University of Nevada, Reno

Galois descent, cohomology, and conjugacy

A thesis submitted in partial fulfillment of the
requirements for the degree of Master of Science
in Mathematics

by

Jenna L. Moore

Dr. Christopher L. Rogers/Thesis Advisor

May, 2021

THE GRADUATE SCHOOL

We recommend that the thesis
prepared under our supervision by

JENNA L. MOORE

entitled

Galois descent, cohomology, and conjugacy

be accepted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE

Christopher L. Rogers, Ph.D.
Advisor

Stanislav Jabuka, Ph.D.
Committee Member

Jonathan Beardsley, Ph.D.
Committee Member

Jennifer L. Lanterman, Ph.D.
Graduate School Representative

David W. Zeh, Ph.D., Dean
Graduate School

May, 2021

Abstract

We give a concise exposition on the application of non-abelian Galois cohomology to descent problems in algebra, as developed by A. Borel, J.-P. Serre, and others in the late fifties and early sixties. Although its origins lie in algebraic number theory, this abstract framework allows one to formalize and address a very general question: If two algebraic objects defined over a field $\Bbbk$ are found to be isomorphic over a field extension $\Omega/\Bbbk$, are they also isomorphic over $\Bbbk$?

In this thesis, we focus on explicit descent problems over a field of characteristic zero in which the algebraic objects involved can be described as points in Zariski closed subsets of affine space, and whose automorphism groups are subgroups of the algebraic group GL_n. In our cases of interest, the action of the automorphism group arises by the conjugation action of GL_n on various spaces of $\Bbbk$-linear maps.

Our presentation follows closely the 2010 monograph G. Berhuy. Our contribution is that we fill in numerous details in the proofs found there, in particular those involving techniques from algebraic geometry. We clarify the relationship between the classical Hilbert's Theorem 90 for cyclic extensions and the more general non-abelian Hilbert's Theorem 90, which is one of the fundamental basic tools used in Galois cohomology. Finally, we give a complete proof that the descent problem for a finite dimensional associative $\Bbbk$-algebra A is controlled by the Galois cohomology set $H^1(\mathcal{G}_\Omega, \mathrm{Aut}(A)(\Omega))$.

Acknowledgments

The author would like to thank: her advisor, Chris Rogers, for his invaluable guidance and unwavering support while preparing this thesis, and her fiancé, Cody Judd, for keeping her grounded during the process.

Contents

1 Introduction

1.1 What is descent?

Most problems in algebra either begin or end with finding solutions to a system of polynomial equations. Finding an explicit formula for solutions is often impossible, even in the single variable case, as was famously demonstrated by the work of É. Galois. For this reason we must step back and take a more coarse-grained approach. In particular, we can instead ask if the system of equations have at least one solution, never mind what the solution is. The answer to this simpler question is also quite subtle, and can depend on the kinds of numbers we allow as valid solutions. For example, the polynomial equation

$$x^4 - x^2 - 2 = 0$$

of degree 4 has either four solutions, two solutions, or no solutions depending on whether or not we consider real and imaginary numbers, only real numbers, or only rational numbers, respectively, as valid candidates for solutions. More abstractly, if an algebraic problem defined over a field $\Bbbk$ has a solution in a larger field Ω containing $\Bbbk$, we would like to know whether or not it also has a solution over $\Bbbk$.

Questions of this kind are called **Galois descent problems**, and they often arise when one is trying to classify algebraic structures relative to some fixed initial $\Bbbk$-linear data. For instance, suppose we are interested in classifying, up to conjugacy, linear endomorphisms on an n-dimensional vector space over an infinite field $\Bbbk$. Then we fix a square matrix $M_0 \in \mathrm{Mat}_n(\Bbbk)$ and suppose $M \in \mathrm{Mat}_n(\Bbbk)$ is another matrix which we deduce is conjugate to M_0 after passing to the algebraic closure $\overline{\Bbbk}$. That is, there exists a $n \times n$ invertible matrix $P \in \mathrm{GL}_n(\overline{\Bbbk})$ with entries in $\overline{\Bbbk}$ such that $M = PM_0P^{-1}$. (Perhaps we needed to exploit certain techniques to verify this which only hold over algebraically closed fields.) However, we are actually interested in whether or not M is equivalent to M_0 over the original field $\Bbbk$. That is, does there exist an invertible matrix $R \in \mathrm{GL}_n(\Bbbk)$ with entries in $\Bbbk$ that conjugates M and M_0?

It is important to note that above we are <u>not</u> asking for – nor do we need – P and R to be the same matrix in order to verify that M and M_0 are equivalent over $\Bbbk$. We only need to determine whether or not such a R exists given the existence of P. It turns out that the answer to this descent

problem is "yes" for any fixed matrix M_0. The proof is a well known exercise in linear algebra.

On the other hand, if we adjust the problem by requiring P and the desired R to instead be invertible matrices with determinant equal to 1, the answer to the descent problem depends on the matrix M_0 and is "no" in general. The reason why is closely related to the problem we began with: finding solutions of polynomial equations. The constraint on the determinant of the conjugating matrix in this case turns a linear problem into a non-linear polynomial one, which may or may not have solutions depending on the field extension we work over.

1.1.1 The basic ingredients of a descent problem

There are several takeaways from the above matrix conjugation problem that become reoccurring themes in the kinds of descent problems that we consider in this thesis.

- First, there is the set $F(\Bbbk)$ of algebraic structures over $\Bbbk$ which we would like to classify, and we have an "extension of scalars" operation, which provides a way of interpreting these structures as elements of a set $F(\Omega)$ over any extension field Ω of $\Bbbk$.

- Next, we can characterize the symmetries of the algebraic structures via a group action of a subgroup $G(\Bbbk)$ of the general linear group $\mathrm{GL}_n(\Bbbk)$, which gives us an equivalence relation on $F(\Bbbk)$ the corresponding "orbit space". Two algebraic structures are considered equivalent if they lie in the same orbit of this group action. Furthermore, the group action by $G(\Bbbk)$ is naturally compatible with the action of an analogous group $G(\Omega)$ on $F(\Omega)$ via the extension of scalars.

- The descent problem is characterized by fixing one algebraic structure $A_0 \in F(\Bbbk)$ and then considering the so-called "twisted forms" of A_0 that "split" over a field extension $\Omega/\Bbbk$. These are isomorphism classes of algebraic structures $A \in F(\Bbbk)$ which become isomorphic to A_0 as objects in $F(\Omega)$ via the action of $G(\Omega)$.

- Finally, the Galois group of any Galois extension $\Omega/\Bbbk$ acts on the set of structures $F(\Omega)$ and the group of symmetries $G(\Omega)$ in a functorial way. The way we determine whether or not the descent problem has a "positive" or "negative" solution is by checking to see if a twisted

form split over Ω "descends" back down to $F(\Bbbk)$ by taking the fixed points of the Galois group action.

1.2 Why profinite groups?

In order to determine whether or not a descent problem for $\Omega/\Bbbk$ has a positive answer, we need a way to get from Ω down to $\Bbbk$. If Ω is a finite Galois extension of $\Bbbk$, one way to do this is to look at the fixed field of Ω by the Galois group of $\Omega/\Bbbk$, which is exactly $\Bbbk$.

However, this approach runs into problems when considering algebraic extensions such as the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, which is arguably the most important extension of the rationals from an elementary number theoretic perspective. Indeed, $\overline{\mathbb{Q}}$ is an infinite Galois extension of $\mathbb{Q}$, and its intermediate extensions are not in bijection with subgroups of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, as there are proper subgroups of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ whose fixed field is $\mathbb{Q}$. In order to rescue the fundamental theorem of Galois theory for infinite Galois extensions $\Omega/\Bbbk$, we restrict our attention to the closed subgroups of the Galois group with respect to the "Krull topology". Endowed with this topological structure, $\mathrm{Gal}(\Omega/\Bbbk)$ is isomorphic as a topological group to $\varprojlim_L \mathrm{Gal}(L/\Bbbk)$ where L runs through all finite Galois subextensions of $\Omega/\Bbbk$. In other words, $\mathrm{Gal}(\Omega/\Bbbk)$ is a profinite group.

1.3 Why non-abelian cohomology?

In full generality, the objects at hand when setting up a Galois descent problem are a group scheme G acting on a functor F, both equipped with an action by the profinite group $\mathcal{G} = \mathrm{Gal}(\Omega/\Bbbk)$, where the action of $\mathcal{G}$ on the group scheme G is continuous. The orbit-stabilizer theorem says that for all elements a in $F(\Bbbk)$ there is a bijection between the set of left cosets $G(\Omega)/\mathrm{Stab}_{G(\Omega)}(a)$ and the orbit of a, resulting in an exact sequence of pointed sets

$$1 \to \mathrm{Stab}_G(a) \to G \to G(\Omega) * a \to 1.$$

where $G(\Omega) * a$ denotes the orbit of a. No assumption that the groups involved in this construction are abelian nor do subgroups need to be normal. Indeed, the orbit $G(\Omega) * a$ is not a group in general.

Yet, as alluded to above, in order to "descend" back down to $\Bbbk$, we want to take Galois fixed points, i.e. $\mathcal{G}$-invariants, of the above sequence. As is the case in standard group cohomology, the

Galois fixed point functor $(-)^{\mathcal{G}}$ need not be right exact. In fact, the failure of this functor to preserve right exactness is the obstruction to a "positive" answer to descent problems involving the algebraic structure $a \in F(\Bbbk)$.

Much like the case of ordinary homological algebra, there is, in fact, a way to repair the failure of right exactness by extending the sequence $1 \to \mathrm{Stab}_G(a)^{\mathcal{G}} \to G^{\mathcal{G}} \to (G(\Omega) * a)^{\mathcal{G}}$ to a "long exact" sequence of pointed sets of the form

$$1 \to \mathrm{Stab}_G(a)^{\mathcal{G}} \to G^{\mathcal{G}} \to (G(\Omega) * a)^{\mathcal{G}} \xrightarrow{\delta_0} H^1(\mathcal{G}, \mathrm{Stab}_G(a)(\Omega)) \to H^1(\mathcal{G}, G(\Omega)).$$

The pointed sets $H^1(\mathcal{G}, -)$ in the above sequence are called the "degree 1 non-abelian Galois cohomology sets" of $\mathcal{G}$. Conveniently, these sets are constructed by means of considering continuous non-abelian valued cochains within the familiar cochain complex used to compute ordinary group cohomology.

The continuity of cocycles in this construction yields a characterization of profinite cohomology in terms of ordinary group cohomology when the coefficents are abelian. Specifically, for a profinite group Γ and a discrete Γ-module A, we have an isomorphism

$$H^n(\Gamma, A) \cong \varinjlim_{U} H^n_{\mathsf{Grp}}(\Gamma/U, A^U)$$

where U ranges through open normal subgroups of Γ, a rather desirable result as finite group cohomology is well understood and easier to work with.

2 Main results

This thesis provides a concise exposition on the application of non-abelian Galois cohomology to descent problems in algebra, with a focus on classification problems of algebraic structures. Our presentation follows closely the monograph G. Berhuy [1]. In particular, we review basic facts and key theorems concerning: profinite Galois groups (Sec. 3.2.2), group schemes (Sec. 4), profinite non-abelian group cohomology, as developed by A. Borel and J.-P. Serre [4] (Sec. 5.1) and twisted forms (Sec. 6.1). Our exposition culminates with the characterization of a Galois descent problem via the Descent Lemma (Thm. 6.11), a result of Serre. We also give a thorough treatment of the matrix conjugacy problem via Galois descent in Sec. 8.1.

However, we provide several novel additions as well: we fill in numerous details in the proofs given in [1], particularly those involving techniques from algebraic geometry (Section 4.1); we clarify in Section 7 the relationship between the classical Hilbert's Theorem 90 for cyclic extensions and the more general non-abelian Hilbert's Theorem 90, which is one of the fundamental basic tools used in Galois cohomology. In Section 8.2 we give a complete proof that the descent problem for a finite dimensional associative $\Bbbk$-algebra A is controlled by the Galois cohomology set $H^1(\mathcal{G}_\Omega, \mathrm{Aut}(A)(\Omega))$. Finally, in Section 9 we discuss applications to finite-dimensional graded polynomial algebras equipped with a degree +1 derivation as a possible direction for future work.

3 Preliminaries

3.1 Conventions

Throughout this thesis, we adopt the following conventions and notations:

- $\Bbbk$ denotes a field of characteristic zero.
- $\overline{K}$ denotes an algebraic closure of any field K.
- If Ω/K is a Galois extension the Galois group $\mathrm{Gal}(\Omega/K)$ will be denoted $\mathcal{G}_\Omega$ whenever K is clear from the context.
- We use multiplicative notation for all groups, abelian or otherwise.
- Set denotes the category whose objects are sets, and whose morphisms are functions.
- Set_* denotes the category whose objects are pointed sets and whose morphisms are maps of pointed sets.
- Grp denotes the category whose objects are groups and whose morphisms are group homomorphisms. AbGrp is the category whose objects are abelian groups and whose morphisms are group homomorphisms.
- $\mathsf{Alg}_\Bbbk$ denotes the category whose objects are unital commutative $\Bbbk$-algebras and whose morphisms are unit preserving $\Bbbk$-algebra homomorphisms.
- $\mathsf{Fld}_\Bbbk$ denotes the full subcategory of $\mathsf{Alg}_\Bbbk$ whose objects are field extensions of $\Bbbk$.

3.2 Results from elementary Galois theory

We begin by recalling standard results from elementary Galois theory. We refer to Morandi's book [3] for details and a more thorough introduction.

Definition 3.1. Let K and K' be fields, let L/K and L'/K' be extensions. Let $\iota\colon K \to K'$ be a ring homomorphism. We say that $\phi\colon L \to L'$ is an **extension** of ι if and only if $\phi|_K = \iota$.

Theorem 3.2. *Let K be a field and L/K be an algebraic extension. Let E be an algebraically closed field, and let $\tau\colon K \to E$ be a ring homomorphism. Then there exists a ring homomorphism $\sigma\colon L \to E$ such that $\sigma|_K = \tau$. That is, there exists an extension $\sigma\colon L \to E$ of τ.*

Corollary 3.3. *Let K and K' be fields, and let $\iota\colon K \to K'$ be a ring homomorphism. Then there exists an extension $\phi\colon \overline{K} \to \overline{K'}$ of ι.*

Let Ω denote the infinite extension $\mathbb{Q}(\{\sqrt{p} \mid p \text{ prime}\})$ of $\mathbb{Q}$. In the following example, we show $\Omega/\mathbb{Q}$ is Galois, and exhibit a proper subgroup H of $\mathrm{Gal}(\Omega/\mathbb{Q})$ such that $\Omega^H = \Omega^{\mathrm{Gal}(\Omega/\mathbb{Q})} = \mathbb{Q}$. This shows that the fundamental theorem of Galois theory for finite extensions fails for infinite extensions.

Example 3.4. Set $\Omega = \mathbb{Q}(\{\sqrt{p} \mid p \text{ prime}\})$. Then $\Omega/\mathbb{Q}$ is normal since Ω is the splitting field of the collection of polynomials $\{x^2 - p \mid p \text{ prime}\} \subseteq \mathbb{Q}[x]$. Since $\Omega/\mathbb{Q}$ is an algebraic extension and $\mathrm{char}\ \mathbb{Q} = 0$, then $\Omega/\mathbb{Q}$ is separable. Hence $\Omega/\mathbb{Q}$ is an infinite Galois extension. Now for each prime p, let σ_p be the element of $\mathrm{Gal}(\Omega/\mathbb{Q})$ defined by $\sqrt{p} \mapsto -\sqrt{p}$ and $\sqrt{p'} \mapsto \sqrt{p'}$ for all $p' \neq p$. Now consider the subgroup $H = \langle\{\sigma_p \mid p \text{ prime}\}\rangle$ of $\mathrm{Gal}(\Omega/\mathbb{Q})$. Note that H does not contain the element $\sigma \in \mathrm{Gal}(\Omega/\mathbb{Q})$ which maps $\sqrt{p}$ to $-\sqrt{p}$ for all prime p. Hence $H \neq \mathrm{Gal}(\Omega/\mathbb{Q})$. We claim that $\Omega^H = \mathbb{Q}$. Since $\Omega/\mathbb{Q}$ is Galois, for any $x \in \Omega$, the roots of the minimal polynomial of x belong to Ω. Hence if $x = \sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n}$ are the the n distinct roots of the minimal polynomial of x, then x is contained in the subfield $E = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n}) \subseteq \Omega$. Since $x \in \Omega$ is separable over $\Bbbk$, it follows that $E/\mathbb{Q}$ is a finite Galois extension. Now suppose $x \in \Omega^H$. Then x is fixed by $\sigma_{p_1}, \ldots, \sigma_{p_n} \in H$, and since $\mathrm{Gal}(E/\mathbb{Q}) = \langle\sigma_{p_1}, \ldots, \sigma_{p_n}\rangle$ we conclude that $x \in \mathbb{Q}$.

Proposition 3.5. *Let $\Bbbk$ be a field and $\Omega/\Bbbk$ a Galois extension. Let*

$$\mathcal{N} := \{\mathrm{Gal}(\Omega/L) \mid \Bbbk \subset L \subset \Omega \text{ and } L/\Bbbk \text{ is finite Galois}\}$$

*Then the **Krull topology** on $\mathrm{Gal}(\Omega/\Bbbk)$ is the unique topology such that for all $\sigma \in \mathrm{Gal}(\Omega/\Bbbk)$ the set $\{\sigma H \mid H \in \mathcal{N}\}$ is a basis of open neighborhoods of σ.*

Theorem 3.6 (Fundamental Theorem of Galois Theory (Thm 17.8 [3]))**.** *Let $\Omega/\Bbbk$ be a Galois extension. With the Krull topology on $\mathrm{Gal}(\Omega/\Bbbk)$, the assignment between subfields L of Ω and subgroups*

of $\mathrm{Gal}(\Omega/\Bbbk)$ *given by*

$$L \longmapsto \mathrm{Gal}(\Omega/L)$$

$$\Omega^H \longmapsto H$$

induces a bijection between the following sets:

1. *The set of subfields* $\Bbbk \subset L \subset \Omega$ *and the set of closed subgroups of* $\mathrm{Gal}(\Omega/\Bbbk)$.
2. *The set of subfields* $\Bbbk \subset L \subset \Omega$ *such that* $[L\colon \Bbbk] < \infty$ *and the set of open subgroups of* $\mathrm{Gal}(\Omega/\Bbbk)$.
3. *The set of subfields* $\Bbbk \subset L \subset \Omega$ *such that* $L/\Bbbk$ *is a finite Galois extension and the set of open normal subgroups of* $\mathrm{Gal}(\Omega/\Bbbk)$.

Moreover, if H *is an open normal subgroup of* $\mathrm{Gal}(\Omega/\Bbbk)$ *then we have*

$$\mathrm{Gal}(\Omega^H/\Bbbk) \cong \mathrm{Gal}(\Omega/\Bbbk)/H.$$

In particular, for any finite Galois subextension $\Bbbk \subset L \subset \Omega$ *we have*

$$\mathrm{Gal}(\Omega/\Bbbk)/\mathrm{Gal}(\Omega/L) \cong \mathrm{Gal}(L/\Bbbk).$$

3.2.1 Morphisms of Galois extensions

Proposition 3.7 (Prop. I.2.9 [1])**.** *Let* K *and* K' *be fields, let* Ω/K *and* Ω'/K' *be Galois extensions, and let* $\iota\colon K \to K'$ *be a ring homomorphism. Assume that there exist extensions* $\phi_1, \phi_2\colon \Omega \to \Omega'$. *Then for all* $\tau' \in \mathrm{Gal}(\Omega'/K')$, *there exists a unique* $\tau \in \mathrm{Gal}(\Omega/K)$ *such that*

$$\tau' \circ \phi_1 = \phi_2 \circ \tau.$$

In particular, there exists $\rho \in \mathrm{Gal}(\Omega/K)$ *such that* $\phi_1 = \phi_2 \circ \rho$.

