AN INTRODUCTION TO GALOIS COHOMOLOGY AND ITS APPLICATIONS

GRÉGORY BERHUY

Contents

1. Introduction 1
2. Cohomology sets 6
3. Hilbert's 90^{th} theorem 9
4. Exact sequences in cohomology 12
5. (The) matrix (case) reloaded 16
6. Functors 19
7. Functorial group actions 21
8. Twisted forms 22
9. The Galois descent condition 23
10. Stabilizers 24
11. Galois descent lemma 25
12. The conjugacy problem again 29
13. The case of infinite Galois extensions 33

1. 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

Date: March 23, 2018.

$\begin{pmatrix} i\sqrt{2} & 0 \\ 0 & -i\sqrt{2} \end{pmatrix}$. 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 $\overline{Q} = Q$, 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

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

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 $M, M_0 \in \mathrm{M}_n(k)$ two matrices such that

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

Does there exists $P \in G(k)$ 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

$$\alpha^Q : \mathrm{Gal}(\Omega/k) \to Z_G(M_0)(\Omega), \sigma \mapsto \alpha^Q_\sigma = Q(\sigma\cdot Q)^{-1}.$$

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 $\alpha^Q : \mathrm{Gal}(\Omega/k) \to Z_G(M_0)(\Omega)$, 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

$$\alpha : \mathrm{Gal}(\Omega/k) \to Z_G(M_0)(\Omega), \sigma \mapsto \alpha_\sigma$$

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

$$\sigma\cdot(C_1C_2) = (\sigma\cdot C_1)(\sigma\cdot C_2) \text{ for all } C_1, C_2 \in G(\Omega), \sigma \in \mathrm{Gal}(\Omega/k).$$

Thus, for all $\sigma \in \mathrm{Gal}(\Omega/k)$, we have

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

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 $\alpha : \mathrm{Gal}(\Omega/k) \to Z_G(M_0)(\Omega), \sigma \mapsto \alpha_\sigma$ 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

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

Two cocycles $\alpha, \alpha' : \mathrm{Gal}(\Omega/k) \to Z_G(M_0)(\Omega)$ 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 $\alpha^{QP^{-1}} = \alpha^Q$. 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 then show that, in the case where every cocycle $\alpha : \mathrm{Gal}(\Omega/k) \to Z_G(M_0)(\Omega), \sigma \mapsto \alpha_\sigma$ 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 $x_1^2+\cdots+x_n^2$ 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, and Galois cohomology may be of great interest in this situation. However, to avoid technicalities we will assume that Ω/k is finite, and come back to the infinite case at the very end.

2. Cohomology sets

Definition 2.1. Let G be a finite group. A set A is called a G**-set** if G acts on A on the left. A group A is called a G**-group** if G acts on A by group morphisms, i.e.

$$\sigma\cdot(a_1a_2) = (\sigma\cdot a_1)(\sigma\cdot a_2) \text{ for } \sigma\in G, a_1, a_2\in A.$$

A G-group which is commutative is called a G**-module**.

A **morphism** of G-sets (resp. G-groups, G-modules) is a map (resp. a group morphism) $f: A\to A'$ satisfying the following property:

$$f(\sigma\cdot a) = \sigma\cdot f(a) \text{ for all } \sigma\in G \text{ and all } a\in A.$$

Examples 2.2.

(1) Let Ω/k be a Galois extension of group $\mathcal{G}_\Omega$. Then the map

$$\mathcal{G}_\Omega\times\Omega\to\Omega, (\sigma, x)\mapsto \sigma\cdot x = \sigma(x)$$

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

(2) Let Ω/k be a Galois extension of group $\mathcal{G}_\Omega$. Then $\mathcal{G}_\Omega$ acts naturally on $\mathrm{GL}_n(\Omega)$ as follows: for $\sigma\in\mathcal{G}_\Omega$ and $M = (m_{ij})\in\mathrm{GL}_n(\Omega)$, set

$$\sigma\cdot M = (\sigma(m_{ij})).$$

Clearly, this is an action by group automorphisms. The same is true for other matrix groups such as $\mathrm{SL}_n(\Omega)$ or $\mathrm{O}_n(\Omega)$.

At this point, we may define the 0^{th}-cohomology set $H^0(\mathcal{G}_\Omega, A)$.

Definition 2.3. For any G-set A, we set

$$H^0(G, A) = A^G.$$

If A is a G-group, this is a subgroup of A. The set $H^0(G, A)$ is called the $\mathbf{0^{th}}$ **cohomology set of** G **with coefficients in** A.

We will not really use this notation except once or twice, preferring writing A^G instead of $H^0(G, A)$. We now come to the main object of these lectures:

Definition 2.4. Let A be a G-group. A **1-cocycle** with values in A is a map $\alpha: G\to A, \sigma\mapsto\alpha_\sigma$ such that

$$\alpha_{\sigma\tau} = \alpha_\sigma\,\sigma\cdot\alpha_\tau \text{ for } \sigma, \tau\in G.$$

We denote by $Z^1(G, A)$ the set of all 1-cocycles of G with values in A. The constant map $\alpha_\sigma = 1$ is an element of $Z^1(G, A)$, which is called the **trivial** 1-cocycle. Notice also that for any 1-cocycle α, we have $\alpha_1 = 1$.

Remark 2.5. If G acts trivially on A, a 1-cocycle is just a morphism $\alpha: G\to A$.

In order to define the cohomology set $H^1(G, A)$, we need now an appropriate notion of cohomologous cocycles, which coincide with the one defined in the introduction in a particular case. This will be provided by the following lemma:

Lemma 2.6. *Let A be a G-group and let $\alpha : G \to A$ be a 1-cocycle. Then for all $a \in A$, the map*

$$\alpha' : G \to A, \sigma \mapsto a\alpha_\sigma \, \sigma\cdot a^{-1}$$

is again a 1-cocycle.

This leads to the following definition:

Definition 2.7. Two 1-cocycles α, α' are said to be **cohomologous** if there exists $a \in A$ satisfying

$$\alpha'_\sigma = a\alpha_\sigma \, \sigma\cdot a^{-1} \text{ for all } \sigma \in G.$$

It is denoted by $\alpha \sim \alpha'$.

Remark 2.8. The symbol '$\sigma\cdot a^{-1}$' may seem ambiguous at first sight, since it could denote $(\sigma\cdot a)^{-1}$ as well as $\sigma\cdot(a^{-1})$. However, these two elements are equal in our setting, since G acts on A by group automorphisms; we will keep this notation throughout.

Definition 2.9. Let A be a G-group. The relation '$\sim$' is easily checked to be an equivalence relation on $Z^1(G, A)$. We denote by $H^1(G, A)$ the quotient set

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

It is called **the first cohomology set of G with coefficients in A**.

The set $H^1(G, A)$ is not a group in general. However, it has a distinguished element, which is the class of the trivial cocycle. Therefore, $H^1(G, A)$ is a pointed set in the following sense:

Definition 2.10. A **pointed set** is a pair (E, x), where E is a nonempty set and $x \in E$. The element x is called the **base point**. A **map of pointed sets** $f : (E, x) \to (F, y)$ is a set-theoretic map such that $f(x) = y$. We will often forget to specify the base point when it is clear from the context. The **kernel** of a map $f : (E, x) \to (F, y)$ of pointed sets is the preimage of y.

Example 2.11. The set $H^1(G, A)$ is a pointed set, and any abstract group G may be considered as a pointed set, whose base point is the neutral element.

Remark 2.12. If A is a G-module, the set $Z^1(G, A)$ is an abelian group for the pointwise multiplication of functions. This operation is compatible with the equivalence relation, hence it induces an abelian group structure on $H^1(G, A)$.

We now look to the behaviour of these sets when G or A vary.

Definition 2.13. Let G, G' be two finite groups. Let A be a G-group and A' be a G'-group. Moreover, let $\varphi : G' \to G$ and $f : A \to A'$ be two group morphisms.

We say that f and φ are **compatible** if

$$f(\varphi(\sigma') \cdot a) = \sigma' \cdot f(a) \text{ for } \sigma' \in G', a \in A.$$

Notice that it follows from the very definition that if a is fixed by G, then $f(a)$ is fixed by G'. Hence f induces by restriction a map of pointed sets

$$f_* : H^0(G, A) \to H^0(G', A').$$

The following proposition shows that this is also true for H^1.

Proposition 2.14. *Let G, G', A, A' as above, and let $\varphi : G' \to G$ and $f : A \to A'$ be two compatible group morphisms. For any cocycle $\alpha \in Z^1(G, A)$, the map*

$$\beta : G' \to A', \sigma' \mapsto f(\alpha_{\varphi(\sigma')})$$

is a cocycle.

Moreover, the assignment $\alpha \in Z^1(G, A) \mapsto \beta \in Z^1(G', A')$ induces a map of pointed sets (resp. a group morphism if A and A' are abelian)

$$f_* : H^1(G, A) \to H^1(G', A').$$

Proof. By definition, we have $\beta_{\sigma'} = f(\alpha_{\varphi(\sigma')})$. Hence, for all $\sigma', \tau' \in G$, we have $\beta_{\sigma'\tau'} = f(\alpha_{\varphi(\sigma')\varphi(\tau')})$, since φ is a group morphism. Since α is a 1-cocycle, we get

$$\beta_{\sigma'\tau'} = f(\alpha_{\varphi(\sigma')}\, \varphi(\sigma') \cdot \alpha_{\varphi(\tau')}) = f(\alpha_{\varphi(\sigma')}) f(\varphi(\sigma') \cdot \alpha_{\varphi(\tau')}).$$

By compatibility, we get that

$$\beta_{\sigma'\tau'} = f(\alpha_{\varphi(\sigma')})\, \sigma' \cdot f(\alpha_{\varphi(\tau')}) = \beta_{\sigma'} \sigma' \cdot \beta_{\tau'}.$$

Hence β is a 1-cocycle.

Now we have to show that if α and α' are cohomologous, then the corresponding β and β' are also cohomologous, so assume that

$$\alpha'_\sigma = a \alpha_\sigma\, \sigma \cdot a^{-1} \text{ for all } \sigma \in G,$$

for some $a \in A$. Applying this relation to $\sigma = \varphi(\sigma')$ and taking f on both sides gives

$$\beta'_{\sigma'} = f(a \alpha_{\varphi(\sigma')} \varphi(\sigma') \cdot a^{-1}).$$

Since f is a group morphism which is compatible with φ, we get

$$\beta'_{\sigma'} = f(a) f(\alpha_{\varphi(\sigma')})\, \sigma' \cdot f(a)^{-1} = f(a) \beta_{\sigma'}\, \sigma' \cdot f(a)^{-1}.$$

Hence β and β' are cohomologous. Finally, it is clear from the definition that f_* maps the trivial class onto the trivial class. □

Example 2.15. Assume that $G = G'$ and $\varphi = \mathrm{Id}_G$. Then a compatible map $f : A \to A'$ is just a morphism of G-groups, and the map f_* just sends the cohomology class of α to the cohomology class of $f \circ \alpha$. Moreover, if $g : A' \to A''$ is a morphism of G-sets (or G-groups, etc), we have $(g \circ f)_* = g_* \circ f_*$.

In the sequel, f_* will always denote the map induced by Id_G and f. We now provide one example of computation of a Galois cohomology set.

3. Hilbert's 90^{th} theorem

To prove the so-called Hilbert's 90^{th} theorem, we will need some preliminary results on semi-linear actions.

Definition 3.1. Let Ω/k be a Galois extension of Galois group $\mathcal{G}_\Omega$, and let U be a (right) vector space over Ω with an action $*$ of $\mathcal{G}_\Omega$ on U. We will denote by '$\cdot$' the standard linear action of $\mathcal{G}_\Omega$ on Ω. We say that $\mathcal{G}_\Omega$ acts **by semi-linear automorphisms** on U if we have for all $u, u' \in U, \lambda \in \Omega$

$$\begin{array}{lll} \sigma * (u + u') & = & \sigma * u + \sigma * u'; \\ \sigma * (u\lambda) & = & (\sigma * u)(\,\sigma\cdot\lambda). \end{array}$$

Examples 3.2.

