an R-algebra split by σ, are given in terms of the Pierce spectrum functor and its adjoint, which maps a profinite space X onto the ring $\mathcal{C}(X, R)$ of continuous functions from the space X to the ring R provided with the discrete topology. In fact the adjunction formed by Spec and $\mathcal{C}(-, R)$ localizes as an adjunction between the categories of S-algebras and that of profinite spaces over $\mathsf{Spec}(S)$; an R-algebra A is split by σ when the counit of this adjunction is an isomorphism at the S-algebra $S \otimes_R A$. And σ is of *Galois* descent when for each profinite space over $\mathsf{Spec}(S)$, the corresponding S-algebra given by adjunction, seen as an R-algebra, is split by σ. These categorical definitions generalize the classical corresponding notions in the case of fields and constitute the core of a categorical approach to Galois theory. The interested reader will find in section A.1 a historical discussion throwing light on the evolution of the notions, from the classical algebraic case to the categorical one.

But the major difference with the case of fields is the replacement of the Galois group by a Galois groupoid. The groupoids appear in Galois theory of commutative rings first in the papers of O.E. Villamayor and D. Zelinsky (see [73] and [74]). A.R. Magid uses what he calls Galois groupoids instead of Galois groups, and those groupoids have a profinite topology which makes them not equivalent (as topological groupoids) to any kind of a topological family of groups – unlike the ordinary groupoids (although R. Brown has good reasons to say that even ordinary groupoids should never be replaced by families of groups!).

Let us now explain how groupoids enter the story. Given a Galois descent morphism $\sigma\colon R \longrightarrow S$, the objects of the Galois groupoid are the elements of the spectrum of S, while the arrows are the elements of the spectrum of the cokernel pair of σ. The construction of the spectrum is functorial and contravariant; the two canonical morphisms from S to the cokernel pair of σ define the "domain" and "codomain" operations of the Galois groupoid. Observe that by definition, this groupoid lives in the category of profinite spaces. Again, in the case of fields, the spectrum of S is reduced to a singleton, thus the groupoid has a single object and therefore is a group: it is exactly the classical Galois group.

There is a last piece of the puzzle to generalize: the profinite spaces on which the topological Galois group acts. A set on which a group acts is exactly a presheaf on that group considered as a one object category. Thus the category to consider here will be that of internal presheaves on the internal Galois groupoid, in the category of profinite spaces. The Galois theorem for rings asserts that this category of internal presheaves on the Galois groupoid is equivalent to the category of R-algebras split by σ. Chapter 4 is devoted to developing this Galois theory of rings.

Chapter 5 is the core of this book. Taking our inspiration from the situation for rings, we first formalize the categorical context in which a general Galois theorem holds, and then give some applications. The Pierce spectrum functor between the category of rings and that of profinite spaces is replaced by an arbitrary functor between arbitrary categories. We exhibit the assumptions required to infer a Galois theorem proving an equivalence of categories between "split algebras" for this adjunction and the internal presheaves on some internal Galois groupoid. The main sources of inspiration for this are [36], [37], [39], [41].

The central extensions of groups are not usually considered as a part of

Galois theory, and therefore they are not included in the scheme above. However, they turn out to be precisely the objects split over extensions in a certain "non-Grothendieck" special case of categorical Galois theory, as explained in section 5.2.

Next we devote attention to another particularization of the general Galois theory of section 5.1: the case of semi-left-exact reflections, of which the situation of chapter 4 is a special case. Such an adjunction is given by a full reflective subcategory $r \dashv i\colon \mathcal{R} \overset{\longleftarrow}{\longrightarrow} \mathcal{C}$ such that for each object $C \in \mathcal{C}$, one keeps a full reflective subcategory $r_C \dashv i_C\colon \mathcal{R}/r(C) \overset{\longleftarrow}{\longrightarrow} \mathcal{C}/C$ by localizing the situation over the object C. This property holds in particular when the reflection r is left exact, from which we borrowed the terminology. We further particularize this study in a topological context. Eilenberg and Whyburn have studied the monotone–light factorization of a continuous map. Our Galois theory allows an elegant treatment of various aspects of this theory in the general context of compact Hausdorff spaces. We exhibit in particular Galois descent morphisms related to the Stone–Cěch compactification.

Chapter 6 focuses on the notion of covering map of topological spaces, defined classically as a continuous map $f\colon A \longrightarrow B$ such that every point in B has an open neighbourhood U whose inverse image is a disjoint union of open subsets, each of which is mapped homeomorphically onto U by f. One usually says that $A = (A, f)$ is a covering space over B (or of B) when $f\colon A \longrightarrow B$ is a covering map.

If B is connected and locally connected, and has a universal (i.e. the "largest" connected) covering (E, p), then all connected coverings of B are quotients of (E, p) and there is a bijection between (the isomorphic classes of) them and the subgroups of the automorphism group $\mathsf{Aut}(E, p)$. That bijection is constructed precisely as the standard Galois correspondence for separable field extensions, but in the dual category $(\mathsf{Top}/B)^{\mathsf{op}}$ of bundles over B.

Actually this result appears in most books on algebraic topology only in the special case when the Chevalley fundamental group $\mathsf{Aut}(E, p)$ is isomorphic to the usual Poincaré fundamental group of B. The general case was first studied by C. Chevalley (see [23], where however the Galois correspondence is not explicitly mentioned) who actually called $\mathsf{Aut}(E, p)$ the Poincaré group.

Finally, in chapter 7, we show first that it is possible to get a Galois theorem in the general context of descent theory, without necessarily a Galois assumption. This yields in particular a Galois theorem for every field extension $K \subseteq L$, without any further assumption. The price to pay is that the Galois group or the Galois groupoid must now be replaced by the more general notion of precategory. But in some cases of interest, even without any Galois assumption, the Galois precategory turns out to be again a groupoid. For example, the Galois theorem for toposes, due to Joyal and Tierney, enters the context of our generalized theory, without any Galois assumption. It asserts that every topos is equivalent to a category of étale presheaves on an open étale groupoid.

This book originated in a French manuscript that the first author wrote for his students. The second author convinced him to transform these notes into an actual book in English, and offered later to write an additional chapter, which became chapter 6 of the present book. Of course, most of the material of chapters 4, 5 and 7 is originally also due to the second author and his coauthors, and certainly the role of these coauthors in the genesis of the results should be emphasized here.

We tried to make this book accessible to a wide audience. First courses in algebra and general topology, together with some familiarity with the categorical notions of limit and adjoint functors, are sufficient to read it. The first chapters require even fewer prerequisites.

We thank all those who helped us or supported us in the preparation of this book, even if we cannot cite all of them. We cite first the participants in the Louvain-la-Neuve category seminar, with whom the original French version of this work was first discussed. Among them, Gilberte van den Bossche is worth a special mention, and the first author wants to dedicate this book to her memory. We thank also R. Brown, A. Carboni, G.M. Kelly, A.R. Magid, R. Paré, D. Schumacher, R.H. Street, W. Tholen, and all others whose ideas and proofs have provided a big part of the material in this book. The second author wants to add that most of his joint work with the persons just cited was carried out during his various visits to them and supported by their universities and national councils, especially of Australia, Belgium, Canada, Italy and the UK.

Finally we express our special thanks to René Lavendhomme and Hvedri Inassaridze who were our teachers a long time ago, and to Saunders Mac Lane, since like most category-theorists in the world, we feel we are his students too – but also for his important particular advice concerning categorical Galois theory.