Introduction

A recurrent problem arising in mathematics is to decide if two given mathematical structures defined over a field k are isomorphic. Quite often, it is easier to deal with this problem after scalar extension to a bigger field Ω containing k, for example an algebraic closure of k, or a finite Galois extension. In the case where the two structures happen to be isomorphic over Ω, this leads to the natural descent problem: if two k-structures are isomorphic over Ω, are they isomorphic over k? Of course, the answer is no in general. For example, consider the following matrices $M, M_0 \in \mathrm{M}_2(\mathbb{R})$:

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

It is easy to see that they are conjugate by an element of $\mathrm{GL}_2(\mathbb{C})$, since they have same eigenvalues $\pm i\sqrt{2}$, and therefore are both similar to $\begin{pmatrix} i\sqrt{2} & 0 \\ 0 & -i\sqrt{2} \end{pmatrix}$. In fact we have

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} M \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}^{-1} = M_0,$$

so M and M_0 are even conjugate by an element of $\mathrm{SL}_2(\mathbb{C})$.

A classical result in linear algebra says that M and M_0 are already conjugate by an element of $\mathrm{GL}_2(\mathbb{R})$, but this is quite obvious here since

the equality above rewrites

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} M \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{-1} = M_0.$$

However, they are not conjugate by an element of $\mathrm{SL}_2(\mathbb{R})$. Indeed, it is easy to check that a matrix $P \in \mathrm{GL}_2(\mathbb{R})$ such that $PM = M_0P$ has the form

$$P = \begin{pmatrix} a & 2c \\ c & -a \end{pmatrix}.$$

Since $\det(P) = -(a^2 + 2c^2) < 0$, P cannot belong to $\mathrm{SL}_2(\mathbb{R})$. Therefore, M and M_0 are conjugate by an element of $\mathrm{SL}_2(\mathbb{C})$ but not by an element of $\mathrm{SL}_2(\mathbb{R})$.

Hence, the descent problem for conjugacy classes of matrices has a positive answer when we conjugate by elements of the general linear group, but has a negative one when we conjugate by elements of the special linear group. So, how could we explain the difference between these two cases? This is where Galois cohomology comes into play, and we would like now to give an insight of how this could be used to measure the obstruction to descent problems on the previous example. If k is a field, let us denote by $G(k)$ the group $\mathrm{GL}_2(k)$ or $\mathrm{SL}_2(k)$ indifferently.

Assume that $QMQ^{-1} = M_0$ for some $Q \in G(\mathbb{C})$. The idea is to measure how far is Q to have real coefficients, so it is natural to consider the difference $Q\overline{Q}^{-1}$, where $\overline{Q}$ is the matrix obtained from Q by letting the complex conjugation act coefficientwise. Indeed, we will have $Q \in G(\mathbb{R})$ if and only if $\overline{Q} = Q$, that is if and only if $Q\overline{Q}^{-1} = I_2$. Of course, if $Q\overline{Q}^{-1} = I_2$, then M and M_0 are conjugate by an element of $G(\mathbb{R})$, but this is not the only case when this happens to be true. Indeed, if we assume that $PMP^{-1} = M_0$ for some $P \in G(\mathbb{R})$, then we easily get that $QP^{-1} \in G(\mathbb{C})$ commutes with M_0. Therefore, there exists $C \in Z_G(M_0)(\mathbb{C}) = \{C \in G(\mathbb{C}) \mid CM_0 = M_0C\}$ such that $Q = CP$. We then easily have $\overline{Q} = \overline{C}\,\overline{P} = \overline{C}P$, and therefore

$$Q\overline{Q}^{-1} = C\overline{C}^{-1} \text{ for some } C \in Z_G(M_0)(\mathbb{C}).$$

Conversely, if the equality above holds then $P = C^{-1}Q$ is an element of $G(\mathbb{R})$ satisfying $PMP^{-1} = M_0$. Indeed, we have

$$\overline{P} = \overline{C}^{-1}\overline{Q} = C^{-1}Q = P,$$

so $P \in G(\mathbb{R})$, and

$$PMP^{-1} = C^{-1}QMQ^{-1}C = C^{-1}M_0C = M_0C^{-1}C = M_0.$$

Thus, M and M_0 will be congugate by an element of $G(\mathbb{R})$ if and only if

$$Q\overline{Q}^{-1} = C\overline{C}^{-1} \text{ for some } C \in Z_G(M_0)(\mathbb{C}).$$

Notice also for later use that $Q\overline{Q}^{-1} \in G(\mathbb{C})$ commutes with M_0, as we may check by applying complex conjugation on both sides of the equality $QMQ^{-1} = M_0$.

