Galois descent

Joshua Ruiter

July 3, 2020

The goal of these notes is to understand the following situation. Suppose we have a field K, and a Galois extension L/K. Suppose we have some object A "over K", such as a K-vector space, a K-algebra, a K-scheme, an algebraic K-group, etc. By "tensoring up" to L, we obtain a L-object of the same type, typically denoted A_L. Given a K-object A, an L/K-form of A is a K-object B such that $A_L \cong B_L$. We would like to understand the following.

1. Given a L-object (or L-morphism), when does it come from a K-object (or K-morphism)?
2. How to determine if an object B is an L/K-form of A.
3. What does the set of all L/K-forms of A look like?
4. How is the set of L/K-forms of A related to the Galois group $\mathrm{Gal}(L/K)$?

The last question is the most interesting, since it turns out that $\mathrm{Gal}(L/K)$ and some associated group cohomology groups are in bijection with L/K-forms of A. This relationship and the various associated theory and proof techniques are known as Galois descent.

Let's consider a motivating example. Let $K = \mathbb{R}, L = \mathbb{C}$. Let $A = \mathrm{M}_2(\mathbb{R})$ be the $\mathbb{R}$-algebra of 2×2 matrices with real entries, and let $B = \mathbb{H}$ be the Hamilton quaternions. We can write B as

$$B = \{a + bi + cj + dij : a, b, c, d \in \mathbb{R}\}$$

subject to the multiplication relations

$$i^2 = j^2 = -1 \qquad ij = -ji$$

Both A and B are 4-dimensional algebras over $\mathbb{R}$. They both have a unit, both are non-commutative, and both are "central" and "simple" algebras, whatever that means. We claim, however, that they are NOT isomorphic as $\mathbb{R}$-algebras. The simplest way to see this is that $\mathbb{H}$ is a division algebra, while $M_2(\mathbb{R})$ is not. To see that $M_2(\mathbb{R})$ is not a division algebra, it suffices to exhibit one non-invertible nonzero matrix. For example,

$$x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R})$$

is not invertible. On the other hand, every nonzero element of $\mathbb{H}$ is a unit. I'll omit the details, but if $q = a + bi + cj + dij \in \mathbb{H}$ and $q \neq 0$, the inverse is given by

$$q^{-1} = \frac{\overline{q}}{N(q)} = \frac{a - bi - cj - dij}{a^2 + b^2 + c^2 + d^2}$$

So at this point we have two non-isomorphic 4-dimensional $\mathbb{R}$-algebras, A and B. Using the extension $\mathbb{C}/\mathbb{R}$, we can tensor both up to $\mathbb{C}/\mathbb{R}$.

$$\begin{aligned} A_{\mathbb{C}} &= \mathrm{M}_2(\mathbb{R}) \otimes_{\mathbb{R}} \mathbb{C} \cong \mathrm{M}_2(\mathbb{C}) \\ B_{\mathbb{C}} &= \mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \end{aligned}$$

$A_{\mathbb{C}}$ is straightforward - tensoring a matrix algebra up to a bigger field just gives the matrix algebra over the bigger field. However, $B_{\mathbb{C}}$ is somewhat more mysterious. It would take some theory to explain why, but the upshot is that as a $\mathbb{C}$-algebra,

$$B_{\mathbb{C}} = \mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathrm{M}_2(\mathbb{C})$$

Essentially, this happens because $\mathbb{H}$ contains an isomorphic copy of $\mathbb{C}$, given by the elements $a+bi$. The two algebras A and B which were not isomorphic over $\mathbb{R}$ became isomorphic after extending scalars. In general, this may happen - two different objects over a smaller field may collapse into a single isomorphism class after extension. So while tensoring up to a field extension is always possible, "descending" is harder, because there may be more than one object below. For example, the $\mathbb{C}$-algebra $M_2(\mathbb{C})$ does not "lie above" a unique $\mathbb{R}$-algebra, since both $\mathrm{M}_2(\mathbb{R})$ and $\mathbb{H}$ lie below it. This example raises questions like

1. Given the $\mathbb{C}$-algebra $M_2(\mathbb{C})$, can we recover the collection of all $\mathbb{R}$-algebras A such that $A_{\mathbb{C}} \cong M_2(\mathbb{C})$?

2. What is the relationship between $\mathrm{M}_2(\mathbb{R})$ and $\mathbb{H}$ which makes them the same after $\otimes_{\mathbb{C}}$?

These and other questions are the goal of these notes to explore.

Contents

Note on notation

Throughout K is a field, and L/K is usually a Galois extension. Sometimes we require L/K to be finite, but we want all of our main results to hold when L/K is infinite as well. By a vector space over K, we always mean a finite dimensional vector space over K. Many results still hold for infinite dimensional vector spaces, but not all.

1 Group cohomology

1.1 Discrete groups acting on abelian groups

Let G be a group and A be a G-module (a module over the group ring $\mathbb{Z}[G]$). The fixed point functor $A \mapsto A^G$ from G-modules to abelian groups is left exact, so we may form its right derived functors, which are denoted $H^i(G, -)$. In particular,

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

There is also an interpretation of $H^i(G, A)$ in terms of something called cochains, which allows for more concrete interpretations of the abelian group $H^i(G, A)$ in terms of functions from a product of copies of G to A satisfying certain properties. In particular, $H^1(G, A)$ can be identified with "crossed homomorphisms" $G \to A$ modulo some equivalence.

Definition 1.1. Let G be a group and A a G-module. A **crossed homomorphism** is a map $f : G \to A$ satisfying

$$f(gh) = \big(f(g)\big) + \big(g \cdot f(h)\big)$$

for all $g, h \in G$. Note that $+$ denotes addition in A and $\cdot$ denotes the action of G on A. Crossed homomorphisms are also sometimes called **1-cocycles**. The set of 1-cocycles is denoted $Z^1(G, A)$.

$$Z^1(G, A) = \big\{f : G \to A \mid f(gh) = \big(f(g)\big) + \big(g \cdot f(h)\big),\ \forall g, h \in G\big\}$$

Note that $Z^1(G, A)$ forms an abelian group under pointwise addition.

Definition 1.2. Let G be a group and A a G-module. For any $a \in A$, the function

$$f : G \to A \qquad g \mapsto g \cdot a - a$$

is a crossed homomorphism, as the calculation below demonstrates.

$$f(gh) = (gh) \cdot a - a = (gh) \cdot a - g \cdot a + g \cdot a - a = g \cdot (h \cdot a - a) + g \cdot a - a = g \cdot f(h) + f(g)$$

Such a map is called a **trivial crossed homomorphism**, or a **1-coboundary**. The set of 1-coboundaries is denoted $B^1(G, A)$.

$$\boldsymbol{B^1(G, A)} = \{f : G \to A \mid \exists a \in A, f(g) = ga - a, \forall g \in G\}$$

Note that $B^1(G, A)$ forms a subgroup of $Z^1(G, A)$.