(1) Let V be a k-vector space, and let $U = V \otimes_k \Omega$. The action of $\mathcal{G}_\Omega$ on U defined on elementary tensors by

$$\sigma * (v \otimes \lambda) = v \otimes (\,\sigma\cdot\lambda) \text{ for all } v \in V, \lambda \in \Omega$$

is an action by semi-linear automorphisms.

(2) Let $U = \Omega^n$, and let $\mathcal{G}_\Omega$ act in an obvious way on each coordinate. We obtain that way an action by semi-linear automorphisms. Morever, $U^{\mathcal{G}_\Omega} = k^n$, and we have a canonical isomorphism of Ω-vector spaces

$$U^{\mathcal{G}_\Omega} \otimes_k \Omega \to U, u \otimes \lambda \mapsto u\lambda.$$

Notice that this isomorphism is also an isomorphism of $\mathcal{G}_\Omega$-modules.

The following lemma generalizes the previous example.

Lemma 3.3. *[Galois descent of vector spaces] Let U be a vector space over Ω. If $\mathcal{G}_\Omega$ acts on U by semi-linear automorphisms, then $U^{\mathcal{G}_\Omega} = \{u \in U \mid \sigma * u = u \text{ for all } \sigma \in \mathcal{G}_\Omega\}$ is a k-vector space and the map*

$$f : U^{\mathcal{G}_\Omega} \otimes_k \Omega \to U, u \otimes \lambda \mapsto u\lambda$$

is an isomorphism of Ω-vector spaces.

Proof. It is clear that $U^{\mathcal{G}_\Omega}$ is a k-vector space, and that f is Ω-linear. We first prove the surjectivity of f. Let $u\in U$, let $\lambda_1,\ldots,\lambda_n$ be a k-basis of Ω and let $\sigma_1=\mathrm{Id}_\Omega,\sigma_2,\ldots,\sigma_n$ be the elements of $\mathcal{G}_\Omega$. Let

$$u_i=\sum_j \sigma_j*(u\lambda_i).$$

For all $k=1,\ldots,n$, we have

$$\sigma_k*u_i=\sum_j(\sigma_k\sigma_j)(u\lambda_i).$$

Hence the action of σ_k on $\sum\limits_j\sigma_j*(u\lambda_i)$ just permutes the terms of the sum, so $u_i\in U^{\mathcal{G}_\Omega}$.
Since $\sigma_1,\ldots,\sigma_n$ are precisely the n k-automorphisms of Ω, they are linearly independent over Ω in $\mathrm{End}_k(\Omega)$ (this is Dedekind's Lemma). Hence the matrix $M=(\sigma_j{\cdot}\lambda_i)_{i,j}$ lies in $\mathrm{GL}_n(\Omega)$. By definition of u_j, we have $u_j=\sum\limits_k(\sigma_k*u)(\sigma_k{\cdot}\lambda_j)$. Now if $M^{-1}=(m'_{ij})$, from the equation $M^{-1}M=I_n$, we get

$$(\sum_j m'_{1j}(\sigma_k{\cdot}\lambda_j)=\delta_{1k}\text{ for all }k=1,\ldots n,$$

by comparing first rows. Hence we have

$$\sum_j u_jm'_{1j}=\sum_j\sum_k(\sigma_k*u)(\sigma_k{\cdot}\lambda_j)m'_{1j}=\sum_k(\sigma_k*u)\delta_{1k}=\sigma_1*u=u,$$

the last equality coming from the fact that $\sigma_1=\mathrm{Id}_\Omega$. Therefore, we have

$$u=\sum_j u_jm'_{1j}=f(\sum_j u_j\otimes m'_{1j}),$$

which proves the surjectivity of f. To prove its injectivity, it is enough to prove the following:

Claim: Any vectors $u_1,\ldots,u_r\in U^{\mathcal{G}_\Omega}$ which k-linearly independent remain Ω-linearly independent in U.

Indeed, assume that the claim is proved, and let $x\in\ker(f)$. One may write

$$x=u_1\otimes\mu_1+\ldots+u_r\otimes\mu_r,$$

for some $\mu_1,\ldots,\mu_r\in\Omega$ and some $u_1,\ldots,u_r\in U^{\mathcal{G}_\Omega}$ which are linearly independent. By assumption, $f(x)=0=u_1\mu_1+\ldots+u_r\mu_r$. Now the claim implies that $\mu_1=\ldots=\mu_r=0$, and thus $x=0$, proving the injectivity of f.

It remains to prove the claim. We are going to do it by a way of contradiction. Assume that we have k-linearly independent vectors

$u_1, \dots, u_r \in U^{\mathcal{G}_\Omega}$ for which there exists $\mu_1, \dots, \mu_r \in \Omega$, not all them being zero, such that

$$u_1\mu_1 + \dots + u_r\mu_r = 0.$$

We may assume that r is minimal, $r > 1$ and $\mu_1 = 1$. By assumption, the μ_i's are not all in k, so we may also assume that $\mu_2 \notin k$. Choose $\sigma \in \mathcal{G}_\Omega$ such that $\sigma\cdot\mu_2 \neq \mu_2$. We have

$$\sigma * (\sum_i u_i\mu_i) = \sum_i (\sigma * u_i)(\sigma\cdot\mu_i) = \sum_i u_i(\sigma\cdot\mu_i) = 0$$

and therefore we get $\sum_{i\geq 2} u_i(\sigma\cdot\mu_i - \mu_i) = 0$, a non-trivial relation with fewer terms. This is a contradiction, and this concludes the proof. □

Remark 3.4. If we endow $U^{\mathcal{G}_\Omega} \otimes_k \Omega$ with the natural semi-linear action as in Example 3.2 (1), we claim that the isomorphism f above is an isomorphism of $\mathcal{G}_\Omega$-modules, that is f is equivariant with respect to the two semi-linear actions.

To check this, it is enough to do it on elementary tensors. Now for all $u \in U^{\mathcal{G}_\Omega}, \lambda \in \Omega$ and $\sigma \in \mathcal{G}_\Omega$, we have

$$f(\sigma * (u \otimes \lambda)) = u(\sigma\cdot\lambda) = (\sigma * u)(\sigma\cdot\lambda) = \sigma * (u\lambda) = \sigma * f(u \otimes \lambda),$$

hence the claim.

We are now ready for our first example.

Proposition 3.5 (Hilbert 90)**.** *For every Galois extension Ω/k, we have $H^1(\mathcal{G}_\Omega, \mathrm{GL}_n(\Omega)) = 1$.*

Proof. Let $\alpha \in Z^1(\mathcal{G}_\Omega, \mathrm{GL}_n(\Omega))$. We twist the natural action of $\mathcal{G}_\Omega$ on $U = \Omega^n$ in an action by semi-linear automorphisms:

$$\sigma * u = \alpha_\sigma(\sigma\cdot u) \text{ for all } u \in U, \sigma \in \mathcal{G}_\Omega.$$

We then get an isomorphism $f : U^{\mathcal{G}_\Omega} \otimes_k \Omega \xrightarrow{\sim} U$ from the previous lemma. In particular, we have

$$\dim_k(U^{\mathcal{G}_\Omega}) = \dim_\Omega(U^{\mathcal{G}_\Omega} \otimes_k \Omega) = \dim_\Omega(U) = n.$$

Let $v_1, \dots, v_n$ be a k-basis of $U^{\mathcal{G}_\Omega}$ (which is also an Ω-basis of U), and let $P \in \mathrm{GL}_n(\Omega)$ be the matrix whose columns are $v_1, \dots, v_n$. Then for all $\sigma \in \mathcal{G}_\Omega$, the matrix $\sigma\cdot P$ is the matrix whose columns are $\sigma\cdot v_1, \dots, \sigma\cdot v_n$. Now $v_1, \dots, v_n \in U^{\mathcal{G}_\Omega}$, and therefore we have

$$v_i = \sigma * v_i = \alpha_\sigma(\sigma\cdot v_i) \text{ for all } i = 1, \dots, n.$$

Written in terms of matrices, this reads

$$P = \alpha_\sigma(\sigma\cdot P) \text{ for all } \sigma \in \mathcal{G}_\Omega.$$

It readily follows that α is cohomologous to the trivial cocycle, and this concludes the proof. □

Remark 3.6. Assume that Ω/k is a finite cyclic extension of degree n, and let γ be a generator of $\mathcal{G}_\Omega$. If $\alpha \in Z^1(\mathcal{G}_\Omega, \Omega^\times)$ is a 1-cocycle, we have

$$\alpha_{\gamma^n} = \alpha_{\gamma^{n-1}} \gamma^{n-1} \cdot \alpha_\gamma = \ldots = N_{\Omega/k}(\alpha_\gamma).$$

Since $\gamma^n = 1$, we get $N_{\Omega/k}(\alpha_\gamma) = 1$. Conversely, any element $x \in \Omega^\times$ of norm 1 determines completely a cocycle with values in $\Omega^\times$ by the formula

$$\alpha_{\gamma^m} = \prod_{0 \leq i \leq m-1} \gamma^i \cdot x \text{ for all } 0 \leq m \leq n-1.$$

Now let $x \in \Omega^\times$ satisfying $N_{\Omega/k}(x) = 1$, and let α be the corresponding cocycle. By Hilbert 90, we know that α is cohomologous to the trivial cocycle, so there exists $z \in \Omega^\times$ such that $\alpha_\sigma = \dfrac{\sigma(z)}{z}$ for all $\sigma \in \mathcal{G}_\Omega$. Applying this equality to $\sigma = \gamma$, we get $x = \dfrac{\gamma(z)}{z}$, which is the classical version of Hilbert 90.

4. Exact sequences in cohomology

Definition 4.1. Let $f : A \to B$ be a map of pointed sets. Recall that the kernel of f is the preimage of the base point of B.
A sequence of pointed sets

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, "g"] & C \end{tikzcd}$$

is called **exact** at B if $\mathrm{im} f = \ker g$.

A sequence of pointed sets

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

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

An exact sequence of groups (resp. of G-groups, resp. of G-modules) is an exact sequence of pointed sets such that all the maps involved are group morphisms (resp. morphisms of G-groups, resp. of G-modules).

For example, the sequence

$$\begin{tikzcd} B \arrow[r, "g"] & C \arrow[r] & 1 \end{tikzcd}$$

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

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "f"] & B \end{tikzcd}$$

is exact if and only if f has trivial kernel. This does **not** imply that f is injective, unless A and B are groups and f is a group morphism.

Assume that we have an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 1 \end{tikzcd}$$

of pointed G-sets. The goal of the next paragraphs is to derive some exact sequences in cohomology, under some reasonable conditions on A, B and C. We will keep this notation throughout.

Assume that A and B are G-groups, that f is a group morphism (hence f is injective), and that g induces a bijection of G-sets $B/f(A) \simeq C$, where $B/f(A)$ is the set of right cosets modulo $f(A)$. In other words, g is surjective and for all $b, b' \in B$ we have

$$g(b) = g(b') \iff b' = bf(a) \text{ for some } a \in A.$$

For instance, these conditions are satisfied in the following cases:

(1) A is a G-subgroup of B, $C = B/A$, f is the inclusion and g is the natural projection.

(2) C is a G-group and g is a group morphism (this will be the case in the next subsection).

As pointed out previously in Example 2.15, f and g induce maps on fixed points by restriction, namely $f_* : A^G \to B^G$ and $g_* : B^G \to C^G$. Our next goal is to define a map of pointed sets

$$\delta^0 : C^G \to H^1(G, A).$$

Let $c \in C^G$, and let $b \in B$ any preimage of c under g, i.e. $g(b) = c$. By assumption, we have $c = \sigma \cdot c$ for all $\sigma \in G$. Therefore, we have

$$g(\sigma \cdot b) = \sigma \cdot g(b) = \sigma \cdot c = c = g(b).$$

By assumption on g, there exists a unique element $\alpha_\sigma \in A$ such that $f(\alpha_\sigma) = b^{-1}\,\sigma \cdot b$.