Corollary 3.8 (Cor. I.2.10 [1])**.** *Let* K *and* K' *be fields, let* Ω/K *and* Ω'/K' *be Galois extensions, and let* $\iota\colon K \to K'$ *be a ring homomorphism. Let* $\phi\colon \Omega \to \Omega'$ *be an extension of* ι. *For all* $\tau' \in \mathrm{Gal}(\Omega'/K')$, *let* $\overline{\phi}(\tau')$ *be the unique element of* $\mathrm{Gal}(\Omega/K)$ *such that*

$$\tau' \circ \phi = \phi \circ \overline{\phi}(\tau').$$

Then the map $\overline{\phi}\colon\ \mathrm{Gal}(\Omega'/K') \to \mathrm{Gal}(\Omega/K)$ *is a continuous group homomorphism. Moreover, if* ϕ' *is another extension of* ι*, then there exists* $\rho \in \mathrm{Gal}(\Omega/K)$ *such that* $\phi = \phi' \circ \rho$*, and we have*

$$\overline{\phi'} = \mathsf{Inn}(\rho) \circ \overline{\phi}.$$

3.2.2 The Galois group as a profinite group

Recall that a **directed set** is a partially ordered set $(I, \preceq)$, such that for all $i, j \in I$, there exists $k \in I$ such that $i \preceq k$ and $j \preceq k$. A **projective system** in a category $\mathcal{C}$ is a collection of objects $\{C_i\}_{i\in I}$ indexed by a directed set I together with morphisms $\phi_{ij}\colon C_j \to C_i$ for any $i, j \in I$ with $i \preceq j$, satisfying the following properties:

1. $\phi_{ii} = \mathrm{id}_{C_i}$ for all $i \in I$.

2. $\phi_{ij} \circ \phi_{jk} = \phi_{ik}$ for all $i, j, k \in I$ with $i \preceq j \preceq k$.

Let $\Omega/\Bbbk$ be a Galois extension. Then the set of all finite Galois subextensions of $\Omega/\Bbbk$ with the partial order relation "$\subseteq$" is a directed set. For any finite Galois extension $L/\Bbbk$, set $X_L = \mathrm{Gal}(L/\Bbbk)$, and for any $L/\Bbbk, L'/\Bbbk$ with $L \subset L'$, let $\phi_{LL'}$ be the group homomorphism

$$\begin{aligned} \phi_{LL'}\colon X_{L'} &\longrightarrow X_L \\ \sigma &\mapsto \sigma|_L. \end{aligned}$$

Together this forms a projective system of groups.

Definition 3.9. If $((C_i)_{i\in I}, (\phi_{ij}))$ is a projective system in a category $\mathcal{C}$, the **inverse limit** $\varprojlim C_i$ is given by

$$\varprojlim C_i = \left\{ (x_i)_{i\in I} \in \prod_{i\in I} C_i \;\middle|\; \phi_{ij}(x_j) = x_i \text{ for all } i \preceq j \right\}.$$

If $((C_i)_{i\in I}, (\phi_{ij}))$ is a projective system of topological spaces (resp. groups), then the inverse limit is also a topological space (resp. group) with respect to the topology induced by the product topology.

Definition 3.10. A topological group Γ is **profinite** if it is isomorphic as a topological group to an inverse limit of finite groups, each of them being endowed with the discrete topology.

Theorem 3.11 (Thm I.2.18 [1]). *Let $\Omega/\Bbbk$ be a Galois extension. Then $\mathrm{Gal}(\Omega/\Bbbk)$ equipped with the Krull topology is a profinite group. In particular, there is an isomorphism of topological groups*

$$\mathrm{Gal}(\Omega/\Bbbk) \cong \varprojlim_{L} \mathrm{Gal}(L/\Bbbk)$$

where $L/\Bbbk$ runs over all finite Galois subextensions of $\Omega/\Bbbk$.

Below is a proposition which establishes nice properties of profinite groups.

Proposition 3.12 (Thm 2 [5]). *The following are equivalent conditions.*

1. *Γ is a profinite group.*
2. *Γ is a compact, Hausdorff group in which each neighborhood of 1 contains an open normal subgroup of Γ.*
3. *Γ is a compact, totally disconnected, Hausdorff group.*

Closed subsets of a compact Hausdorff space are compact sets, so the above proposition implies that closed subgroups of a profinite group are again profinite. Moreover, every open subgroup of a profinite group is closed. For all $\sigma \in \Gamma$, the collection $\{\sigma U \mid U \text{ open in } \Gamma\}$ forms a basis of open neighborhoods of σ, and the topology generated by this basis is called the **profinite topology**.

3.3 Category theoretic notions

Here we present tools from category theory which we appeal to throughout the thesis.

Definition 3.13. Let $\mathcal{C}$ be a category, let $\mathcal{D}$ be a subcategory of Set and let $F\colon \mathcal{C} \to \mathcal{D}$ be a functor. A functor $F'\colon \mathcal{C} \to \mathcal{D}$ is a **subfunctor** of F if the following properties hold:

1. For all $A \in \mathcal{C}$, we have $F'(A) \subset F(A)$.
2. For all $A, B \in \mathcal{C}$, and every map $f \in \hom_{\mathcal{C}}(A, B)$, the induced morphism $F'(f)\colon F'(A) \to F'(B)$ is the restriction of $F(f)\colon F(A) \to F(B)$. In other words, the diagram

$$\begin{array}{ccc} F'(A) & \xrightarrow{F'(f)} & F'(B) \\ \downarrow & & \downarrow \\ F(A) & \xrightarrow[F(f)]{} & F(B) \end{array}$$

commutes.

Definition 3.14. Let $\mathcal{C}$ and $\mathcal{D}$ be categories and $F, G\colon \mathcal{C} \rightrightarrows \mathcal{D}$ be functors. A **natural transformation** of functors $\Theta\colon F \to G$ is a rule which assigns a morphism $\Theta_A\colon F(A) \to G(A)$ of $\mathcal{D}$ to each object $A \in \mathcal{C}$ such that for every morphism $f\colon A \to B$ of $\mathcal{C}$ the diagram

$$\begin{array}{ccc} F(A) & \xrightarrow{\Theta_A} & G(A) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(B) & \xrightarrow[\Theta_B]{} & G(B) \end{array}$$

commutes. The collection of morphisms Θ_A are called the **components** of Θ. If every component Θ_A is an isomorphism, then Θ is a **natural isomorphism**, and we write $\Theta\colon F \cong G$

3.3.1 Representable functors

Let $\mathcal{C}$ be a category. Let $A \in \mathcal{C}$ and define $h_A\colon \mathcal{C} \to \mathsf{Set}$ as follows. For every object $B \in \mathcal{C}$ set $h_A(B) := \hom_{\mathcal{C}}(A, B)$ and for each morphism $f\colon B \to C$ of $\mathcal{C}$ let $h_A(f)\colon h_A(B) \to h_A(C)$ be the morphism defined by

$$\begin{aligned} h_A(f)\colon \hom_{\mathcal{C}}(A, B) &\longrightarrow \hom_{\mathcal{C}}(B, C) \\ \phi &\longmapsto f \circ \phi. \end{aligned}$$

Let $\phi \in \hom_{\mathcal{C}}(A, B)$. Then $h_A(\mathrm{id}_B)(\phi) = \mathrm{id}_B \circ \phi = \phi$, and so $h_A(\mathrm{id}_B) = \mathrm{id}_{h_A(B)}$. If $f\colon B \to C$ and $g\colon C \to D$ are morphisms of $\mathcal{C}$, then

$$\begin{aligned} h_A(g \circ f)(\phi) &= (g \circ f) \circ \phi = g \circ (f \circ \phi) \\ &= h_A(g)(f \circ \phi) = h_A(g) \circ h_A(f)(\phi). \end{aligned}$$

Hence h_A is a functor.

Definition 3.15. Let $F\colon \mathcal{C} \to \mathsf{Set}$ be a functor. We say that F is **representable** if there is a natural isomorphism of functors $F \cong h_A$ for some object $A \in \mathrm{Ob}(\mathcal{C})$. In this case we say F is **represented by A**.

Lemma 3.16 (The Yoneda Lemma (Lemma III.7.13 [1]))**.** *Let $\mathcal{C}$ be a category. For every pair of objects $A, B \in \mathrm{Ob}(\mathcal{C})$, there is a one-to-one correspondence between the set of morphisms $\phi\colon B \to$*

A and the set of natural transformations $\Theta\colon h_A \to h_B$.

Remark 3.17. The bijection in the Yoneda lemma sends $\Theta(\mathrm{id}_{h_A})$ to ϕ.

4 Group schemes

In this section, we define algebraic group schemes, which are a main component in defining the Galois cohomology functor in Section 5. We recall tools from algebraic geometry and use them to obtain the representability of two main group schemes appearing in this thesis, which, for a finite dimensional vector space V and a finite dimensional $\Bbbk$-algebra A, are the algebraic group $\mathrm{GL}(V)$ and the algebraic group scheme $\mathrm{Aut}(A)$.

4.1 Representable functors from algebraic geometry

We recall some basic terminology from the algebraic geometry of affine varieties and their generalizations. A standard reference is [6, §1]. However, here we will consider base fields $\Bbbk$ of characteristic zero other than the complex numbers, which we do not assume to be algebraically closed, and we allow the possibility of non-radical ideals. The best way for dealing with such spaces is via the theory of finite-type (reduced) affine $\Bbbk$-schemes [2, §II.2]. But this approach is overkill for the rather unsophisticated results that we need here.

In what follows, $\Bbbk$ denotes a field not necessarily algebraically closed.

4.1.1 Affine varieties

Given an ideal $I \trianglelefteq \Bbbk[x_1, \ldots, x_n]$ and a $\Bbbk$-algebra $R \in \mathsf{Alg}_{\Bbbk}$, we consider I as a subset of $R[x_1, \ldots, x_n]$ and define

$$\mathbb{V}(I)(R) := \{\mathbf{r} := (r_1, r_2, \ldots, r_n) \in R^n \mid g(\mathbf{r}) = 0 \text{ for all } g \in I\}. \tag{1}$$

In particular, let $Z := \mathbb{V}(I)(\Bbbk)$. Then $Z \subseteq \Bbbk^n$ is, by definition, a closed subset in the Zariski topology on affine n-space $\Bbbk^n$. Denote by $\Bbbk[Z]$ the finitely generated $\Bbbk$-algebra

$$\Bbbk[Z] := \Bbbk[x_1, \ldots, x_n]/I.$$

We recall that a $\Bbbk$-algebra $R \in \mathsf{Alg}_{\Bbbk}$ is a **reduced $\Bbbk$-algebra** if it contains no nilpotent elements [6, §2.1]. If R is finitely generated and $R = \Bbbk[x_1, \ldots, x_n]/I$ with $I \trianglelefteq \Bbbk[x_1, \ldots, x_n]$, then R is reduced

if and only if I is a **radical ideal** i.e. $I = \mathrm{rad}(I)$ where

$$\mathrm{rad}(I) := \{f \in \Bbbk[x_1, \ldots, x_n] \mid f^n \in I \text{ for some } n > 0\}.$$

Definition 4.1. Let be an ideal $I \trianglelefteq \Bbbk[x_1, \ldots, x_n]$. We say that the Zariski closed subset

$$Z = \mathbb{V}(I)(\Bbbk) \subseteq \Bbbk^n$$

is an **affine $\Bbbk$-variety** if I is a radical ideal. The reduced $\Bbbk$-algebra

$$\Bbbk[Z] = \Bbbk[x_1, \ldots, x_n]/I$$

is called the **coordinate ring** of the variety Z.

Remark 4.2. If $Z = \mathbb{V}(I)(\Bbbk) \subseteq \Bbbk^n$ is the zero locus of an ideal I that is not radical, then Z corresponds to the set of geometric points of the finite-type affine $\Bbbk$-scheme $\mathrm{Spec}(\Bbbk[x_1, \ldots, x_n]/I)$.

The general linear group $\mathrm{GL}_n(\Bbbk)$ as an affine variety The main example of an affine $\Bbbk$-variety appearing throughout this thesis is the group $\mathrm{GL}_n(\Bbbk)$ of $n \times n$ invertible matrices with entries in a field. Identify the set of $n \times n$ matrices with the affine space $\Bbbk^{n^2}$:

$$\begin{aligned}\mathrm{Mat}_n(\Bbbk) &= \{(a_{ij}) \mid a_{ij} \in \Bbbk, 1 \leq i, j \leq n\} \\ &= \Bbbk^{n^2}.\end{aligned}$$

Then the determinant function $\det\colon \mathrm{Mat}_n(\Bbbk) \to \Bbbk$ becomes a homogeneous degree n polynomial in the n^2 variables (x_{ij}):

$$\det(x_{ij}) \in \Bbbk[(x_{ij})].$$

In the next proposition, we analyze the zero locus of the polynomial of $n^2 + 1$ variables $y \det(x_{ij}) - 1 \in \Bbbk[(x_{ij}), y]$.

Proposition 4.3. *Denote by* $\mathrm{GL}_n(\Bbbk) := \{(a_{ij}) \in \mathrm{Mat}_n(\Bbbk) \mid \det(a_{ij}) \neq 0\}$ *the set of* $n \times n$ *invertible matrices with entries in* $\Bbbk$.

1. *The function*

$$\gamma\colon \mathrm{GL}_n(\Bbbk) \to \Bbbk^{n^2+1}, \quad \gamma(a_{ij}) := \left(a_{ij}, \det(a_{ij})^{-1}\right)$$

is injective, and its image is the Zariski closed subset

$$Z := \mathbb{V}(\langle\, y \det(x_{ij}) - 1 \,\rangle).$$

2. *The above identification with Z gives $\mathrm{GL}_n(\Bbbk)$ the structure of an affine $\Bbbk$-variety with coordinate ring*

$$\Bbbk[\mathrm{GL}_n] := \Bbbk[(x_{ij}), y]/\big\langle y \det(x_{ij}) - 1 \big\rangle.$$

Proof.

1. Observe that the function γ is just the embedding of the graph of the composition of the matrix inverse function $(a_{ij}) \mapsto (a_{ij})$ with the determinant into $\Bbbk^{n^2+1}$.

2. We need to show $\Bbbk[\mathrm{GL}_n]$ is a reduced $\Bbbk$-algebra, i.e. that the ideal $\big\langle g \big\rangle$, where $g := y \det(x_{ij}) - 1$ is radical. Since every prime ideal is a radical ideal, and a polynomial in $\Bbbk[\mathrm{GL}_n]$ is prime if and only if it is irreducible, it suffices to show that g is irreducible.

   We first prove that $\det(x_{ij}) \in \Bbbk[(x_{ij})]$ is an irreducible polynomial via an induction argument on n, the number of variables in $\det(x_{ij})$. The base case is obvious. Let $n > 1$, and suppose the polynomial $\det(u_{k\ell})$ in $n-1$ variables $\{u_{k\ell}\}_{1 \le k,\ell \le n-1}$ is irreducible. For $i, j = 1, \ldots, n$, let X_{ij} denote the (i,j)-minor of the matrix (x_{ij}). Then each $\det X_{ij}$ is the determinant polynomial in $n-1$-variables and therefore irreducible by the induction hypothesis. Note further that $\det X_{ij}$ cannot be a multiple of $\det X_{i'j'}$ if $X_{ij} \neq X_{i'j'}$. Now expand $\det(x_{ij})$ across the first row

$$\det(x_{ij}) = x_{11} \det X_{11} - x_{12} \det X_{12} + \cdots + (-1)^{n+1} x_{1n} \det X_{1n}.$$

   The right hand side is linear in the variables $x_{11}, x_{12}, \ldots, x_{1n}$ none of which appear in any of the polynomials $\det X_{ij}$. Hence, if $\det(x_{ij})$ has a non-trivial factorization, then the polynomials $\det X_{ij}$ have a non-trivial common divisor, which is impossible.

   Now returning to $g = y \det(x_{ij}) - 1$, we work in the ring $\Bbbk[y][x_{ij}]$ of polynomials in the variables x_{ij} with coefficients in $\Bbbk[y]$. Suppose f, h give a non-trivial factorization $g = fh$. Write $f = \sum_{d \ge 0} f_d$ and $h = \sum_{d \ge 0} h_d$ for the decomposition of f and h into homogeneous pieces (with respect to degree in x_{ij}'s). Note that $g \in \Bbbk[y][x_{ij}]$ is concentrated in homogeneous degrees n

and 0. Then $f_0 h_0 = -1$ and for $1 \leq k \leq n-1$, $\sum_{d=0}^{k} f_{k-d} h_d = 0$. Substitution then shows that the degree n term $\sum_{d=0}^{n} f_{k-d} h_d$ is a non-trivial factorization of $y \det(x_{ij})$. This contradicts the fact that $\det(x_{ij})$ is irreducible. Hence g is irreducible.

□

Remark 4.4. For any field $\Bbbk$, the **vanishing ideal** $\mathbb{I}(S) \trianglelefteq \Bbbk[x_1, \ldots, x_n]$ of a subset $S \subseteq \Bbbk^n$ is the radical ideal

$$\mathbb{I}(S) := \{f \in \Bbbk[x_1, \ldots, x_n] \mid f(\mathbf{a}) = 0 \; \forall \mathbf{a} \in S\}$$

Clearly $S \subseteq \mathbb{V}(\mathbb{I}(S))$, and it is easy to see that $\mathbb{V}(\mathbb{I}(S))$ the Zariski closure of S. In particular, for any ideal $J \trianglelefteq \Bbbk[x_1, \ldots, x_n]$, we have $\mathbb{V}(J) = \mathbb{V}(\mathbb{I}(J))$.

If $\Bbbk$ is algebraically closed, then Hilbert's *Nullstellensatz* implies that $\mathrm{rad}(J) = \mathbb{I}(\mathbb{V}(J))$ for any ideal $J \trianglelefteq \Bbbk[x_1, \ldots, x_n]$. If $\Bbbk \neq \bar{\Bbbk}$, then the strict containment $\mathrm{rad}(J) \subsetneq \mathbb{I}(\mathbb{V}(J))$ is possible, e.g. take J to be the maximal ideal $\langle x^2 + 1 \rangle \trianglelefteq \mathbb{R}[x]$.

4.1.2 The functor of points for an affine variety

A $\Bbbk$-algebra morphism $\phi\colon R \to R'$ in $\mathsf{Alg}_{\Bbbk}$ extends uniquely to a morphism between polynomial rings $\tilde{\phi}\colon R[x_1, \ldots, x_n] \to R'[x_1, \ldots, x_n]$ with the property that $\tilde{\phi}(f) = f$ for all $f \in \Bbbk[x_1, \ldots, x_n]$.

It then follows that for any ideal $I \trianglelefteq \Bbbk[x_1, \ldots, x_n]$, we can functorially assign to each morphism $\phi\colon R \to R'$ in $\mathsf{Alg}_{\Bbbk}$ a function between the corresponding sets in (1)

$$\mathbb{V}(I)(R) \to \mathbb{V}(I)(R'), \quad (r_1, r_2, \ldots, r_n) \mapsto (\phi(r_1), \phi(r_2), \ldots, \phi(r_n)).$$

Definition 4.5. The **functor of points** of an affine $\Bbbk$-variety $Z = \mathbb{V}(I) \subseteq \Bbbk^n$ is the functor

$$\mathbb{V}(I)(-)\colon \mathsf{Alg}_{\Bbbk} \to \mathsf{Set}, \quad R \mapsto \mathbb{V}(I)(R)$$

The elements of the set $\mathbb{V}(I)(R)$ are called the R**-points** of the variety Z.

Let $I \trianglelefteq \Bbbk[x_1, \ldots, x_n]$ be an ideal and $\Bbbk[Z] = \Bbbk[x_1, \ldots, x_n]/I$. Let $\pi_Z\colon \Bbbk[x_1, \ldots, x_n] \to \Bbbk[Z]$ denote the canonical surjection. Then for any $R \in \mathsf{Alg}_{\Bbbk}$, we have a function induced by precompo-

sition by π_Z:

$$\pi_Z^*(R)\colon\ \hom_{\mathsf{Alg}_{\Bbbk}}(\Bbbk[Z], R) \to \hom_{\mathsf{Alg}_{\Bbbk}}(\Bbbk[x_1, \ldots, x_n], R), \quad \pi_Z^*(R)(\alpha) := \pi_Z \circ \alpha.$$

Proposition 4.6. *Let $I \trianglelefteq \Bbbk[x_1, \ldots, x_n]$ be an ideal, and let $\Bbbk[Z]$ be the $\Bbbk$-algebra as above.*

1. *For every $R \in \mathsf{Alg}_{\Bbbk}$, the function $\Theta(R)\colon\ \hom_{\mathsf{Alg}_{\Bbbk}}(\Bbbk[x_1, \ldots, x_n], R) \to R^n$ defined as*

$$\Theta(R)(\alpha) := \big(\alpha(x_1), \alpha(x_2), \ldots, \alpha(x_n)\big)$$

   is a bijection of sets.

