Galois descent

Joshua Ruiter

September 3, 2020

Contents

1 Motivating example - $\mathrm{M}_2(\mathbb{R})$ and $\mathbb{H}$

The algebra $\mathrm{M}_2(\mathbb{R})$ of 2×2 matrices with real entries is something we all know and love. Perhaps less familiar is the Hamilton quaternions, which is another 4-dimensional $\mathbb{R}$-algebra. We can describe it as

$$\mathbb{H} = \left\{a + bj + ck + djk : a, b, c, d \in \mathbb{R}, j^2 = k^2 = -1, jk = -kj\right\}$$

I like to think of it via the following presentation.

$$\mathbb{H} = \left\langle 1, j, k, jk : j^2 = k^2 = -1, jk = -kj \right\rangle$$

where the angle brackets denote span over $\mathbb{R}$.

1.1 Not isomorphic as $\mathbb{R}$-algebras

So we have two 4-dimensional algebras over $\mathbb{R}$, a natural question to ask is whether they are isomorphic. They are not.

Proposition 1.1. $\mathrm{M}_2(\mathbb{R}) \not\cong \mathbb{H}$.

Proof. We show $\mathbb{H}$ is a division algebra. Given $q = a + bj + ck + djk$, define

$$\overline{q} = a - bj - ck - djk \qquad N(q) = q\overline{q} = a^2 + b^2 + c^2 + d^2$$

Then

$$\frac{q\overline{q}}{N(q)} = 1$$

so if $q \neq 0$, it has an inverse $q^{-1} = \frac{\overline{q}}{N(q)}$. On the other hand, $\mathrm{M}_2(\mathbb{R})$ is clearly NOT a division algebra, since it has zero divisors, for example

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$\square$

So $\mathbb{H}$ and $\mathrm{M}_2(\mathbb{R})$ are different, at least in this sense. However, they are the same in a different sense. What happens when we extend scalars by tensoring with $\mathbb{C}$? Well clearly if we extend scalars to $\mathbb{C}$ for $\mathrm{M}_2(\mathbb{R})$, we just get $\mathrm{M}_2(\mathbb{C})$.

$$\mathrm{M}_2(R) \otimes_{\mathbb{R}} \mathbb{C} \xrightarrow{\cong} \mathrm{M}_2(\mathbb{C})$$

An explicit isomorphism is given by

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \otimes z_1 + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \otimes z_2 + \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix} \otimes z_3 + \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix} \otimes z_4 \mapsto \begin{pmatrix} z_1 a & z_2 b \\ z_3 c & z_4 c \end{pmatrix}$$

1.2 Become isomorphic after extension to $\mathbb{C}$

Somewhat more surprisingly, if we consider the tensor product $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}$, we ALSO get $\mathrm{M}_2(\mathbb{C})$.

Proposition 1.2. $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathrm{M}_2(\mathbb{C})$.

Proof. Since $1, j, k, jk$ is an $\mathbb{R}$-basis of $\mathbb{H}$, $1 \otimes 1, j \otimes 1, k \otimes 1, jk \otimes 1$ is a $\mathbb{C}$-basis of $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}$. So to define a $\mathbb{C}$-linear map $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \to \mathrm{M}_2(\mathbb{C})$, it suffices to define it on the generators.

$$\begin{aligned}
1 \otimes 1 &\mapsto 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
j \otimes 1 &\mapsto \widehat{j} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \\
k \otimes 1 &\mapsto \widehat{k} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\
jk \otimes 1 &\mapsto \widehat{\ell} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}
\end{aligned}$$

Since the images are four $\mathbb{C}$-linearly independent elements of $\mathrm{M}_2(\mathbb{C})$ and $\mathrm{M}_2(\mathbb{C})$ is 4-dimensional over $\mathbb{C}$, we get that the map described above is bijective. To verify this is a homomorphism of algebras, we just need to verify that the relations $\widehat{j}^2 = \widehat{k}^2 = -1$ and $\widehat{j}\widehat{k} = \widehat{\ell}$ and $\widehat{j}\widehat{k} = -\widehat{k}\widehat{j}$, which are quick matrix calculations. $\square$

So something a bit funny is going on with $\mathbb{H}$ and $\mathrm{M}_2(\mathbb{R})$. Let's draw a diagram.

$$\begin{tikzcd}
\mathbb{C}\text{-algebras} & \mathrm{M}_2(\mathbb{C}) & \\
\mathbb{R}\text{-algebras} \arrow[u, "(-)\otimes_{\mathbb{R}}\mathbb{C}"] & \mathrm{M}_2(\mathbb{R}) \arrow[u, squiggly] & \mathbb{H} \arrow[ul, squiggly]
\end{tikzcd}$$

As $\mathbb{R}$-algebras, they are distinct isomorphism classes. But after extending scalars, they are the same. They are what we call **twisted forms** of each other. This leads us to our next definition.