Lemma 4.2. *The map $\alpha : G \to A, \sigma \mapsto \alpha_\sigma$ is a 1-cocycle, and its class in $H^1(G, A)$ does not depend on the choice of $b \in B$.*

Proof. Let us prove that α is a cocycle. By definition of α, for all $\sigma, \tau \in G$, we have

$$f(\alpha_{\sigma\tau}) = b^{-1}\sigma\tau \cdot b = b^{-1}\,\sigma \cdot (bb^{-1}\tau \cdot b) = (b^{-1}\sigma \cdot b)\,\sigma \cdot (b^{-1}\tau \cdot b).$$

Hence we have

$$f(\alpha_{\sigma\tau}) = f(\alpha_\sigma)\,\sigma \cdot f(\alpha_\tau) = f(\alpha_\sigma) f(\,\sigma \cdot \alpha_\tau) = f(\alpha_\sigma\,\sigma \cdot \alpha_\tau).$$

By injectivity of f, we get $\alpha_{\sigma\tau} = \alpha\,\sigma \cdot \alpha_\tau$.

Let us prove now that the cohomology class of α does not depends on the choice of b. Let $b' \in B$ be another preimage of c under g. We then have $g(b') = c = g(b)$, so $b' = bf(a^{-1}) = bf(a)^{-1}$ for some $a \in A$ by assumption on g, and let α' be the corresponding 1-cocycle. We then have

$$f(\alpha'_\sigma) = f(a)b^{-1}\,\sigma \cdot (bf(a^{-1})) = f(a)f(\alpha_\sigma)\,\sigma \cdot f(a)^{-1} = f(a\alpha_\sigma\,\sigma \cdot a^{-1}),$$

so by injectivity of f, this implies that α and α' are cohomologous. This concludes the proof. □

We then have constructed a map of pointed sets

$$\delta^0 : C^G \to H^1(G,A), c \mapsto [\alpha],$$

where the cocycle α is defined by the relations

$$f(\alpha_\sigma) = b^{-1}\,\sigma{\cdot}b \text{ for all } \sigma \in G,$$

for an arbitrary preimage $b \in B$ of c.

Definition 4.3. The map $\delta^0 : C^G \to H^1(G,A)$ is called the 0^{th} **connecting map**.

Proposition 4.4. *The sequence of G-sets*

$$\begin{tikzcd} 1 \arrow[r] & A^G \arrow[r, "f_*"] & B^G \arrow[r, "g_*"] & C^G \arrow[r, "\delta^0"] & H^1(G,A) \arrow[r, "f_*"] & H^1(G,B) \end{tikzcd}$$

is exact.

Proof. The fact that the sequence

$$1 \to A^G \to B^G \to C^G$$

is exact is left to the reader.

Exactness at C^G: clearly if $c = g(b)$ for some $b \in B^G$, then its image under δ^0 is the trivial class. Conversely, assume that $\delta^0(c)$ is trivial, i.e. $\alpha_\sigma = a\,\sigma{\cdot}a^{-1}$ for some $a \in A$. Let $b \in B$ be a preimage of c under g. We then have

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

so $f(a)\sigma{\cdot}f(a)^{-1} = b^{-1}\sigma{\cdot}b$. Hence $bf(a) \in B^G$, and we have $g(bf(a)) = g(b) = c$ by assumption on g. Hence $\ker(\delta^0) = \mathrm{im}(g_*)$, which is what we wanted to prove.

Exactness at $H^1(G,A)$: Let $c \in C^G$ and let $b \in B$ satisfying $c = g(b)$. Then by definition of f_* and $\delta^0(c)$, $f_*(\delta^0(c))$ is the class of the 1-cocycle $G \to B, \sigma \mapsto b^{-1}\,\sigma{\cdot}b$, which is cohomologous to the trivial cocycle. Now if $[\alpha] \in H^1(G,A)$ satisfies $f_*([\alpha]) = 1$, then $f(\alpha_\sigma) = b^{-1}\,\sigma{\cdot}b$ for some b in B. Therefore, we have

$$\sigma{\cdot}g(b) = g(\,\sigma{\cdot}b) = g(bf(\alpha_\sigma)) = g(b) \text{ for all } \sigma \in G.$$

Hence $c = g(b)$ lies in C^G. Thus $b \in B$ is a preimage of $c \in C^G$ under g and $[\alpha] = \delta^0(c)$ by definition of δ^0. This concludes the proof. □

Example 4.5. We have an exact sequence of $\mathcal{G}_\Omega$-groups

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{SL}_n(\Omega) \arrow[r] & \mathrm{GL}_n(\Omega) \arrow[r] & \Omega^\times \arrow[r] & 1 \end{tikzcd},$$

where the last map is the determinant. Hence we have an exact sequence in cohomology

$$\begin{tikzcd} \mathrm{GL}_n(k) \arrow[r] & k^\times \arrow[r, "\delta^0"] & H^1(\mathcal{G}_\Omega, \mathrm{SL}_n(\Omega)) \arrow[r] & H^1(\mathcal{G}_\Omega, \mathrm{GL}_n(\Omega)) \end{tikzcd}$$

where the first map is the determinant. By Hilbert 90, we get an exact sequence

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

Since the determinant map is surjective, and since the sequence above is exact at $k^\times$, it follows that the 0^{th} connecting map is trivial, hence we get $H^1(\mathcal{G}_\Omega, \mathrm{SL}_n(\Omega)) = 1$.

Before continuing, we need to define an action of B^G in C^G. Let $\beta \in B^G$ and $c \in C^G$. Let $b \in B$ be a preimage of c under g, and set

$$\beta \cdot c = g(\beta b) \in C.$$

Let us check that it does not depends on the choice of b. If $b' \in B$ is another preimage of c under g, then $b' = bf(a)$ for some $a \in A$, hence $g(\beta b') = g(\beta bf(a)) = g(\beta b)$ by assumption on g. Hence $\beta \cdot c$ does not depend the choice of b.

We now show that $\beta \cdot c \in C^G$. For $\sigma \in G$, we have

$$\sigma\cdot(\beta\cdot c) = \sigma\cdot g(\beta b) = g(\sigma\cdot(\beta b)) = g((\sigma\cdot\beta)(\sigma\cdot b)).$$

Since $\beta \in B^G$, we get $\sigma\cdot(\beta \cdot c) = g(\beta(\sigma\cdot b))$ for all $\sigma \in G$. Now $g(\sigma\cdot b) = \sigma\cdot g(b) = \sigma\cdot c = c$ since $c \in C^G$, so $\sigma\cdot b$ is also a preimage of c. Since $\beta \cdot c$ does not depend on the choice of a preimage of c, we conclude that $\sigma\cdot(\beta\cdot c) = \beta\cdot c$ for all $\sigma \in G$, so $\beta\cdot c \in C^G$.

It is then clear that the map

$$B^G \times C^G \to C^G, (\beta, c) \mapsto \beta\cdot c$$

gives rise to an action of B^G on C^G. The next result identifies the corresponding orbit set.

Corollary 4.6. *There is a natural bijection between the orbit set of the group B^G in C^G and $\ker(H^1(G,A) \to H^1(G,B))$.*

More precisely, the bijection sends the orbit of $c \in C^G$ onto $\delta^0(c)$.

Proof. Let us denote by C^G/B^G the orbit set of B^G in C^G. By the previous proposition, we have $\ker(H^1(G,A) \to H^1(G,B)) = \mathrm{im}(\delta^0)$. Hence we have to construct a bijection between C^G/B^G and $\mathrm{im}(\delta^0)$.

Let $c, c' \in C^G$ lying in the same orbit, that is $c' = \beta\cdot c$ for some $\beta \in B^G$. Then $c' = g(\beta b)$, for some preimage $b \in B$ of c, and βb is a preimage of c'. Since we have $(\beta b)^{-1}\sigma\cdot(\beta b) = b^{-1}\beta^{-1}(\sigma\cdot\beta)(\sigma \cdot b) = b^{-1}\sigma\cdot b$, it turns out that $\delta^0(c') = \delta^0(c)$. Therefore, the map

$$\varphi : C^G/B^G \to \mathrm{im}(\delta^0), B^G \cdot c \mapsto \delta^0(c)$$

is a well-defined surjective map. It remains to prove its injectivity. Let $c, c' \in C^G$ such that $\delta^0(c') = \delta^0(c)$, and let α and α' be the cocycles representing $\delta^0(c)$ and $\delta^0(c')$ respectively. By assumption, there exists $a \in A$ such that $\alpha'_\sigma = a\alpha_\sigma\,\sigma\cdot a^{-1}$ for all $\sigma \in G$. If b (resp. b') is a preimage of c (resp. c') in B, applying f to this last equality implies that

$$b'^{-1}\,\sigma\cdot b' = f(a)b^{-1}(\,\sigma\cdot b)(\sigma\cdot f(a))^{-1}.$$

It easily turns out that $b'f(a)b^{-1} \in B^G$, so $b'f(a) = \beta b$, for some $\beta \in B^G$. Hence $c' = g(b') = g(b'f(a)) = g(\beta b) = \beta\cdot c$. Therefore, c and c' lie in the same orbit, showing that φ is injective. This concludes the proof. □

We now assume that we have an exact sequence of G-groups

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "f"] & B \arrow[r, "g"] & C \arrow[r] & 1 \end{tikzcd}$$

so A can be identified with a normal subgroup of B.

Proposition 4.7. *The sequence*

$$1 \to A^G \to B^G \to C^G \to H^1(G,A) \to H^1(G,B) \to H^1(G,C)$$

is exact.

Proof. By Proposition 4.4, only the exactness at $H^1(G,B)$ needs a proof. If $[\beta] = f_*([\alpha])$ for some $[\alpha] \in H^1(G,A)$, the we have

$$g_*([\beta]) = g_*(f_*([\alpha])) = (g\circ f)_*([\alpha]) = 1,$$

since $g\circ f$ is trivial by assumption. Hence $\mathrm{im}(f_*) \subset \ker(g_*)$.

Conversely, let $[\beta] \in H^1(G,B)$ such that $g_*([\beta]) = 1$. Then there exists $c \in C$ such that $g(\beta_\sigma) = c^{-1}\,\sigma\cdot c$ for all $\sigma \in G$.

Write $c = g(b)$. We then have $g(\beta_\sigma) = g(b^{-1}\,\sigma{\cdot}b)$, so $\beta_\sigma = b^{-1}(\,\sigma{\cdot}b)f(a_\sigma)$, for some $a_\sigma \in A$. Since $f(A)$ is normal in B, $(\,\sigma{\cdot}b)f(a_\sigma)(\,\sigma{\cdot}b)^{-1} \in f(A)$, so $\beta_\sigma = b^{-1}f(\alpha_\sigma)\,\sigma\cdot b$ for some $\alpha_\sigma \in A$, and thus

$$b\beta_\sigma\,\sigma\cdot b^{-1} = f(\alpha_\sigma) \text{ for all } \sigma \in G.$$

The fact that the map $G \to B, \sigma \to b\beta_\sigma\,\sigma\cdot b^{-1}$ is a 1-cocycle and the injectivity of f imply easily that α is a cocycle. Moreover, by construction of α, we have $[\beta] = f_*([\alpha]) \in \mathrm{im}(g_*)$. This concludes the proof. □

We would like now to go back to the general Galois descent problem: if two k-structures are isomorphic over Ω, are they isomorphic over k? First we need an appropriate setting in order for all these words to make sense. We therefore starting by examining carefully our solution to the conjugacy problem for matrices.

5. (The) matrix (case) reloaded

In this paragraph, we would like to extract the essential arguments of our solution to the conjugacy problem, and rewrite them in a more concise and formal way, in order to find a general way to attack the general

Galois descent problem. Let us first reformulate the result we obtained. In fact, we have proved in the introduction that the set of $G(k)$-conjugacy classes of matrices $M \in \mathrm{M}_n(\Omega)$ which are $G(\Omega)$-conjugate to a given matrix $M_0 \in \mathrm{M}_n(k)$ is in one-to-one correspondence with the set of cohomology classes $[\alpha] \in H^1(\mathcal{G}_\Omega, Z_G(M_0)(\Omega))$, which may be written $[\alpha] = [\alpha^C]$ for some $C \in G(\Omega)$, where α^C is the cocycle

$$\alpha^C : \mathcal{G}_\Omega \to Z_G(M_0)(\Omega), \sigma \mapsto C(\sigma{\cdot}C)^{-1}.$$

This set of cohomology classes is nothing but the kernel of the map

$$H^1(\mathcal{G}_\Omega, Z_G(M_0)(\Omega)) \to H^1(\mathcal{G}_\Omega, G(\Omega))$$

induced by the inclusion $Z_G(M_0)(\Omega) \subset G(\Omega)$.