2. *For every $R \in \mathsf{Alg}_{\Bbbk}$, the composition of functions*

$$\Theta(R) \circ \pi_Z^*(R)\colon\ \hom_{\mathsf{Alg}_{\Bbbk}}(\Bbbk[Z], R) \to R^n$$

   is injective with image

$$\operatorname{im}(\Theta(R) \circ \pi_Z^*(R)) = \mathbb{V}(I)(R).$$

   In particular, for $R = \Bbbk$, the above gives a bijection of sets

$$\hom_{\mathsf{Alg}_{\Bbbk}}(\Bbbk[Z], \Bbbk) \cong Z.$$

Proof.

1. $\Bbbk[x_1, \ldots, x_n]$ is the free commutative $\Bbbk$-algebra generated by the $\Bbbk$-vector space $V := \operatorname{span}_{\Bbbk}\{x_1, x_2, \ldots, x_n\}$. Hence, restriction of a $\Bbbk$-algebra morphism $\alpha\colon\ \Bbbk[x_1, \ldots, x_n] \to R$ to its generators induces a one-to-one correspondence

$$\hom_{\mathsf{Alg}_{\Bbbk}}(\Bbbk[x_1, \ldots, x_n], R) \xrightarrow{\cong} \hom_{\Bbbk}(V, R)$$

   where $\hom_{\Bbbk}(V, R)$ denotes the $\Bbbk$-vector space of $\Bbbk$-linear maps from V into R. Composing the above bijection with the canonical $\Bbbk$-linear isomorphism

$$\hom_{\Bbbk}(V, R) = \hom_{\Bbbk}\big(\bigoplus_{i=1}^{n} \Bbbk x_i, R\big) \cong \bigoplus_{i=1}^{n} \hom_{\Bbbk}(\Bbbk, R) \cong R^n$$

   provides the inverse to the function $\Theta(R)$.

2. To show injectivity of $\Theta(R) \circ \pi_Z^*(R)$, we only need to verify that $\pi^*(R)$ is injective, which follows immediately from the fact that $\pi_Z \colon \Bbbk[x_1, \ldots, x_n] \to \Bbbk[Z]$ is surjective.

   Next we prove $\operatorname{im}\big(\Theta(R) \circ \pi_Z^*(R)\big) = \mathbb{V}(I)(R)$. For each $i = 1, \ldots, n$, let $\bar{x}_i := \pi_Z(x_i)$. Let $g \in \Bbbk[x_1, \ldots, x_n]$ be a polynomial which we write in multi-index notation

   $$g(x_1, \ldots, x_n) = \sum_{\vec{i}} a_{\vec{i}} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}, \quad \vec{i} := (i_1, i_2, \ldots, i_n) \in \mathbb{N}_0^n, \quad a_{\vec{i}} \in \Bbbk.$$

   Then, since π_Z is a $\Bbbk$-algebra morphism, we have the equality

   $$\pi_Z(g) = \sum_{\vec{i}} a_{\vec{i}} \bar{x}_1^{i_1} \bar{x}_2^{i_2} \cdots \bar{x}_n^{i_n}.$$

   To show $\operatorname{im}\big(\Theta(R) \circ \pi_Z^*(R)\big) \subseteq \mathbb{V}(I)(R)$, let $\beta \colon \Bbbk[Z] \to R$ be a $\Bbbk$-algebra morphism, and let

   $$\mathbf{r} = \big(\Theta(R) \circ \pi_Z^*(R)\big)(\beta) = (\beta(\bar{x}_1), \beta(\bar{x}_2), \ldots, \beta(\bar{x}_n)) \in R^n.$$

   Let $g \in I \trianglelefteq \Bbbk[x_1, \ldots, x_n]$. Evaluation of g with $\mathbf{r}$ gives:

   $$\begin{aligned} g(\mathbf{r}) &= \sum_{\vec{i}} a_{\vec{i}} r_1^{i_1} r_2^{i_2} \cdots r_n^{i_n} \\ &= \sum_{\vec{i}} a_{\vec{i}} \beta(\pi_Z(x_1^{i_1})) \beta(\pi_Z(x_2^{i_2})) \cdots \beta(\pi_Z(x_n^{i_n})) \\ &= \beta\big(\pi_Z\big(g(x_1, x_2, \ldots, x_n)\big)\big) \\ &= 0, \end{aligned}$$

   where the last equality follows from the fact that $I = \ker \pi_Z$. Hence $\mathbf{r} \in \mathbb{V}(I)(R)$.

   For the other containment, suppose $\mathbf{r} \in \mathbb{V}(I)(R)$, and let $\alpha \colon \Bbbk[x_1, \ldots, x_n] \to R$ be the unique $\Bbbk$-algebra morphism such that $\alpha(x_i) = r_i$ for each $i = 1, \ldots, n$. Then $g(\mathbf{r}) = 0$ for all $g \in R$ implies that $\alpha(g) = 0$, since α is an algebra morphism. Hence $I \subseteq \ker \alpha$, and so there exists a unique $\Bbbk$-algebra morphism $\beta \colon \Bbbk[Z] \to R$ such that $\beta \circ \pi_Z = \alpha$. Therefore

   $$\Theta(R) \circ \pi_Z^*(R)(\beta) = \Theta(R)(\beta \circ \pi_Z) = \Theta(R)(\alpha) = \mathbf{r}.$$

   Hence, $\mathbf{r} \in \operatorname{im}\big(\Theta(R) \circ \pi_Z^*(R)\big)$, and this completes the proof.

□

Corollary 4.7. *The functor of points* $\mathbb{V}(I)(-)\colon \mathsf{Alg}_{\Bbbk} \to \mathsf{Set}$ *of an affine* $\Bbbk$*-variety* $Z = \mathbb{V}(I) \subseteq \Bbbk^n$ *is represented by its coordinate ring* $\Bbbk[Z]$.

Proof. The bijective function $\Theta(R) \circ \pi_Z^*(R)\colon \ \hom_{\mathsf{Alg}_{\Bbbk}}(\Bbbk[Z], R) \to \mathbb{V}(I)(R)$ from Prop. 4.6 defines a natural isomorphism of functors

$$\Theta \circ \pi_Z^*\colon h_{\Bbbk[Z]}(-) \xrightarrow{\cong} \mathbb{V}(I)(-).$$

□

Corollary 4.8. *The functor* $\mathrm{GL}_n\colon \mathsf{Alg}_{\Bbbk} \to \mathsf{Set}$ *defined as*

$$\mathrm{GL}_n(R) := \{(a_{ij}) \in \mathrm{Mat}_n(R) \mid \det(a_{ij}) \neq 0\}$$

is isomorphic to the functor of points of the affine $\Bbbk$*-variety* $\mathrm{GL}_n(\Bbbk)$.

Proof. Follows from combining Cor. 4.3 with Cor. 4.7. □

Theorem 4.9. *Let* $I, J \trianglelefteq \Bbbk[x_1, \ldots, x_n]$ *be ideals. If* $F\colon \mathsf{Alg}_{\Bbbk} \to \mathsf{Set}$ *is a functor such that* $F(R) = \mathbb{V}(I)(R) \cap \mathbb{V}(J)(R)$ *for all* $R \in \mathsf{Alg}_{\Bbbk}$*, then* F *is represented by the finitely generated* $\Bbbk$*-algebra* $\Bbbk[x_1, \ldots, x_n]/(I + J)$.

Proof. The equality $F(R) = \mathbb{V}(I)(R) \cap \mathbb{V}(J)(R)$ for all R implies that $F(-) = \mathbb{V}(I+J)(-)$. As in the proof of Cor. 4.7, we deduce from Prop. 4.6 that F is represented by $\Bbbk[x_1, \ldots, x_n]/(I + J)$. □

Remark 4.10. Recall that if $I, J \trianglelefteq \Bbbk[x_1, \ldots, x_n]$ are radical ideals then $I + J$ need not be radical. Hence, if $F\colon \mathsf{Alg}_{\Bbbk} \to \mathsf{Set}$ is a functor satisfying $F(R) = \mathbb{V}(I)(R) \cap \mathbb{V}(J)(R)$ as in Thm. (4.9) above, then $F(\Bbbk)$ need not be an affine variety, even if both $\mathbb{V}(I)(\Bbbk)$ and $\mathbb{V}(J)(\Bbbk)$ are affine varieties.

4.2 Algebraic group schemes

Definition 4.11. Let $\Bbbk$ be a field. A **group-scheme** defined over $\Bbbk$ is a functor $G\colon \mathsf{Alg}_{\Bbbk} \to \mathsf{Grp}$. An **affine group-scheme** defined over $\Bbbk$ is a group scheme $G\colon \mathsf{Alg}_{\Bbbk} \to \mathsf{Grp}$ which is representable as a functor $\mathsf{Alg}_{\Bbbk} \to \mathsf{Set}$. An **algebraic group-scheme** defined over $\Bbbk$ is an affine group-scheme G which is represented by a finitely generated $\Bbbk$-algebra A. Furthermore, if A is reduced, we say that G is an **algebraic group** defined over $\Bbbk$.

4.2.1 The algebraic group $\mathrm{GL}(V)$

Theorem 4.12. *Let V be a finite dimensional $\Bbbk$-vector space, with $\dim_{\Bbbk} V = n$. The group scheme $\mathrm{GL}(V)\colon \mathsf{Alg}_{\Bbbk} \to \mathsf{Grp}$ given by $\mathrm{GL}(V)(R) := \mathrm{GL}(V \otimes_{\Bbbk} R)$ is an algebraic group.*

Proof. By choosing a basis for V we see that $\mathrm{GL}(V)$ is naturally isomorphic to GL_n. Hence, it suffices to show GL_n is an algebraic group, which follows immediately from Cor. 4.8. □

The following proposition will play an important role in Sec 7 when generalizing cohomological Hilbert's Theorem 90 to arbitrary Galois extensions.

Proposition 4.13 (Ex III.7.19 (2) [1])**.** *Let A be a finite dimensional $\Bbbk$-algebra. Then the functor $\mathrm{GL}_1(A)\colon \mathsf{Alg}_{\Bbbk} \to \mathsf{Grp}$ given by $\mathrm{GL}_1(A)(R) = (A \otimes_{\Bbbk} R)^{\times}$ is an algebraic group scheme.*

4.2.2 The algebraic group scheme $\mathrm{Aut}(A)$

Theorem 4.14. *Let A be a finite dimensional (not necessarily commutative) $\Bbbk$-algebra, with $\dim_{\Bbbk} A = n$. The functor $\mathrm{Aut}(A)\colon \mathsf{Alg}_{\Bbbk} \to \mathsf{Grp}$ defined as*

$$\mathrm{Aut}(A)(R) := \mathrm{Aut}_{\mathrm{Alg}_R}(A \otimes_{\Bbbk} R)$$

is an algebraic group scheme.

Proof. Let $R \in \mathsf{Alg}_{\Bbbk}$ and let $\phi \in \mathrm{Aut}(A)(R)$. Then $\phi\colon A \otimes_{\Bbbk} R \to A \otimes_{\Bbbk} R$ is a ring homomorphism that is also a R-module isomorphism and therefore belongs to $\mathrm{GL}(A)(R)$. From Thm. 4.12 we have $\mathrm{GL}(A)(-) \cong \mathbb{V}(I)(-)$, where

$$I = \langle y \det(x_{ij}) - 1 \rangle \trianglelefteq \Bbbk[y, x_{ij}].$$

In what follows, we will construct an ideal $J \trianglelefteq \Bbbk[y, x_{ij}]$ such that for all $R \in \mathsf{Alg}_{\Bbbk}$

$$\mathrm{Aut}(A)(R) = \mathbb{V}(J)(R) \cap \mathbb{V}(I)(R).$$

Then Thm. 4.9 will imply that $\mathrm{Aut}(A)$ is an algebraic group scheme.

So let $\phi \in \mathrm{Aut}(A)(\Bbbk) = \mathrm{Aut}_{\mathsf{Alg}_{\Bbbk}}(A)$. Let $\{e_i\}_{i=1}^n$ be a $\Bbbk$-linear basis for A. Then for all

$i = 1, \ldots, n$

$$\phi(e_i) = \sum_{j=1}^{n} b_{ij} e_j$$

where each $b_{ij} \in \Bbbk$. Since $\phi\colon A \to A$ is a $\Bbbk$-linear isomorphism in $\mathrm{GL}(A)(\Bbbk)$, the matrix (b_{ij}) is a point in the affine variety $\mathrm{GL}(A)(\Bbbk) = \mathbb{V}(I)(\Bbbk)$. The basis $\{e_i\}_{i=1}^n$ for A also induces a basis $\{e_\ell \otimes e_k\}_{\ell,k=1}^n$ for $A \otimes_\Bbbk A$. Let $\mu\colon A \otimes_\Bbbk A \to A$ denote the associative product on A. For each $\ell, k = 1, \ldots, n$ we have

$$\mu(e_\ell \otimes e_k) = \sum_{s=1}^{n} c_{\ell k s} e_s$$

where each $c_{\ell k s} \in \Bbbk$. Since ϕ is compatible with the product μ, we have for each $\ell, k = 1, \ldots, n$

$$\phi(\mu(e_\ell \otimes e_k)) - \mu(\phi(e_\ell) \otimes \phi(e_k)) = 0. \tag{2}$$

On the other hand:

$$\begin{aligned}
\phi(\mu(e_\ell \otimes e_k)) - \mu(\phi(e_\ell) \otimes \phi(e_k)) &= \sum_{s=1}^{n} c_{\ell k s} \phi(e_s) - \mu\left(\sum_{s=1}^{n} b_{\ell s} b_{k s} (e_s \otimes e_s)\right) \\
&= \sum_{s=1}^{n} \sum_{j=1}^{n} c_{\ell k s} b_{sj} e_j - \sum_{s=1}^{n} b_{\ell s} b_{k s} \mu(e_s \otimes e_s) \\
&= \sum_{j=1}^{n} \sum_{s=1}^{n} (c_{\ell k s} b_{sj} - b_{\ell s} b_{k s} c_{ssj}) e_j.
\end{aligned}$$

Hence, since $\{e_i\}_{i=1}^n$ is a basis, Eq. 2 implies that for each $j = 1, \ldots, n$, the matrix $(b_{ij}) \in \mathrm{GL}(A)(\Bbbk)$ satisfies the equation

$$\sum_{j=1}^{n} c_{\ell k s} b_{sj} - b_{\ell s} b_{k s} c_{ssj} = 0.$$

In other words, $\phi\colon A \to A$ is an automorphism of $\Bbbk$-algebras if and only if $(b_{ij}) \in \mathrm{GL}(A)(\Bbbk) \cap \mathbb{V}(J)(\Bbbk)$, where

$$J = \left\langle \{P_{\ell k}^s(y, x_{ij}) \mid s = 1, \ldots, n\} \right\rangle \trianglelefteq \Bbbk[y, x_{ij}]$$

and $\{P_{\ell k}^s\}$ are the quadratic polynomials

$$P_{\ell k}^s(y, x_{ij}) := -\sum_{j=1}^{n} \big(c_{ssj} x_{\ell s} x_{k s} - c_{\ell k s} x_{sj}\big)$$

Finally, observe that for any $R \in \mathsf{Alg}_\Bbbk$, the tensors $\{e_i \otimes 1\}_{i=1}^n$ are a basis for the R-algebra $A \otimes_\Bbbk R$,

and this extends to a basis on the free R-module $(A \otimes_{\Bbbk} R) \otimes_R (A \otimes_{\Bbbk} R)$. Hence, the same calculation as the one above shows that

$$\mathrm{Aut}(A)(R) = \mathrm{GL}(A)(R) \cap \mathbb{V}(J)(R),$$

and this completes the proof. $\square$

5 Galois cohomology

In this section, we present the abstract framework needed to define Galois cohomology, beginning with an exposition of profinite group cohomology, as developed by Serre (see [4].) We explain how a short exact sequence $1 \to H \to G \to S \to 1$ of Γ-sets for a profinite group Γ under certain conditions induces a long exact sequence in cohomology, a key result which allows us to deduce a bijection between the orbit set S^Γ/G^Γ and the kernel of the map $H^1(\Gamma, H) \to H^1(\Gamma, G)$. The bijection is a fundamental ingredient in the proof of the Galois descent lemma in Section 6.3.

5.1 Profinite group cohomology

Throughout this section we fix a profinite group Γ. We will use the notation "$\bullet$" to denote a Γ action and "$\cdot$" to denote multiplication in a not necessarily abelian group A.

5.1.1 Cohomology sets

Definition 5.1. A left action of Γ on a set A is **continuous** if for all $a \in A$, the set

$$\mathrm{Stab}_\Gamma(a) = \{\sigma \in \Gamma \mid \sigma \bullet a = a\}$$

is an open subgroup of Γ. Note that the definition is equivalent to asking for the assignment $\Gamma \times A \to A$ given by $(\sigma, a) \mapsto \sigma \bullet a$ to be continuous, i.e., the usual notion of continuous action. Sets with a continuous left action of Γ are called Γ-**sets**. A group A which is also a Γ-set is called a Γ-**group** if Γ acts by group homomorphisms, meaning

$$\sigma \bullet (a_1 a_2) = (\sigma \bullet a_1) \cdot (\sigma \bullet a_2) \text{ for all } \sigma \in \Gamma,\ a_1, a_2 \in A.$$

Furthermore, if A is abelian then A is called a Γ-**module**. We denote by $\mathbf{Set}_\Gamma$ the category of left Γ-sets. Similarly, $\mathbf{Grp}_\Gamma$ and $\mathbf{Mod}_\Gamma$ denote the categories of left Γ-groups and left Γ-modules, respectively. In what follows, we use $\mathcal{C}_\Gamma$ to denote the category Set_Γ, Grp_Γ or Mod_Γ. A **morphism** of $\mathcal{C}_\Gamma$ is a morphism $f\colon A \to A'$ of $\mathcal{C}$ such that

$$f(\sigma \bullet a) = \sigma \bullet f(a) \text{ for all } \sigma \in \Gamma,\ a \in A.$$

Below we give two simple examples of a Γ-set, and an example of a Γ-module.

Example 5.2.

1. Assume Γ is a finite group. Then any set A on which Γ acts on the left is a Γ-set.

2. Any set A on which Γ acts trivially is a Γ-set.

3. Let $\Omega/\Bbbk$ be a Galois extension, and $\mathcal{G}_\Omega = \mathrm{Gal}(\Omega/\Bbbk)$. Then the map

$$\begin{aligned} \mathcal{G}_\Omega \times \Omega &\longrightarrow \Omega \\ (\sigma, x) &\longmapsto \sigma(x) \end{aligned}$$

   endows Ω with the structure of a $\mathcal{G}_\Omega$-module.

Lemma 5.3. *Let A be set equipped with a left Γ-action. Then the action of Γ on A is continuous if and only if*

$$\bigcup_{U \in \mathcal{N}} A^U$$

where $\mathcal{N}$ denotes the set of open normal subgroups of Γ.

Proof. First suppose the action of Γ on A is continuous and let $a \in A$. Then by Proposition 5.1 $\mathrm{Stab}_\Gamma(a)$ is an open subgroup of Γ. Since Γ is profinite, all open subgroups of Γ are closed and are therefore profinite. Moreover, since $\mathrm{Stab}_\Gamma(a)$ contains 1, there exists $U \in \mathcal{N}$ such that $U \subseteq \mathrm{Stab}_\Gamma(a)$. Hence $a \in A^U$. Since $A^U \subset A$ for all $U \in \mathcal{N}$, it follows that

$$A = \bigcup_{U \in \mathcal{N}} A^U.$$

Now assume that the above equality holds, and let $a \in A$. Then there exists $U \in \mathcal{N}$ such that $a \in A^U$, and hence for all $\sigma \in U$ we have $\sigma \cdot a = a$. Let $\tau \in \mathrm{Stab}_\Gamma(a)$. Then for all $\sigma \in U$, $\tau\sigma \cdot a = \tau a = a$. Therefore $\tau U \subseteq \mathrm{Stab}_\Gamma(a)$ for all $\tau \in \mathrm{Stab}_\Gamma(a)$. Since $1 \in U$ we have that $\mathrm{Stab}_\Gamma(a) \subseteq \bigcup_{\tau \in \mathrm{Stab}_\Gamma(a)} \tau U$. Hence we have shown that

$$\mathrm{Stab}_\Gamma(a) = \bigcup_{\tau \in \mathrm{Stab}_\Gamma(a)} \tau U.$$

Since each τU is open it follows that $\mathrm{Stab}_\Gamma(a)$ is open. □

Definition 5.4.