Definition 1.3. Two crossed homomorphisms $G \to A$ are **equivalent** or **cohomologous** if their difference is a trivial crossed homomorphism. The equivalence class of a crossed homomorphism is called its **cohomology class**.

Proposition 1.4. *$H^1(G, A)$ is isomorphic to the quotient group of crossed homomorphisms modulo trivial crossed homomorphisms, that is, the set of cohomology classes.*

$$H^1(G, A) \cong \frac{Z^1(G, A)}{B^1(G, A)} = \frac{\{f : G \to A \mid f(gh) = f(g) + gf(h), \forall g, h \in G\}}{\{f : G \to A \mid \exists a \in A, f(g) = ga - a, \forall g \in G\}}$$

Example 1.5. Let K be a field, and L/K a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. We may view L as an additive group and a G-module, or view $L^\times$ as a multiplicative group, also as a G-module. In these cases, the fixed points are $K, K^\times$ respectively.

$$H^0(G, L) = K$$
$$H^0(G, L^\times) = K^\times$$

One version of a classical result known as Hilbert's Theorem 90 says that

$$H^1(G, L) = 0$$
$$H^1(G, L^\times) = 0$$

1.2 Profinite groups acting on abelian groups

Now suppose G is a profinite group, and A is a topological G-module, meaning that A is a topological abelian group and the G-action map $G \times A \to A$ is continuous with respect to the topology on A and the profinite topology on G. Sometimes we refer to such an A as a **continuous G-module**.

Definition 1.6. Let G be a profinite group and A a topological G-module. A is a **discrete** topological G-module if the map $G \times A \to A$ is still continuous if we replace the topology on A with the discrete topology. Equivalently, the stabilizer of each $a \in A$ is an open subgroup of G.

Definition 1.7. Let G be a profinite group and A a topological G-module. In parallel with the discrete case, define

$$\boldsymbol{H^0_{\mathrm{cts}}(G, A)} = A^G$$

We may also define the **continuous 1-cocycles** and **continuous 1-coboundaries** as

$$Z^1_{\mathrm{cts}}(G, A) = \big\{f : G \to A \text{ continuous} \mid f(gh) = \big(f(g)\big) + \big(g \cdot f(h)\big),\ \forall g, h \in G\big\}$$
$$B^1_{\mathrm{cts}}(G, A) = \{f : G \to A \text{ continuous} \mid \exists a \in A, f(g) = ga - a, \forall g \in G\}$$

Then we define $H^1_{\mathrm{cts}}(G, A)$ to be the set of cohomology classes.

$$\boldsymbol{H^1_{\mathrm{cts}}(G, A)} = \frac{Z^1_{\mathrm{cts}}(G, A)}{B^1_{\mathrm{cts}}(G, A)}$$

These are once again abelian groups, H^1 being a group under pointwise addition. In a mild abuse of notation, when G is profinite and A is a topological G-module, we will drop the subscript cts and just write $H^0(G, A), H^1(G, A)$ for these groups.

Example 1.8. Let L/K be an infinite Galois extension, with Galois group $G = \mathrm{Gal}(L/K)$. Then G is a profinite group, and both L (as an additive group) and $L^\times$ (as a multiplicative group) are discrete continuous G-modules. The computations are mostly the same as previously.

$$\begin{aligned} H^0(G, L) &= K \\ H^0(G, L^\times) &= K^\times \\ H^1(G, L) &= 0 \\ H^1(G, L^\times) &= 0 \end{aligned}$$

Remark 1.9. Let K be a field and $G = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ be the absolute Galois group and let A be a continuous G-module. So we have associated cohomology groups

$$H^0(G, A) \qquad H^1(G, A)$$

Since this situation arises so commonly and G is entirely determined by K, the notation frequently substitutes K for G. So the groups above are denoted

$$H^0(K, A) \qquad H^1(K, A)$$

This is not meant to imply in any way that k acts as a group (either additively or multiplicatively) on A, but is just a shorthand for $H^1(G, A)$.

1.3 Discrete groups acting on nonabelian groups

Definition 1.10. Let G be a group. A **G-group** is a group A with a group action $G \times A \to A$ such that elements of G act by automorphisms. If A is an abelian group, then we recover the notion of a G-module.

Definition 1.11. Let G be a group and let A, B be G-groups. A **morphism of G-groups** is a group homomorphism $\phi : A \to B$ such that

$$\phi(ga) = g\phi(a)$$

for all $g \in G, a \in A$. In other words, for every $g \in G$, the following diagram commutes.

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{\phi} & B \end{array}$$

Definition 1.12. Let G be a group and let A be a G-group. Paralleling the definitions above, define

$$\boldsymbol{H^0(G, A)} = A^G$$

Note that this is a subgroup of A.

Definition 1.13. Let $\phi : A \to B$ be a morphism of G-groups. Then $\phi|_{A^G} : A^G \to B$ has image which lands in B^G, since

$$g\phi(a) = \phi(ga) = \phi(a)$$

for $a \in A^G$. Thus ϕ induces a map on H^0, which is just $\phi|_{A^G}$. We denote it by ϕ^0.

$$\phi^0 : H^0(G, A) \to H^0(G, B)$$

This makes $H^0(G, -)$ into a covariant functor.

Definition 1.14. Let G be a group and A be a G-group. A **crossed homomorphism** or **1-cocycle** is a map $f : G \to A$ satisfying

$$f(gh) = \big(f(g)\big) * \big(g \cdot f(h)\big) \qquad \forall g, h \in G$$

where $\cdot$ denotes the G-action on A and $*$ denotes the operation in A. Once again, we denote the set of such 1-cocycles by $Z^1(G, A)$.

$$\boldsymbol{Z^1(G,A)} = \big\{f : G \to A \mid f(gh) = \big(f(g)\big) * \big(g \cdot f(h)\big),\ \forall g, h \in G\big\}$$

Note that $Z^1(G, A)$ is no longer necessarily a group under the pointwise operation in A. Nevertheless, $Z^1(G, A)$ is a set, and it is always non-empty, since it contains the constant map $G \to A, g \mapsto 1$ where 1 is the identity element of A. This constant map is called the **unit cocycle**.