This observation will allow us to give a more conceptual (and less miraculous) explanation of our result. Notice first that the congugacy class of a matrix may be reinterpreted as an orbit under the action of $G = \mathbf{GL}_n$ of $\mathbf{SL}_n$ by conjugation. This action will be denoted by $*$ in the sequel. The next crucial observation is then the following one: if $M_0 \in \mathrm{M}_n(k)$, we may rewrite $Z_G(M_0)(\Omega)$ as

$$Z_G(M_0)(\Omega) = \{C \in G(\Omega) \mid C * M_0 = M_0\}.$$

In other words, $Z_G(M_0)(\Omega)$ is nothing but the stabilizer of M_0 (viewed as an element of $\mathrm{M}_n(\Omega)$) with respect to the action of $G(\Omega)$ on $\mathrm{M}_n(\Omega)$.

The second important point is that the action of G_Ω on $G(\Omega)$ restricts to an action on $Z_G(M_0)(\Omega)$. To see this, recall that the action of $\mathcal{G}_\Omega$ on a matrix $S = (s_{ij}) \in \mathrm{M}_n(\Omega)$ is given by

$$\sigma{\cdot}S = (\sigma(s_{ij})).$$

In particular, the following properties hold:

(i) $\mathrm{M}_n(\Omega)^{\mathcal{G}_\Omega} = \mathrm{M}_n(k)$

(ii) For all $S \in \mathrm{M}_n(\Omega), C \in G(\Omega)$ and $\sigma \in \mathcal{G}_\Omega$, we have

$$\sigma{\cdot}(C * S) = (\sigma{\cdot}C) * (\sigma{\cdot}S).$$

We have in fact an even more general property. If $\iota : K \to L$ is a morphism of field extensions of k and $S \in \mathrm{M}_n(K)$, set

$$\iota \cdot S = (\iota(s_{ij})).$$

We then have

(ii′) For all morphism of extensions $\iota : K \to L, S \in \mathrm{M}_n(K)$ and $C \in G(K)$, we have

$$\iota \cdot (C * S) = (\iota \cdot C) * (\iota \cdot S).$$

If now $C \in Z_G(M_0)(\Omega)$ and $\sigma \in G(\Omega)$, we have

$$(\sigma{\cdot}C) * M_0 = (\sigma{\cdot}C) * (\,\sigma{\cdot}M_0)$$

by *(i)*, since $M_0 \in \mathrm{M}_n(k)$. Using *(ii)*, we then get

$$(\sigma{\cdot}C) * M_0 = \,\sigma{\cdot}(C * M_0) = \,\sigma{\cdot}M_0 = M_0,$$

the second equality coming from the fact that $C \in Z_G(M_0)(\Omega)$. Hence the action of $\mathcal{G}_\Omega$ on $G(\Omega)$ restricts to an action on $Z_G(M_0)(\Omega)$ as claimed. Now it follows from elementary group theory that we have a bijection

$$G(\Omega)/Z_G(M_0)(\Omega) \simeq G(\Omega) * M_0.$$

Equivalently, we have an exact sequence

$$1 \to Z_G(M_0)(\Omega) \to G(\Omega) \to G(\Omega) * M_0 \to 1,$$

which may be easily seen to be an exact sequence of pointed G_Ω-sets satisfying the conditions explained in § 4, the base point of $G(\Omega) * M_0$ being M_0.

The apparition of $\ker[H^1(\mathcal{G}_\Omega, Z_G(M_0)(\Omega)) \to H^1(\mathcal{G}_\Omega, G(\Omega))]$ is not a real surprise then, in view of Corollary 4.6. The same corollary says that this kernel is in one-to-one correspondence with the orbit set of $G(\Omega)^{\mathcal{G}_\Omega}$ in $(G(\Omega) * M_0)^{\mathcal{G}_\Omega}$.

Let us now check that this orbit set is precisely the set of $G(k)$-conjugacy classes of matrices which become $G(\Omega)$-conjugate to M_0. Notice that since $G = \mathbf{GL}_n$ or $\mathbf{SL}_n$, we have

(iii) $G(\Omega)^{\mathcal{G}_\Omega} = G(k)$.

Moreover, by definition of the action of $G(\Omega)$ on $\mathrm{M}_n(\Omega)$, $G(\Omega)*M_0$ is the set of matrices of $\mathrm{M}_n(\Omega)$ which are $G(\Omega)$-conjugate to M_0. Therefore by (i), $(G(\Omega) * M_0)^{\mathcal{G}_\Omega}$ is the set of matrices of $\mathrm{M}_n(k)$ which are $G(\Omega)$-conjugate to M_0.
Notice now that the action $G(\Omega)^{\mathcal{G}_\Omega} = G(k)$ on $(G(\Omega) * M_0)^{\mathcal{G}_\Omega}$ defined before Corollary 4.6 is simply the restriction of the action of $G(k)$ on $\mathrm{M}_n(k)$ by conjugation. Indeed, if $M \in \mathrm{M}_n(k)$ has the form $M = Q*M_0$ for some $Q \in G(\Omega)$, and if $P \in G(k)$, Q is a preimage of M under the map $G(\Omega) \to G(\Omega) * M_0$, and therefore we have

$$P \cdot M = (PQ) * M_0 = P * (Q * M_0) = P * M.$$

Thus the orbit set of $G(\Omega)^{\mathcal{G}_\Omega}$ in $(G(\Omega) * M_0)^{\mathcal{G}_\Omega}$ is nothing but the set of $G(k)$-conjugacy classes of matrices $M \in \mathrm{M}_n(k)$ which become $G(\Omega)$-conjugate to M_0.

Therefore, we have proved that our solution the conjugacy problem for matrices was nothing but an application of Corollary 4.6, and we have identified three important properties which make this actually work. Notice that (i) and (iii) may seem redundant a priori, but this is only due to our specific example. In more abstract situations, both conditions may be of different nature. For example, one may replace matrices by quadratic forms of dimension n and study the Galois descent problem for isomorphism classes of quadratic forms. In this case, we see that properties (i) and (iii) do not concern the same objects.

Our next goal is now to reformulate this new approach in a more abstract context, and derive a solution for general Galois descent problems. In particular, we will need to find appropriate substitutes for $Z_G(M_0)(\Omega)$ and properties $(i)-(iii)$. Of course, Galois descent problems only makes sense if the algebraic objects may be 'defined over an arbitrary field', and if we have a notion of 'scalar extension' of our objects. For example, to each field extension K/k of a field k, we can consider the set $\mathrm{M}_n(K)$ of matrices with coefficients in K, and if $K \to L$ is a morphism of extensions of k, one can associate a map $\mathrm{M}_n(K) \to \mathrm{M}_n(L), M = (m_{ij}) \mapsto (\iota(m_{ij}))$. which is in fact the canonical inclusion. Another example may be obtained by considering the set $\mathbf{Alg}_n(K)$ of K-algebras of dimension n over K. In this case, the map $\mathbf{Alg}_n(K) \to \mathbf{Alg}_n(L)$ associated to a morphism $K \to L$ is given by the tensor product $\otimes_K L$. In both cases, scalar extension maps satisfy some natural properties: the scalar extension map from K to itself is the identity map, and extending scalars from K to L, then from L to M is the same as extending scalars from K to M.

We now formalize this situation by introducing the concept of a functor.

6. Functors

Definition 6.1. Let k be a field. A **functor** defined over k is a rule $\mathbf{F}$ which associates to every field extension K/k a set (a group, a ring...) $\mathbf{F}(K)$, and to any morphism of field extensions $\varphi : K \to K'$ a map (group morphism, ring morphism) $\mathbf{F}(\varphi) : \mathbf{F}(K) \to \mathbf{F}(K')$ such that the following properties hold:
(1) For all K/k, $\mathbf{F}(\mathrm{Id}_K) = \mathrm{Id}_{\mathbf{F}(K)}$
(2) For all $\varphi_1 : K_1 \to K_2$, $\varphi_2 : K_2 \to K_3$, we have

$$\mathbf{F}(\varphi_2 \circ \varphi_1) = \mathbf{F}(\varphi_2) \circ \mathbf{F}(\varphi_1).$$

The maps $\mathbf{F}(\varphi)$ has to be understood as 'scalar extension maps'. If $\varphi : K \to L$ is a morphism of extensions, for all $x \in \mathbf{F}(K)$ we will denote by x_L the element $\mathbf{F}(\varphi)(x)$ if there is no ambiguity in the choice of the map φ.

Examples 6.2.
(1) The rules

$$K \to \mathrm{M}_n(K), K \to \mathrm{GL}_n(K), K \to \mathrm{SL}_n(K)$$

are functors. If $\iota : K \to L$ is a morphism of extensions, the induced map is just

$$(m_{ij}) \mapsto (\iota(m_{ij})).$$

(2) If A is a k-algebra, the rule

$$h_A : K \mapsto \mathrm{Hom}_{k-alg}(A, K)$$

is a functor.

Therefore, the algebraic objects we are going to work with are points of a functor $\mathbf{F}$. What we need now is an action of $\mathcal{G}_\Omega$ on $\mathbf{F}(\Omega)$ for every Galois extension Ω/k, playing the role of the action of $\mathcal{G}_\Omega$ on matrices.

Notice that if $\mathbf{F}$ is a functor, then for any Galois extension Ω/k and every $\sigma \in \mathcal{G}_\Omega$, we have an induced bijection

$$\mathbf{F}(\sigma) : \mathbf{F}(\Omega) \to \mathbf{F}(\Omega).$$

For $x \in \mathbf{F}(\Omega)$ and $\sigma \in \mathcal{G}_\Omega$, we set

$$\sigma \cdot x = \mathbf{F}(\sigma)(x).$$

Lemma 6.3. *The map*

$$\mathcal{G}_\Omega \times \mathbf{F}(\Omega) \to \mathbf{F}(\Omega), (\sigma, x) \mapsto \sigma \cdot x = \mathbf{F}(\sigma)(x)$$

gives rise to an action of $\mathcal{G}_\Omega$ on $\mathbf{F}(\Omega)$.

If Ω/k and Ω'/k are two Galois extensions such that $\Omega \subset \Omega'$, we have

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

Moreover, if $\mathbf{F}$ is a group-valued functor, the action above is an action by group automorphisms, that is

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

Proof. Since $\mathbf{F}$ is a functor, we have $\mathbf{F}(\mathrm{Id}_\Omega) = \mathrm{Id}_{\mathbf{F}(\Omega)}$. Therefore,

$$\mathrm{Id}_\Omega \cdot x = x \text{ for all } x \in \mathbf{F}(\Omega).$$

Now let $\sigma, \tau \in \mathcal{G}_\Omega$. Since $\mathbf{F}$ is a functor, we have

$$\mathbf{F}(\sigma \circ \tau) = \mathbf{F}(\sigma) \circ \mathbf{F}(\tau),$$

and thus $(\sigma \circ \tau) \cdot x = \sigma \cdot (\tau \cdot x)$ for all $x \in \mathbf{F}(\Omega)$. This proves the first part of the lemma.