1. Let $A \in \mathsf{Set}_\Gamma$. We set
$$H^0(\Gamma, A) := A^\Gamma$$
where A^Γ is the set of fixed points of A. If $A \in \mathsf{Grp}_\Gamma$, this is a subgroup of A. The set $H^0(\Gamma, A)$ is called the $0th$ **cohomology set of** Γ **with coefficients in** A.

2. Let $A \in \mathsf{Grp}_\Gamma$. A **1-cocycle** of Γ with values in A is a continuous map $\alpha\colon \Gamma \to A$ such that
$$\alpha(\sigma\tau) = \alpha(\sigma) \cdot (\sigma \bullet \alpha(\tau)) \text{ for all } \sigma, \tau \in \Gamma.$$
We denote by $Z^1(\Gamma, A)$ the set of all 1-cocycles of Γ with values in A. The constant map $\Gamma \to A$ which assigns each $\sigma \in \Gamma$ to $1 \in A$ is an element of $Z^1(\Gamma, A)$. This map is called the **trivial** cocycle. For any 1-cocycle α we have that $\alpha(1) = 1$.

Lemma 5.5. *Let $A \in \mathsf{Grp}_\Gamma$ and let $\alpha\colon \Gamma \to A$ be a 1-cocycle. Then for all $a \in A$, the map*
$$\begin{aligned} \alpha'\colon \Gamma &\longrightarrow A \\ \sigma &\longmapsto a \cdot \alpha(\sigma) \cdot (\sigma \bullet a^{-1}) \end{aligned}$$
is also a 1-cocycle.

Proof. Let $\sigma, \tau \in \Gamma$. Then by definition
$$\alpha'(\sigma) \cdot (\sigma \bullet \alpha'(\tau)) = (a \cdot \alpha(\sigma) \cdot (\sigma \bullet a^{-1})) \cdot (\sigma \bullet (a \cdot \alpha(\tau) \cdot (\tau \bullet a^{-1}))).$$
Since $A \in \mathsf{Grp}_\Gamma$, Γ acts on A by group automorphisms. Hence
$$\alpha'(\sigma) \cdot (\sigma \bullet \alpha'(\tau)) = a \cdot \alpha(\sigma) \cdot (\sigma \bullet \alpha(\tau)) \cdot (\sigma\tau \bullet a^{-1}) = a \cdot \alpha(\sigma\tau) \cdot (\sigma\tau \bullet a^{-1}) = \alpha'(\sigma\tau).$$
It remains to show that $\alpha'\colon \Gamma \to A$ is continuous. Let V be an open subset of A. In order to show that $\alpha'^{-1}(V)$ is open in Γ we will show that $\alpha'^{-1}(\{v\})$ is open for all $v \in V$, since
$$\alpha'^{-1}(V) = \bigcup_{v \in V} \alpha'^{-1}(\{v\}).$$
If v is not in the image of α', then $\alpha'^{-1}(\{v\}) = \emptyset$ is open. So we assume that $\alpha'^{-1}(\{v\})$ is nonempty. Therefore there exists $\sigma \in \Gamma$ such that $\alpha'(\sigma) = v$. Note that $\{1\}$ is open in A. Then since α is a

1-cocycle and is therefore continuous, we have that $\alpha^{-1}(\{1\})$ is open in Γ. Moreover, since Γ acts continuously on A, $\mathrm{Stab}_\Gamma(a)$ is an open subgroup of Γ. Hence $U = \alpha^{-1}(\{1\}) \cap \mathrm{Stab}_\Gamma(a)$ is open in Γ, and thus σU is also open in Γ. Let $\tau \in U$. Then $\alpha(\tau) = 1$ and $\tau \cdot a = a$. Therefore

$$\begin{aligned}\alpha'(\sigma\tau) &= a \cdot \alpha(\sigma\tau) \cdot (\sigma\tau \cdot a^{-1}) = a \cdot \alpha(\sigma) \cdot (\sigma \cdot \alpha(\tau)) \cdot (\sigma\tau \cdot a^{-1}) \\ &= a \cdot \alpha(\sigma) \cdot (\sigma\tau \cdot a^{-1}) = a \cdot \alpha(\sigma) \cdot (\sigma \cdot a^{-1}) = \alpha'(\sigma) = v.\end{aligned}$$

This shows that $\sigma U \subseteq \alpha'^{-1}(\{v\})$. Since the collection $\{\sigma U \mid U \text{ open in } \Gamma\}$ is a basis of open neighborhoods of σ, it follows that $\alpha'^{-1}(\{v\})$ is open. □

Definition 5.6. Two 1-cocycles α and α' are **cohomologous** if there exists $a \in A$ satisfying

$$\alpha'(\sigma) = a \cdot \alpha(\sigma) \cdot (\sigma \cdot a^{-1}) \text{ for all } \sigma \in \Gamma.$$

In this case we write $\alpha \sim \alpha'$.

Since $A \in \mathsf{Grp}_\Gamma$, then Γ acts on A by group automorphisms. Therefore

$$(\sigma \cdot a)^{-1} = \sigma \cdot (a^{-1})$$

so the notation $\sigma \cdot a^{-1}$ in the above definition is unambiguous. Moreover, one can easily show that $\sim$ is an equivalence relation on $Z^1(\Gamma, A)$.

Definition 5.7. Let Γ be a profinite group, and let $A \in \mathsf{Grp}_\Gamma$. We denote by $H^1(\Gamma, A)$ the quotient set

$$H^1(\Gamma, A) = Z^1(\Gamma, A)/\sim .$$

This set is called the **first cohomology set of** Γ **with coefficients in** A.

Remark 5.8.

1. For $A \in \mathsf{Grp}_\Gamma$, pointwise multiplication of functions generally does not give $Z^1(\Gamma, A)$ a group structure, and therefore does not induce a group structure on $H^1(\Gamma, A)$ in general. The class of the trivial cocycle is a basepoint of $H^1(\Gamma, A)$, making it a pointed set. However, if $A \in \mathsf{Mod}_\Gamma$ then $Z^1(\Gamma, A)$ is an abelian group with respect to pointwise multiplication and induces an abelian group structure on $H^1(\Gamma, A)$.

2. For $A \in \mathsf{Mod}_\Gamma$, higher cohomology $H^n(\Gamma, A)$ for $n \geq 2$ are the ordinary n^{th} cohomology groups of Γ with coefficients in A, but with continuous cocycles.

Definition 5.9. Let Γ, Γ' be profinite groups. Let $A \in \mathsf{Set}_\Gamma$ and $A' \in \mathsf{Set}_{\Gamma'}$. Moreover, let $\phi\colon \Gamma' \to \Gamma$ be a morphism of profinite groups (in particular, ϕ is continuous), and let $f\colon A \to A'$ be a map. If A and A' are groups, we require f to be a group homomorphism. We say that f and ϕ are **compatible** if

$$f(\phi(\sigma') \cdot a) = \sigma' \cdot f(a) \text{ for all } \sigma' \in \Gamma', a \in A$$

By the above definition, we have that if $a \in A^\Gamma = H^0(\Gamma, A)$ then $f(a) \in A'^{\Gamma'} = H^0(\Gamma', A')$. Hence by restriction f induces a map of pointed sets

$$f_*\colon H^0(\Gamma, A) \to H^0(\Gamma', A').$$

The following proposition shows that f also induces a map on degree 1 cohomology sets.

Proposition 5.10 (Prop II.3.19 [1])**.** *Let Γ, Γ', A, A' be as in Definition 5.9, and let $\phi\colon \Gamma' \to \Gamma$ and $f\colon A \to A'$ be compatible maps. For any 1-cocycle $\alpha \in Z^1(\Gamma, A)$, the map*

$$\begin{aligned} f_*(\alpha)\colon \Gamma' &\longrightarrow A' \\ \sigma &\longmapsto f(\alpha(\phi(\sigma))) \end{aligned}$$

is a 1-cocycle, and the map

$$\begin{aligned} f_*\colon H^1(\Gamma, A) &\longmapsto H^1(\Gamma', A') \\ [\alpha] &\longmapsto [f_*(\alpha)] \end{aligned}$$

is a well-defined map of pointed sets (resp. group homomorphism if A and A' are abelian).

Now we give two examples of an induced map on degree 1 cohomology we obtain from Prop. 5.10 for a morphism of profinite groups with a compatible map.

Example 5.11.

1. Assume $\Gamma = \Gamma'$ and $\phi = \mathrm{id}_\Gamma$. Then a compatible map $f\colon A \to A'$ is simply a morphism in $\mathcal{C}_\Gamma$ and f_* is the map

$$\begin{aligned} f_*\colon H^1(\Gamma, A) &\longrightarrow H^1(\Gamma, A') \\ [\alpha] &\longmapsto [f \circ \alpha]. \end{aligned}$$

Moreover, if $g\colon A' \to A''$ is a morphism in $\mathcal{C}_\Gamma$ then

$$(g \circ f)_*([\alpha]) = [(g \circ f) \circ \alpha] = [g \circ (f \circ \alpha)] = g_*([f \circ \alpha]) = g_*(f_*([\alpha])).$$

Therefore in this case $(g \circ f)_* = g_* \circ f_*$.

2. Assume $\Gamma = \Gamma'$. Let $A \in \mathsf{Grp}_\Gamma$, let $\rho \in \Gamma$ and set $\phi = \mathsf{Inn}(\rho)$. Define $f\colon A \to A$ by

$$\begin{aligned} f\colon A &\longrightarrow A \\ a &\longmapsto \rho^{-1} \cdot a \end{aligned}$$

Then f and ϕ are compatible and the induced map $f_*\colon H^1(\Gamma, A) \to H^1(\Gamma, A)$ is the identity.

Remark 5.12. From now on, if $f\colon A \to B$ is a morphism in $\mathcal{C}_\Gamma$, then f_* will denote the map on cohomology obtained when taking $\phi = \mathrm{id}_\Gamma$ as in Example 1 above.

Proposition 5.13 (Prop II.3.26 [1])**.** *Let $A_i \in \mathcal{C}_{\Gamma_i}$ for $i = 1, \ldots, 4$. Suppose the diagrams*

$$\begin{array}{ccc} A_1 & \xrightarrow{f_1} & A_2 \\ {\scriptstyle f_3}\downarrow & & \downarrow{\scriptstyle f_2} \\ A_4 & \xrightarrow[f_4]{} & A_3 \end{array} \qquad \begin{array}{ccc} \Gamma_1 & \xleftarrow{\phi_1} & \Gamma_2 \\ {\scriptstyle \phi_3}\uparrow & & \uparrow{\scriptstyle \phi_2} \\ \Gamma_4 & \xleftarrow[\phi_4]{} & \Gamma_3 \end{array}$$

are commutative, where for each $i = 1, \ldots, 4$, ϕ_i is a morphism of profinite groups compatible with f_i. Then the diagram

$$\begin{array}{ccc} H^1(\Gamma_1, A_1) & \xrightarrow{f_{1*}} & H^1(\Gamma_2, A_2) \\ {\scriptstyle f_{3*}}\downarrow & & \downarrow{\scriptstyle f_{2*}} \\ H^1(\Gamma_4, A_4) & \xrightarrow[f_{4*}]{} & H^1(\Gamma_3, A_3) \end{array}$$

is commutative.

The following theorem gives a useful characterization of profinite cohomology in terms of ordinary group cohomology.

Theorem 5.14 (Theorem II.3.33 [1])**.** *Let Γ be a profinite group, and let $A \in \mathsf{Grp}_\Gamma$. Then*

$$\varinjlim_{U \in \mathcal{N}} H^n(\Gamma/U, A^U) \cong H^n(\Gamma, A)$$

is an isomorphism of pointed sets, where $\mathcal{N}$ is the set of open normal subgroups of Γ.

5.1.2 Cohomology sequences

In ordinary group cohomology, there are useful results regarding exact sequences of G-modules, particularly the induced long exact sequence on cohomology obtained by via connecting maps. In this section we describe analogous results in the setting of profinite group cohomology.

Let $f\colon A \to B$ be a map of pointed sets. The **kernel** of f is the preimage the basepoint of B under f. A sequence $A \xrightarrow{f} B \xrightarrow{g} C$ is called **exact** at B if $\operatorname{im} f = \ker g$. A sequence of pointed sets

$$A_0 \longrightarrow A_1 \longrightarrow \cdots \longrightarrow A_{i-1} \longrightarrow A_i \longrightarrow A_{i+1} \longrightarrow \cdots$$

is called **exact** if it is exact at A_i for all $i \geq 1$. Then the sequence

$$B \xrightarrow{g} C \longrightarrow 1$$

is exact if and only if g is surjective, and the sequence

$$1 \longrightarrow A \xrightarrow{f} B$$

is exact if and only if f has trivial kernel.

Remark 5.15. It is important to note that f having trivial kernel only implies f is injective if A and B are groups.

Notation 5.16. In what follows we assume that we have an exact sequence

$$1 \longrightarrow H \hookrightarrow G \xrightarrow{\phi} S \longrightarrow 1$$

where $G \in \mathsf{Grp}_\Gamma$, H is a Γ-subgroup of G and $S \in \mathsf{Set}_\Gamma$. Then $S \cong G/H$ is a bijection where G/H are the left cosets.

Next we will define a map of pointed sets $S^\Gamma \to H^1(\Gamma, H)$. Let $x \in S^\Gamma$ and let $g \in G$ be any preimage of x under ϕ. Since $\sigma \cdot x = x$ for all $\sigma \in \Gamma$, then

$$\phi(\sigma \cdot g) = \sigma \cdot \phi(g) = \sigma \cdot x = x = \phi(g).$$

and hence for all $\sigma \in \Gamma$ there exists $h \in H$ such that $\sigma \cdot g = gh$, i.e. $h = g^{-1} \cdot (\sigma \cdot g)$. Therefore

if $\alpha\colon \Gamma \to A$ is a map, there is a unique element $\alpha(\sigma) \in H$ such that $\alpha(\sigma) = g^{-1} \cdot (\sigma \cdot g)$.

Lemma 5.17 (Lemma II.4.2 [1])**.** *The map $\alpha\colon \Gamma \to H$ is a 1-cocycle, and its class in $H^1(\Gamma, H)$ does not depend on the choice of $g \in G$.*

Therefore we have a well-defined map

$$\delta^0\colon S^\Gamma \longrightarrow H^1(\Gamma, H)$$

$$x \longmapsto [\alpha]$$

where α is the cocycle defined by

$$\alpha(\sigma) = g^{-1} \cdot (\sigma \cdot g) \text{ for all } \sigma \in \Gamma$$

for an arbitrary preimage $g \in G$ of x. The map δ^0 is called the $0th$ **connecting map**. By the assumption that ϕ is a morphism of pointed sets, the preimage of the basepoint $x_0 \in S^\Gamma$ under ϕ is the identity element $1_H \in H$. Since H is a Γ-group, Γ acts on H by group homomorphisms, and so $\sigma \cdot 1_H = \sigma \cdot (1_H 1_H) = (\sigma \cdot 1_H) \cdot (\sigma \cdot 1_H)$ for all $\sigma \in \Gamma$. Then it must be that $\sigma \cdot 1_H = 1_H$ for all $\sigma \in \Gamma$, hence under δ^0 the basepoint x_0 is assigned to the trivial class. Therefore δ^0 is a map of pointed sets.

Proposition 5.18 (Prop II.4.4 [1] (due to Borel-Serre [4]))**.** *We have an exact sequence*

$$1 \longrightarrow H^\Gamma \longrightarrow G^\Gamma \xrightarrow{\phi_*} S^\Gamma \xrightarrow{\delta^0} H^1(\Gamma, H) \longrightarrow H^1(\Gamma, G) \tag{3}$$

of pointed sets.

Next we define an action of G^Γ on S^Γ. For $\tilde{g} \in G^\Gamma$ and $x \in S^\Gamma$ let $g \in G$ be a preimage of x under ϕ, and set

$$\tilde{g} \star x = \phi(\tilde{g} g) \in S.$$

First note that if $g' \in G$ is another preimage of x under ϕ then since $S \cong G/H$ is a bijection of Γ-sets, there exists $h \in H$ such that $g' = gh$. Then we have $\phi(\tilde{g} g') = \phi(\tilde{g} g h) = \phi(\tilde{g} g)$. Therefore $\tilde{g} \star x$ does not depend on the choice of g. Next we show that $\tilde{g} \star x \in S^\Gamma$. Since ϕ is a morphism of Γ-sets and G is a Γ-group, then for all $\sigma \in \Gamma$ we have that

$$\sigma \cdot (\tilde{g} \star x) = \sigma \cdot \phi(\tilde{g} g) = \phi(\sigma \cdot (\tilde{g} g)) = \phi((\sigma \cdot \tilde{g}) \cdot (\sigma \cdot g)).$$

Since $\tilde{g} \in G^\Gamma$ it follows that $\sigma \cdot (\tilde{g} \star x) = \phi(\tilde{g} \cdot (\sigma \cdot g))$ for all $\sigma \in \Gamma$. Moreover since $x \in S^\Gamma$ we have $\phi(\sigma \cdot g) = \sigma \cdot \phi(g) = \sigma \cdot x = x$ for all $\sigma \in \Gamma$. Hence $\sigma \cdot g$ is also a preimage of x under ϕ. Since $\tilde{g} \star x$ does not depend on the choice of preimage it follows that $\sigma \cdot (\tilde{g} \star x) = \tilde{g} \star x$. Hence $\tilde{g} \star x \in S^\Gamma$ and so we have a well defined map

$$G^\Gamma \times S^\Gamma \longrightarrow S^\Gamma$$

$$(\tilde{g}, x) \longmapsto \tilde{g} \star x.$$

This map gives rise to an action of G^Γ on S^Γ. We denote by $S^\Gamma / \sim_{G^\Gamma}$ the orbit set of G^Γ in S^Γ. Note that $S^\Gamma / \sim_{G^\Gamma}$ is a pointed set whose basepoint is the orbit of 1.

Corollary 5.19. *There is a bijection*

$$\Phi \colon S^\Gamma / \sim_{G^\Gamma} \to \ker(H^1(\Gamma, H) \to H^1(\Gamma, G))$$

of pointed sets which assigns the orbit of $x \in S^\Gamma$ to $\delta^0(x)$.

Proof. Exactness of the sequence (3) at $H^1(\Gamma, H)$ implies $\ker(H^1(\Gamma, H) \to H^1(\Gamma, G)) = \mathrm{im}(\delta^0)$. So it suffices to construct a bijection $\phi \colon S^\Gamma / \sim_{G^\Gamma} \to \mathrm{im}(\delta^0)$. Set $\Phi(G^\Gamma \star x) = \delta^0(x)$. Suppose $x, x' \in S^\Gamma$ are in the same orbit. Therefore there exists $\tilde{g} \in G^\Gamma$ such that $x' = \tilde{g} \star x$. Then we have $x' = \phi(\tilde{g}g)$ for some preimage $g \in G$ of x. Note that $\tilde{g}g$ is a preimage of x'. Then since $(\tilde{g}g)^{-1} \cdot (\sigma \cdot (\tilde{g}g)) = g^{-1} \cdot (\sigma \cdot g)$, we have $\delta^0(x) = \delta^0(x')$. This shows that Φ is well-defined and surjective. To prove injectivity, suppose $\delta^0(x) = \delta^0(x')$. Then if α and α' are the cocycles representing $\delta^0(x)$ and $\delta^0(x')$ respectively, we have $[\alpha] = [\alpha']$. Then α and α' are cohomologous, so there exists $h \in H$ such that $\alpha'(\sigma) = h \cdot \alpha(\sigma) \cdot (\sigma \cdot h^{-1})$ for all $\sigma \in \Gamma$. Let g be a preimage of x and g' a preimage of x'. This implies $g'^{-1} \cdot (\sigma \cdot g') = h \cdot (g^{-1} \cdot (\sigma \cdot g)) \cdot (\sigma \cdot h)^{-1}$. It follows that $\tilde{g} = g'hg^{-1} \in G^\Gamma$. Therefore since $H = \ker \phi$ we get

$$x' = \phi(g') = \phi(g'h) = \phi(\tilde{g}g) = \tilde{g} \star x.$$

So x and x' are in the same orbit, which shows Φ is injective. □

5.2 The Galois cohomology functor

We start by proving a useful result about representable functors which we will use to deduce that algebraic group schemes admit a continuous Galois action. First we introduce some notation.