Notation. Since the parentheses are starting to get somewhat unwieldy in the notation above, we describe an alternative notation for 1-cocycles in the nonabelian case. Let G be a group and A a G-group. For a 1-cocycle $f : G \to A$, we use the notation

$$f_\sigma := f(\sigma)$$

and for $a \in A$ and $\sigma \in G$, we use the notation

$${}^\sigma a := \sigma \cdot a$$

In this notation, the usual relations for G acting on A by automorphisms are expressed as

$${}^\sigma 1 = 1 \qquad ({}^\sigma a)({}^\sigma b) = {}^\sigma(ab) \qquad \forall a, b \in A, \sigma \in G$$

and the requirement that a map $\phi : A \to B$ be a morphism of G-groups is expressed as

$${}^\sigma(\phi a) = \phi({}^\sigma a)$$

Using this notation, the cocycle condition translates to

$$f(\sigma\tau) = \big(\sigma \cdot f(\tau)\big) * \big(f(\sigma)\big) \qquad \rightsquigarrow \qquad f_{\sigma\tau} = f_\sigma * {}^\sigma f_\tau = f_\sigma {}^\sigma f_\tau$$

So we can write

$$Z^1(G, A) = \{f : G \to A \mid f_{\sigma\tau} = f_\sigma {}^\sigma f_\tau,\ \forall \sigma, \tau \in G\}$$

Definition 1.15. Let $\phi : A \to B$ be a morphism of G-groups, and let $f \in Z^1(G, A)$ be a crossed homomorphism. Then consider the composition

$$\phi \circ f : G \to B$$

We claim that this is also a crossed homomorphism. Let $g, h \in G$. Then

$$(\phi \circ f)_{\sigma\tau} = \phi\,(f_{\sigma\tau}) = \phi\,(f_\sigma{}^\sigma f_\tau) = \phi(f_\sigma)\phi({}^\sigma f_\tau) = \phi(f_\sigma)^\sigma\phi(f_\tau) = (\phi \circ f)_\sigma{}^\sigma(\phi \circ f)_\tau$$

Thus $\phi \circ f \in Z^1(G, B)$ is a crossed homomorphism. Hence post-composition with ϕ induces a map

$$\widetilde{\phi} : Z^1(G, A) \to Z^1(G, B) \qquad f \mapsto f \circ \phi$$

Definition 1.16. Let G be a group and A be a G-group. The notion of 1-coboundaries does not quite generalize to the nonabelian setting, so instead of an analog for $B^1(G, A)$, we have to replace it by a suitable equivalence relation on $Z^1(G, A)$, which accomplishes the same task. Let $\alpha, \beta \in Z^1(G, A)$ be 1-cocycles. They are **equivalent** or **cohomologous** if there exists $c \in A$ such that

$$\beta_\sigma = c^{-1}\alpha_\sigma{}^\sigma c$$

for all $\sigma \in G$.

Remark 1.17. The above is an equivalence relation, as we now verify. Reflexivity is clear, take $c = 1$, and note that ${}^g 1 = 1$ since G acts by automorphisms. If $\alpha \sim \beta$ with

$$\beta_\sigma = c^{-1}\alpha_\sigma{}^\sigma c \qquad \forall \sigma \in G$$

then

$$\alpha_\sigma = c\beta_\sigma({}^\sigma c)^{-1} = (c^{-1})^{-1}\beta_\sigma{}^\sigma(c^{-1}) \qquad \forall \sigma \in G$$

hence $\beta \sim \alpha$, so the relation is symmetric. If $\alpha \sim \beta$ and $\beta \sim \gamma$, we have $c, d \in A$ such that

$$\alpha_\sigma = c^{-1}\beta_\sigma{}^\sigma c, \beta_\sigma = d^{-1}\gamma_\sigma{}^\sigma d \qquad \forall \sigma \in G$$

Then

$$\alpha_\sigma = c^{-1}(d^{-1}\gamma_\sigma{}^\sigma d)^\sigma c = c^{-1}d^{-1}\gamma_\sigma{}^\sigma d^\sigma c = (dc)^{-1}\gamma_\sigma{}^\sigma(dc)$$

hence $\alpha \sim \gamma$, so the relation is transitive.

Definition 1.18. Let G be a group and A be a G-group. We define $\boldsymbol{H^1(G, A)}$ to be the set of equivalence classes under the above relation on $Z^1(G, A)$. Note that $H^1(G, A)$ is not a group, merely a set. The equivalence classes are called **cohomology classes**.

Remark 1.19. If A is abelian, the previous definition recovers the definition of $H^1(G, A)$ as the quotient Z^1/B^1. In particular, in this situation, $H^1(G, A)$ is an abelian group.

Definition 1.20. Let $\phi : A \to G$ be a morphism of G-groups, with induced map on 1-cocycles,

$$\widetilde{\phi} : Z^1(G, A) \to Z^1(G, B) \qquad f \mapsto f \circ \phi$$

We claim that this descends to a map $H^1(G,A) \to H^1(G,B)$. It is clear that we can compose $\widetilde{\phi}$ with the quotient map $Z^1(G,B) \to H^1(G,B)$. The question then becomes whether equivalent cocycles in $H^1(G,A)$ get mapped to equivalent cocycles in $H^1(G,B)$.

To verify this, we need to show that if $\alpha, \beta \in Z^1(G,A)$ are equivalent, then $\phi \circ \alpha, \phi \circ \alpha$ are equivalent (represent the same class in $H^1(G,B)$). Suppose $\alpha, \beta \in Z^1(G,A)$ are equivalent. Then there exists $c \in A$ such that

$$\beta_\sigma = c^{-1} \alpha_\sigma {}^\sigma c$$

for all $\sigma \in G$. Then

$$\begin{aligned}
(\phi \circ \beta)_\sigma &= \phi(\beta_\sigma) \\
&= \phi(c^{-1} \alpha_\sigma {}^\sigma c) \\
&= \phi(c^{-1}) \phi(\alpha_\sigma) \phi({}^\sigma c) \\
&= \phi(c)^{-1} (\phi \circ \alpha)_\sigma {}^\sigma \phi(c)
\end{aligned}$$

This holds for all $\sigma \in G$, so $\phi \circ \beta$ and $\phi \circ \alpha$ are equivalent using $d = \phi(c) \in B$. The upshot of all of this is that a morphism $\phi : A \to B$ of G-groups induces a map

$$\phi^1 : H^1(G,A) \to H^1(G,B) \qquad \phi^1[f] = [\phi \circ f]$$

where the brackets represent equivalence/cohomology classes.

Definition 1.21. A **pointed set** is a pair (X, x_0) where X is a set and $x_0 \in X$ is an element, usually called the **distinguished element**.

Definition 1.22. Let G be a group and A a G-group, not necessarily abelian. Recall that inside $Z^1(G,A)$ we have the unit cocycle $G \to A, g \mapsto 1$. The class of the unit cocycle is called the **distinguished element** of $H^1(G,A)$. This makes $H^1(G,A)$ into a pointed set, which is all the structure we can ascribe to it in the situation where A is nonabelian.

Definition 1.23. Let (X, x_0) and (Y, y_0) be pointed sets. A **morphism of pointed sets** is a set map $\psi : X \to Y$ such that $\psi(x_0) = y_0$. The **image** of ψ is the pointed set $(\psi(X), \psi(x_0) = y_0)$. Then **kernel** of ψ is the pointed set $(\psi^{-1}(y_0), x_0)$.