If we go back to our previous example, we have $Q = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, and therefore $Q\overline{Q}^{-1} = -I_2$. Easy computations show that we have

$$Z_G(M_0)(\mathbb{C}) = \left\{ C \in G(\mathbb{C}) \mid C = \begin{pmatrix} z & -2z' \\ z' & z \end{pmatrix} \text{ for some } z, z' \in \mathbb{C} \right\}.$$

Therefore, we will have $C \in Z_G(M_0)(\mathbb{C})$ and $C\overline{C}^{-1} = Q\overline{Q}^{-1} = -I_2$ if and only if

$$C = \begin{pmatrix} iu & -2iv \\ iv & iu \end{pmatrix} \text{ for some } u, v \in \mathbb{R}, (u, v) \neq (0, 0).$$

Notice that the determinant of the matrix above is $-(u^2 + 2v^2) < 0$. Thus, if $G(\mathbb{C}) = \mathrm{GL}_2(\mathbb{C})$, one may take $u = 1$ and $v = 0$, but if $G(\mathbb{C}) = \mathrm{SL}_2(\mathbb{C})$, the equation $C\overline{C}^{-1} = -I_2 = Q\overline{Q}^{-1}$ has no solution in $Z_G(M_0)(\mathbb{C})$. This explains a bit more conceptually the difference between the two descent problems. In some sense, if $QMQ^{-1} = M_0$ for some $Q \in G(\mathbb{C})$, the matrix $Q\overline{Q}^{-1}$ measures how far is M to be conjugate to M_0 over $\mathbb{R}$.

Of course, all the results above remain valid if M and M_0 are square matrices of size n, and if $G(k) = \mathrm{GL}_n(k), \mathrm{SL}_n(k), \mathrm{O}_n(k)$ or even $\mathrm{Sp}_{2n}(k)$. If we have a closer look to the previous computations, we see that the reason why all this works is that $\mathbb{C}/\mathbb{R}$ is a Galois extension, whose Galois group is generated by complex conjugation.

Let us consider now a more general problem: let Ω/k be a finite Galois extension, and let $M, M_0 \in \mathrm{M}_n(k)$ be two matrices such that

$$QMQ^{-1} = M_0 \text{ for some } Q \in G(\Omega).$$

Does there exist $P \in G(k)$ such that $PMP^{-1} = M_0$?

Since Ω/k is a finite Galois extension, then for all $x \in \Omega$, we have $x \in k$ if and only if $\sigma(x) = x$ for all $\sigma \in \mathrm{Gal}(\Omega/k)$. If now $Q \in G(\Omega)$, then let us denote by $\sigma \cdot Q \in G(\Omega)$ the matrix obtained from Q by letting σ act coefficientwise. Then we have

$$\begin{array}{rcl} Q \in G(k) & \iff & \sigma \cdot Q = Q \text{ for all } \sigma \in \mathrm{Gal}(\Omega/k) \\ & \iff & Q(\sigma \cdot Q)^{-1} = I_2 \text{ for all } \sigma \in \mathrm{Gal}(\Omega/k). \end{array}$$

As before, applying $\sigma \in \mathrm{Gal}(\Omega/k)$ to the equality $QMQ^{-1} = M_0$, we see that $Q(\sigma \cdot Q)^{-1} \in Z_G(M_0)(\Omega)$. We therefore get a map

$$\alpha^Q : \begin{array}{c} \mathrm{Gal}(\Omega/k) \longrightarrow Z_G(M_0)(\Omega) \\ \sigma \longmapsto Q(\sigma \cdot Q)^{-1}. \end{array}$$

Arguing as at the beginning of this introduction, one can show that M and M_0 will be conjugate by an element of $G(k)$ if and only if there exists $C \in Z_G(M_0)(\Omega)$ such that $\alpha^Q = \alpha^C$, that is if and only if there exists $C \in Z_G(M_0)(\Omega)$ such that

$$Q(\sigma \cdot Q)^{-1} = C(\sigma \cdot C)^{-1} \text{ for all } \sigma \in \mathrm{Gal}(\Omega/k).$$

To summarize, to any matrix $M \in \mathrm{M}_n(k)$ which is conjugate to M_0 by an element of $G(\Omega)$, we may associate a map $\alpha^Q : \mathrm{Gal}(\Omega/k) \longrightarrow Z_G(M_0)(\Omega)$, which measures how far is M to be conjugate to M_0 by an element of $G(k)$.