Notation 5.20. If $F\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Set}$ is a functor, we simply write $F(K)$ instead of $F(K/\Bbbk)$ for all $K \in \mathsf{Fld}_{\Bbbk}$. If $K \to L$ is a morphism in $\mathsf{Fld}_{\Bbbk}$, then for every $x \in F(K)$ we let $x_L \in F(L)$ denote the image of x under the map $F(K) \to F(L)$ as long as there is no ambiguity in the choice of the map $K \to L$.

Lemma 5.21 (Lemma III.7.15 [1])**.** *The map*

$$\mathcal{G}_\Omega \times F(\Omega) \longrightarrow F(\Omega)$$

$$(\sigma, x) \mapsto \sigma \cdot x := F(\sigma)(x)$$

gives rise to an action of $\mathcal{G}_\Omega$ on $F(\Omega)$. If Ω/K and Ω'/K are Galois extensions such that $\Omega \subset \Omega'$, we have

$$\sigma' \cdot x_{\Omega'} = (\sigma'|_\Omega \cdot x)_{\Omega'} \text{ for all } x \in F(\Omega), \sigma' \in \mathcal{G}_{\Omega'}.$$

Moreover, if $F\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Grp}$ is a group-valued functor, the above action is a group by automorphisms, i.e.,

$$\sigma \cdot (xy) = (\sigma \cdot x) \cdot (\sigma \cdot y) \text{ for all } \sigma \in \mathcal{G}_\Omega,\ x, y \in F(\Omega).$$

Lemma 5.22. *Let $F\colon \mathsf{Alg}_{\Bbbk} \to \mathsf{Set}$ be a functor represented by a commutative $\Bbbk$-algebra A. Then the following properties hold:*

1. *For every Galois extension Ω/K, the map $F(K) \to F(\Omega)$ is injective and induces a bijection (resp. a group isomorphism if F is a group-valued functor)*

$$F(K) \cong F(\Omega)^{\mathcal{G}_\Omega}$$

2. *Suppose A is finitely generated over $\Bbbk$, and let Ω/K be a Galois extension. For every finite intermediate Galois extension $K \subset L \subset \Omega$, let $\iota_L : F(L) \to F(\Omega)$ denote the map induced by the inclusion $L \subset \Omega$. Then $\mathcal{G}_\Omega$ acts continuously on $F(\Omega)$, and we have*

$$F(\Omega) = \bigcup_{L \subset \Omega} \iota_L(F(L))$$

Proof. Let $\psi\colon F \to h_A$ denote the natural isomorphism. For every morphism of $\Bbbk$-algebras $\phi\colon R \to S$ the diagram

$$\begin{array}{ccc} F(R) & \xrightarrow{\psi_R} & h_A(R) \\ {\scriptstyle F(\phi)}\downarrow & & \downarrow{\scriptstyle h_A(\phi)} \\ F(S) & \xrightarrow[\psi_S]{} & h_A(S) \end{array}$$

commutes. Therefore if $a \in F(R)$ and $f = \psi_R(a) \in h_A(R)$ then $h_A(\phi) \circ \psi_R(a) = h_A(\phi)(f) = \phi \circ f$ and hence $\psi_S = F(\phi)(a) = \phi \circ f$. We will repeatedly appeal to this observation in the proof.

1. Let Ω/K be a Galois extension and let $\epsilon\colon K \hookrightarrow \Omega$ denote the inclusion. Let $a_1, a_2 \in F(K)$ and suppose $F(\epsilon)(a_1) = F(\epsilon)(a_2)$. Then $\psi_\Omega \circ F(\epsilon)(a_1) = \psi_\Omega \circ F(\epsilon)(a_2)$. We have $\psi_\Omega \circ F(\epsilon)(a_1) = \epsilon \circ f_1$ and $\psi_\Omega \circ F(\epsilon)(a_2) = \epsilon \circ f_2$ where $f_1 = \psi_K(a_1)$ and $f_2 = \psi_K(a_2)$. Hence $\psi_K(a_1) = \psi_K(a_2)$. Since ψ is a natural isomorphism, ψ_K is an isomorphism. Hence $a_1 = a_2$ which proves that $F(\epsilon)$ is injective. Next we show that $F(K) \cong F(\Omega)^{\mathcal{G}_\Omega}$. We first show that $\mathrm{im}(F(\epsilon)) = F(\Omega)^{\mathcal{G}_\Omega}$, then injectivity of $F(\epsilon)$ shows $\mathrm{im}(F(\epsilon)) \cong F(K)$. Let $\sigma \in \mathcal{G}_\Omega$ and let $a \in F(\Omega)$. Set $f = \psi_\Omega(a) \in h_A(\Omega)$. If $a \in \mathrm{im}(F(\epsilon))$ then there exists $a' \in F(K)$ such that $F(\epsilon)(a') = a$. Hence $\epsilon \circ \psi_K(a') = \psi_\Omega \circ F(\epsilon)(a') =$. Let $f' = \psi_K(a') \in h_A(K)$. Then we have $\epsilon \circ f' = f$. Let $x \in K$. Since ϵ denotes the inclusion $K \subset \Omega$, then $\epsilon(x) \in K$. Since Ω/K is a Galois extension we have $\Omega^{\mathcal{G}_\Omega} = K$. It follows that $\sigma(\epsilon(x)) = \epsilon(x)$, and hence $\sigma \circ \epsilon = \epsilon$. Therefore

$$\sigma \circ f = \sigma \circ (\epsilon \circ f') = (\sigma \circ \epsilon) \circ f' = \epsilon \circ f = f.$$

Note that $\psi_\Omega \circ F(\sigma)(a) = \sigma \circ f = f$ and that $F(\sigma)(a) = \sigma \cdot a$. Hence we have $\psi_\Omega(\sigma \cdot a) = f = \psi_\Omega(a)$, where ψ_Ω is an isomorphism, since ψ is a natural isomorphism. Thus $\sigma \cdot a = a$, and so $a \in F(\Omega)^{\mathcal{G}_\Omega}$. This shows that $\mathrm{im}(F(\epsilon)) \subseteq F(\Omega)^{G_\Omega}$. Now let $a \in F(\Omega)^{\mathcal{G}_\Omega}$. Then $\sigma \cdot a = a$ for all $\sigma \in \mathcal{G}_\Omega$, and so $\psi_\Omega(\sigma \cdot a) = \psi_\Omega(a)$. Hence we have

$$f = \psi_\Omega(a) = \psi_\Omega(\sigma \cdot a) = \psi_\Omega(F(\sigma)(a)) = \sigma \circ f.$$

If $x \in A$, then $\sigma(f(x)) = f(x)$ and therefore $f(x) \in \Omega^{\mathcal{G}_\Omega} = K$. Therefore we have a well

defined map

$$f' \colon A \longrightarrow K$$
$$x \longmapsto f(x).$$

Since $f \in h_A(\Omega)$ we have that f' is a K-algebra homomorphism. Now let $a' \in F(K)$ be the element so that $\psi_K(a') = f'$. Since $f(x) \in K$ and ϵ is the inclusion $K \subset \Omega$, then $\epsilon(f(x)) \in K = \Omega^{\mathcal{G}_\Omega}$. Therefore it follows that $\epsilon(f'(x)) = \epsilon(f(x)) = f(x)$ since $\epsilon \in \mathcal{G}_\Omega$, and so $\epsilon \circ f' = f$. Then we have

$$\psi_\Omega(a) = f = \epsilon \circ f' = \psi_\Omega \circ F(\epsilon)(a')$$

and injectivity of ψ_Ω implies $a = F(\epsilon)(a')$. Hence $a \in \mathrm{im}(F(\epsilon))$, which shows $F(\Omega)^{\mathcal{G}_\Omega} \subseteq \mathrm{im}(F(\epsilon))$.

2. Let $a \in F(\Omega)$ let $f = \psi_\Omega(a) \in h_A(\Omega)$. By assumption A is finitely generated over $\Bbbk$. Let $\alpha_1, \ldots, \alpha_n$ be a set of generators of A. Let

$$K' := K(f(\alpha_1), \ldots, f(\alpha_n)).$$

Note that $K \subset K' \subset \Omega$ is an intermediate extension and K'/K is finite. Then by the Fundamental Theorem of Galois Theory, $\mathrm{Gal}(\Omega/K')$ is an open subgroup of $\mathcal{G}_\Omega$. Let $\sigma \in \mathcal{G}_\Omega$. By the same argument as before, $\sigma \cdot a = a$ if and only if $\sigma \cdot f = f$. By definition of K', $\sigma \cdot f = f$ if and only if $\sigma|_{K'} = \mathrm{id}$, that is $\sigma \in \mathrm{Gal}(\Omega/K)$. This shows that $\mathrm{Stab}_{\mathcal{G}_\Omega}(a) = \mathrm{Gal}(\Omega/K')$, hence $\mathrm{Stab}_{\mathcal{G}_\Omega}(a)$ is an open subgroup of $\mathcal{G}_\Omega$ for all $a \in F(\Omega)$. Therefore the action of $\mathcal{G}_\Omega$ on $F(\Omega)$ is continuous, and by Lemma 5.3 we have

$$F(\Omega) = \bigcup_{U \in \mathcal{N}} F(\Omega)^U$$

where $\mathcal{N}$ denotes the set of open normal subgroups of $\mathcal{G}_\Omega$. The Fundamental Theorem of Galois Theory gives a one-to-one correspondence between finite Galois subextensions of L/K of Ω/K and the the open normal subgroups $U \in \mathcal{N}$, which assigns L to $\mathrm{Gal}(\Omega/L)$ and U to Ω^U. It follows that

$$F(\Omega) = \bigcup_{L \subset \Omega} F(\Omega)^{\mathrm{Gal}(\Omega/L)}$$

where L runs through all finite Galois subextensions of Ω/K. For each such L, statement (1)

implies $\iota_L \colon F(L) \to F(\Omega)$ is injective and $\iota_L(F(L)) = F(\Omega)^{\mathrm{Gal}(\Omega/L)}$. Therefore

$$F(\Omega) = \bigcup_{L \subset \Omega} \iota_L(F(L))$$

which concludes the proof.

□

Definition 5.23. A group scheme $G \colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Grp}$ is a **Galois functor** if for every $K \in \mathsf{Fld}_{\Bbbk}$ and every Galois extension Ω/K, the following conditions are satisfied:

1. The map $G(K) \to G(\Omega)$ is injective, and induces a group isomorphism

$$G(K) \cong G(\Omega)^{\mathcal{G}_\Omega}$$

2. $G(\Omega) = \bigcup_{L \subset \Omega} \iota_{L,\Omega}(G(L))$, where L/K runs over the set of finite Galois subextensions of Ω and $\iota_{L,\Omega} \colon G(L) \to G(\Omega)$ is the map induced by the inclusion $L \subset \Omega$.

Example 5.24. An algebraic group scheme $G \colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Grp}$ is a Galois functor by Lemma 5.22.

Proposition 5.25. *Let $G \colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Grp}$ be a Galois functor. Then if $K \in \mathsf{Fld}_{\Bbbk}$ and Ω/K is Galois, $G(\Omega)$ is a $\mathcal{G}_\Omega$-group. Therefore we can consider the pointed set $H^1(\mathcal{G}_\Omega, G(\Omega))$.*

Proof. By combining condition (1) and (2) in Def. 5.23 we have

$$G(\Omega) = \bigcup_{L \subset \Omega} G(\Omega)^{\mathcal{G}_L}.$$

By the Galois correspondence, finite Galois subextensions L of Ω/K are in bijection with open normal subgroups $\mathcal{G}_L$ of $\mathcal{G}_\Omega$. Therefore it follows from Lemma 5.3 that $\mathcal{G}_\Omega$ acts continuously on $G(\Omega)$ via the assignment

$$\mathcal{G}_\Omega \times G(\Omega) \longrightarrow G(\Omega)$$

$$(\sigma, g) \longmapsto \sigma \cdot g = G(\sigma)(g).$$

Hence $G(\Omega)$ is a $\mathcal{G}_\Omega$-set. By Lemma 5.21 the above action is an action by group automorphisms, showing $G(\Omega)$ is a $\mathcal{G}_\Omega$-group. □

By using Theorem 5.14 we obtain a characterization of Galois cohomology of $\mathcal{G}_\Omega$ in terms of the Galois cohomology of its finite Galois subextensions in the following theorem.

Theorem 5.26 (Thm III.7.30 [1]). *Let $G\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Grp}$ be a Galois functor. Then for every $K \in \mathsf{Fld}_{\Bbbk}$ and every Galois extension Ω/K*

$$\varinjlim_{L\subset\Omega} H^n(\mathcal{G}_L, G(L)) \cong H^n(\mathcal{G}_\Omega, G(\Omega))$$

is an isomorphism of pointed sets, where L runs through the finite Galois subextensions of Ω/K.

Next we establish some functorial properties of Galois cohomology. Let $\iota\colon K \to K'$ be a morphism in $\mathsf{Fld}_{\Bbbk}$. Let Ω/K and Ω'/K' be Galois extensions and assume that we have a morphism $\phi\colon \Omega \to \Omega'$ in $\mathsf{Fld}_{\Bbbk}$ which extends ι. Let $\overline{\phi}\colon \mathcal{G}_{\Omega'} \to \mathcal{G}_\Omega$ be the continuous group homomorphism associated to ϕ by Corollary 3.8. Let $G\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Grp}$ be a Galois functor.

Lemma 5.27 (Lemma III.7.32 [1]). *The maps $\overline{\phi}\colon \mathcal{G}_{\Omega'} \to \mathcal{G}_\Omega$ and $G(\phi)\colon G(\Omega) \to G(\Omega')$ are compatible.*

Proposition 5.28. *Let $\phi\colon \Omega \to \Omega'$ be an extension of ι. Then since $\overline{\phi}\colon \mathcal{G}_{\Omega'} \to \mathcal{G}_\Omega$ and $G(\Omega)\colon G(\Omega) \to G(\Omega')$ are compatible, we get an induced map*

$$R_\phi\colon H^1(\mathcal{G}_\Omega, G(\Omega)) \to H^1(\mathcal{G}_{\Omega'}, G(\Omega'))$$

which only depends on ι.

Proof. Suppose $\phi\colon \Omega \to \Omega'$ is another extension of ι. We will show that $R_\phi = R_{\phi'}$, in which case R_ϕ does not depend on the choice of extension of ι, it only depends on ι. By Corollary 3.8 there exists $\rho \in \mathcal{G}_\Omega$ such that $\phi = \phi' \circ \rho$ so that $\overline{\phi'} = \mathsf{Inn}(\rho) \circ \overline{\phi}$. Then $\phi' = \phi \circ \rho^{-1}$, and since G is a functor we have

$$G(\phi')(g) = G(\phi \circ \rho^{-1})(g) = (G(\phi) \circ G(\rho^{-1}))(g) = G(\phi)(\rho^{-1} \cdot g)$$

for all $G \in G(\Omega)$. Hence, if $\rho^{-1}\bullet\colon G(\Omega) \to G(\Omega)$ is the map given by $g\colon \to \rho^{-1} \cdot g$, then the diagram

$$\begin{array}{ccc} G(\Omega) & \xrightarrow{\rho^{-1}\bullet} & G(\Omega) \\ {\scriptstyle G(\phi')}\downarrow & & \downarrow{\scriptstyle G(\phi)} \\ G(\Omega') & \xrightarrow[\mathrm{id}]{} & G(\Omega') \end{array}$$

is commutative. On the other hand, since $\overline{\phi'} = \mathsf{Inn}(\rho) \circ \overline{\phi}$ we have the following commutative diagram

$$\begin{array}{ccc} \mathcal{G}_\Omega & \xleftarrow{\mathsf{Inn}(\rho)} & \mathcal{G}_\Omega \\ {\scriptstyle \overline{\phi'}}\uparrow & & \uparrow{\scriptstyle \overline{\phi}} \\ \mathcal{G}_{\Omega'} & \xleftarrow[\mathrm{id}]{} & \mathcal{G}_{\Omega'} \end{array}$$

Recall that Example 5.11 shows $\mathsf{Inn}(\rho)$ and $\rho^{-1}\bullet$ are compatible. Therefore the above two diagrams satisfy the conditions of Proposition 5.13, hence the diagram

$$\begin{array}{ccc} H^1(\mathcal{G}_\Omega, G(\Omega)) & \xrightarrow{\rho^{-1}\bullet_*} & H^1(\mathcal{G}_\Omega, G(\Omega)) \\ {\scriptstyle G(\phi')_*}\downarrow & & \downarrow{\scriptstyle G(\phi)_*} \\ H^1(\mathcal{G}_{\Omega'}, G(\Omega')) & \xrightarrow[\mathrm{id}]{} & H^1(\mathcal{G}_{\Omega'}, G(\Omega')) \end{array}$$

is commutative. By definition $G(\phi')_* = R_{\phi'}$ and $G(\phi)_* = R_\phi$, and Example 5.11 shows $\rho^{-1}\bullet_*$ is the identity. Therefore it follows that $R_{\phi'} = R_\phi$. □

Remark 5.29. By Proposition 5.10, the morphism R_ϕ in Prop 5.28 is the induced map $G(\phi)_*$ on the 1st cohomology sets. Hence R_ϕ is given by

$$\begin{aligned} R_\phi \colon H^1(\mathcal{G}_\Omega, G(\Omega)) &\longrightarrow H^1(\mathcal{G}_{\Omega'}, G(\Omega')) \\ [\alpha] &\longmapsto [G(\phi)_*(\alpha)] \end{aligned}$$

where $G(\phi)_*(\alpha)$ is the cocycle defined by

$$\begin{aligned} G(\phi)_*(\alpha) \colon \mathcal{G}_{\Omega'} &\longrightarrow G(\Omega') \\ \sigma' &\longmapsto G(\phi)(\alpha(\overline{\phi}(\sigma'))). \end{aligned}$$

Let $\iota \colon K \to L$ be a morphism in $\mathsf{Fld}_{\Bbbk}$. Let $\overline{K}$ and $\overline{L}$ be algebraic closures of K and L respectively. By Corollary 3.3 there exists and extension $\phi \colon \overline{K} \to \overline{L}$ of ι. Let $\overline{\phi} \colon \mathcal{G}_{\overline{L}} \to \mathcal{G}_{\overline{K}}$ be the continuous group homomorphism associated to ϕ by Corollary 3.8. Then Prop. 5.28 gives us a map

$$R_\phi \colon H^1(\mathcal{G}_{\overline{K}}, G(\overline{K})) \to H^1(\mathcal{G}_{\overline{L}}, G(\overline{L})). \tag{4}$$

which only depends on ι. In the case where $K = L$ and $\iota = \mathrm{id}_K$ we may take $\phi = \mathrm{id}_{\overline{K}}$ in which case R_ϕ is the identity map.

Lemma 5.30 (Lemma III.7.35 [1])**.** *Let $\iota\colon K \to L$ and $\eta\colon L \to M$ be morphisms in $\mathsf{Fld}_{\Bbbk}$. Let $\phi\colon \overline{K} \to \overline{L}$ and $\psi\colon \overline{L} \to \overline{M}$ be extensions of ι and η respectively. Then*

$$R_{\psi\circ\phi} = R_\psi \circ R_\phi$$

Corollary 5.31 (Cor. III.7.36 [1])**.** *For any $K \in \mathsf{Fld}_{\Bbbk}$, the set $H^1(\mathcal{G}_{\overline{K}}, G(\overline{K}))$ does not depend on the choice of algebraic closure $\overline{K}$, up to canonical bijection.*

Definition 5.32. Let $G\colon \mathsf{Alg}_{\Bbbk} \to \mathsf{Grp}$ be a Galois functor, and $K/\Bbbk$ an extension.

1. We define the **1st Galois cohomology set** of G by

$$H^1(K, G) = H^1(\mathcal{G}_{\overline{K}}, G(\overline{K})).$$

   If G is abelian, that is if $G(R)$ is an abelian group for all $R \in \mathsf{Alg}_{\Bbbk}$, then $H^1(K, G)$ is a group.