Definition 1.24. Let $\psi : (X, x_0) \to (Y, y_0)$ and $\phi : (Y, y_0) \to (Z, z_0)$ be morphisms of pointed sets. The sequence

$$(X, x_0) \xrightarrow{\psi} (Y, y_0) \xrightarrow{\phi} (Z, z_0)$$

is **exact** if the image of ψ is equal to the kernel of ϕ. More concretely, if we just think of $\psi : X \to Y$ and $\phi : Y \to Z$ as set maps, exactness means that $\psi(X) = \psi^{-1}(z_0)$.

Remark 1.25. Let $\phi : A \to B$ be a morphism of G-groups. It is clear that the induced map $\widetilde{\psi} : Z^1(G,A) \to Z^1(G,B)$ maps the unit cocycle to the unit cocycle, so the induced map $\psi^1 : H^1(G,A) \to H^1(G,B)$ maps the distinguished element of $H^1(G,A)$ to the distinguished element of $H^1(G,B)$, so ψ^1 is a morphism of pointed sets.

Proposition 1.26. *Let G be a group and suppose we have a short exact sequence of G-modules.*

$$1 \to A \xrightarrow{a} B \xrightarrow{b} C \to 1$$

Then there is an exact sequence of pointed sets

$$1 \to A^G \xrightarrow{a^0} B^G \xrightarrow{b^0} C^G \xrightarrow{\delta} H^1(G, A) \xrightarrow{a^1} H^1(G, B) \xrightarrow{b^1} H^1(G, C)$$

Proof. Omitted. □

Remark 1.27. We think of A^G as a pointed set with distinguished element $1 \in A^G$, and it is clear that a^0 is then a map of pointed sets $A^G \to B^G$.

1.4 Profinite groups acting on nonabelian groups

As in the case of abelian cohomology, we have a profinite version of nonabelian cohomology.

Definition 1.28. Let G be a profinite group. A **topological *G*-group** is a topological group A which is also a G-group, such that the map $G \times A \to A$ is continuous. A topological G-group A is **discrete** if the stabilizer of each $a \in A$ is an open subgroup of G.

Definition 1.29. A **morphism of topological *G*-groups** or ***G*-morphism** is a morphism of G-groups which is also continuous with respect to the topology on A.

Definition 1.30. Let G be a profinite group and A be a discrete topological G-group. Define

$$H^0_{\text{cts}}(G, A) = H^0(G, A) = A^G$$

to be the fixed points of the G-action. Also define

$$Z^1_{\text{cts}}(G, A) = \{f : G \to A, \text{ continuous} \mid f_{gh} = f_g {}^g f_h, \ \forall g, h \in G\}$$

We define a relation on $Z^1_{\text{cts}}(G, A)$ by the same formula as in the discrete case.

$$\alpha \sim \beta \qquad \iff \qquad \exists c \in A, \beta_g = c^{-1} \alpha_g {}^g c, \forall g \in G$$

As in the discrete case, this is an equivalence relation, and we define $H^1_{\text{cts}}(G, A)$ to be the set of equivalence classes. We will abuse notation and just write this as $H^1(G, A)$. As before, this is not a group if A is nonabelian, but it is has a distinguished element given by the class of the unit cocycle. (The unit cocycle is continuous because A is discrete.)

Definition 1.31. As before, a morphism of topological G-groups $\phi : A \to B$ induces maps of pointed sets

$$\phi^0 : H^0_{\text{cts}}(G, A) \to H^0(G, B)$$
$$\phi^1 : H^1_{\text{cts}}(G, A) \to H^1(G, B)$$

Remark 1.32. The exact sequence from before also has a profinite version, when the G-groups involved are discrete. That is, if

$$1 \to A \to B \to C \to 1$$

is a short exact sequence of discrete topological G-groups, there is an associated exact sequence of pointed sets

$$1 \to H^0_{\text{cts}}(G, A) \to H^0_{\text{cts}}(G, B) \to H^0_{\text{cts}}(G, C) \to H^1_{\text{cts}}(G, A) \to H^1_{\text{cts}}(G, B) \to H^1_{\text{cts}}(G, C)$$

1.5 Twisted actions

Definition 1.33. Let G be a group and let A be a G-group. Let X be a G-set and an A-set, that is, both G and A act on X. The actions are **compatible** if for all $x \in X, a \in A, \sigma \in G$,

$$\sigma \cdot (a \cdot x) = (\sigma \cdot a) \cdot (\sigma \cdot x)$$

In the above, $\cdot$ is used for all of the actions, of G on A, G on X, and A on X. If X is a G-set and A-set with compatible actions, we also call X a **(G, A)-set**.

Definition 1.34. Let K/k be a finite Galois extension with Galois group G. Let W be a K-vector space, and suppose we have an action of G on W. If this action is compatible with the G-action on K and the K-action on W, we say that the action of G is **semilinear**.

Example 1.35. Let K/k be a Galois extension and $G = \mathrm{Gal}(K/k)$. G acts on K in the usual way, since elements of G are by definition automorphisms of K.

$$G \times K \to K \qquad \sigma \cdot \lambda = \sigma(\lambda)$$

Let V be a k-vector space, and consider the tensor product $V_K = V \otimes_k K$, which is a K-vector space. As a K-vector space, it has a K-action in the obvious way.

$$K \times V_K \to V_K \qquad \mu \cdot (v \otimes \lambda) = v \otimes \mu\lambda$$

where $\mu, \lambda \in K, v \in V$. V_K also has a convenient G-action.

$$G \times V_K \to V_K \qquad \sigma \cdot (v \otimes \lambda) = v \otimes \sigma\lambda$$

where $\sigma \in G, v \in V, \lambda \in K$. These actions are compatible, that is, G acts semilinearly on V_K. Said another way, V_K is a (G, K)-set.

$$\sigma \cdot (\mu \cdot (v \otimes \lambda)) = \sigma \cdot (v \otimes \mu\lambda) = v \otimes \sigma(\mu\lambda) = \sigma(\mu)(v \otimes \sigma\lambda) = (\sigma \cdot \mu) \cdot (\sigma \cdot (v \otimes \lambda))$$

Definition 1.36. Let G be a group, A a G-group, and X a (G, A)-set, and let $\cdot$ denote all of the involved actions. Let $a \in Z^1(G, A)$ be a 1-cocycle. We define the **twisted action by the cocycle $\boldsymbol{a}$** of G on X via

$$G \times {}_aX \to {}_aX \qquad (\sigma, x) \mapsto \sigma * x = a_\sigma \cdot (\sigma \cdot x)$$

where ${}_aX$ is the same as the set X, just notated differently, and $\sigma \in G, x \in X$. We now verify that this is in fact a group action: for $\sigma, \tau \in G$ and $x \in X$,

$$\begin{aligned}(\sigma\tau) * x = a_{\sigma\tau} \cdot \Big((\sigma\tau) \cdot x\Big) &= \Big(a_\sigma(\sigma \cdot a_\tau)\Big) \cdot \Big(\sigma \cdot (\tau \cdot x)\Big) = a_\sigma \cdot (\sigma \cdot a_\tau) \cdot \Big(\sigma \cdot (\tau \cdot x)\Big) \\ = a_\sigma \cdot \Big(\sigma \cdot \big(a_\tau \cdot (\tau \cdot x)\big)\Big) &= \sigma * \Big(a_\tau \cdot (\tau \cdot x)\Big) = \sigma * (\tau * x)\end{aligned}$$

The second equality uses the cocycle property of a, and the first equality of the second line uses the compatibility of the G, A-actions on X. This verifies that $*$ gives a group action on X. In such a situation, we use the notation $\boldsymbol{{}_aX}$ to denote the set X with the twisted G-action.