2 Galois descent

2.1 Twisted forms

Definition 2.1. Let L/K be a field extension. Let A be a K-algebra. A **twisted L/K-form** of A is a K-algebra B such that $A \otimes_K L \cong B \otimes_K L$.

$$\begin{tikzcd} L\text{-algebras} & A \otimes_K L \arrow[r, dash, "\cong"] & B \otimes_K L \\ K\text{-algebras} \arrow[u, "(-)\otimes_K L"] & A \arrow[u, squiggly] & B \arrow[u, squiggly] \end{tikzcd}$$

Given an K-algebra A, we'll denote the set of (K-isomorphism classes) of twisted forms of A by $TF_L(A)$.

This definition makes sense for any field extension, but the case when L/K is a Galois extension is when we can say something about the situation. The process of extending scalars, of applying the functor $(-) \otimes_K L$ is called **Galois ascent**. **Galois descent** is the study of the much more tricky reverse process. The goal is to answer questions like:

1. Given A, and a twisted form B, what is the relationship between A and B?
2. Given an L-algebra C, what can I say about the set of all K-algebras A such that $A \otimes_K L \cong C$? That is, can I locate a given A, and what does the set of all twisted forms of A look like?

2.2 Galois action on L-morphisms

Definition 2.2. Let L/K be a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$, and let A, B be K-algebras. Given $\sigma \in G$, the map

$$\mathrm{Id} \otimes \sigma : A \otimes_K L \to A \otimes_K L \qquad a \otimes \ell \mapsto a \otimes \sigma(\ell)$$

is an automorphism of A_L as an L-algebra. This allows G to act on the set of L-algebra homomorphisms $A_L \to B_L$ as follows.

$$G \times \mathrm{Hom}_L(A_L, B_L) \qquad (\sigma, f) \mapsto {}^{\sigma}f = (\mathrm{Id}_B \otimes \sigma) \circ f \circ (\mathrm{Id}_A \otimes \sigma^{-1})$$

Here's a diagram.

$$\begin{tikzcd} A \otimes_K L \arrow[r, "\mathrm{Id}_A \otimes \sigma^{-1}"] \arrow[rrr, bend right, "{}^{\sigma}f"'] & A \otimes_K L \arrow[r, "f"] & B \otimes_K L \arrow[r, "\mathrm{Id}_B \otimes \sigma"] & B \otimes_K L \end{tikzcd}$$

This is a group action, which means that

$${}^{\sigma}\left({}^{\tau}f\right) = {}^{(\sigma\tau)}f$$

The particular case $A = B$ is important, since it says that G acts on the set $\mathrm{Aut}_L(A_L)$ of automorphisms of A_L. In that case, the diagram is simpler.

$$\begin{tikzcd}
A \otimes_K L \arrow[r, "\mathrm{Id} \otimes \sigma^{-1}"] \arrow[rrr, bend right, "{}^{\sigma} f"'] & A \otimes_K L \arrow[r, "f"] & A \otimes_K L \arrow[r, "\mathrm{Id} \otimes \sigma"] & A \otimes_K L
\end{tikzcd}$$

Also note that G acts on the group $X = \mathrm{Aut}_L(A_L)$ by automorphisms. This means

$${}^{\sigma}(f \circ g) = ({}^{\sigma} f) \circ ({}^{\sigma} g) \qquad ({}^{\sigma} f)^{-1} = {}^{\sigma}(f^{-1})$$

2.3 Given a twisted form of A, obtain a cocycle

We fix a Galois extension L/K, and a K-algebra A. Let A be a K-algebra, and let B be a twisted L/K-form of A. Remember this means we have an L-algebra isomorphism

$$f : A_L \xrightarrow{\cong} B_L$$

We will associate to B a function $\mathrm{Gal}(L/K) \to \mathrm{Aut}_L(A_L)$, which will turn out to have some nice cocycle properties. So we'll define a map

$$a : \mathrm{Gal}(L/K) \to \mathrm{Aut}_L(A_L) \qquad \sigma \mapsto a_\sigma = f^{-1} \circ {}^{\sigma} f$$

Here's a diagram.

$$\begin{tikzcd}
A \otimes_K L \arrow[r, "\mathrm{Id} \otimes \sigma^{-1}"] \arrow[rrr, bend right, "{}^{\sigma} f"'] \arrow[rrrr, bend right=40, "a_\sigma = f^{-1} \circ {}^{\sigma} f"'] & A \otimes_K L \arrow[r, "f"] & B \otimes_K L \arrow[r, "\mathrm{Id} \otimes \sigma"] & B \otimes_K L \arrow[r, "f^{-1}"] & A \otimes_K L
\end{tikzcd}$$

At the moment, the notation a_σ seems bad since it implies that things don't depend on the choice of f. It is true that a_σ depends on f, but in a minute we'll see that it doesn't depend on f in a bad way. Now we can do the following calculation, which is saying that the function a is a cocycle.