This has a kind of a converse: for any map

$$\alpha : \begin{array}{c} \mathrm{Gal}(\Omega/k) \longrightarrow Z_G(M_0)(\Omega) \\ \sigma \longmapsto \alpha_\sigma \end{array}$$

such that $\alpha = \alpha^Q$ for some $Q \in G(\Omega)$, one may associate a matrix of $M_n(k)$ which is conjugate to M_0 by an element of $G(k)$ by setting $M_\alpha = Q^{-1}M_0Q$. To see that M_α is indeed an element of $\mathrm{M}_n(k)$, notice first that we have

$$\sigma \cdot (CM'C^{-1}) = (\sigma \cdot C)(\sigma \cdot M')(\sigma \cdot C)^{-1}$$

for all $C \in G(\Omega), M' \in \mathrm{M}_n(\Omega), \sigma \in \mathrm{Gal}(\Omega/k)$. Thus, for all $\sigma \in$

$\mathrm{Gal}(\Omega/k)$, we have

$$\begin{aligned}\sigma\cdot M_\alpha &= (\sigma\cdot Q)^{-1}M_0(\sigma\cdot Q)\\ &= Q^{-1}Q(\sigma\cdot Q)^{-1}M_0(\sigma\cdot Q)\\ &= Q^{-1}M_0Q(\sigma\cdot Q)^{-1}(\sigma\cdot Q)\\ &= Q^{-1}M_0Q\\ &= M_\alpha,\end{aligned}$$

the third equality coming from the fact that $\alpha_\sigma = Q(\sigma\cdot Q)^{-1}$ lies in $Z_G(M_0)(\Omega)$.

Not all the maps $\alpha\colon \mathrm{Gal}(\Omega/k) \longrightarrow Z_G(M_0)(\Omega)$ may be written α^Q for some $Q \in G(\Omega)$. In fact, easy computations show that a necessary condition for this to hold is that α is a **cocycle**, that is

$$\alpha_{\sigma\tau} = \alpha_\sigma\, \sigma\cdot\alpha_\tau \text{ for all } \sigma,\tau \in \mathrm{Gal}(\Omega/k).$$

This condition is not sufficient in general. However, it happens to be the case if $G(\Omega) = \mathrm{GL}_n(\Omega)$ or $\mathrm{SL}_n(\Omega)$ (this will follow from Hilbert 90).

Notice that until now we picked a matrix $Q \in G(\Omega)$ which conjugates M into M_0, but this matrix Q is certainly not unique. We could therefore wonder what happens if we take another matrix $Q' \in G(\Omega)$ which conjugates M into M_0. Computations show that we have $Q'Q^{-1} \in Z_G(M_0)(\Omega)$. Therefore, there exists $C \in Z_G(M_0)(\Omega)$ such that $Q' = CQ$, and we easily get that

$$\alpha_\sigma^{Q'} = C\alpha_\sigma^Q(\sigma\cdot C)^{-1} \text{ for all } \sigma \in \mathrm{Gal}(\Omega/k).$$

Two cocycles $\alpha, \alpha'\colon \mathrm{Gal}(\Omega/k) \longrightarrow Z_G(M_0)(\Omega)$ such that

$$\alpha'_\sigma = C\alpha_\sigma(\sigma\cdot C)^{-1} \text{ for all } \sigma \in \mathrm{Gal}(\Omega/k)$$

for some $C \in Z_G(M_0)(\Omega)$ will be called **cohomologous**. Being cohomologous is an equivalence relation on the set of cocycles, and the set of equivalence classes is denoted by $H^1(\mathrm{Gal}(\Omega/k), Z_G(M_0)(\Omega))$. If α is a cocycle, we will denote by $[\alpha]$ the corresponding equivalence class. Therefore, to any matrix $M \in \mathrm{M}_n(k)$ which is conjugate to M_0 by an element of $G(\Omega)$, one may associate a well-defined cohomology class $[\alpha^Q]$, where $Q \in G(\Omega)$ is any matrix satisfying $QMQ^{-1} = M_0$.