Remark 1.37. Let X be a (G, A)-set, and $a \in Z^1(G, A)$ a 1-cocycle. If X is a group, and G and A act on it by automorphisms, then the twisted action on ${}_aX$ is also by automorphisms. Similarly, if X is a vector space over somefield k, and G, A act by automorphisms, then the twisted action is by automorphisms.

Remark 1.38. The twisted action above does not descend to the level of cohomology classes. That is, the twisted action depends on the cocycle, not just on the cohomology class of the cocycle.

Example 1.39. Let L/K be a finite Galois extension and $G = \mathrm{Gal}(L/K)$. Let $A = \mathrm{GL}_n(L)$ and $X = \mathrm{GL}_n(L)$. G acts on A, X by applying an automorphism $\sigma \in G$ to each entry of a matrix $a \in A$ or $x \in X$. A acts on X by conjugation,

$$A \times X \to X \qquad (b, x) \mapsto bxb^{-1}$$

These actions are compatible, since for $\sigma \in G$,

$$\sigma \cdot (b \cdot x) = \sigma \cdot (bxb^{-1}) = (\sigma \cdot b)(\sigma \cdot x)(\sigma \cdot b^{-1}) = (\sigma \cdot b) \cdot (\sigma \cdot x)$$

Consider the unit cocycle $1 : G \to A, \sigma \mapsto 1$. Twisting by this cocycle gives the same G-action on X.

$$G \times {}_1X \to {}_1X \qquad (\sigma, x) \mapsto \sigma * x = 1 \cdot (\sigma \cdot x) = \sigma \cdot x$$

That is, ${}_1X$ has the same G-action as X. On the other hand, choose a 1-cocycle $a : G \to A$ such that for some $\tau \in G$, a_τ is not central in A, that is, a_τ is not a scalar matrix. We omit the justification, but such a cocycle exists. Then consider the G-twisted action on ${}_aX$.

$$G \times {}_aX \to {}_aX \qquad (\sigma, x) \mapsto \sigma * x = a_\sigma \cdot (\sigma \cdot x)$$

We claim this is not the same as the original G-action on X. Since a_τ is not central in $\mathrm{GL}_n(L)$, choose $x \in X = \mathrm{GL}_n(L)$ so that $\tau \cdot x$ does not commute with a_τ. Then

$$\tau * x = a_\tau \cdot (\tau \cdot x) = a_\tau(\tau \cdot x)a_\tau^{-1} \neq \tau \cdot x$$

Hence the action is not the same. Finally, we do not spend the time or space to justify it here, but it is known that $H^1(G, A)$ is trivial; in particular, a is cohomologous to the unit cocycle. Hence we have two cocycles which represent the same cohomology class, but induce distinct twisted actions.

Lemma 1.40. *Let X be a (G, A)-set, and let $a \in Z^1(G, A)$ be a cocycle. Let G act on ${}_aX$ via the twisted action, and let A act on ${}_aX$ in the same way as A acting on X. If A is abelian, then this makes ${}_aX$ into a (G, A)-set, which is to say, the twisted action and the A-action on X are compatible.*

Proof. Since there are are approximately one million [1] actions floating around, let's set a bunch of notation to try to be as clear as possible. We denote the various actions as follows.

$$\begin{array}{rl} G \times X \to X & (\sigma, x) \mapsto \sigma \cdot x \\ A \times X \to X & (b, x) \mapsto b \odot x \\ G \times A \to A & (\sigma, b) \mapsto \sigma \diamond b \\ G \times {}_aX \to {}_aX & (\sigma, x) \mapsto \sigma * x = a_\sigma \odot (\sigma \cdot x) \\ A \times {}_aX \to {}_aX & (b, x) \mapsto b \odot x \\ A \times A \to A & (b, c) \mapsto b + c \end{array}$$

Using this notation, the fact that the G, A-actions on X are compatible is written

$$\sigma \cdot (b \odot x) = (\sigma \diamond b) \odot (\sigma \cdot x)$$

The fact that A acts on X as a group says that

$$b \odot (c \odot x) = (b + c) \odot x$$

We wish to show that the G, A-actions on ${}_aX$ are compatible, which amounts to showing the equality

$$\sigma * (b \odot x) = (\sigma \diamond b) \odot (\sigma * x)$$

We work with each side.

$$\begin{aligned} LHS &= \sigma * (b \odot x) \\ &= a_\sigma \odot \Big(\sigma \cdot (b \odot x)\Big) \\ &= a_\sigma \odot \Big((\sigma \diamond b) \odot (\sigma \cdot x)\Big) \\ &= \Big(a_\sigma + (\sigma \diamond b)\Big) \odot (\sigma \cdot x) \\ RHS &= (\sigma \diamond b) \odot (\sigma * x) \\ &= (\sigma \diamond b) \odot \Big(a_\sigma \odot (\sigma \cdot x)\Big) \\ &= \Big((\sigma \diamond b) + a_\sigma\Big) \odot (\sigma \cdot x) \end{aligned}$$

So if A is abelian, then $a_\sigma + (\sigma \diamond b) = (\sigma \diamond b) + a_\sigma$, in which case these expressions are equal, so the actions are compatible as claimed. □

Remark 1.41. I suspect that the previous proof could be wrangled a bit to show that A is abelian if and only if the actions considered are compatible, but it isn't necessary to prove this for later so I haven't tried. Suffice it to say, if A is not abelian, we should not expect the actions to be compatible.

[1] Five is approximately one million in situations like this.