Let Ω/k and Ω'/k be two Galois extensions such that $\Omega \subset \Omega'$, and let $\mathbf{F}(\iota) : \mathbf{F}(\Omega) \to \mathbf{F}(\Omega')$ be the map induced by the inclusion $\iota : \Omega \subset \Omega'$. For all $\sigma' \in \mathcal{G}_{\Omega'}$, the diagram

$$\begin{tikzcd}
\Omega \arrow[r, "\sigma'_{|_\Omega}"] \arrow[d, "\iota"] & \Omega \arrow[d, "\iota"] \\
\Omega' \arrow[r, "\sigma'"] & \Omega'
\end{tikzcd}$$

is commutative. Therefore, it induces a commutative diagram

$$\begin{tikzcd}
\mathbf{F}(\Omega) \arrow[r, "\mathbf{F}(\sigma'_{|_\Omega})"] \arrow[d, "\mathbf{F}(\iota)"] & \mathbf{F}(\Omega') \arrow[d, "\mathbf{F}(\iota)"] \\
\mathbf{F}(\Omega') \arrow[r, "\mathbf{F}(\sigma')"] & \mathbf{F}(\Omega)
\end{tikzcd}$$

In other words, for all $x \in \mathbf{F}(\Omega)$, we have

$$\mathbf{F}(\iota) \circ \mathbf{F}(\sigma'_{|\Omega})(x) = \mathbf{F}(\sigma') \circ \mathbf{F}(\iota)(x),$$

that is

$$(\sigma'_{|\Omega} \cdot x)_{\Omega'} = \sigma' \cdot x_{\Omega'}.$$

Finally, if $\mathbf{F}$ is a group-valued functor, $\mathbf{F}(\sigma)$ is a group morphism and the last part follows. This concludes the proof. □

Example 6.4. If $\mathbf{F} = \mathbf{M}_n, \mathbf{GL}_n$ or $\mathbf{SL}_n$, this action of σ is nothing but

$$\sigma \cdot (m_{ij}) = (\sigma(m_{ij})).$$

In particular, functors give a cheap way to produce $\mathcal{G}_\Omega$-sets and $\mathcal{G}_\Omega$-groups.
Now that the decor is set and the actors are in place, we are ready look at general Galois descent problems.

7. Functorial group actions

To setup the Galois descent problem for conjugacy classes of matrices, we needed an action of some subfunctor of $\mathbf{GL}_n$ on matrices. As we have seen in a previous paragraph, this action has some nice functorial properties. This leads to the following definition:

Definition 7.1. Let G be a group-valued functor, and let $\mathbf{F}$ any functor. We say that G **acts on F** if the following conditions hold:

(1) For every field extension K/k, the group $G(K)$ acts on the set $\mathbf{F}(K)$. This action will be denoted by $*$.
(2) For every morphism $\iota : K \to L$ of field extensions, the following diagram is commutative:

$$\begin{tikzcd}
G(K) \times \mathbf{F}(K) \arrow[r] \arrow[d, "(G(\iota){,}\mathbf{F}(\iota))"] & \mathbf{F}(K) \arrow[d, "\mathbf{F}(\iota)"] \\
G(L) \times \mathbf{F}(L) \arrow[r] & \mathbf{F}(L)
\end{tikzcd}$$

that is $\mathbf{F}(\iota)(g * a) = G(\iota)(g) * \mathbf{F}(\iota)(a)$ for all $a \in \mathbf{F}(K), g \in G(K)$.

In other words, for every field extension K/k, we have a group action of $G(K)$ on $\mathbf{F}(K)$ which is functorial in K.

Notice that the last condition rewrites

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

for a given field extension L/K if we use the short notation introduced at the beginning of the previous paragraph.

Examples 7.2.

(1) Let $G = \mathbf{GL}_n, \mathbf{SL}_n, \mathbf{O}_n, \mathbf{Sp}_{2n}, \ldots$ and let $\mathbf{F}$ be the functor defined by $\mathbf{F}(K) = K^n$ for every field extension K/k. Then G acts by left multiplication on $\mathbf{F}$.

(2) If $G = \mathbf{GL}_n, \mathbf{SL}_n, \mathbf{O}_n, \mathbf{Sp}_{2n}, \ldots$ and $\mathbf{F} = \mathbf{M}_n$, then G acts on $\mathbf{F}$ by conjugation.

Remark 7.3. Let Ω/k be Galois extension. Recall from Lemma 6.3 that, given a functor $\mathbf{F}$, we have a natural action of $\mathcal{G}_\Omega$ on $\mathbf{F}(\Omega)$ defined by

$$\mathcal{G}_\Omega \times \mathbf{F}(\Omega) \to \mathbf{F}(\Omega), (\sigma, a) \mapsto \sigma \cdot a = \mathbf{F}(\sigma)(a).$$

If G is a group-scheme acting on $\mathbf{F}$, we have by definition

$$\mathbf{F}(\sigma)(g * a) = G(\sigma)(g) * \mathbf{F}(\sigma)(a) \text{ for all } a \in \mathbf{F}(\Omega), \sigma \in \mathcal{G}_\Omega,$$

which rewrites as

$$\sigma \cdot (g * a) = (\sigma \cdot g) * (\sigma \cdot a) \text{ for all } a \in \mathbf{F}(\Omega), \sigma \in \mathcal{G}_\Omega.$$

We would like to continue by giving a reformulation of the general Galois descent problem. For, we need to introduce the concept of a twisted form.

8. Twisted forms

Let G be a group-valued functor acting on a functor $\mathbf{F}$. This action of G allows us to define an equivalence relation on the set $\mathbf{F}(K)$ for every field extension K/k by identifying two elements which are in the same $G(K)$-orbit. For example, in the case of matrices, two matrices of $\mathrm{M}_n(K)$ will be equivalent if and only if they are $G(K)$-conjugate. More precisely, we have the following definition:

Definition 8.1. Let G be a group-scheme defined over k acting on $\mathbf{F}$. For every field extension K/k we define an equivalence relation $\sim_K$ on $\mathbf{F}(K)$ as follows: two elements $b, b' \in \mathbf{F}(K)$ are **equivalent over** K if there exists $g \in G(K)$ such that $b = g * b'$. We will denote by $[b]$ the corresponding equivalence class.

We may now formulate a general descent problem.

Galois descent problem: let $\mathbf{F}$ be a functor, and let G be a group-valued functor acting on $\mathbf{F}$. Finally, let Ω/k be a Galois extension and let $a, a' \in \mathbf{F}(k)$. Assume that $a_\Omega \sim_\Omega a'_\Omega$. Do we have $a \sim_k a'$?

Notice that the answer to this question only depends on the $G(k)$-equivalence class of a and a'. We now give a special name to elements of $\mathbf{F}$ which become equivalent to a fixed element $a \in \mathbf{F}(k)$.

Definition 8.2. Let $a \in \mathbf{F}(k)$, and let Ω/k be a Galois extension. An element $a' \in \mathbf{F}(k)$ is called **a twisted form of** a if $a'_\Omega \sim_\Omega a_\Omega$.

Clearly, if $a' \in \mathbf{F}(k)$ is a twisted form of a and $a' \sim_k a''$, then a'' is also a twisted form of a, so the equivalence relation $\sim_k$ restricts to the set of twisted forms of a.

We denote by $\mathbf{F}_a(\Omega/k)$ the set of k-equivalence classes of twisted forms of a, that is

$$\mathbf{F}_a(\Omega/k) = \{[a'] \mid a' \in \mathbf{F}(k), a'_\Omega \sim_\Omega a_\Omega\}.$$

Notice that $\mathbf{F}_a(\Omega/k)$ always contains the class of a, so it is natural to consider $\mathbf{F}_a(\Omega/k)$ as a pointed set, where the base point is $[a]$.

Example 8.3. As pointed out before, if $\mathbf{F} = \mathbf{M}_n$, then $G \subset \mathbf{GL}_n$ acts on $\mathbf{F}$ by conjugation, and two matrices $M, M' \in \mathrm{M}_n(k)$ are then equivalent if and only if they are conjugate by an element of $G(k)$. Moreover, if $M_0 \in \mathrm{M}_n(k)$, then $\mathbf{F}_{M_0}(\Omega/k)$ is the set of $G(k)$-conjugacy classes of matrices $M \in \mathrm{M}_n(k)$ which are $G(\Omega)$-conjugate to M_0.

Using the notation introduced previously, the Galois descent problem may be reinterpreted in terms of twisted forms. Given $a \in \mathbf{F}(k)$ and a Galois extension Ω/k, do we have $\mathbf{F}_a(\Omega/k) = \{[a]\}$?

We would like to describe $\mathbf{F}_a(\Omega/k)$ in terms of Galois cohomology of a suitable group-valued functor associated to a, under some reasonable conditions on $\mathbf{F}$ and G. To do this, we will continue to try to generalize the approach described in § 5.

9. The Galois descent condition

One of the crucial property we used to solve the conjugacy problem is the equality

$$\mathrm{M}_n(\Omega)^{\mathcal{G}_\Omega} = \mathrm{M}_n(k),$$

where we let $\mathcal{G}_\Omega$ act on $S \in \mathrm{M}_n(\Omega)$ coefficientwise. This action is nothing but the action of $\mathcal{G}_\Omega$ induced by the functorial properties of M_n, as described in Lemma 6.3. Now let us go back to our more general setting. For every Galois extension Ω/k, we have an action of $\mathcal{G}_\Omega$ on the set $\mathbf{F}(\Omega)$ given by

$$\sigma \cdot a = \mathbf{F}(\sigma)(a) \text{ for } \sigma \in \mathcal{G}_\Omega \text{ and } a \in \mathbf{F}(\Omega).$$

The second part of Lemma 6.3, applied to the Galois extensions k/k and Ω/k, then yields

$$\sigma \cdot a_\Omega = a_\Omega \text{ for all } \sigma \in \mathcal{G}_\Omega, a \in \mathbf{F}(k).$$

However, contrary to the case of matrices, an element of $\mathbf{F}(\Omega)$ on which $\mathcal{G}_\Omega$ acts trivially does not necessarily comes from an element of $\mathbf{F}(k)$.

Example 9.1. Let us consider the functor $\mathbf{F}$ defined as follows: for a field extension K/k, set

$$\mathbf{F}(K) = \begin{cases} \{0\} & \text{if } [K:k] \leq 1 \\ \{0,1\} & \text{if } [K:k] \geq 2 \end{cases}$$

the map induced by a morphism $K \to K'$ being the inclusion of sets. In particular, for every Galois extension Ω/k, the Galois group $\mathcal{G}_\Omega$ acts trivially on $\mathbf{F}(\Omega)$. However, if $[\Omega : k] > 1$, the element $1 \in \mathbf{F}(\Omega)$ does not come from an element of $\mathbf{F}(k)$.

These considerations lead to the following definition:

Definition 9.2. We say that a functor $\mathbf{F}$ satisfies the **Galois descent condition** if for every Galois extension Ω/k the map $\mathbf{F}(k) \to \mathbf{F}(\Omega)$ is injective and induces a bijection

$$\mathbf{F}(k) \simeq \mathbf{F}(\Omega)^{\mathcal{G}_\Omega}.$$

Example 9.3. The functor $\mathbf{M}_n$ satisfies the Galois descent condition.

Notice that this condition was also needed on the group-scheme G in the final argument.

10. Stabilizers

It follows from the considerations of the previous paragraph that it is reasonable to consider Galois descent problems for elements of a functor satisfying the Galois descent condition. Now that we have set a suitable framework for the general Galois descent problem, we need an appropriate substitute for the set $Z_G(M_0)(\Omega)$. As noticed before, denoting by $*$ the action of $G \subset \mathbf{GL}_n$ on matrices by conjugation, the subgroup $Z_G(M_0)(\Omega)$ may be reinterpreted as the stabilizer of M_0 with respect to the action of $G(\Omega)$ on $\mathrm{M}_n(\Omega)$, that is

$$Z_G(M_0)(\Omega) = \mathbf{Stab}_G(M_0)(\Omega) = \{C \in G(\Omega) \mid C * M_0 = M_0\}.$$

Since in our general setting we have a group-scheme acting on $\mathbf{F}$, it seems sensible to introduce the following definition:

Definition 10.1. Let G be a group-valued functor acting on $\mathbf{F}$. For $a \in \mathbf{F}(k)$, and every field extension K/k, we set

$$\mathbf{Stab}_G(a)(K) = \{g \in G(K) \ \mid \ g * a_K = a_K\} \text{ for all } K/k.$$

If $K \to K'$ is a morphism of field extensions, the map $G(K) \to G(K')$ restricts to a map $\mathbf{Stab}_G(a)(K) \to \mathbf{Stab}_G(a)(K')$. Indeed, for every $g \in \mathbf{Stab}_G(a)(K)$, we have

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

We then get a functor $\mathbf{Stab}_G(a)$, called the **stabilizer** of a.