2. Let $\iota\colon K \to L$ be a morphism in $\mathsf{Fld}_{\Bbbk}$. The map (4) defined from $H^1(K, G)$ to $H^1(L, G)$ corresponding to ι is called the **restriction map** and is denoted by $\mathsf{Res}_{L/K}$.

Theorem 5.33. *Let $G\colon \mathsf{Alg}_{\Bbbk} \to \mathsf{Grp}$ be a Galois functor. Then*

$$H^1(-, G)\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Set}_*$$

is a functor which assigns each $K \in \mathsf{Fld}_{\Bbbk}$ to the pointed set $H^1(K, G)$ and assigns each morphism $\iota\colon K \to L$ in $\mathsf{Fld}_{\Bbbk}$ to the map $\mathsf{Res}_{L/K}\colon H^1(K, G) \to H^1(L, G)$ of pointed sets. In the case where G is abelian and the restriction map is a group homomorphism, we obtain a functor

$$H^1(-, G)\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{AbGrp}\,.$$

Proof. If we take $\iota = \mathrm{id}_K$, then $\mathsf{Res}_{L/K}$ is the identity. Moreover, for any field extensions $K \to L \to M$ we have

$$\mathsf{Res}_{M/K} = \mathsf{Res}_{M/L} \circ \mathsf{Res}_{L/K}$$

by Lemma 5.30. □

6 Galois descent

In this section, we state the Galois descent problem for a group scheme $G\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Grp}$ acting on a functor $F : \mathsf{Fld}_{\Bbbk} \to \mathsf{Set}$. We then present the remaining ingredients needed to state the Galois descent lemma, first by defining a twisted form for a fixed element $a \in F(\Bbbk)$ and obtaining a twisted form functor $F_a\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Set}_*$. We then define the Galois descent condition for a functor F, and highlight examples of the types of functors which satisfy the condition. We introduce a key example of a Galois functor, the stabilizer subfunctor of the group scheme G, and conclude by giving detailed proof of the Galois descent lemma, a fundamental result which we use as a tool in determining the answer to Galois descent problems.

6.1 Twisted forms

Definition 6.1. Let $G\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Grp}$ be a group valued functor. An **action** of G on a functor $F\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Set}$ is the assignment to each $K \in \mathsf{Fld}_{\Bbbk}$ a group action

$$G(K) \times F(K) \to F(K)$$

$$(g, a) \mapsto g * a$$

which is natural in K. That is, for every morphism $\iota\colon K \to L$ in $\mathsf{Fld}_{\Bbbk}$, the following diagram commutes:

$$\begin{array}{ccc} G(K) \times F(K) & \longrightarrow & F(K) \\ {\scriptstyle (G(\iota),F(\iota))}\downarrow & & \downarrow \\ G(L) \times F(L) & \longrightarrow & F(L) \end{array}$$

or, in terms of elements

$$(g * a)_L = g_L * a_L \text{ for all } a \in F(K),\, g \in G(K).$$

Definition 6.2. Let $F\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Set}$ be a functor and $G\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Grp}$ be a group scheme acting on F. For every $K \in \mathsf{Fld}_{\Bbbk}$ we say $b, b' \in F(K)$ are **equivalent over** K if there exists $g \in G(K)$ such that $b = g * b'$.

We have presented all the required ingredients to state a general Galois descent problem.

The Galois descent problem: Let $F\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Set}$ be a functor, $G\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Grp}$ be a group scheme acting on F, and Ω/K a Galois extension.

Suppose that $a_\Omega \sim_\Omega a'_\Omega$. Do we have $a \sim_K a'$?

Definition 6.3. Let $a \in F(\Bbbk)$, let $K \in \mathsf{Fld}_{\Bbbk}$ and let Ω/K be a Galois extension. An element $a' \in F(K)$ is called a **twisted K-form of a (split by Ω)** if $a'_\Omega \sim_\Omega a_\Omega$.

The action of $G(K)$ on $F(K)$ restricts to the set of twisted K-forms of a, since if we assume $a' \in F(K)$ is a twisted K-form of a and $a' \sim_K a''$ then a'' is also a twisted K-form of a. We have $a'_\Omega \sim_\Omega a_\Omega$ and $a' \sim_K a''$, hence there exists $g \in G(\Omega)$ and $g' \in G(K)$ such that $a'_\Omega = g * a_\Omega$ and $a'' = g' * a'$. Since the action of $G(K)$ on $F(K)$ is functorial in K, then it follows that $a''_\Omega = (g' * a')_\Omega = g'_\Omega * a'_\Omega$. Therefore $g'_\Omega g$ is an element of $G(\Omega)$ such that

$$g'_\Omega g * a_\Omega = g'_\Omega * (g * a_\Omega) = g'_\Omega * a'_\Omega = a''_\Omega$$

Definition 6.4. We denote by

$$F_a(\Omega/K) = \{[a'] \mid a' \in F(K),\ a'_\Omega \sim_\Omega a_\Omega\}$$

the set of K-equivalence classes of twisted K-forms of a which split over Ω. Then $F_a(\Omega/K)$ is a pointed set with base point $[a_K]$.

Remark 6.5. Note that $F_a(\Omega/K)$ is the collection of elements for which the answer to the descent problem is negative. In particular the answer to the descent problem is positive if and only of $F_a(\Omega/K) = [a_K]$.

Theorem 6.6. *We obtain a functor $F_a\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Set}_*$ by assigning $F_a(K) = F_a(\overline{K}/K)$ to each $K \in \mathsf{Fld}_{\Bbbk}$ and assigning the map*

$$\begin{aligned} F_a(\iota)\colon F_a(\overline{K}/K) &\longrightarrow F_a(\overline{K'}/K') \\ [a'] &\longmapsto [a'_{K'}] \end{aligned}$$

to each morphism $\iota\colon K \to K'$ in $\mathsf{Fld}_{\Bbbk}$.

Proof. We show that the map $F(K) \to F(K')$ induces a map $F_a(\iota)$ is a well defined morphism of pointed sets. Then the functorial properties of F_a are inherited by F. Let $\phi\colon \overline{K} \to \overline{K'}$ be an extension of ι and let $a' \in F(K)$ be a twisted K-form of a. We will show that $a'_{K'}$ is a twisted K'-from of a. Since ϕ is an extension of ι, we have $\epsilon' \circ \iota = \phi \circ \epsilon$ where ϵ and ϵ' denote the inclusions $K \subset \overline{K}$ and $K' \subset \overline{K'}$, respectively. Then since F is a functor it follows that

$$\begin{aligned}(a'_{K'})_{\overline{K'}} &= (F(\iota)(a'))_{\overline{K'}} = F(\epsilon')(F(\iota)(a')) = F(\epsilon' \circ \iota)(a') \\ &= F(\phi \circ \epsilon)(a') = F(\phi)(F(\epsilon)(a')) = (F(\epsilon)(a'))_{\overline{K'}} = (a'_{\overline{K}})_{\overline{K'}}\end{aligned}$$

Now since a' is a twisted K-form of a, there exists $g \in G(\overline{K})$ such that $g * a'_{\overline{K}} = a_{\overline{K}}$. Therefore since the action of $G(K)$ on $F(K)$ is functorial in K, we have

$$g_{\overline{K'}} * (a'_{K'})_{\overline{K'}} = g_{\overline{K'}} * (a'_{\overline{K}})_{\overline{K'}} = (g * a'_{\overline{K}})_{\overline{K'}} = (a_{\overline{K}})_{\overline{K'}} = a_{\overline{K'}}$$

Hence $a'_{K'}$ is a twisted K'-form of a, and since this does not depend on the choice of extension of ϕ of ι we have shown $F_a(\iota)$ is well-defined. $F_a(\iota)$ is a morphism of pointed sets by construction, since $F([a_K]) = [a_{K'}]$. □

We need a suitable condition on the functor F in order to establish a relationship between F_a and the Galois cohomology of a certain group-scheme which is associated to a. Below we state the required condition.

Definition 6.7. A functor $F\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Set}$ satisfies the **Galois descent condition** if for every $K \in \mathsf{Fld}_{\Bbbk}$ and every Galois extension Ω/K the map $F(K) \to F(\Omega)$ is injective and induces a bijection

$$F(K) \cong F(\Omega)^{\mathcal{G}_\Omega}.$$

Now we give examples of the types of functors which satisfy the Galois descent condition.

Example 6.8.

1. M_n satisfies the Galois descent condition.

2. Representable functors satisfy the Galois descent condition by Lemma 5.22.

3. By definition, Galois functors satisfy the Galois descent condition.

6.2 Stabilizers

Definition 6.9. Let $G\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Grp}$ be a group valued functor acting on a functor $F\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Set}$. For $a \in F(\Bbbk)$ and every $K \in \mathsf{Fld}_{\Bbbk}$ we set

$$\mathrm{Stab}_G(a)(K) = \{g \in G(K) \mid g * a_K = a_K\}$$

For all extensions $K \in \mathsf{Fld}_{\Bbbk}$, $\mathrm{Stab}_G(a)(K) \subseteq G(K)$. Moreover, if $\iota\colon K \to K'$ is a morphism in $\mathsf{Fld}_{\Bbbk}$, the map $G(\iota)\colon G(K) \to G(K')$ restricts to a map $\mathrm{Stab}_G(a)(K) \to Stab_G(a)(K')$. Indeed, if $g \in \mathrm{Stab}_G(a)(K)$ then

$$g_{K'} * a_{K'} = g_{K'} * (a_K)_{K'} = (g * a_K)_{K'} = (a_K)_{K'} = a_{K'}$$

showing that $g_{K'} \in \mathrm{Stab}_G(a)(K')$. Hence we have a subfunctor $\mathrm{Stab}_G(a)\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Grp}$ of G called the **stabilizer** of a.

Let $K \in \mathsf{Fld}_{\Bbbk}$, let Ω/K a Galois extension and let $\sigma \in \mathrm{Gal}(\Omega/K)$. Then the map

$$\mathrm{Stab}_G(a)(\sigma)\colon \mathrm{Stab}_G(a)(\Omega) \to \mathrm{Stab}_G(a)(\Omega)$$

is obtained by restriction of the map $G(\sigma)\colon G(\Omega) \to G(\Omega)$. Hence the action $\mathcal{G}_\Omega$ on $G(\Omega)$ via Lemma 5.21 restricts to an action on $\mathrm{Stab}_G(a)(\Omega)$.

Lemma 6.10 (Lemma III.8.13 [1])**.** *Let $G\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Grp}$ be a Galois functor acting on a functor $F\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Set}$ which satisfies the Galois descent condition. Then for all $a \in F(\Bbbk)$, $\mathrm{Stab}_G(a)$ is a Galois functor. In particular, for every $K \in \mathsf{Fld}_{\Bbbk}$ and every Galois extension Ω/K, $\mathrm{Stab}_G(a)(\Omega)$ is a $\mathcal{G}_\Omega$-group.*

Thus we obtain a Galois cohomology set

$$H^1(\mathcal{G}_\Omega, \mathrm{Stab}_G(a)(\Omega))$$

for any Galois extension Ω/K and more generally a functor

$$H^1(-, \mathrm{Stab}_G(a))\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Set}_*\,.$$

6.3 Galois descent lemma

We now have all the ingredients to state the Galois descent lemma, a result which describes $F_a(\Omega/K)$, the set of elements which yield a negative answer to the Galois descent problem, in terms of Galois cohomology.

Theorem 6.11 (Galois descent lemma (due to Serre [4]))**.** *Let $F\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Set}$ be a functor satisfying the Galois decent condition, let $G\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Grp}$ be a Galois functor acting on F, and let $a \in F(\Bbbk)$. Then*

1. *For every $K \in \mathsf{Fld}_{\Bbbk}$ and every Galois extension Ω/K*

$$F_a(\Omega/K) \xrightarrow{\cong} \ker\Big(H^1\big(\mathcal{G}_\Omega, \mathrm{Stab}_G(a)(\Omega)\big) \xrightarrow{\jmath_*} H^1\big(\mathcal{G}_\Omega, G(\Omega)\big)\Big)$$

   is a bijection of pointed sets, where $\jmath\colon \mathrm{Stab}_G(a)(\Omega) \to G(\Omega)$ is the inclusion.

2. *The above bijection is functorial in Ω. That is, if $\iota\colon K \to K'$ is a morphism in $\mathsf{Fld}_{\Bbbk}$, Ω/K and Ω'/K' are Galois extensions and $\phi\colon \Omega \to \Omega'$ is an extension of ι, then the diagram*

$$\begin{array}{ccc} F_a(\Omega/K) & \xrightarrow{\cong} & \ker(\jmath_*) \\ \downarrow & & \downarrow{\scriptstyle R_\phi} \\ F_a(\Omega'/K') & \xrightarrow{\cong} & \ker(\jmath'_*) \end{array}$$

   is commutative. In particular, we have a natural isomorphism between functors from $\mathsf{Fld}_{\Bbbk}$ to Set_*

$$F_a \cong \ker[H^1(-, \mathrm{Stab}_G(a)) \to H^1(-, G)].$$

   Therefore if $H^1(-, G) = 1$, we have a natural isomorphism of functors

$$F_a \cong H^1(-, \mathrm{Stab}_G(a)).$$

Proof.

1. The action of $\mathcal{G}_\Omega$ on $G(\Omega)$ restricts to an action on $\mathrm{Stab}_G(a)(\Omega)$, and by Lemma 6.10 this action is continuous. Hence $\mathrm{Stab}_G(a)(\Omega)$ is a $\mathcal{G}_\Omega$-subgroup of $G(\Omega)$, and we have a bijection $G(\Omega)/\mathrm{Stab}_G(a)(\Omega) \cong G(\Omega) * a_\Omega$ where $G(\Omega) * a_\Omega$ denotes the orbit of a_Ω. This bijection is

equivalently written as a short exact sequence

$$1 \longrightarrow \mathrm{Stab}_G(a)(\Omega) \longrightarrow G(\Omega) \longrightarrow G(\Omega) * a_\Omega \longrightarrow 1$$

of pointed sets. By Corollary 5.19 there is a one-to-one correspondence

$$(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega} / \sim_{G(\Omega)^{\mathcal{G}_\Omega}} \overset{\cong}{\longleftrightarrow} \ker(\jmath_*)$$

where $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega} / \sim_{G(\Omega)^{\mathcal{G}_\Omega}}$ is the orbit set of $G(\Omega)^{\mathcal{G}_\Omega}$ in $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$. To prove the first part of the theorem, it suffices to show there is a bijection between $F_a(\Omega/K)$ and $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega} / \sim_{G(\Omega)^{\mathcal{G}_\Omega}}$. Recall that the assignment

$$\begin{aligned} G(\Omega)^{\mathcal{G}_\Omega} \times (G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega} &\longrightarrow (G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega} \\ (g, a') &\longmapsto g \star a' \end{aligned}$$

gives rise to an action of $G(\Omega)^{\mathcal{G}_\Omega}$ on $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$ defined by $g \star a' := (gg') * a_\Omega$ where g' is a preimage of a' under the map $G(\Omega) \to G(\Omega) * a_\Omega$.

Now notice that

$$\begin{aligned} G(\Omega) * a_\Omega &= \{a' \in F(\Omega) \mid g * a_\Omega = a' \text{ for some } g \in G(\Omega)\} \\ &= \{a' \in F(\Omega) \mid a_\Omega \sim_\Omega a'\}. \end{aligned}$$

Then since F satisfies the Galois descent condition, $F(K) \cong F(\Omega)^{\mathcal{G}_\Omega}$ and hence

$$(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega} = \{a' \in F(\Omega)^{\mathcal{G}_\Omega} \mid a_\Omega \sim_\Omega a'\} = \{a'_\Omega \in F(K) \mid a'_\Omega \sim_\Omega a_\Omega\}.$$

Therefore if $K_a = \{a' \in F(K) \mid a'_\Omega \sim_\Omega a_\Omega\}$ is the set of twisted K-forms of a, then $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$ is the image of the K_a under the map $F(K) \to F(\Omega)$. That is to say $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega} = (K_a)_\Omega$ and so elements of $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$ are of the form a'_Ω for $a' \in K_a$. Also, since G is a Galois functor the map $G(\epsilon)\colon G(K) \to G(\Omega)$ is injective and $G(K) \cong G(\Omega)^{\mathcal{G}_\Omega}$ where ϵ denotes the inclusion $K \subset \Omega$. Therefore $G(\epsilon)\colon G(K) \overset{\cong}{\to} \mathrm{im}(G(\epsilon))$ is a bijection, and since $G(K) \cong G(\Omega)^{\mathcal{G}_\Omega}$ it follows that $G(\Omega)^{\mathcal{G}_\Omega} \cong \mathrm{im}(G(\epsilon))$. That is, elements of $G(\Omega)^{\mathcal{G}_\Omega}$ are of the form g_Ω for $g \in G(K)$. In view of these two observations, the orbit set of $G(\Omega)^{\mathcal{G}_\Omega}$ in $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$ gives an equivalence relation $\sim_{G(\Omega)^{\mathcal{G}_\Omega}}$ on $(K_a)_\Omega$ for which $a'_\Omega, a''_\Omega \in (K_a)_\Omega$ are

equivalent if and only if there exists $g_\Omega \in G(\Omega)^{\mathcal{G}_\Omega}$ such that $g_\Omega \star a'_\Omega = a''_\Omega$. Next recall that the action of $G(K)$ on $F(K)$ restricts to the set K_a of twisted K-forms of a. Hence $\sim_K$ is an equivalence relation on K_a. Thus we have two surjective maps,

$$q_1 \colon K_a \to K_a/\sim_K := F_a(\Omega/K)$$

and

$$q_2 \colon (K_a)_\Omega \to (K_a)_\Omega/\sim_{G(\Omega)^{\mathcal{G}_\Omega}} := (G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}/\sim_{G(\Omega)^{\mathcal{G}_\Omega}} .$$

Claim: Set $f = q_2 \circ F(\epsilon)|_{K_a}$. Then $a' \sim_K a''$ if and only if $f(a') = f(a'')$. We first show that if $g_\Omega \in G(\Omega)^{\mathcal{G}_\Omega}$ and $a'_\Omega \in (G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$ then $g_\Omega \star a'_\Omega = (g * a')_\Omega$. Since a' is a twisted K- form of a, then there exists $g' \in G(\Omega)$ such that $a'_\Omega = g' * a_\Omega$. Hence g' is a preimage of a'_Ω under the map $G(\Omega) \to G(\Omega) * a_\Omega$ and thus

$$g_\Omega \star a'_\Omega = (g_\Omega g') * a_\Omega = g_\Omega * (g' * a_\Omega) = g_\Omega * a'_\Omega = (g * a')_\Omega.$$

Now let $a', a'' \in K_a$ and suppose $a' \sim_K a''$. Then there exists $g \in G(K)$ such that $g * a' = a''$, and so $a''_\Omega = (g * a')_\Omega = g_\Omega \star a'_\Omega$. Hence $a'_\Omega \sim_{G(\Omega)^{\mathcal{G}_\Omega}} a''_\Omega$ which shows $f(a') = q_2(a'_\Omega) = q_2(a''_\Omega) = f(a'')$. Conversely, if $f(a') = f(a'')$ then $q_2(a'_\Omega) = q_2(a'_\Omega)$. That is $a'_\Omega \sim_{G(\Omega)^{\mathcal{G}_\Omega}} a''_\Omega$, so there exists $g_\Omega \in G(\Omega)^{\mathcal{G}_\Omega}$ such that $g_\Omega \star a'_\Omega = a''_\Omega$. It then follows from the above argument that $(g * a')_\Omega = a''_\Omega$. Since F satisfies the Galois descent condition the map $F(K) \to F(\Omega)$ is injective, so we get that $g * a' = a''$. Thus $a' \sim_K a''$, which proves the claim. The forward implication of the claim shows that f descends to the quotient. Therefore there exists a map

$$\phi \colon F_a(\Omega/K) \to (G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}/\sim_{G(\Omega)^{\mathcal{G}_\Omega}}$$

such that $f = \phi \circ q_1$. Since f is surjective it follows that ϕ is also surjective. The reverse implication of the claim along with $f = \phi \circ q_1$ gives us that ϕ is injective. Hence ϕ is a bijection between $F_a(\Omega/K)$ and the orbit set of $G(\Omega)^{\mathcal{G}_\Omega}$ in $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$ which assigns a K- equivalence class $[a']$ to the orbit of a'_Ω in $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$.