Given $\sigma, \tau \in G$,

$$\begin{aligned}
a_{\sigma\tau} &= f^{-1} \circ ({}^{\sigma\tau} f) \\
&= f^{-1} \circ ({}^{\sigma} ({}^{\tau} f)) \\
&= f^{-1} \circ ({}^{\sigma} f) \circ ({}^{\sigma} f)^{-1} \circ ({}^{\sigma} ({}^{\tau} f)) \\
&= f^{-1} \circ ({}^{\sigma} f) \circ ({}^{\sigma} f^{-1}) \circ ({}^{\sigma} ({}^{\tau} f)) \\
&= a_\sigma \circ ({}^{\sigma} f^{-1}) \circ ({}^{\sigma} ({}^{\tau} f)) \\
&= a_\sigma \circ \left({}^{\sigma} \left(f^{-1} \circ ({}^{\tau} f)\right)\right) \\
&= a_\sigma \circ ({}^{\sigma} a_\tau)
\end{aligned}$$

We can also write this without the composition and parentheses if we want, to be fancy.

$$a_{\sigma\tau} = a_\sigma {}^{\sigma} a_\tau$$

This equality is called the **cocycle condition**. For those who know some group cohomology, this is saying that

$$a \in Z^1(G, \mathrm{Aut}_L(A_L))$$

Definition 2.3. Let G be a group and let X be another group on which G acts by automorphisms.

$$G \times X \to X \qquad (g, x) \mapsto {}^g x$$

A **1-cocyle** or **crossed homomorphism** is a map

$$a : G \to X \qquad \sigma \mapsto a_\sigma$$

satisfying

$$a_{\sigma\tau} = a_\sigma {}^\sigma a_\tau$$

for all $\sigma, \tau \in G$. If you try to write this without all the nice notation, it looks something like

$$a(\sigma\tau) = a(\sigma) * \Big(\sigma \cdot a(\tau)\Big)$$

where $\cdot$ is the action of G on X and $*$ is the multiplication in X. Obviously a homomorphism $G \to X$ would satisfy $a_{\sigma\tau} = a_\sigma a_\tau$, so this is why we say "crossed" homomorphism. The set of all 1-cocycles is denoted

$$Z^1(G, X)$$

2.4 Equivalence of cocycles, nonabelian H^1

Definition 2.4. Let G be a group and X be a group on which G acts by automorphisms. Let $a, b \in Z^1(G, X)$ by 1-cocycles. They are **equivalent** or **cohomologous** if there exists $x \in X$ such that

$$b_\sigma = x^{-1} a_\sigma {}^\sigma x$$

for all $\sigma \in G$. This is an equivalence relation. Reflexivity is easy (use $x = 1$), symmetry is easy (use x^{-1}). Transitivity is tricky to track all the notation, but if $a \sim b$ using x and $b \sim c$ using x', then $a \sim b$ using $x'x$.

Definition 2.5. Let G, X be as above. The set of equivalence (cohomology) classes in $Z^1(G, X)$ is denoted $H^1(G, X)$.

Remark 2.6. Notice that the definition above did not involve X being an abelian group. In particular, we want to study this when $X = \mathrm{Aut}_L(A_L)$, which is generally not abelian.

For those who know some group cohomology, if X is abelian, this coincides with the usual definition of H^1. However, in the abelian case, there is an infinite sequence $H^1(G, X), H^2(G, X) \dots$ of groups, and here we don't get that. Even worse, $H^1(G, X)$ does NOT have a group structure. It's just a set. It's a little better than a set, since it has a distinguished element, but really it's just a pointed set.

2.5 From a twisted form to a cohomology class

Ok, so what have we done? Let $X = \mathrm{Aut}_L(A_L)$. We took an L-isomorphism $f : A_L \to B_L$, and associated to it a cocycle $a : G \to X$. So we have a map

$$\beta : \Big\{ \text{isomorphisms } A_L \xrightarrow{\cong} B_L \Big\} \to Z^1(G, A) \qquad f \mapsto a = (\sigma \mapsto a_\sigma = f^{-1} \circ {}^\sigma f)$$

But we don't want this dependence on the choice of isomorphism f, we want to really just understand the relationship between A and B, without reference to a particular L-isomorphism f. The following lemma handles this well.