1.6 Some cohomology facts without proof

Proposition 1.42. *Let G be a finite cyclic group of order n with generator σ. Let A be a G-module (A is abelian). Let*

$$N_G = \sum_{\tau \in G} \tau$$

be the norm element in $\mathbb{Z}[G]$, which gives a map $N_G : A \to A$. The group cohomology groups $H^i(G, A)$ are

$$H^i(G,A) = \begin{cases} A^G & i = 0 \\ \ker N_G/(\sigma - 1)A & i = 1, 3, \ldots \\ A^G/N_G A & i = 2, 4, \ldots \end{cases}$$

2 Descent for vector spaces

2.1 Semilinear Γ-modules

Definition 2.1. Let K/k be a Galois extension with Galois group $G = \mathrm{Gal}(K/k)$, and let M be a K-vector space. Suppose we have a k-linear action of G on M.

$$G \times M \to M \qquad (\sigma, m) \mapsto \sigma(m)$$

By k-linear, we mean that if $\mu \in k$, then $\sigma(\mu m) = \mu\sigma(m)$. Such an action is **semilinear** if it satisfies

$$\sigma(\lambda m) = (\sigma\lambda)(\sigma m)$$

for all $\sigma \in G, \lambda \in K, m \in M$.

Definition 2.2. Let K/k be a Galois extension with Galois group G. A **semilinear G-modules** is a K-vector space M with semilinear G-action as defined above. A semilinear G-module M is **continuous** if for every $m \in M$, the stabilizer subgroup

$$\mathrm{stab}(m) = \{\sigma \in G : \sigma m = m\}$$

is open with respect to the Krull topology on G. Suppose M, N are continuous semilinear G-modules. A **morphism of G-modules** is a K-linear map $M \to N$ which is also a G-module homomorphism, that is, the map commutes with any $\sigma \in G$.

Definition 2.3. Let K/k be a Galois extension with Galois group $G = \mathrm{Gal}(K/k)$ and let V be a k-vector space. Then

$$G \times V_K \to V_K \qquad \sigma(v \otimes \lambda) = v \otimes \sigma\lambda$$

where $\sigma \in G, v \in V, \lambda \in K$ is a semilinear action. It is also continuous, assuming the Krull topology on G and the discrete topology on V_K. Given a morphism $\phi : V \to W$ of k-vector spaces, the induced map

$$\phi_K : V_K \to W_K$$

is a morphism of G-modules, since

$$\phi_K(\sigma(v \otimes \lambda)) = \phi_K(v \otimes \sigma\lambda) = \phi(v) \otimes \sigma\lambda = \sigma(\phi(v) \otimes \lambda)$$

All this to say, the assignment $V \rightsquigarrow V_K$ is a covariant functor from the category Vec_k of k-vector spaces to the category Mod_G of continuous semilinear G-modules.

Conversely, if we start with a continuous semilinear G-module M, we can take the G-fixed points M^G.

$$M^G = \{m \in M : \sigma m = m, \forall \sigma \in G\}$$

We then regard M^G as a k-vector space. It is clear that M^G is closed under addition; it is also closed under the k-action since if $m \in M^G$ and $\lambda \in k$ and $\sigma \in G$, then

$$\sigma(\lambda m) = \sigma(\lambda)\sigma(m) = \lambda\sigma(m) = \lambda m$$

where $\sigma(\lambda) = \lambda$ because λ is the fixed field of $\mathrm{Gal}(K/k) = G$. Given a morphism $f : M \to N$ of continuous semilinear G-modules, the image of M^G lands in N^G, so we have a map

$$f^G = f|_{M^G} : M^G \to N^G$$

which is k-linear. Hence $M \rightsquigarrow M^G$ is a covariant functor $\mathrm{Mod}_G \to \mathrm{Vec}_k$.

Lemma 2.4. *Let K/k be a Galois extension with Galois group G and V be a k-vector space. Then every element of $(V_K)^G$ is of the form $v \otimes 1$ for some $v \in V$. That is, we get an identification*

$$(V_K)^G \cong V$$

Proof. Choose a k-basis $\{e_i\}_{i\in I}$ for V. Then $\{e_i \otimes 1\}_{i\in I}$ is a K-basis for V_K. Let $x \in V_K$, and write it in terms of this basis.

$$x = \sum_{i\in I} x_i(e_i \otimes 1) = \sum_i e_i \otimes x_i$$

where $x_i \in K$ are uniquely determined by x. Suppose $x \in (V_K)^G$. Then for $\sigma \in G$,

$$\sum_i x_i(e_i \otimes 1) = x = \sigma x = \sum_i e_i \otimes \sigma x_i = \sum_i (\sigma x_i)(e_i \otimes 1)$$

Since $\{e_i \otimes 1\}_{i\in I}$ is a K-basis, the coefficients are equal, which is to say, $\sigma x_i = x_i$ for all $\sigma \in G$. That is, $x_i \in k$ for all i. So

$$x = \sum_i e_i \otimes x_i = \sum_i (x_i e_i) \otimes 1 = \left(\sum_i x_i e_i\right) \otimes 1$$

Thus $x \in (V_K)^G$ is of the required form. □

Later on we'll need a slight generalization of this lemma where we replace V_K by a q-fold tensor product $(V_K)^{\otimes q}$. The proof is basically the same.

Definition 2.5. Let V be a k-vector space and K/k a Galois extension with Galois group G. We can extend the G-action on V_K to a G-action on $(V_K)^{\otimes q}$ where $q \in \mathbb{Z}_{\geq 1}$.

$$G \times (V_K)^{\otimes q} \to (V_K)^{\otimes q} \qquad \sigma(x_1 \otimes \cdots \otimes x_q) = (\sigma x_1) \otimes \cdots \otimes (\sigma x_q)$$

Lemma 2.6. *Let K/k be a Galois extension with Galois group G and V be a k-vector space. Let $q \in \mathbb{Z}_{\geq 0}$. Then every element of $((V_K)^{\otimes q})^G$ is a k-linear combination of elements*

$$(v_1 \otimes 1) \otimes \cdots \otimes (v_q \otimes 1)$$

for some $v_1, \ldots, v_q \in V^{\otimes q}$. That is, we get an identification

$$((V_K)^{\otimes q})^G \cong (V_K)^{\otimes q}$$

Proof. Choose a k-basis $\{e_i\}_{i\in I}$ for V. Then $\{f_i = e_i \otimes 1\}_{i\in I}$ is a K-basis for V_K. Then

$$\left\{f_{i_1} \otimes \cdots \otimes f_{i_q} : i_1, \ldots, i_q \in I\right\}$$

is a K-basis for $(V_K)^{\otimes q}$. Let $x \in (V_K)^{\otimes q}$, and write it in terms of this basis.

$$x = \sum_{(i_1,\ldots,i_q)\in I^q} x_{(i_1,\ldots,i_q)}(f_{i_1} \otimes \cdots \otimes f_{i_q})$$

where $x_i \in K$ are uniquely determined by x. Suppose $x \in ((V_K)^{\otimes q})^G$. Then for $\sigma \in G$,

$$\sum_{(i_1,\ldots,i_q)\in I^q} x_{(i_1,\ldots,i_q)}(f_{i_1} \otimes \cdots \otimes f_{i_q}) = x = \sigma x = \sum_{(i_1,\ldots,i_q)\in I^q} (\sigma x_{(i_1,\ldots,i_q)})(f_{i_1} \otimes \cdots \otimes f_{i_q})$$

Since these are coefficients when written in terms of a basis, they are equal. That is, $\sigma x_{(i_1,\ldots,i_q)} = x_{(i_1,\ldots,i_q)}$ for all multi-indices $(i_1, \ldots, i_q)$, which is to say, the coefficients are all in k. $\square$

Lemma 2.7 (Conrad 1.6)**.** *Let K/k be a field extension. Let V be a K-vector space, and $W \subset V$ be a nonzero k-vector subspace of V. The following are equivalent.*

1. *Any k-basis of W is a K-basis of V.*
2. *Some k-basis of W is a K-basis of V.*
3. *The K-linear map*
$$W \otimes_k K \to V \qquad w \otimes a \mapsto aw$$
is an isomorphism of K-vector spaces.