Aside: The bijection between $F_a(\Omega/K)$ and $\ker(\jmath_*)$ is explicitly given by

$$\psi\colon F_a(\Omega/K) \longrightarrow \ker(\jmath_*)$$
$$[a'] \longmapsto [\alpha]$$

where we pick $g \in G(\Omega)$ with $g * a'_\Omega = a_\Omega$ so that α is the cocycle

$$\alpha\colon \mathcal{G}_\Omega \longrightarrow \mathrm{Stab}_G(a)(\Omega)$$
$$\sigma \longmapsto g \cdot (\sigma \bullet g^{-1}).$$

Indeed, if $[a'] \in F_a(\Omega/K)$, then under ϕ the corresponding orbit of $G(\Omega)^{\mathcal{G}_\Omega}$ in $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$ is the orbit of a'_Ω. Since a' is a twisted K-form of a, by definition there exists $g \in G(\Omega)$ such that $g * a'_\Omega = a_\Omega$. Thus

$$a'_\Omega = (g^{-1}g) * a'_\Omega = g^{-1} * (g * a'_\Omega) = g^{-1} * a_\Omega.$$

So g^{-1} is a preimage of a'_Ω under the map $G(\Omega) \to G(\Omega) * a_\Omega$. Then under the bijection established in Corollary 5.19, we assign the orbit of a'_Ω to the cohomology class $\delta^0(a'_\Omega) = [\alpha] \in H^1(\mathcal{G}_\Omega, \mathrm{Stab}_G(a)(\Omega))$ where α is the above cocycle.

2. Let $\iota\colon K \to K'$ be a morphsim in $\mathsf{Fld}_{\mathbb{k}}$, let Ω/K and Ω'/K' be Galois extensions and assume that we have an extension $\phi\colon \Omega \to \Omega'$ of ι. Let $\overline{\phi}\colon \mathcal{G}_{\Omega'} \to \mathcal{G}_\Omega$ be the continuous group homomorphism associated to ϕ by Corollary 3.8. We first show that the map

$$R_\phi\colon H^1(\mathcal{G}_\Omega, \mathrm{Stab}_G(a)(\Omega)) \to H^1(\mathcal{G}_{\Omega'}, \mathrm{Stab}_G(a)(\Omega'))$$

restricts to the map

$$R_\phi\colon \ker(\jmath_*) \to \ker(\jmath'_*).$$

Let $[\xi] \in \ker(\jmath_*)$. Then ξ is cohomologous to the trivial cocycle, and hence there exists an element $g \in G(\Omega)$ such that $\xi(\sigma) = g \cdot (\sigma \bullet g^{-1})$ for all $\sigma \in \mathcal{G}_\Omega$. We will show that $R_\phi([\xi])$ is represented by the cocycle

$$\mathcal{G}_{\Omega'} \longrightarrow \mathrm{Stab}_G(a)(\Omega')$$
$$\sigma' \longmapsto g_{\Omega'} \cdot (\sigma' \bullet g_{\Omega'}^{-1})$$

which shows $R_\phi([\xi])$ is represented by the trivial cocycle, and thus $R_\phi([\xi]) \in \ker(\jmath'_*)$. By

definition, $R_\phi([\xi]) = [\xi']$ where ξ' is the cocycle

$$\begin{aligned} \xi' \colon \mathcal{G}_{\Omega'} &\longrightarrow \mathrm{Stab}_G(a)(\Omega') \\ \sigma' &\longmapsto \mathrm{Stab}_G(a)(\phi)(\xi(\overline{\phi}(\sigma'))). \end{aligned}$$

Recall that $\mathrm{Stab}_G(a)(\phi)$ is the restriction of $G(\phi)$. Then since $G(\phi)$ is a group homomorphism and $\mathcal{G}_{\Omega'}$ acts on $G(\Omega)$ by group automorphisms, for all $\sigma' \in \mathcal{G}_{\Omega'}$ we have

$$\xi'(\sigma') = G(\phi)(\xi(\overline{\phi}(\sigma'))) = G(\phi)(g \cdot (\overline{\phi}(\sigma') \cdot g^{-1})) = (G(\phi)(g)) \cdot (G(\phi)(\overline{\phi}(\sigma') \cdot g))^{-1}.$$

Since $G(\phi)$ and $\overline{\phi}$ are compatible, it follows that

$$\xi'(\sigma') = (G(\phi)(g)) \cdot (G(\phi)(\overline{\phi}(\sigma') \cdot g))^{-1} = (G(\phi)(g)) \cdot (\sigma' \cdot [G(\phi)(g)]^{-1}) = g_{\Omega'} \cdot (\sigma' \cdot g_{\Omega'}^{-1}).$$

Therefore $R_\phi([\xi])$ is indeed represented by the desired cocycle. Now let $[a'] \in F_a(\Omega/K)$ and let $g \in G(\Omega)$ be an element so that $g * a'_\Omega = a_\Omega$. Then since $(a'_{K'})_{\Omega'} = a'_{\Omega'}$ and

$$g_{\Omega'} * a'_{\Omega'} = g_{\Omega'} * (a'_\Omega)_{\Omega'} = (g * a'_\Omega)_{\Omega'} = (a_\Omega)_{\Omega'} = a_{\Omega'}$$

we have that $g_{\Omega'} \in G(\Omega')$ is an element so that $g_{\Omega'} * (a'_{K'})_{\Omega'} = a_{\Omega'}$. Hence $\psi \circ F_a(\iota)([a']) = \psi([a'_{K'}]) = [\beta]$ where β is the cocycle

$$\begin{aligned} \beta \colon \mathcal{G}_{\Omega'} &\longrightarrow \mathrm{Stab}_G(a)(\Omega') \\ \sigma' &\longmapsto g_{\Omega'} \cdot (\sigma' \cdot g_{\Omega'}^{-1}). \end{aligned}$$

On the other hand, $R_\phi(\psi([a'])) = R_\phi([\alpha])$, and since $[\alpha]$ in this case belongs to $\ker(\jmath_*)$, then it follows from the previous calculations that $R_\phi([\alpha]) = [\beta]$. Thus $\psi \circ F_a(\iota) = R_\phi \circ \psi$, which shows that the bijection ψ is functorial in Ω.

□

The following theorem draws a direct connection between Galois descent and cohomology. In particular, we show that the failure of the Galois fixed point functor to preserve right exactness of a short exact sequence obtained via the orbit stabilizer theorem is the obstruction to a positive answer to a Galois descent problem.

Theorem 6.12. *Let* $F\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Set}$ *be a functor satisfying the Galois decent condition, let* $G\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Grp}$ *be a Galois functor acting on* F*, and let* $a \in F(\Bbbk)$*. Then for every* $K \in \mathsf{Fld}_{\Bbbk}$ *and every Galois extension* Ω/K *the sequence*

$$1 \longrightarrow \mathrm{Stab}_G(a)(\Omega)^{\mathcal{G}_\Omega} \longrightarrow G(\Omega)^{\mathcal{G}_\Omega} \xrightarrow{\pi_*} (G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega} \longrightarrow 1 \tag{5}$$

is exact if and only if the Galois descent problem for $a \in F(\Bbbk)$ *has a positive answer, where* $\pi : G(\Omega) \to G(\Omega) * a_\Omega$ *is the natural projection.*

Proof. First note that by Prop. 5.18, the sequence of pointed sets

$$1 \to \mathrm{Stab}_G(a)(\Omega)^{\mathcal{G}_\Omega} \to G(\Omega)^{\mathcal{G}_\Omega} \xrightarrow{\pi_*} (G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega} \xrightarrow{\delta^0} H^1(\mathcal{G}_\Omega, \mathrm{Stab}_G(a)(\Omega)) \xrightarrow{\jmath_*} H^1(\mathcal{G}_\Omega, G(\Omega)) \tag{6}$$

is exact, where δ^0 is the $0th$ connecting map and $\jmath : \mathrm{Stab}_G(a)(\Omega) \to G(\Omega)$ is the inclusion. Next recall that the Galois descent problem for $a \in F(\Bbbk)$ has a positive answer if and only if $F_a(\Omega/K) = \{[a_K]\}$ (Remark 6.5). Hence we show the sequence (5) is exact if and only if $F_a(\Omega/K) = \{[a_K]\}$. Now suppose the sequence (5) is exact. Then $G(\Omega)^{\mathcal{G}_\Omega}/\mathrm{Stab}_G(a)(\Omega)^{\mathcal{G}_\Omega} = (G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$, and by exactness of the sequence (6) we have $\ker \delta^0 = \operatorname{im} \pi_*$. Therefore $\ker \delta^0 = (G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$ which implies $\operatorname{im} \delta^0 = \{[\mathrm{id}]\}$, where id is the trivial 1-cocycle. Exactness of (6) implies $\operatorname{im} \delta^0 = \ker \jmath_*$, so we have $\ker \jmath_* = \{[\mathrm{id}]\}$. By Theorem 6.11, $F_a(\Omega/K) \cong \ker \jmath_*$ is a bijection of pointed sets, hence $F_a(\Omega/K) = \{[a_K]\}$. Conversely, suppose $F_a(\Omega/K) = \{[a_K]\}$. Then it follows from Theorem 6.11 that $\operatorname{im} \delta^0 = \ker \jmath_* = \{[id]\}$. Therefore $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega} = (\delta^0)^{-1}(\{[id]\}) = \ker \delta^0 = \operatorname{im} \pi_*$, thus the sequence (5) is exact. □

7 Generalizations of Hilbert's Theorem 90

In this section, we prove cohomological Hilbert's Theorem 90 via Dedekind characters, and as a corollary, we prove Hilbert's Theorem 90 in its classic form. These results culminate in a generalization of cohomological Hilbert's Theorem 90 for arbitrary Galois extensions $\Omega/\Bbbk$, from which we deduce that $H^1(\mathcal{G}_\Omega, \mathrm{GL}_n(\Omega)) = 1$. This is a key result used in Section 8 where we describe two specific Galois descent problems.

Let $E/\Bbbk$ be a finite Galois extension. Recall that for $a \in E$, the **norm** of a is the product

$$N(a) := \prod_{\sigma \in \mathcal{G}_E} \sigma(a).$$

The norm induces a group homomorphism $N\colon E^\times \to \Bbbk^\times$. First, if $a \in E^\times$ then $N(a) \in \Bbbk$. To show this it suffices to show that $N(a)$ is fixed by $\mathcal{G}_E$, since $E/\Bbbk$ is Galois. Write $N(a)$ as $\sigma_1(a)\cdots\sigma_n(a)$, where $\mathcal{G}_E = \{\sigma_1, \ldots, \sigma_n\}$. Let $\tau \in \mathcal{G}_E$. Then since τ is a ring homomorphism and $\mathcal{G}_E$ acts on $E^\times$

$$\tau(N(a)) = \tau(\sigma(a))\cdots\tau(\sigma_n(a)) = (\tau\sigma_1)(a)\cdots(\tau\sigma_n)(a).$$

Recall that left multiplication by τ induces an element of $\mathrm{Aut}_{\mathsf{Set}}(\mathcal{G}_E) \cong \mathbb{S}_n$. Then

$$\tau(N(a)) = \sigma_{i_1}(a)\cdots\sigma_{i_n}(a) = N(a)$$

since $E^\times$ is an abelian group. Hence $N(a) \in \Bbbk$. If $a, b \in E^\times$ then

$$N(ab) = \prod_{\sigma \in \mathcal{G}_E} \sigma(ab) = \prod_{\sigma \in \mathcal{G}_E} \sigma(a)\sigma(b) = \left(\prod_{\sigma \in \mathcal{G}_E} \sigma(a)\right)\left(\prod_{\sigma \in \mathcal{G}_E} \sigma(b)\right).$$

This shows that N is a group homomorphism.

Recall that a **Dedekind character** on a group G is a group homomorphism $\chi\colon G \to E^\times$.

Lemma 7.1 (Dedekind's Lemma)**.** *Let G be a group and let $\tau_1, \ldots, \tau_n\colon G \to E^\times$ be a distinct set of characters. Then $\{\tau_i\}$ is linearly independent over E, that is, if there exist $c_1, \ldots, c_n \in E$ such that $\sum_{i=1}^n c_i\tau_i(g) = 0$ for all $g \in G$, then $c_i = 0$ for all $i = 1, \ldots, n$.*

Proof. Leading to a contradiction, suppose $\sum_{i=1}^n c_i\tau_i(g) = 0$ for all $g \in G$ and that there exists $c_i \neq 0$. Let k be the smallest positive integer such that, after relabeling indices, $c_1 \neq 0, c_2 \neq 0 \ldots, c_k \neq 0$

and $\sum_{i=1}^{k} c_i\tau_i(g) = 0$ for all $g \in G$. Note that $k \geq 2$. Since $\{\tau_i\}$ are distinct, there exists $h \in G$ such that $\tau_1(h) \neq \tau_2(h)$. We have

$$\tau_1(h)\sum_{i=1}^{k} c_i\tau_i(g) = \sum_{i=1}^{k} c_i\tau_1(h)\tau_i(g) = 0$$

and on the other hand,

$$\sum_{i=1}^{k} c_i\tau_i(h)\tau_i(g) = \sum_{i=1}^{k} c_i\tau_i(hg) = 0.$$

This implies that $\sum_{i=1}^{k} c_i(\tau_1(h) - \tau_i(h))\tau_i(g) = 0$ for all $g \in G$. Hence we have $\sum_{i=2}^{k} \tilde{c}_i\tau_i(g) = 0$ for all $g \in G$ where $\tilde{c}_i = c_i(\tau_1(h) - \tau_i(h))$. Since $\tau_1(h) \neq \tau_2(h)$, $\{\tilde{c}_i\}_{i=2}^{k}$ is a collection of $k-1$ coefficients not all equal to zero satisfying $\sum_{i=2}^{k} \tilde{c}_i\tau_i(g) = 0$. This contradicts the minimality of k. Thus $\{\tau_i\}$ are linearly independent over E. □

Theorem 7.2 (Hilbert's Theorem 90: Cohomological)**.** *Let $E/\Bbbk$ be a finite Galois extension. Then the degree* 1 *group cohomology $H^1(\mathcal{G}_E, E^\times)$ is trivial, that is $H^1(\mathcal{G}_E, E^\times) = 1$.*

Proof. Let $\alpha\colon \mathcal{G}_E \to E^\times$ be a 1-cocycle. We show there exists $a \in E$ such that $\alpha(\tau) = \tau(a)a^{-1}$ for all $\tau \in \mathcal{G}_E$. Then α is both a 1-cocycle and a 1-coboundary, which shows α is the trivial cocycle. Note for all $\sigma \in \mathcal{G}_E$, $\sigma\colon E^\times \to E^\times$ is a Dedekind character on $\mathcal{G}_E$. Consider $\sum_{\sigma\in\mathcal{G}_E} \alpha(\sigma)\sigma(a) \in E$ for any $a \in E$. Since $\alpha(a)$ is nonzero and belongs to E, Dedekind's Lemma implies there exists $a \in E^\times$ such that $b := \sum_{\sigma\in\mathcal{G}_E} \alpha(\sigma)\sigma(a) \neq 0$. Let $\tau \in \mathcal{G}_E$. Then since τ is a ring homomorphism $\tau(b) = \sum_{\sigma\in\mathcal{G}_E} \tau(\alpha(\sigma))\tau\sigma(a)$. Since α is a 1-cocycle, this implies that

$$\alpha(\tau)(\tau(b)) = \sum_{\sigma\in\mathcal{G}_E} \alpha(\tau)\tau(\alpha(\sigma))\tau\sigma(a) = \sum_{\sigma\in\mathcal{G}_E} \alpha(\tau\sigma)\tau\sigma(a) = b$$

where the last equality follows by reindexing. Let $a = b^{-1}$. Then $\alpha(\tau) = \tau(a)a^{-1}$.

□

Corollary 7.3 (Hilbert's Theorem 90: Classical)**.** *Let $E/\Bbbk$ is a finite cyclic Galois extension, that is the Galois group $\mathcal{G}_E$ is cyclic, and let $\sigma \in \mathcal{G}_E$ be a generator. If $u \in E^\times$ is a unit, then $N(u) = 1$ if and only if there exists $a \in E^\times$ such that $u = \sigma(a)a^{-1}$.*

Proof. Suppose there exists $a \in E^\times$ such that $u = \sigma(a)a^{-1}$. Above we proved $N\colon E^\times \to \Bbbk^\times$ is a

group homomorphism, and it is clear from the proof that $N(\sigma(a)) = N(a)$. Hence we have

$$N(u) = N(\sigma(a))N(a^{-1}) = N(a)N(a^{-1}) = 1.$$

Conversely, suppose $N(u) = 1$ and let $\sigma \in \mathcal{G}_E$ be a generator for $\mathcal{G}_E$. Define $\alpha\colon \mathcal{G}_E \to E^\times$ by $\alpha(\mathrm{id}) = 1$, $\alpha(\sigma) = u$ and $\alpha(\sigma^i) = u\sigma(u)\sigma^2(u)\cdots\sigma^{i-1}(u)$ for $i < n$ where $n = |\mathcal{G}_E|$. Let $0 \leq i, j < n$. In the case where $i + j < n$,

$$\begin{aligned}\alpha(\sigma^i\sigma^j) = \alpha(\sigma^{i+j}) &= u\sigma(u)\cdots\sigma^{i+j-1}(u)\\ &= (u\sigma(u)\cdots\sigma^{i-1}(u))\sigma^i(u\sigma(u)\cdots\sigma^{j-1}(u))\\ &= \alpha(\sigma^i)\sigma^i(\alpha(\sigma^j)).\end{aligned}$$

If $i + j \geq n$ then $0 \leq i + j - n < n$. Hence

$$\alpha(\sigma^i\sigma^j) = \alpha(\sigma^{i+j}) = \alpha(\sigma^{i+j-n}) = u\sigma(u)\cdots\sigma^{i+j-n-1}(u).$$

It then follows that

$$\begin{aligned}\alpha(\sigma^i)\sigma^i(\alpha(\sigma^j)) &= (u\sigma(u)\cdots\sigma^{i-1}(u))\sigma^i(u\sigma(u)\cdot\sigma^{j-1}(u))\\ &= (u\sigma(u)\cdots\sigma^{i+j-n-1}(u))\sigma^{i+j-n}(u\sigma(u)\cdots\sigma^{n-1}(u))\\ &= \alpha(\sigma^i\sigma^j)N(u)\\ &= \alpha(\sigma^i\sigma^j)\end{aligned}$$

In both cases α is a 1-cocycle. Hence by the proof of Cohomological Hilbert Theorem 90, there exists $a \in E^\times$ such that $\alpha(\sigma^i) = \sigma^i(a)a^{-1}$ for all i. Therefore for $i = 1$, $u = \sigma(a)a^{-1}$. □

There is a considerable generalization of the cohomological version of Hilbert's Theorem 90 which can be applied to the degree 1 non-abelian Galois cohomology set with coefficents in the group of units of a nice class of $\Bbbk$-algebras.

Recall that a finite dimensional associative $\Bbbk$-algebra A is **simple** if and only if it has no non-trivial 2-sided ideals.

Theorem 7.4 (Prop III.8.24 [1])**.** *Let A be a simple $\Bbbk$-algebra and let $\Omega/\Bbbk$ be a Galois extension.*

Then the degree 1 *Galois cohomology set* $H^1(\mathcal{G}_\Omega, \mathrm{GL}_1(A)(\Omega))$ *is trivial, that is*

$$H^1(\mathcal{G}_\Omega, \mathrm{GL}_1(A)(\Omega)) = 1.$$

As a corollary, we obtain a useful result that will help characterize those descent problems involving actions of the algebraic group GL_n.

Corollary 7.5. *Let* $\Omega/\Bbbk$ *be a Galois extension. Then* $H^1(\mathcal{G}_\Omega, \mathrm{GL}_n(\Omega)) = 1$.

Proof. The $n \times n$ matrix algebra $\mathrm{M}_n(\Bbbk)$ with entries in $\Bbbk$ is a simple $\Bbbk$-algebra. This follows from the fact that $I \trianglelefteq \mathrm{M}_n(\Bbbk)$ is an ideal if and only if there exists $J \trianglelefteq \Bbbk$ such that $I = \mathrm{M}_n(J)$, thus there are no non-trivial ideals of $\mathrm{M}_n(\Bbbk)$. Since $\mathrm{GL}_1(\mathrm{M}_n)(\Omega) = \mathrm{GL}_n(\Omega)$, Thm. 7.4 implies the desired result. □

8 Applications

We now apply the abstract formalism developed in the previous sections to two explicit examples of interest. Specifically, we apply the Galois descent lemma and the triviality of the degree 1 cohomology of G_Ω with coefficients in $\mathrm{GL}_n(\Omega)$ for an arbitrary Galois extension $\Omega/\Bbbk$ to the matrix conjugacy problem and a classification problem for associative $\Bbbk$-algebras.