Example 10.2. If $\mathbf{F} = \mathbf{M}_n$ and $M_0 \in \mathrm{M}_n(k)$, then

$$\mathbf{Stab}_G(M_0)(K) = Z_G(M_0)(K) \text{ for all } K/k.$$

Remark 10.3. Let Ω/k be a Galois extension. By definition, the map $\mathbf{Stab}_G(a)(\sigma) : \mathbf{Stab}_G(a)(\Omega) \to \mathbf{Stab}_G(a)(\Omega)$ is obtained by restriction of the map $G(\Omega) \to G(\Omega)$. Hence, the natural action of $\mathcal{G}_\Omega$ on $G(\Omega)$ restricts to an action on $\mathbf{Stab}_G(a)(\Omega)$.

We then obtain a Galois cohomology set $H^1(\mathcal{G}_\Omega, \mathbf{Stab}_G(a)(\Omega))$ for any Galois extension Ω/k.

11. Galois descent lemma

We are now ready to state and prove the Galois descent lemma:

Theorem 11.1 (Galois Descent Lemma)**.** *Let* $\mathbf{F}$ *be a functor, let* G *be a group-valued functor acting on* $\mathbf{F}$*, and let* $a \in \mathbf{F}(k)$*. Assume that* $\mathbf{F}$ *and* G *satisfy the Galois descent condition. Then for every Galois extension* Ω/k*, we have a bijection of pointed sets*

$$\mathbf{F}_a(\Omega/k) \overset{\sim}{\to} \ker[H^1(\mathcal{G}_\Omega, \mathbf{Stab}_G(a)(\Omega)) \to H^1(\mathcal{G}_\Omega, G(\Omega))].$$

In particular, if $H^1(\mathcal{G}_\Omega, G(\Omega)) = 1$*, we have a bijection*

$$\mathbf{F}_a(\Omega/k) \overset{\sim}{\to} H^1(\mathcal{G}_\Omega, \mathbf{Stab}_G(a)(\Omega)).$$

The bijection works as follows:

(1) *If* $[a'] \in \mathbf{F}_a(\Omega/k)$ *is the equivalence class of a twisted form* $a' \in \mathbf{F}(k)$ *of* a*, pick* $g \in G(\Omega)$ *such that* $g * a'_\Omega = a_\Omega$*. The corresponding cohomology class in the kernel of the map*

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

is the class of the cocycle

$$\alpha : \mathcal{G}_\Omega \to \mathbf{Stab}_G(a)(\Omega), \alpha_\sigma \mapsto \alpha_\sigma = g\,\sigma{\cdot}g^{-1}.$$

(2) *If* $[\alpha] \in \ker[H^1(\mathcal{G}_\Omega, \mathbf{Stab}_G(a)(\Omega))) \to H^1(\mathcal{G}_\Omega, G(\Omega))]$*, pick* $g \in G(\Omega)$ *such that* $\alpha_\sigma = g\,\sigma{\cdot}g^{-1}$ *for all* $\sigma \in \mathcal{G}_\Omega$*; the corresponding class in* $\mathbf{F}_a(\Omega/k)$ *is the equivalence class of the unique element* $a' \in \mathbf{F}(k)$ *satisfying* $a'_\Omega = g^{-1} * a_\Omega$*.*

Remark 11.2. Saying that we have a bijection of pointed sets means that it preserves the base points. Hence the class of $[a]$ corresponds to the class of the trivial cocycle.

Proof. The key ingredient of the proof is Corollary 4.6. By Remark 10.3, the action of $\mathcal{G}_\Omega$ on $G(\Omega)$ restricts to an action on $\mathbf{Stab}_G(a)(\Omega)$. Moreover, we have an exact sequence

$$1 \to \mathbf{Stab}_G(a)(\Omega) \to G(\Omega) \to G(\Omega) * a_\Omega \to 1$$

which satisfies the conditions of § 4. By Corollary 4.6, the kernel of $H^1(\mathcal{G}_\Omega, \mathbf{Stab}_G(a)(\Omega)) \to H^1(\mathcal{G}_\Omega, G(\Omega))$ is in one-to-one correspondence with the orbit set of $G(\Omega)^{\mathcal{G}_\Omega}$ in $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$. Notice that $G(\Omega) * a_\Omega$ is simply the set of elements of $\mathbf{F}(\Omega)$ which are equivalent to a_Ω. Since $\mathbf{F}$ satisfies the Galois descent condition, it implies that $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$ is equal to the set

$$\{a'_\Omega \mid a' \in \mathbf{F}(k), a'_\Omega \sim_\Omega a_\Omega\}.$$

In other words, $(G(\Omega) * a)^{\mathcal{G}_\Omega}$ is the image of the set of twisted forms of a under the map $\mathbf{F}(k) \to \mathbf{F}(\Omega)$. Now since G is Galois functor, $G(\Omega)^{\mathcal{G}_\Omega}$ is the image of $G(k)$ under the map $G(k) \to G(\Omega)$.

Now we claim that if $g_\Omega \in G(\Omega)^{\mathcal{G}_\Omega}$ and $a'_\Omega \in (G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$, then we have $g_\Omega \cdot a'_\Omega = (g * a')_\Omega$, where '$\cdot$' denotes here the action defined before Corollary 4.6.

Indeed, since a' is a twisted form of a, we may write $a'_\Omega = g' * a_\Omega$ for some $g' \in G(\Omega)$. Then g' is a preimage of a'_Ω under the map $G(\Omega) \to G(\Omega) * a_\Omega$ and thus

$$\begin{aligned} g_\Omega \cdot a'_\Omega &= (g_\Omega g') * a_\Omega \\ &= g_\Omega * (g' * a_\Omega) \\ &= g_\Omega * a'_\Omega \\ &= (g * a')_\Omega. \end{aligned}$$

We then get the $G(\Omega)^{\mathcal{G}_\Omega}$ orbit of a'_Ω in $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$ is the image of $G(k) * a'$ under the map $\mathbf{F}(k) \to \mathbf{F}(\Omega)$. Hence the map $\mathbf{F}(k) \to \mathbf{F}(\Omega)$ induces a bijection between $\mathbf{F}_a(\Omega/k)$ and the orbit set of $G(\Omega)^{\mathcal{G}_\Omega}$ in $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$. This proves the first part.

Let us now make the bijection a bit more explicit. If $[a'] \in \mathbf{F}_a(\Omega/k)$, the corresponding orbit of $G(\Omega)^{\mathcal{G}_\Omega}$ in $(G(\Omega) * a_\Omega)^{\mathcal{G}_\Omega}$ is the orbit of a'_Ω. By a definition of a twisted form, we may write $g * a'_\Omega = a_\Omega$ for some $g \in G(\Omega)$. Thus g^{-1} is a preimage of a'_Ω under the map $G(\Omega) \to G(\Omega) * a_\Omega$. By Corollary 4.6, the corresponding cohomology class is $\delta^0(g^{-1})$, that is the cohomology class represented by the cocycle

$$\alpha : \mathcal{G}_\Omega \to \mathbf{Stab}_G(a)(\Omega), \sigma \mapsto g\, \sigma \cdot g^{-1}.$$

Conversely, if $[\alpha] \in \ker[H^1(\mathcal{G}_\Omega, \mathbf{Stab}_G(a)(\Omega)) \to H^1(\mathcal{G}_\Omega, G(\Omega))]$, then there exists $g \in G(\Omega)$ such that

$$\alpha_\sigma = g\, \sigma \cdot g^{-1} \text{ for all } \sigma \in \mathcal{G}_\Omega.$$

In other words, we have $[\alpha] = \delta^0(g^{-1})$, and the corresponding element in $\mathbf{F}_a(\Omega/k)$ is represented by the unique element $a' \in \mathbf{F}(\Omega)$ satisfying $a'_\Omega = g^{-1} * a_\Omega$. □

We now give several examples of use of Galois descent.

Example 11.3. Let $\mathbf{F}$ be the functor defined by

$$\mathbf{F}(K) = \{ \text{ regular quadratic forms of dimension } n \text{ over } K\},$$

the induced map being

$$\mathbf{F}(K) \to \mathbf{F}(L), q \mapsto q_L.$$

Then $\mathrm{GL}_n(K)$ acts on $\mathbf{F}(K)$ by $(f, q) \mapsto q \circ f^{-1}$, and this action is functorial. The corresponding equivalence relation is the usual 'isometry relation'. Moreover, the stabilizer of the unit form

$$k^n \to k, (x_1, \ldots, x_n) \mapsto x_1^2 + \ldots + x_n^2$$

is $\mathbf{O}_n$.

It is not difficult to see that all the conditions of the Galois descent lemma are satisfied. Hence, we have a bijection between the set of isometry classes of quadratic forms of dimension n which becomes isometric to the unit form over Ω and $H^1(\mathcal{G}_\Omega, \mathrm{O}_n(\Omega))$.

Example 11.4. Let $\underline{A}$ be a finite dimensional k-vector space. For any field extension K/k, let $\mathbf{F}(K)$ be the set of K-algebras with underlying K-vector space $\underline{A}_K = \underline{A} \otimes_k K$. If $\iota : K \to L$ is a morphism of field extensions of k, we define the induced map by

$$\mathbf{F}(\iota) : \mathbf{F}(K) \to \mathbf{F}(L), A \mapsto A_L = A \otimes_k L.$$

We then obtain a functor $\mathbf{F}$. Now let $f \in \mathrm{GL}(\underline{A}_K)$, and let A be a K-algebra. We will write $x \cdot_A y$ for the product of two elements $x, y \in A$. The map

$$\underline{A}_K \times \underline{A}_K \to \underline{A}_K, (x, y) \mapsto f(f^{-1}(x) \cdot_A f^{-1}(y))$$

endows $\underline{A}_K$ with a structure of a K-algebra, that we will denote by $f \cdot A$. Straightforward computations show that this induces an action of $\mathbf{GL}(\underline{A})$ on $\mathbf{F}$. Notice that by definition, we have

$$f(x) \cdot_{f \cdot A} f(y) = f(x \cdot_A y) \text{ for all } x, y \in A,$$

so that f is an isomorphism of K-algebras from A onto $f \cdot A$. It easily follows that two K-algebras A and B are equivalent if and only if there are isomorphic as K-algebras.

Now fix a K-algebra $A \in \mathbf{F}(k)$. Then $\mathbf{Stab}_{\mathbf{GL}(\underline{A})}(A)$ is nothing but the functor $\mathbf{Aut}_{alg}(A)$ defined by

$$\mathbf{Aut}_{alg}(A)(K) = \mathrm{Aut}_{K-alg}(A \otimes_k K).$$

It is easy to check that $\mathbf{F}$ and $\mathbf{GL}(\underline{A})$ satisfy the conditions of the Galois descent lemma. Hence for any k-algebra A, the pointed set $H^1(\mathcal{G}_\Omega, \mathbf{Aut}_{alg}(A)(\Omega))$ classifies the isomorphism classes of k-algebras which become isomorphic to A over Ω. Moreover, the class of the trivial cocycle corresponds to the isomorphism class of A.

Remark 11.5. Let A be a k-algebra and let Ω/k be a Galois extension. If B is a k-algebra such that there exists an isomorphism $f : B_\Omega \overset{\sim}{\to} A_\Omega$ of Ω-algebras, the corresponding cohomology class is represented by the cocycle

$$\alpha : \mathcal{G}_\Omega \to \mathrm{Aut}_\Omega(A_\Omega), \sigma \mapsto f \circ \sigma{\cdot} f^{-1}.$$

Indeed, since f is a Ω-algebra isomorphism, we have

$$x \cdot_{f \cdot B_\Omega} y = f(f^{-1}(x) \cdot_{A_\Omega} f^{-1}(y)) = x \cdot_{A_\Omega} y \text{ for all } x, y \in A_\Omega,$$

and therefore $f \cdot B_\Omega = A_\Omega$. The description of the bijection in the Galois descent lemma then yields the result.

Conversely, the k-algebra corresponding to a cohomology class $[\alpha] \in H^1(\mathcal{G}_\Omega, \mathbf{Aut}_{\Omega-alg}(A_\Omega))$ is the isomorphism class of

$$B = \{a \in A_\Omega \mid \alpha_\sigma(\sigma{\cdot}a) = a \text{ for all } \sigma \in \mathcal{G}_\Omega\},$$

where the k-algebra structure is given by restriction of the algebra structure on A_Ω.