Lemma 2.7. *Let L/K be a Galois extension, let A be a K-algebra, and let B be a twisted L/K-form of A, and let β be the map described above.*

1. *If f, g are isomorphisms $A_L \to B_L$, then $\beta(f), \beta(g)$ are cohomologous. That is, $\operatorname{im}\beta$ is contained in a single equivalence class in $Z^1(G, X)$.*

2. *If $a, b \in Z^1(G, X)$ are cohomologous and $a \in \operatorname{im}\beta$, then $b \in \operatorname{im}\beta$. That is, $\operatorname{im}\beta$ is an entire equivalence class.*

Proof. (1) Let f, g be isomorphisms $A_L \to B_L$, and let $a = \beta(f), b = \beta(g)$.

$$\begin{aligned} a : G \to A \qquad & \sigma \mapsto a_\sigma = f^{-1} \circ {}^\sigma f \\ b : G \to A \qquad & \sigma \mapsto b_\sigma = g^{-1} \circ {}^\sigma g \end{aligned}$$

Then let $x = g^{-1}f \in X = \operatorname{Aut}_L(A_L)$, and compute

$$\begin{aligned} x^{-1} b_\sigma {}^\sigma x &= \left(g^{-1} f\right)^{-1} \left(b_\sigma\right) \left({}^\sigma(g^{-1}f)\right) \\ &= \left(f^{-1} g\right) \left(g^{-1} \circ {}^\sigma g\right) \left(\left({}^\sigma g^{-1}\right) {}^\sigma f\right) \\ &= f^{-1} \cancel{g g^{-1}} \cancel{({}^\sigma g)({}^\sigma g)^{-1}} {}^\sigma f \\ &= f^{-1} \circ {}^\sigma f \\ &= a_\sigma \end{aligned}$$

Thus a, b are cohomologous.

(2) Let $a, b \in Z^1(G, X)$ be cohomologous and suppose $a = \beta(f)$, so $a_\sigma = f^{-1} \circ {}^\sigma f$ for all $\sigma \in G$. Then there exists $x \in X$ such that

$$b_\sigma = x^{-1} a_\sigma {}^\sigma x = x^{-1} f^{-1} \circ {}^\sigma f {}^\sigma x = (fx)^{-1} \circ {}^\sigma (fx)$$

hence $b = \beta(fx)$.

$\square$

Remark 2.8. The previous lemma says that given a twisted form B of an algebra A, the associated cohomology class in $H^1(G, A)$ which is the image of β above does not depend on the choice of isomorphism $f : A_L \to B_L$. Hence we have obtained a map

$$TF_L(A) \to H^1(G, X \qquad B \mapsto [\beta(f)] = [a]$$

To summarize, given a twisted form B:

1. Choose an L-isomorphism $f : A_L \to B_L$.

2. Associated to f is a cocycle $a \in Z^1(G, X)$, which is $a : G \to \operatorname{Aut}_L(X), a \mapsto f^{-1} \circ {}^\sigma f$. This cocycle does depend on the choice of f.

3. Take the equivalence class of a to get $[a] \in H^1(G, X)$. While the cocyle a depends on f, the class $[a]$ only depends on B.

2.6 Main correspondence

This finally allows me to state the main fact which I wanted to get to.

Theorem 2.9. *The map $TF_L(A) \to H^1(G, X)$ above is a bijection.*

Remark 2.10. There is a lot of interesting things to say about the proof. In particular, the inverse map can be described via a similarly convoluted construction, which is also very interesting. In fact, describing the inverse map involves more true flavor of Galois descent techniques, but I don't have time for it unfortunately.

3 Examples

3.1 Return to $\mathrm{M}_2(\mathbb{R})$ and $\mathbb{H}$

To try to understand the theorem better, let's examine our starting example. We take $K = \mathbb{R}, L = \mathbb{C}, G = \mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}, A = \mathrm{M}_2(\mathbb{R}), B = \mathbb{H}$. First let's try to understand $X = \mathrm{Aut}_L(A_L)$. Well we know $A_L = \mathrm{M}_2(\mathbb{C})$, so the question is, what are the automorphisms of $\mathrm{M}_2(\mathbb{C})$ as a $\mathbb{C}$-algebra? Well, given $x \in \mathrm{GL}_2(\mathbb{C})$, we can do conjugation by x.