Proof. (1) $\implies$ (2) obvious.

(2) $\implies$ (3) Suppose $\{e_i\}$ is a k-basis of W which is also an K-basis of V. Then the K-linear map

$$W \otimes_k K \to V \qquad w \otimes a \mapsto aw$$

sends $1 \otimes e_i$ to e_i. That is, it sends the K-basis $\{1 \otimes e_i\}$ of $W \otimes_k K$ to the K-basis $\{e_i\}$ of V, so it is an isomorphism.

(3) $\implies$ (1) Suppose the map is an isomorphism. Given a k-basis $\{e_i\}$ of W, $\{1 \otimes e_i\}$ is a K-basis of $W \otimes_k K$, so under the isomorphism the image $\{1e_i\}$ of $\{1 \otimes e_i\}$ is a K-basis of V. $\square$

Lemma 2.8 (Conrad 2.11)**.** *Let K/k be a Galois extension with Galois group G. Let V be a K-vector space with a semilinear G-action, and let $V' \subset V$ be a K-subspace which is preserved (setwise) by G. Then the quotient space V/V' has a semilinear G-action given by*

$$G \times V/V' \to V/V' \qquad \sigma(v + V') = \sigma(v) + V'$$

Proof. This is mostly just checking well-defined-ness. $\square$

Lemma 2.9 (Conrad 2.13)**.** *Let K/k be a finite Galois extension with Galois group G. Let V be a K-vector space with a semilinear G-action. Define*

$$\mathrm{Tr} : V \to V \qquad \mathrm{Tr}(v) = \sum_{\sigma \in G} \sigma v$$

Then

1. $\mathrm{Tr}(V) \subset V^G$.
2. *If $v \in V$ and $v \neq 0$, then there exists $a \in K$ such that $\mathrm{Tr}(av) \neq 0$.*
3. *If $V \neq 0$, then $V^G \neq 0$.*

Proof. (1) Let $\tau \in G$. Then

$$\tau \,\mathrm{Tr}(v) = \tau \sum_{\sigma \in G} \sigma v = \sum_{\sigma \in G} \tau\sigma v = \mathrm{Tr}(v)$$

The last equality is because left multiplication by τ is an automorphism of G.

(2) We prove the contrapositive. Assume for some fixed $v \in V$, $\mathrm{Tr}(av) = 0$ for all $a \in K$. Then

$$0 = \sum_{\sigma \in G} \sigma(av) = \sum_{\sigma \in G} \sigma(a)\sigma(v)$$

for all $a \in K$. By linear independence of characters, the characters $\sigma(a)$ of V are linearly independent, so the equality above implies that each $\sigma(v) = 0$. In particular, for $\sigma = \mathrm{Id}_K$, we get $v = 0$.

(3) If $V \neq 0$, choose $v \neq 0$. Then by (2), $\mathrm{Tr}(av) \neq 0$ for some v, and $\mathrm{Tr}(av) \in V^G$. □

Lemma 2.10 (part of Conrad 2.14)**.** *Let K/k be a Galois extension with Galois group G. Let V be a K-vector space with a semilinear G-action. If $\{w_i\}$ is a collection of k-linearly independent vectors in V^G, then they are K-linearly independent in V.*

Proof. Suppose the result is false, which is to say, there exists a set $\{w_i\}$ of k-linearly independent vectors in V^G which are K-linearly dependent. That is, we have a relation

$$\sum_{i=1}^{n} a_i w_i = 0$$

with $a_i \in K$, and the a_i's are not all zero. We may assume the relation above is minimal in length among such all such relations. Then every a_i is nonzero, every w_i is nonzero, so $n \geq 2$. By scaling, we may assume $a_n = 1$. Now let $\sigma \in G$, and apply it to the relation.

$$0 = \sigma(0) = \sigma \sum_{i=1}^{n} a_i w_i = \sum_{i=1}^{n} \sigma(a_i)\sigma(w_i) = \sum_{i=1}^{n} \sigma(a_i) w_i$$

Subtracting these relations, we get

$$0 = \sum_{i=1}^{n} (a_i - \sigma(a_i)) w_i$$

Since $a_n = \sigma(a_n) = 1$, this is a relation of length at most $n-1$. Since the original relation was minimal in length among nontrivial relations, this new relation must be a trivial one, which is to say, $a_i - \sigma(a_i) = 0$ for all i. Since this happened for every $\sigma \in G$, this tells us that $a_i \in K^\Gamma = k$. But this contradicts the initial assumption that $\{w_i\}$ was k-linearly independent. So we reach a contradiction, and the original claim is true. □

Note: Finiteness of the extension is pretty necessary for the following lemma, at least for the proof given. It doesn't seem likely that this extends to infinite extensions, as stated.

Lemma 2.11 (Speiser's lemma, CSAGC 2.3.8)**.** *Let K/k be a finite Galois extension with Galois group $G = \mathrm{Gal}(K/k)$, and let M be a semilinear G-module. The map*

$$\epsilon_M : (M^G)_K \to M \qquad m \otimes \lambda \mapsto \lambda m \qquad \sum_i m_i \otimes \lambda_i \mapsto \sum_i \lambda_i m_i$$

is a natural isomorphism of Γ-modules. Here, naturality means that if $\psi : M \to N$ is a morphism of semilinear Γ-modules, then the following diagram commutes.

$$\begin{tikzcd} (M^G)_K \arrow[r, "\epsilon_M"] \arrow[d, "(\psi|_{M^G})\otimes \mathrm{Id}_K"'] & M \arrow[d, "\psi"] \\ (N^G)_K \arrow[r, "\epsilon_N"] & N \end{tikzcd}$$

Proof. Let us verify that ϵ_M is a G-module homomorphism. For $\sigma \in G$,

$$\epsilon_M\left(\sigma \sum_i m_i \otimes \lambda_i\right) = \epsilon_M\left(\sum_i m_i \otimes \sigma(\lambda_i)\right) = \sum_i \sigma(\lambda_i) m_i \tag{2.1}$$

$$= \sum_i \sigma(\lambda_i m_i) = \sigma \sum_i \lambda_i m_i = \sigma \epsilon_M\left(\sum_i m_i \otimes \lambda_i\right) \tag{2.2}$$