It is important to notice that the class $[\alpha^Q]$ does not characterize M completely. Indeed, for every $P \in G(k)$, it is easy to check that $\alpha^{QP^{-1}} =$

α^Q. In particular, the cohomology classes associated to the matrices M and PMP^{-1} are equal, for all $P \in G(k)$.

Conversely, if $\alpha = \alpha^Q$ and $\alpha' = \alpha^{Q'}$ are cohomologous, it is not too difficult to see that $P = Q^{-1}C^{-1}Q' \in G(k)$, and that the corresponding matrices M_α and $M_{\alpha'}$ satisfy $PM_{\alpha'}P^{-1} = M_\alpha$.

Thus the previous considerations show that, in the case where every cocycle $\alpha\colon \mathrm{Gal}(\Omega/k) \longrightarrow Z_G(M_0)(\Omega)$ may be written $\alpha = \alpha^Q$ for some $Q \in G(\Omega)$, the set $H^1(\mathrm{Gal}(\Omega/k), Z_G(M_0)(\Omega))$ is in one-to-one correspondence with the set of $G(k)$-conjugacy classes of matrices $M \in \mathrm{M}_n(k)$ which are conjugate to M_0 by an element of $G(\Omega)$.

Many situations can be dealt with in a similar way. For example, reasoning as above and using Hilbert 90, one can show that the set of isomorphism classes of quadratic forms q which are isomorphic to the quadratic form $x_1^2 + \ldots + x_n^2$ over Ω is in one-to-one correspondence with $H^1(\mathrm{Gal}(\Omega/k), \mathrm{O}_n(\Omega))$.The case of k-algebras is a little bit more subtle, but one can show that the set of isomorphism classes of k-algebras which are isomorphic to a given k-algebra A over Ω is in one-to-one correspondence with $H^1(\mathrm{Gal}(\Omega/k), \mathrm{Aut}_{\Omega-\mathrm{alg}}(A \otimes_k \Omega))$.

Quite often, algebraic structures can be well understood over a separable closure k_s of k. In the best cases, they even become isomorphic over k_s. Therefore, it is useful to extend this setting to the case of infinite Galois field extensions. To do this, we will introduce the notion of a profinite group in Chapter 1, and recollect some facts on infinite Galois theory. Then in Chapter 2 we define the cohomology sets $H^i(\Gamma, A)$ for any profinite group Γ and any Γ-group A, and study their functorial properties and their behavior with respect to short exact sequences. We also introduce the cup-product, which is useful to construct higher cohomology classes. Chapter 3 deals with Galois cohomology and the central part of this chapter is devoted to formalize Galois descent and to give applications. We then come back to the conjugacy problem for matrices and compute the total obstruction in an example. In Chapter 4, we study Galois cohomology of quadratic forms and give a cohomological interpretation of some classical invariants attached to quadratic forms, such as the determinant or the Hasse invariant. In Chapter 5, we obtain an algebraic interpretation of Galois field extensions with Galois group G in terms of $H^1(\mathrm{Gal}(k_s/k), G)$. In Chapter 6, we give a cohomological

obstruction of the following Galois embedding problem: given a group extension $1 \longrightarrow A \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1$, where A is a central subgroup of $\tilde{G}$, and given a Galois field extension E/k with Galois group G, does there exists a Galois field extension $\tilde{E}/k$ with Galois group $\tilde{G}$ such that $\tilde{E}^A = E$?