$$\mathrm{M}_2(\mathbb{C}) \to \mathrm{M}_2(\mathbb{C}) \qquad y \mapsto xyx^{-1}$$

This is an automorphism. In fact, all automorphisms of $\mathrm{M}_2(\mathbb{C})$ have this form, but this is not obvious. It is a consequence of the Skolem-Noether theorem, but for the moment, just take my word if you haven't heard of that. Ok so this says that roughly, the automorphisms of $\mathrm{M}_2(\mathbb{C})$ are basically $\mathrm{GL}_2(\mathbb{C})$. But wait, not quite. If $x = \lambda I$ is a scalar matrix, then it commutes with any matrix.

$$(\lambda I)y(\lambda I)^{-1} = \lambda y \lambda^{-1} = \lambda\lambda^{-1}y = y$$

So if x is a scalar matrix, it acts as the identity. Another way to say this is that the action of $\mathrm{GL}_2(\mathbb{C})$ on $\mathrm{M}_2(\mathbb{C})$ factors through the quotient $\mathrm{PGL}_2(\mathbb{C}) = \mathrm{GL}_2(\mathbb{C})/\mathbb{C}^\times$. So the automorphism group $X = \mathrm{Aut}_\mathbb{C}(\mathrm{M}_2(\mathbb{C}))$ is $\mathrm{PGL}_2(\mathbb{C})$.

Recall that the Galois group $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts on this automorphism group, we defined this action in general earlier. In this case, the action is pretty straightforward. Remember that the only nontrivial element of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is complex conjugation, so we just have to understand how that acts on $\mathrm{PGL}_2(\mathbb{C})$. Well, there's a pretty obvious way for it to act, which is to act by complex conjugation entry-wise, and this is how it acts.

So putting things together, the theorem says that there's a correspondence

$$TF_\mathbb{C}\Big(\mathrm{M}_2(\mathbb{R})\Big) \cong H^1\Big(\mathbb{Z}/2\mathbb{Z}, \mathrm{PGL}_2(\mathbb{C})\Big)$$

3.2 Relation to Brauer groups

The previous example generalizes. Let L/K be a finite Galois extension of degree $n = [L : K]$, and let $A = \mathrm{M}_n(K)$. The twisted forms of A are then the central simple K-algebras which become isomorphic to $\mathrm{M}_n(L)$ after tensoring. Such algebras are precisely representatives of the elements of the relative Brauer group $\mathrm{Br}(L/K)$.

$$TF_L\Big(\mathrm{M}_n(K)\Big) \cong \mathrm{Br}(L/K)$$

If L is the separable closure of K (equivalently L is the algebraic closure if $\operatorname{char} K = 0$) then the relative Brauer group is the whole Brauer group. So for instance, in the previous example,

$$TF_{\mathbb{C}}\Big(\mathrm{M}_2(\mathbb{R})\Big) \cong \mathrm{Br}(\mathbb{C}/\mathbb{R}) = \mathrm{Br}(\mathbb{R})$$

Returning to some generality, applying Skolem-Noether as before tells us that $\mathrm{Aut}_L(\mathrm{M}_n(L)) \cong \mathrm{PGL}_n(L)$. So

$$\mathrm{Br}(L/k) \cong TF_L\Big(\mathrm{M}_n(K)\Big) \cong H^1\Big(\mathrm{Gal}(L/K), \mathrm{PGL}_n(L)\Big)$$

3.3 Relation to descent

Let's try and connect our main correspondence to Galois descent. The situation of descent is something like this.

$$\begin{tikzcd}
L\text{-algebras} & & & A_L \arrow[dl, squiggly, "?"'] \arrow[dr, squiggly, "?"] & \\
K\text{-algebras} \arrow[u, "(-)\otimes_K L"] & & ? & A \arrow[u, squiggly] & ?
\end{tikzcd}$$

We want to know what other things on the K-level correspond to our L-algebra A_L. Well the correspondence says something about the set of all the question marks. It says they correspond to some cohomology set.

$$\begin{tikzcd}
L\text{-algebras} & A_L \arrow[d, squiggly, shift left, "?"] & \\
K\text{-algebras} \arrow[u, "(-)\otimes_K L"] & \{?,?,?,\dots\} \arrow[u, squiggly, shift left, "\otimes_L"] \arrow[r, leftrightarrow, "\cong"] & H^1\Big(\mathrm{Gal}(L/K), \mathrm{Aut}(A_L)\Big)
\end{tikzcd}$$

So this tells us that if we want to understand how to descend, it's going involve to the Galois group and its interactions with automorphisms on the L-level.