To see this, notice first that the isomorphism of Ω-vectors spaces

$$f : B_\Omega \xrightarrow{\sim} A_\Omega$$

given by Lemma 3.3 is in fact an isomorphism of Ω-algebras, so that $f \cdot B_\Omega = A_\Omega$. In view of the Galois descent lemma, it is therefore enough to show that we have

$$\alpha_\sigma = f \circ \sigma{\cdot} f^{-1} \text{ for all } \sigma \in \mathcal{G}_\Omega.$$

Since the elements of $B \otimes_k 1$ span A_Ω as an Ω-vector space (this simply comes from the fact that f is an isomorphism), it is enough to check this equality on the elements of the form $x \otimes 1, x \in B$. Now for all $x \in B$ and $\sigma \in \mathcal{G}_\Omega$, we have

$$\begin{array}{rcl} \alpha_\sigma((\,\sigma{\cdot} f)(x\otimes 1)) & = & \alpha_\sigma(\,\sigma{\cdot}(f(\sigma^{-1}\cdot(x\otimes 1)))) \\ & = & \alpha_\sigma(\,\sigma{\cdot}(f(x\otimes 1))) \\ & = & \alpha_\sigma(\,\sigma{\cdot} x) \\ & = & x \\ & = & f(x\otimes 1), \end{array}$$

which is the result we were looking for.

Let us now consider the case of G-algebras.

Definition 11.6. Let k be a field and let G be an abstract group. A G**-algebra** over k is a k-algebra on which G acts faithfully by k-algebra automorphisms. Two G-algebras over k are **isomorphic** if there exists an isomorphism of k-algebras which commutes with the actions of G. It will be denoted by $\simeq_G$.

Example 11.7. Let $\underline{A}$ be a finite dimensional k-vector space and let G be an abstract finite group. For any field extension K/k, let $\mathbf{F}(K)$ be the set of G-algebras over K with underlying vector space $\underline{A}$.
If $\iota : K \to L$ is a morphism of field extensions of k, we define the induced map by

$$\mathbf{F}(\iota) : \mathbf{F}(K) \to \mathbf{F}(L), A \mapsto A_L,$$

where the structure of G-algebra on A_L is given on elementary tensors by

$$g \cdot (a \otimes \lambda) = (g \cdot a) \otimes \lambda \text{ for all } g \in G, a \in A, \lambda \in L.$$

Now let $f \in \mathrm{GL}(\underline{A} \otimes_k K)$, and let A be a G-algebra over K. Consider the K-algebra $f \cdot A$ as defined above. The map

$$G \times f \cdot A \to f \cdot A, (g, x) \mapsto f(g \cdot f^{-1}(x))$$

endows $f \cdot A$ with a structure of a G-algebra over K.

We then get an action of $\mathbf{GL}(\underline{A})$ on $\mathbf{F}$. Moreover, two G-algebras over K are equivalent if and only if they are isomorphic as G-algebras. Once again, all the conditions of the Galois descent lemma are fulfilled, and we get that for any G-algebra A and every Galois extension Ω/k, the pointed set

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

classifies the G-isomorphism classes of G-algebras over k which become G-isomorphic to A over Ω. Moreover, the class of the trivial cocycle corresponds to the G-isomorphism class of A.

12. The conjugacy problem again

Let $G \subset \mathbf{GL}_n$ be a group-valued functor defined by polynomial equations. By Galois descent, the $G(k)$-conjugacy classes over k of matrices M which are $G(\Omega)$-conjugate to M_0 are in one-to-one correspondence with $\ker[H^1(\mathcal{G}_\Omega, Z_G(M_0)(\Omega)) \to H^1(\mathcal{G}_\Omega, G(\Omega))]$. Moreover, the $G(k)$-conjugacy class of M_0 corresponds to the trivial cocycle.

Therefore, the conjugacy problem has a positive answer for all matrices M if and only if the map $H^1(\mathcal{G}_\Omega, Z_G(M_0)(\Omega)) \to H^1(\mathcal{G}_\Omega, G(\Omega))$ has trivial kernel. In particular, if $H^1(\mathcal{G}_\Omega, G(\Omega)) = 1$, the total obstruction to this problem is measured by $H^1(\mathcal{G}_\Omega, Z_G(M_0)(\Omega))$.
Before examining the case of $G = \mathbf{SL}_n$, we need to generalize a bit Hilbert 90:

Proposition 12.1. *Let $L = L_1 \times \cdots \times L_r$, where $L_1, \ldots, L_r$ are finite field extensions of k. Then for every Galois extension Ω/k, we have*

$$H^1(\mathcal{G}_\Omega, (L \otimes_k \Omega)^\times) = 1.$$

Proof. Assume first that $r = 1$, that is L is a field. Set $A = L \otimes_k \Omega$. We will use Galois descent for vector spaces, as for the proof of Hilbert 90. Let $\alpha : \mathcal{G}_\Omega \to A^\times$ be a cocycle. We twist the action of $\mathcal{G}_\Omega$ on A by setting

$$\sigma * x = \alpha_\sigma \, \sigma \cdot x \text{ for all } \sigma \in \mathcal{G}_\Omega, x \in A.$$

The action above is semi-linear and then we have an isomorphism of Ω-vector spaces

$$f : V \otimes_k \Omega \overset{\sim}{\to} A, v \otimes \lambda \mapsto v \cdot \lambda = v(1 \otimes \lambda),$$

where $V = \{x \in A \mid \sigma * x = x \text{ for all } x \in \mathcal{G}_\Omega\}$.
It is easy to check that V is an L-vector space and that f is an isomorphism of A-modules (left as an exercice for the reader). Since $V \otimes_k \Omega \simeq A = L \otimes_k \Omega$, we have

$$\dim_k(V) = \dim_\Omega(V \otimes_k \Omega) = \dim_\Omega(L \otimes_k \Omega) = \dim_k(L),$$

and thus

$$\dim_L(V) = \frac{\dim_k(V)}{\dim_k(L)} = 1.$$

Hence $V = e\cdot L$, for some $e \in V$. Now $e\otimes 1$ is an A-basis of $V\otimes_k\Omega$, so f is just multiplication by $f(e\otimes 1) \in A$. Since f is bijective, $f(e\otimes 1) \in A^\times$. Now $f(e \otimes 1) = e \in V$, and therefore

$$e = \sigma * e = \alpha_\sigma\, \sigma\cdot e \text{ for all } \sigma \in \mathcal{G}_\Omega.$$

This implies that $\alpha = e\,\sigma\cdot e^{-1}$ for all $\sigma \in \mathcal{G}_\Omega$, meaning that α is trivial.

Let us go back to the general case. If $L = L_1 \times \cdots \times L_r$, then we have an isomorphism of $\mathcal{G}_\Omega$-modules,

$$(L \otimes_k \Omega)^\times \simeq (L_1 \otimes_k \Omega)^\times \times \cdots \times (L_r \otimes_k \Omega)^\times.$$

We then have

$$H^1(\mathcal{G}_\Omega, L \otimes_k \Omega) \simeq H^1(\mathcal{G}_\Omega, (L_1 \otimes_k \Omega)^\times) \times \cdots \times H^1(\mathcal{G}_\Omega, (L_r \otimes_k \Omega)^\times),$$

and we use the previous case. □

If E is a finite dimensional algebra over a field F, we denote by $N_{E/F}(x)$ the determinant of left multiplication by x (considered as an endomorphism of the F-vector space E).

Example 12.2. Let $E = k^n, n \geq 1$. If $x = (x_1, \ldots, x_n)$, then we have

$$N_{E/k}(x) = x_1 \cdots x_n,$$

since the representative matrix of ℓ_x in the canonical basis of E is simply the diagonal matrix whose diagonal entries are $x_1, \ldots, x_n$.

Definition 12.3. If L/k is a finite dimensional commutative k-algebra, we denote by $\mathbb{G}_{m,L}^{(1)}$ the functor defined by

$$\mathbb{G}_{m,L}^{(1)}(K) = \{x \in (L \otimes_k K)^\times \mid N_{L\otimes_k K/K}(x) = 1\},$$

for every field extension K/k.

We now compute $H^1(\mathcal{G}_\Omega, \mathbb{G}_{m,L}^{(1)}(\Omega))$ in a special case.

Lemma 12.4. *Let L be a finite dimensional commutative k-algebra, and let Ω/k be a finite Galois extension. Assume that $L \otimes_k \Omega \simeq \Omega^n$ for some $n \geq 1$. Then we have*

$$H^1(\mathcal{G}_\Omega, \mathbb{G}_{m,L}^{(1)}(\Omega)) \simeq k^\times / N_{L/k}(L^\times).$$

Proof. The idea of course is to fit $\mathbb{G}_{m,L}^{(1)}(\Omega)$ into an exact sequence of $\mathcal{G}_\Omega$-modules. We first prove that the norm map

$$N_{L\otimes_k\Omega/\Omega} : (L \otimes_k \Omega)^\times \to \Omega^\times$$

is surjective. For, let $\varphi : L \otimes_k \Omega \overset{\sim}{\to} \Omega^n$ be an isomorphism of Ω-algebras. We claim that we have $N_{L\otimes_k\Omega}(x) = N_{\Omega^n/k}(\varphi(x))$ for all $x \in L \otimes_k \Omega$. Indeed, if $\mathbf{e} = (e_1, \ldots, e_n)$ is a Ω-basis of $L \otimes_k \Omega$, then $\varphi(\mathbf{e}) = (\varphi(e_1), \ldots, \varphi(e_n))$ is a Ω-basis of Ω^n, and we have easily

$$\mathrm{Mat}(\ell_{\varphi(x)}, \varphi(\mathbf{e})) = \mathrm{Mat}(\ell_x, \mathbf{e}).$$

The desired equality then follows immediately. Now for $\lambda \in \Omega^\times$, set $x_\lambda = \varphi^{-1}((\lambda, 1, \dots, 1))$. The equality above and Example 12.2 then yield

$$N_{L\otimes_k\Omega/\Omega}(x_\lambda) = N_{\Omega^n/\Omega}((\lambda, 1, \dots, 1)) = \lambda.$$

Therefore $N_{L\otimes_k\Omega/\Omega}$ is surjective and we have an exact sequence of $\mathcal{G}_\Omega$-modules

$$1 \longrightarrow \mathbb{G}_{m,L}^{(1)}(\Omega) \longrightarrow (L\otimes_k \Omega)^\times \longrightarrow \Omega^\times \longrightarrow 1\ ,$$

where the last map is given by the norm $N_{L\otimes\Omega/\Omega}$. It is known that the condition on L implies in particuliar that L is the direct product of finitely many finite field extensions of k. Applying Galois cohomology and using Proposition 12.1 yield the exact sequence

$$(L\otimes_k 1)^\times \to k^\times \to H^1(\mathcal{G}_\Omega, \mathbb{G}_{m,L}^{(1)}(\Omega)) \to 1,$$

the first map being $N_{L\otimes_k\Omega/\Omega}$. Now it is obvious from the properties of the determinant that we have

$$N_{L\otimes_k\Omega/\Omega}(x\otimes 1) = N_{L/k}(x) \text{ for all } x \in L.$$

The exactness of the sequence above then gives the desired result. □

Remark 12.5. The isomorphim above works as follows:
If $\overline{a} \in k^\times/N_{L/k}(L^\times)$, pick $z \in L\otimes_k \Omega$ such that $a = N_{L\otimes_k\Omega/\Omega}(z)$ (this is possible since $N_{L\otimes_k\Omega/\Omega}$ is surjective). Then the corresponding cohomology class is represented by the cocycle

$$\alpha : \mathcal{G}_\Omega \to \mathbb{G}_{m,L}^{(1)}(\Omega), \sigma \mapsto z^{-1}\sigma\cdot z.$$

Conversely, if $[\alpha] \in H^1(\mathcal{G}_\Omega, \mathbb{G}_{m,L}^{(1)}(\Omega))$, pick $z \in (L\otimes_k \Omega)^\times$ such that

$$\alpha_\sigma = z^{-1}\sigma\cdot z \text{ for all } \sigma \in \mathcal{G}_\Omega.$$

Then $a = N_{L\otimes_k\Omega/}(z)$ lies in fact in $k^\times$, and $\overline{a} \in k^\times/N_{L/k}(L^\times)$ is the class corresponding to $[\alpha]$.