8.1 Conjugacy problem for matrices

Let $K \in \mathsf{Fld}_\Bbbk$ and let Ω/K a Galois extension. A natural descent question then arises: If $M_0, M \in \mathrm{M}_n(K)$ are conjugate by an element in $\mathrm{GL}_n(\Omega)$ (resp. $\mathrm{SL}_n(\Omega)$), are M_0 and M conjugate by an element of $\mathrm{GL}_n(K)$ (resp. $\mathrm{SL}_n(K)$)? This question may be framed as a Galois descent problem. Let $F = \mathrm{M}_n$ and $G \subset \mathrm{GL}_n$ be an algebraic group scheme viewed as a functor from $\mathsf{Fld}_\Bbbk$ to Grp. Then since $F\colon \mathsf{Fld}_\Bbbk \to \mathsf{Set}$ is representable F satisfies the Galois descent condition, and since $G\colon \mathsf{Fld}_\Bbbk \to \mathsf{Grp}$ is an algebraic group scheme G is a Galois functor. For every extension $K \in \mathsf{Fld}_\Bbbk$ the assignment

$$\begin{aligned} G(K) \times F(K) &\longrightarrow F(K) \\ (A, B) &\longmapsto A * B := ABA^{-1} \end{aligned}$$

gives rise to an action of $G(K)$ on the set $F(K)$. Indeed, for every $A, B \in G(K)$ and $C \in F(K)$, $I_n * C = I_n C I_n^{-1} = C$ and

$$A * (B * C) = A * (BCB^{-1}) = A(BCB^{-1})A^{-1} = (AB)C(AB)^{-1} = (AB) * C.$$

This group action is functional in K. If $\iota\colon K \to L$ is a morphism in $\mathsf{Fld}_\Bbbk$, and $A \in G(K), B \in F(K)$, then

$$\begin{aligned} F(\iota)(A * B) = F(\iota)(ABA^{-1}) &= F(\iota)((a_{ij})(b_{ij})(a_{ij})^{-1}) \\ &= \iota((a_{ij})(b_{ij})(a_{ij})^{-1}) = (\iota(a_{ij}))(\iota(b_{ij}))(\iota(a_{ij}))^{-1} \\ &= \iota((a_{ij})) * \iota((b_{ij})) = G(\iota)((a_{ij})) * F(\iota)((b_{ij})) \\ &= G(\iota)(A) * F(\iota)(B) \end{aligned}$$

Therefore G acts on F. Now let $M_0 \in M_n(\Bbbk)$. Then by Theorem 6.11, for every field extension $K \in \mathsf{Fld}_\Bbbk$ and every Galois extension Ω/K, we have a bijection of pointed sets

$$F_{M_0}(\Omega/K) \xrightarrow{\cong} \ker\Big(H^1\big(\mathcal{G}_\Omega, \mathrm{Stab}_G(M_0)(\Omega)\big) \to H^1\big(\mathcal{G}_\Omega, G(\Omega)\big)\Big) \tag{7}$$

Now we consider the case when $G = \mathrm{SL}_n$.

Corollary 8.1. *Let $\Omega/\Bbbk$ be a Galois extension. Then $H^1(\mathcal{G}_\Omega, \mathrm{SL}_n(\Omega)) = 1$.*

Proof. Consider the exact sequence of $\mathcal{G}_\Omega$ -groups

$$1 \longrightarrow \mathrm{SL}_n(\Omega) \hookrightarrow \mathrm{GL}_n(\Omega) \xrightarrow{\det} \Omega^\times \longrightarrow 1.$$

Then by Proposition 5.18 we have an exact sequence

$$\mathrm{GL}_n(\Omega)^{\mathcal{G}_\Omega} \xrightarrow{\det} (\Omega^\times)^{\mathcal{G}_\Omega} \xrightarrow{\delta^0} H^1(\mathcal{G}_\Omega, \mathrm{SL}_n(\Omega)) \xrightarrow{i_*} H^1(\mathcal{G}_\Omega, \mathrm{GL}_n(\Omega))$$

of pointed sets. Note that since $\mathrm{GL}_1(\mathrm{M}_n)$ is a Galois functor, $\mathrm{GL}_n(\Omega)^{\mathcal{G}_\Omega} \cong \mathrm{GL}_n(\Bbbk)$ and $(\Omega^\times)^{\mathcal{G}_\Omega} \cong \Bbbk^\times$, and by Corollary 7.5 we have $H^1(\mathcal{G}_\Omega, \mathrm{GL}_n(\Omega)) = 1$. Therefore we have an exact sequence

$$\mathrm{GL}_n(\Bbbk) \xrightarrow{\det} \Bbbk^\times \xrightarrow{\delta^0} H^1(\mathcal{G}_\Omega, \mathrm{SL}_n(\Omega)) \longrightarrow 1$$

of pointed sets. Observe that the determinant map $\det$ is surjective. Then exactness at $\Bbbk^\times$ gives $\Bbbk^\times = \mathrm{im}\det = \ker\delta^0$. Hence δ^0 is the trivial map, and so $\mathrm{im}\,\delta^0 = 1$. Exactness at $H^1(\mathcal{G}_\Omega, \mathrm{SL}_n(\Omega))$ then implies that the kernel of the surjective map $H^1(\mathcal{G}_\Omega, \mathrm{SL}_n(\Omega)) \to 1$ is trivial. Therefore $H^1(\mathcal{G}_\Omega, \mathrm{SL}_n(\Omega)) = 1$. □

From Corollary 8.1 and (7) we have a bijection of pointed sets

$$F_{M_0}(\Omega/K) \xrightarrow{\cong} H^1(\mathcal{G}_\Omega, \mathrm{Stab}_{\mathrm{SL}_n}(M_0)(\Omega)).$$

Let ϕ denote this bijection. If $[M] \in F_{M_0}(\Omega/K)$ is the K-equivalence class of a twisted K-form of M_0 which splits over Ω, then there exists $Q \in \mathrm{SL}_n(\Omega)$ such that $QMQ^{-1} = M_0$. In this case

$\phi([M]) = [\alpha^Q]$ where α^Q is the cocycle

$$\alpha^Q \colon \mathcal{G}_\Omega \to \mathrm{Stab}_{\mathrm{SL}_n}(M_0)(\Omega)$$
$$\sigma \longmapsto Q(\sigma \cdot Q^{-1}).$$

By definition,

$$F_{M_0}(\Omega/K) = \{[M] \mid M \in F(K) \text{ and } \exists\, Q \in \mathrm{SL}_n(\Omega) \text{ s.t. } QMQ^{-1} = M_0\}$$

The equivalence class $[M_0]$ is the base point of the pointed set $F_{M_0}(\Omega/K)$, and therefore corresponds to the class of the trivial cocycle in the pointed set $H^1(\mathcal{G}_\Omega, \mathrm{Stab}_{\mathrm{SL}_n}(M_0)(\Omega))$. Moreover, for any $M \in [M_0]$ the pair (M, M_0) gives a positive answer to the conjugacy problem. Hence the bijection between $F_{M_0}(\Omega/K)$ and $H^1(\mathcal{G}_\Omega, \mathrm{Stab}_{\mathrm{SL}_n}(M_0)(\Omega))$ tells us the answer to the conjugacy problem for a given pair (M, M_0) is positive if and only if $[\alpha^Q]$ is the trivial class.

We now give an example which yields a negative answer to the conjugacy problem in this case of SL_2 with Galois extension $\overline{\mathbb{Q}}/\mathbb{Q}$.

Example 8.2. Let M_0 and M be the following matrices in $\mathrm{M}_2(\mathbb{Q})$

$$M_0 = \begin{bmatrix} 0 & -2 \\ 1 & 0 \end{bmatrix}, M = \begin{bmatrix} 0 & 2 \\ -1 & 0 \end{bmatrix}$$

Then $Q = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ is a matrix in $\mathrm{SL}_2(\overline{\mathbb{Q}})$ with the property that $QMQ^{-1} = M_0$. Note that α^Q is cohomologous to the trivial cocycle if for all $\sigma \in \mathcal{G}_{\overline{\mathbb{Q}}}$ there exists a matrix $C \in \mathrm{Stab}_{\mathrm{SL}_2}(M_0)(\overline{\mathbb{Q}})$ such that

$$\alpha^Q(\sigma) = C\alpha^I(\sigma)(\sigma \cdot C^{-1}) = C(\sigma \cdot C^{-1}).$$

Let $\sigma \in \mathcal{G}_{\overline{\mathbb{Q}}}$ denote complex conjugation. Then the above equality is $\alpha^Q(\sigma) = C(\sigma \cdot C^{-1}) = C\overline{C}^{-1}$, which is equivalently written $C = -\overline{C}^{-1}$ since

$$\alpha^Q(\sigma) = Q(\sigma \cdot Q^{-1}) = Q\overline{Q}^{-1} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I.$$

Note that $C \in \mathrm{Stab}_{\mathrm{SL}_2}(M_0)(\overline{\mathbb{Q}})$ means $CM_0 = M_0C$. Now let $C = \begin{bmatrix} z_1 & z_2 \\ z_3 & z_4 \end{bmatrix}$ be a matrix in $\mathrm{GL}_2(\overline{\mathbb{Q}})$. Then the two conditions $C = -\overline{C}^{-1}$ and $CM_0 = M_0C$ are satisfied if and only if $C = \begin{bmatrix} iu & -2iv \\ iv & iu \end{bmatrix}$ for some $u, v \in \mathbb{R}$ such that $(u, v) \neq (0, 0)$. Therefore $\det C = -(u^2+2v^2) < 0$ and hence C cannot belong to $\mathrm{SL}_2(\overline{\mathbb{Q}})$. This shows that $[\alpha^Q]$ is not the trivial class, and therefore we conclude M_0 and M are not conjugate by a matrix in $\mathrm{SL}_2(\mathbb{Q})$.

8.2 Classification problem for associative $\Bbbk$-algebras

Here we use the Galois descent lemma to classify isomorphism classes of finite dimensional associative $\Bbbk$-algebras A in terms of the Galois cohomology set of $\mathcal{G}_\Omega$ with coefficients in $\mathrm{Aut}(A)(\Omega)$.

Fix an n-dimensional $\Bbbk$-vector space V. For $K \in \mathsf{Fld}_\Bbbk$, let $F(K)$ denote the set of associative (not necessarily commutative) K-algebra structures on the vector space $V \otimes_\Bbbk K$. That is:

$$F(K) := \Big\{ \mu \colon (V \otimes_\Bbbk K) \otimes_K (V \otimes_\Bbbk K) \to (V \otimes_\Bbbk K) \mid \mathrm{assoc}(\mu) = 0 \Big\} \tag{8}$$

where $\mathrm{assoc}(\mu) \colon (V \otimes_\Bbbk K)^{\otimes 3} \to (V \otimes_\Bbbk K)$ is the K-linear map

$$\mathrm{assoc}(\mu) := \mu \circ (\mu \otimes \mathrm{id}) - \mu \circ (\mathrm{id} \otimes \mu)$$

Extension of scalars then gives us a functor

$$F \colon \mathsf{Fld}_\Bbbk \to \mathsf{Set}$$

Proposition 8.3. *The functor $F \colon \mathsf{Fld}_\Bbbk \to \mathsf{Set}$ satisfies the Galois descent condition.*

Proof. By Lemma 5.22, it suffices to show that F is representable. Hence, by Prop. 4.6, it suffices to exhibit an ideal $I \trianglelefteq \Bbbk[x_1, \ldots, x_m]$ such that we have a natural isomorphism $F \cong \mathbb{V}(I)(-)$, where $F \colon \mathsf{Alg}_\Bbbk \to \mathsf{Set}$ is the obvious extension of (8) to the category of commutative $\Bbbk$-algebras. Choose a $\Bbbk$-linear basis $\{e_i\}$ for the vector space V. Let $R \in \mathsf{Alg}_\Bbbk$, and for each $i = 1, \ldots, n$ let $\tilde{e}_i := e_i \otimes 1_K$. Then $\{\tilde{e}_i\}$ is a basis for the free R-module $V \otimes_\Bbbk R$.

Suppose $\mu \in F(R)$, and let $c_{ijs} \in R$ be elements of R such that

$$\mu(\tilde{e}_i \otimes \tilde{e}_j) = \sum_s c_{ijs}\tilde{e}_s$$

for each $i, j = 1, \ldots, m$. Then $\mathrm{assoc}(\mu) = 0$ if and only if for all $i, j, \ell = 1, \ldots, n$

$$\mathrm{assoc}(\mu)(\tilde{e}_i \otimes \tilde{e}_j \otimes \tilde{e}_\ell) = 0 \in V \otimes_{\Bbbk} R.$$

The latter equality then holds if and only if

$$\sum_{s=1}^{n}(c_{jls}c_{ist} - c_{ijs}c_{s\ell t}) = 0 \quad \text{for } t = 1, \ldots, n.$$

Hence, we deduce that μ is an associative algebra structure on $V \otimes_{\Bbbk} R$ if and only if $\{c_{ijs}\} \in \mathbb{V}(I)(R) \subseteq R^{n^3}$ where $I \trianglelefteq \Bbbk[x_{ijs}]$ is the ideal generated by the polynomials $\{P^t_{ij\ell}\}$ where

$$P^t_{ij\ell} := \sum_{s=1}^{n}(x_{jls}x_{ist} - x_{ijs}x_{s\ell t}).$$

□

There is natural conjugation-like action of the algebraic group scheme $\mathrm{GL}(V)$ on the functor $F\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Set}$. Given $g \in \mathrm{GL}(V)(K)$ and $\mu \in F(K)$ define

$$g * \mu\colon (V \otimes_{\Bbbk} K) \otimes_K (V \otimes_{\Bbbk} K) \to (V \otimes_{\Bbbk} K), \qquad g * \mu := g \circ \mu \circ (g^{-1} \otimes g^{-1}) \tag{9}$$

By construction, the fact that μ is associative implies that $\mathrm{assoc}(g * \mu) = 0$ as well. Furthermore, the K- linear map $g\colon V \otimes_{\Bbbk} K \to V \otimes_{\Bbbk} K$ is automatically an isomorphism of K-algebras

$$g\colon (V \otimes_{\Bbbk} K, g * \mu) \xrightarrow{\cong} (V \otimes_{\Bbbk} K, \mu).$$

In particular, the stabilizer of a fixed $\Bbbk$-algebra $A := (V, \mu)$, with $\mu \in F(\Bbbk)$ under the above $\mathrm{GL}(V)$ action is

$$\mathrm{Stab}_{\mathrm{GL}(V)}(A)(\Bbbk) = \mathrm{Aut}(A)(\Bbbk),$$

where $\mathrm{Aut}(A)\colon \mathsf{Fld}_{\Bbbk} \to \mathsf{Grp}$ is the Galois functor of algebra automorphisms introduced in Sec. 4.2.2.

The Galois descent lemma Thm. 6.11 combined with Cor. 7.5 implies the following characteri-

zation of the Galois descent problem for isomorphism classes of finite-dimensional $\Bbbk$-algebras

Theorem 8.4 (Prop. III.9.1 [1])**.** *Let $K/\Bbbk$ be a field extension, and let Ω/K be Galois. For any $\Bbbk$-algebra $A \in F(\Bbbk)$, the pointed set*

$$H^1(\mathcal{G}_\Omega, \mathrm{Aut}(A)(\Omega))$$

classifies the isomorphism classes of K-algebras which become isomorphic to A over Ω. In particular, the class of the trivial cocycle corresponds to the isomorphism class of $A \otimes_\Bbbk K$.

9 Future work

In this section we describe possible directions for future work. A particular problem of interest, inspired by rational homotopy theory, is to set up a Galois descent problem as described here for finite-dimensional graded polynomial algebras equipped with a degree +1 derivation.

Non graded polynomial rings $\Bbbk[x_1, x_2, \ldots, x_m]$ in $m > 0$ variables are examples of finitely generated, but infinite-dimensional $\Bbbk$-algebras. As a result, the automorphism group $\mathrm{Aut}_{\mathsf{Alg}_\Bbbk}(\Bbbk[x_1, x_2, \ldots, x_n])$ is not a subgroup of GL_n for any n. Hence, our results from Section 4.2.2 concerning representablity, etc. do not apply in this case. Indeed, we easily obtain an infinite number of $\Bbbk$-algebra automorphisms of the ungraded $\Bbbk$-algebra $\Bbbk[x, y]$ as follows. Let $f(y) \in \Bbbk[y]$ and define $\phi_f \colon \Bbbk[x, y] \to \Bbbk[x, y]$ on generators by

$$\phi_f(x) := x + f(y), \quad \phi_f(y) := y$$

Then ϕ_f is a $\Bbbk$-algebra isomorphism with inverse $\psi_f \colon \Bbbk[x, y] \to \Bbbk[x, y]$ given by $\psi_f(x) = x - f(y)$, and $\psi_f(y) = y$.

However, in some nontrivial cases, the *graded commutative* $\Bbbk$-algebra $\Bbbk[x, y]$ is finite dimensional, in which case $\mathrm{Aut}_{\mathsf{grAlg}_\Bbbk}(\Bbbk[x, y])$ is a subgroup of GL_n. For example, suppose $|x| = 1$ and $|y| = 3$ where $|x|$ and $|y|$ denote the degree of x and y respectively. Then since $\Bbbk[x, y]$ is graded commutative, we have

$$xy = (-1)^{|x||y|}yx$$

which shows $xy = -yx$. It then follows that $x^2 = 0$ and $y^2 = 0$ since $\Bbbk$ is a field of characteristic zero. Hence

$$\Bbbk[x, y] \cong \mathrm{span}_\Bbbk\{1, x, y, xy\}$$

is an isomorphism of $\Bbbk$-vector spaces, and therefore

$$\mathrm{Aut}_{\mathsf{Alg}_\Bbbk}(\Bbbk[x, y])(\Bbbk) \subseteq \mathrm{GL}_4(\Bbbk).$$

An interesting descent problem within this framework is the following: Let $A := \Bbbk[x_1, x_2, \ldots, x_n]$ be a finite-dimensional graded $\Bbbk$-algebra. Let $D \colon A \to A$ be a degree 1 deriviation. For any $F \in \mathrm{Aut}_{\mathsf{grAlg}_\Bbbk}(A)(\Bbbk)$, it is easy to show that $D' := F \circ D \circ F^{-1}$ is also a degree 1 derivation. This gives

an action of $\mathrm{Aut}_{\mathsf{grAlg}_{\Bbbk}}(A)(\Bbbk)$ on $\mathrm{Der}(A)(\Bbbk)$, the set of $\Bbbk$-linear degree 1 derivations of A. Now fix two derivations $D, D' \in \mathrm{Der}(A)(\Bbbk)$ and suppose $\Omega/\Bbbk$ is a Galois extension such that D and D' are equivalent, as elements in $\mathrm{Der}(A)(\Omega)$, via the action of $\mathrm{Aut}_{\mathsf{grAlg}_{\Bbbk}}(A)(\Omega)$. Are D and D' then equivalent as derivations over $\Bbbk$?

10 References

[1] G. Berhuy, *An Introduction to Galois Cohomology and its Applications*, London Mathematical Society Lecture Note Series, 377, Cambridge University Press, New York, 2010.

[2] D. Eisenbud and J. Harris, *The geometry of schemes*, Graduate Texts in Mathematics, 197, Springer-Verlag, New York, 2000.

[3] P. Morandi, *Field and Galois Theory*, Graduate Texts in Mathematics, 167, Springer-Verlag, New York, 1996.

[4] J.-P. Serre, *Cohomologie Galoisienne*, Lecture notes in Mathematics, 5, Springer-Verlag, 1965; 5th ed., révisée et complétée, 1994. English translation of the 5th edition: *Galois Cohomology*, Springer-Verlag, 1997.

[5] S. S. Shatz, *Profinite Groups, Arithmetic and Geometry*, Annals of Mathematics Studies, 67, Princeton University Press, 1972.

[6] K. E. Smith et al., *An Invitation to Algebraic Geometry*, Universitext, Springer-Verlag, New York, 2000.