The next chapters describe various applications of Galois cohomology. Chapter 7 is devoted to the study of a certain Galois embedding problem with kernel $A = \mathbb{Z}/2\mathbb{Z}$. In this particular case we prove a formula of Serre which computes the obstruction in terms of the classical invariant of the trace form of E, and we give simple applications. We then study Galois cohomology of central simple algebras with or without involutions in Chapter 8. As an application of Galois cohomology techniques, we compute the Hasse invariant of certain quadratic forms attached to these algebras. In Chapter 9, we briefly introduce the notion of a G-torsor, which gives a geometric interpretation of Galois cohomology. We apply this point of view to derive some results on cohomological invariants of algebraic groups. In Chapter 10, we describe applications of Galois cohomology to the so-called Noether's problem: given a field k and a finite group G, is there a linear faithful representation V of G such that the field extension $k(V)^G/k$ is purely transcendental ? This is known to be true when G is abelian and $k \supset \mu_n$, but false for $G = \mathbb{Z}/8\mathbb{Z}$ and $k = \mathbb{Q}$. We will introduce the residue maps in Galois cohomology and use their properties to prove that Noether's problem has a negative solution when $G = \mathbb{Z}/2^m\mathbb{Z}, m \geq 3$ and $k = \mathbb{Q}$. To do so, we attach to each Galois extension of group G over a field $K \supset k$ a non-vanishing cohomological obstruction. In Chapter 11, we study another kind of rationality problem: given a linear algebraic group G over k, is the underlying variety rational? This is known to be true for classical groups when k is algebraically closed. We will show that the answer is negative in general when k is an arbitrary field. We will focus on the case where G is an automorphism group of some algebra with a symplectic involution. Once again, the answer will come from the existence of a non-zero cohomological obstruction. Finally in Chapter 12, we introduce the notion of essential dimension of a functor, which is an active research topic, for which substantial progress has been made recently. If G is a finite group, the essential dimension of the Galois cohomology functor $H^1(\_, G)$ will be the number of independent parameters needed to describe a Galois extension of group G.

This introduction to Galois cohomology does not pretend to be complete. For example, we are aware that an historical introduction to the subject is missing. The curious reader is referred to [30], p. 446-449, as well as [58] and [59] for more information and numerous references. Moreover, we tried to reduce the prerequisites necessary to read these notes to the minimum. Only some basic knowledge on Galois theory and algebra (definition of group, ring, field, k-algebra, notion of tensor product) is required. Also it was impossible to cover all the 'hot topics' (such as Serre's conjecture II, Hasse principle, Rost invariants) or applications of Galois cohomology. Once again, we refer to [30], [58] and [59]. More advanced material on Galois cohomology may be found in [25],[26], [30] or [58], each of these references focusing on a different aspect of the theory: cohomological invariants (including the construction of Rost invariants) and applications to Noether's problem in [25], Merkurjev-Suslin's theorem in [26], algebras with involution in [30] or cohomology of algebraic groups over fields of small cohomological dimension in [58].

This book is an extended version of notes of some postgraduate lectures on Galois cohomology that we gave at the University of Southampton, which included originally Chapters 1-7. The main goal of these lectures was to introduce enough material on Galois cohomology to fully understand the proof of Serre's formula [61] aiming at an audience having a minimal background in algebra, and to give applications to Galois embedding problems. The method we chose to establish this formula differs a bit from the original one. It was suggested as an alternative proof by Serre himself in [61]. Moreover, it was a good occasion to introduce classical tools such as exact sequences in cohomology, Galois descent, Hilbert 90 and some standard results such as Springer's cohomological interpretation of the Hasse invariant. Consequently, the material introduced in Part I is really basic, but is sufficient to obtain beautiful applications to inverse Galois theory or to the conjugacy problem. We also took a particular care to make the first half of this book self-contained, with an exception made for the section on infinite Galois theory and for Proposition III.7.23. Let us also mention the existence of lectures notes [2] presenting a shortened and simplified exposition of the material introduced in Chapters II and III (in these notes, all Galois extensions considered are finite, only the first cohomology set is presented and the functorial aspect of the theory is not treated). The second part of the book gives an insight of how Galois cohomology may be useful to solve some algebraic problems, and presents active research topics, such as ra-

tionality questions or essential dimension of algebraic groups and often requires more advanced material. Therefore, proofs of the most difficult results are skipped. We hope that these notes will help the reader willing to study more advanced books on this subject, such as those cited above.

This book could not have been written without the encouragements and the support of Gerhard Roerhle, and we would like to thank him warmly. We are also grateful to our colleagues and friends Vincent Beck, Jérôme Ducoat, Jean Fasel, Nicolas Grenier-Boley, Emmanuel Lequeu, Frédérique Oggier, Gerhard Roerhle and Jean-Pierre Tignol, who took time to read partly or integrally some earlier versions of the manuscript, despite the fact they certainly had better things to do. Their careful reading, judicious comments and remarks permitted to improve significantly the exposition and to detect many misprints or inaccuracies. The whole LaTeX support team of Cambridge University Press deserves a special mention for its efficiency and its patience. Finally, we would like to thank Roger Astley, Caroline Brown and Clare Dennison for their helpfulness in the whole editing process.

Part I

An introduction to Galois cohomology