Now let us go back to the conjugacy problem of matrices.

Assume that $M_0 = C_\chi \in \mathrm{M}_n(k)$ is a companion matrix of some monic polynomial $\chi \in k[X]$ of degree $n \geq 1$. In this case, it is known that every matrix commuting with M_0 is a polynomial in M_0, so $Z_G(M_0)(\Omega) = \Omega[M_0] \cap G(\Omega)$. Moreover, the minimal polynomial and the characteristic polynomial are both equal to χ. Set $L = k[X]/(\chi)$, so that we have an isomorphism of k-algebras

$$L \to k[M_0], \overline{P} \to P(M_0),$$

which induces in turn a Galois equivariant isomorphism of Ω-algebras

$$f : L\otimes_k \Omega \xrightarrow{\sim} \Omega[M_0], \overline{X}\otimes\lambda \mapsto \lambda M_0.$$

In particular, f induces an isomorphism of $\mathcal{G}_\Omega$-modules

$$(L\otimes_k \Omega)^\times \simeq \Omega[M_0]^\times.$$

Notice now that if $C \in \mathrm{GL}_n(\Omega)$ commutes with M_0, then C^{-1} also commutes with M_0. Therefore, we have the equalities

$$Z_{\mathbf{GL}_n}(M_0)(\Omega) = \Omega[M_0] \cap \mathrm{GL}_n(\Omega) = \Omega[M_0]^\times,$$

so f induces an isomorphism of $\mathcal{G}_\Omega$-modules

$$(L \otimes_k \Omega)^\times \simeq Z_{\mathbf{GL}_n}(M_0)(\Omega).$$

By Proposition 12.1, we then get $H^1(\mathcal{G}_\Omega, Z_{\mathbf{GL}_n}(M_0)(\Omega)) = 1$, as expected.
Now let us identify $Z_{\mathbf{SL}_n}(M_0)(\Omega)$.
Claim: We have $\det(f(x)) = N_{L\otimes_k\Omega/\Omega}(x)$ for all $x \in L \otimes_k \Omega$.

To see this, set $\alpha = \overline{X} \in L$. Then $\mathbf{e} = (1 \otimes 1, \alpha \otimes 1, \ldots, \alpha^{n-1} \otimes 1)$ is a Ω-basis of $L \otimes_k \Omega$. Let $x = \sum_{i=0}^{n-1} \alpha^i \otimes \lambda_i \in L \otimes_k \Omega$, and let $P = \sum_{i=0}^{n-1} \lambda_i X^i$. Clearly, we have $\ell_x = P(\ell_{\alpha\otimes 1})$. Now the matrix of $\ell_{\alpha\otimes 1}$ in the basis $\mathbf{e}$ is easily seen to be $C_\chi = M_0$, and so the matrix of ℓ_x in the basis $\mathbf{e}$ is $P(M_0) = f(x)$. Therefore $\det(\ell_x) = \det(f(x))$, and we are done.

We then get $Z_{\mathbf{SL}_n}(M_0)(\Omega) \simeq \mathbb{G}_{m,L}^{(1)}(\Omega)$ as a Galois module.

Assume now that χ is separable (i.e. χ has only simple roots in an algebraic closure of k) and that Ω/k is a Galois extension containing all the roots of χ. In this case, we have $L \otimes_k \Omega \simeq \Omega^n$, and by the previous lemma, we have

$$H^1(\mathcal{G}_\Omega, Z_{\mathbf{SL}_n}(M_0)(\Omega)) \simeq k^\times / N_{L/k}(L^\times),$$

which is not trivial in general.
For example, assume that $\mathrm{char}(k) \neq 2$, let $d \in k^\times, d \notin k^{\times 2}$. Set $M_0 = \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix}$ and $M = \begin{pmatrix} 0 & -1 \\ -d & 0 \end{pmatrix}$.
Then M_0 is the companion matrix of $\chi = X^2 - d$ and thus $L = k(\sqrt{d})$. The field $\Omega = k(i, \sqrt{d})$ (where i is a square root of -1) contains all the roots of χ and Ω/k is Galois, with Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^2$ (depending on the fact that $-d$ is whether or not a square in $k^\times$).
Moreover, we have $QMQ^{-1} = M_0 \in \mathrm{M}_2(\Omega)$, with $Q = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, so M and M_0 are conjugate by an element of $\mathrm{SL}_2(\Omega)$.
However, they are not conjugate by an element of $\mathrm{SL}_2(k)$ in general. To see this, let us compute the class in $k^\times/N_{L/k}(L^\times)$ corresponding to the conjugacy class of M. Notice first that $Q\sigma{\cdot}Q^{-1}$ is the identity matrix I_2 if $\sigma(i) = i$ and is -I_2 otherwise. In other words, we have

$$\alpha_\sigma^Q = (iI_2)^{-1}\sigma{\cdot}(iI_2) \text{ for all } \sigma \in \mathcal{G}_\Omega.$$

Via the isomorphism $H^1(\mathcal{G}_\Omega, \mathbb{G}_{m,L}^{(1)}(\Omega)) \simeq H^1(\mathcal{G}_\Omega, Z_{\mathbf{SL}_n}(M_0)(\Omega))$ induced by f_*, the cohomology class $[\alpha^{(Q)}]$ correspond to the cohomology class of the cocycle

$$\beta^{(Q)} : \mathcal{G}_\Omega \to \mathbb{G}_{m,L}^{(1)}(\Omega), \sigma \mapsto (1 \otimes i)^{-1}\sigma \cdot 1 \otimes i.$$

Now $N_{L\otimes\Omega/\Omega}(1 \otimes i) = (1 \otimes i)^2 = -1$, and thus the conjugacy class of M corresponds to the class of -1 in $k^\times/N_{L/k}(L^\times)$. In particular, M and M_0 are conjugate over k if and only if $-1 \in N_{L/k}(L^\times)$. Therefore, to produce counterexamples, one may take for k any subfield of $\mathbb{R}$ and $d < 0$, as we did in the introduction.

13. The case of infinite Galois extensions

In this ultimate paragraph, we would like to indicate quickly how to generalize all this machinery to arbitrary Galois extensions, even infinite ones. I will be extremely vague here, since it can become very quickly quite technical.

Let us come back to the conjugacy problem of matrices one last time, but assuming that Ω/k is completely arbitrary, possibly of infinite degree. The main idea is that the problem locally boils down to the previous case. Let us fix $M_0 \in \mathrm{M}_n(k)$ and let us consider a specific matrix $M \in \mathrm{M}_n(k)$ such that

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

If L/k is any finite Galois subextension of Ω/k with Galois group $\mathcal{G}_L$ containing all the entries of Q, then $Q \in \mathrm{SL}_n(L)$ and the equality above may be read in $\mathrm{M}_n(L)$. Therefore, for this particular matrix M, the descent problem may be solved by examining the corresponding element $[\alpha^{(L)}] \in H^1(\mathcal{G}_L, Z_{\mathrm{SL}_n}(M_0)(L))$. Now if we take another finite Galois subextension L'/k such that $M \in \mathrm{M}_n(L')$ and $Q \in \mathrm{SL}(L')$, we obtain an obstruction $[\alpha^{(L')}] \in H^1(\mathcal{G}_{L'}, Z_{\mathrm{SL}_n}(M_0)(L'))$. But the fact that M is conjugate or not to M_0 by an element of $\mathrm{SL}_n(k)$ is an intrisic property of M and of the field k, and should certainly not depend on the chosen Galois extension L/k. Therefore, we need to find a way to patch these local obstructions together.

There are two ways to proceed. First of all, notice that if L_1/k and L_2/k are two finite Galois extensions such that $L_1 \subset L_2$, then the maps

$$\mathcal{G}_{L_2} \to \mathcal{G}_{L_1}, \sigma_2 \mapsto (\sigma_2)_{|L_1} \text{ and } Z_{\mathrm{SL}_n}(M_0)(L_1) \hookrightarrow Z_{\mathrm{SL}_n}(M_0)(L_2)$$

are compatible, so we have a well-defined map

$$\inf_{L_1,L_2} : H^1(\mathcal{G}_{L_1}, Z_{\mathrm{SL}_n}(M_0)(L_1)) \to H^1(\mathcal{G}_{L_2}, Z_{\mathrm{SL}_n}(M_0)(L_2)),$$

which sends $[\alpha]$ to the class of the cocycle

$$\mathcal{G}_{L_2} \to Z_{\mathrm{SL}_n}(M_0)(L_2), \sigma_2 \mapsto \alpha_{(\sigma_2)_{|L_1}}.$$

If we examine the classes $[\alpha^{(L)}]$ and $[\alpha^{(L')}]$ above, one can check that they are both equal to $[\alpha^{(LL')}]$ when we "push them to LL'". More precisely, we have

$$\inf_{L,LL'}([\alpha^{(L)}]) = [\alpha^{(LL')}] = \inf_{L',LL'}([\alpha^{(L')}]),$$

so we have a whole collection of cohomology classes which coincide when seen "high enough". The idea is then to force all of these classes to be equal by factoring by an appropriate equivalence relation. Of course, there is no particular reason to limit ourselves to $Z_G(M_0)$. If G is a group-valued functor, we may consider the disjoint union

$$\coprod_L H^1(\mathcal{G}_L, G(L)),$$

where L/k runs over all finite Galois subextensions of Ω. We now put the following equivalence relation on this set: we say that $[\alpha] \in H^1(\mathcal{G}_L, G(L))$ and $[\alpha'] \in H^1(\mathcal{G}_{L'}, G(L'))$ are equivalent if there exists a finite Galois extension $L'', L'' \supset L, L'' \supset L'$ such that

$$\inf_{L,L''}([\alpha]) = \inf_{L',L''}([\alpha']).$$

We denote the quotient set by

$$H^1_{ind}(\mathcal{G}_\Omega, G(\Omega)).$$

We then see that our collection of classes $[\alpha^{(L)}]$ define the same element in this set. However, this might be a bit difficult to handle in the applications, so we propose now an alternative.

First of all, we introduce a topology on $\mathcal{G}_\Omega$. The Krull topology is the topology generated by the subsets

$$\sigma \mathrm{Gal}(\Omega/K), \sigma \in \mathcal{G}_\Omega, K \subset \Omega, [K:k] < +\infty.$$

We now consider a group-valued functor G such that:

(1) For all finite Galois subextension L/k, the map $G(L) \to G(\Omega)$ is injective and induces a group isomorphism

$$G(L) \simeq G(\Omega)^{\mathrm{Gal}(\Omega/L)}$$

(2) For all $g \in G(\Omega)$, the subgroup $\{\sigma \in \mathcal{G}_\Omega \mid \sigma \cdot g = g\}$ is open.

These two conditions say that an element $g \in G(\Omega)$ 'comes from' an element of $G(L)$ for some finite Galois subextension L/k of Ω/k, and that the action of $\mathcal{G}_\Omega$ is in fact the same as the action of $\mathcal{G}_L$ on g when viewed as an element of $G(L)$. One can show that any functor G defined by a finite set of polynomial equations with coefficients in k satisfy these assumptions. For example, this is exactly what happens in the case of matrices.

We may then define a cohomology set $H^1_{cont}(\mathcal{G}_\Omega, G(\Omega))$ as in the finite case, but we ask for **continuous** cocycles, where $\mathcal{G}_\Omega$ is endowed with the Krull topology and $G(\Omega)$ is endowed with the discrete topology. The nice thing is that we have

$$H^1_{cont}(\mathcal{G}_\Omega, G(\Omega)) \simeq H^1_{ind}(\mathcal{G}_\Omega, G(\Omega)).$$

Therefore, we have achieved what we wanted, that is finding a way to patch a family of cohomology classes together. Moreover, as long as (1) and (2) are satisfied, all the previous results generalize to arbitrary Galois extensions.

As a final remark, we should point out that we could define the pointed set $H^1(\mathcal{G}_\Omega, G(\Omega))$ dropping the continuity condition, but the equality above does not hold anymore, and therefore one cannot always do patching, so this definition is not really suitable.