Hence ϵ_M commutes with any $\sigma \in G$, so it is a G-module homomorphism. Now we verify that the required diagram commutes. Let $\psi : M \to N$ be a G-module homomorphism. In particular, ψ is K-linear.

$$\epsilon_N \circ (\psi|_{M^G} \otimes \mathrm{Id}_K)\left(\sum_i m_i \otimes \lambda_i\right) = \epsilon_N\left(\sum_i \psi(m_i) \otimes \lambda_i\right)$$

$$= \sum_i \lambda_i \psi(m_i) = \sum_i \psi(\lambda_i m_i) = \psi\left(\sum_i \lambda_i m_i\right) = \psi \circ \epsilon_M\left(\sum_i m_i \otimes \lambda_i\right)$$

Hence the required diagram commutes, so ϵ is a natural transformation. It remains to show that ϵ_M is an isomorphism. Lemma 2.10 says that ϵ_M is injective, so all we need is surjectivity. Consider the image $\mathrm{im}\, \epsilon_M \subset V$, which is an L-subspace. By the algebra in equation 2.1, the image is (setwise) invariant under G. Then by lemma 2.8, the quotient space

$$\overline{M} = M / \mathrm{im}\, \epsilon_M$$

inherits a semilinear G-action from M, which we write as $\sigma(\overline{m}) = \overline{\sigma(m)}$. Let $\mathrm{Tr} : M \to M$ be the trace map defined in lemma 2.9[2]. We also have the trace map $\mathrm{Tr} : \overline{M} \to \overline{M}$. For $\overline{m} \in \overline{M}$, we have

$$\mathrm{Tr}(\overline{m}) = \sum_{\sigma \in G} \sigma(\overline{m}) = \sum_{\sigma \in G} \overline{\sigma(m)} = \overline{\mathrm{Tr}(m)}$$

By lemma 2.9, for any $m \in M$, $\mathrm{Tr}(m) \in M^G$, and it is clear that $M^G \subset \operatorname{im} \epsilon_M$, so

$$\mathrm{Tr}(\overline{m}) = \overline{\mathrm{Tr}(m)} = \overline{0} \in \overline{M}$$

That is to say, $\mathrm{Tr} : \overline{M} \to \overline{M}$ is the zero map, which by part (2) of lemma 2.9 tells us that $\overline{M} = 0$. That is, $M = \operatorname{im} \epsilon_M$, which is to say, ϵ_M is surjective. □

Remark 2.12. Unfortunately, the previous proof does not explicitly describe the inverse map to ϵ_M. However, now that we know the result is true, we can say the following.

For any k-basis $\{m_i\}$ of M^G, $\{m_i \otimes 1\}$ is a K-basis of $(M^G)_K$. Then the isomorphism ϵ_M takes the K-basis $\{m_i \otimes 1\}$ to the set $\{m_i\}$ in M, so it must also be a K-basis of M. This is just a rephrasing of lemma 2.7.

Hence the inverse map to ϵ_M may be described as folllows. Pick a K-basis of M which is also a k-basis of M^G, call it $\{m_i\}$. Then the inverse map is

$$\epsilon_M^{-1} : M \to (M^G)_K \qquad \sum_i \lambda_i m_i \mapsto \sum_i m_i \otimes \lambda_i$$

2.2 Equivalence of categories $\mathrm{Vec}_k \cong \mathrm{Mod}_G$

This proof attempts to establish the equivalence by directly describing natural isomorphisms of functors. It is incomplete. The natural transformations are constructed, the problem that remains is to show that they are isomorphisms on objects.

Note that the assumption of finiteness for the Galois extension is only used in one step - the surjectivity of ϵ_M. The result actually does extend to the infinite case, which we'll hopefully describe later.

Proposition 2.13 (Conrad 2.14, or Milne A.64, or Milne 3.36)**.** *Let K/k be a finite Galois extension with Galois group G. Let Vec_k be the category of k-vector spaces, and let Mod_G be the category of continuous semilinear G-modules. The covariant functors*

$$\begin{aligned} F &: \mathrm{Vec}_k \to \mathrm{Mod}_G & \qquad V &\mapsto V_K \\ H &: \mathrm{Mod}_G \to \mathrm{Vec}_k & \qquad M &\mapsto M^G \end{aligned}$$

are quasi-inverses, hence give a covariant equivalence of categories.

Proof. We need to construct natural isomorphisms $\epsilon : FH \to \mathrm{Id}_{\mathrm{Mod}_G}$ and $\eta : \mathrm{Id}_{\mathrm{Vec}_k} \to HF$. We start with η. We need, for every $V \in \mathrm{ob}(\mathrm{Vec}_k)$, an isomorphism (in Vec_k)

$$\eta_V : V \to HF(V) = H(V_K) = (V_K)^\Gamma$$

such that for any k-linear map $\phi : V \to W$, the following diagram commutes.

[2] Here is where we are using the fact that K/k is finite.

$$\begin{array}{ccc}
V & \xrightarrow{\eta_V} & HF(V) \\
\Big\downarrow{\scriptstyle \phi} & & \Big\downarrow{\scriptstyle HF(\phi)} \\
W & \xrightarrow{\eta_W} & HF(W)
\end{array}$$

We define η_V by

$$\eta_V : V \to (V_K)^G \qquad \eta(v) = v \otimes 1$$

This has image in $(V_K)^G$, since if $\sigma \in G$,

$$\sigma(v \otimes 1) = v \otimes \sigma(1) = v \otimes 1$$

It is also clearly k-linear. Now we verify that the required square commutes. Let $v \in V$. Then

$$\eta_W(\phi(v)) = \phi(v) \otimes 1 = \phi_K(v \otimes 1) = H(\phi_K)(v \otimes 1) = HF(\phi)(v \otimes 1) = HF(\phi) \circ \eta_V(v)$$

so the square commutes, and η is a natural transformation. It remains to show that η_V is an isomorphism. It is clear that η_V has trivial kernel, so it is injective. By Lemma 2.4, η_V is surjective. So it is an isomorphism.

The natural isomorphism ϵ is defined and all necessary properties established in lemma 2.11. □

Remark 2.14. Let's connect this with our original goals. In this setting, our k-objects are just k-vector spaces, and the associated K-objects are semilinear $G = \mathrm{Gal}(K/k)$-modules.

1. Every K-object comes from a k-object, since $V \rightsquigarrow V_K$ is essentially surjective.
2. V, W are K-forms of each other $\iff V_K \cong W_K \iff V \cong W$.
3. (2) above says that the only K-form of V is V itself (up to isomorphism).
4. Since K-forms of V have no structure (the set is just a point) it's not clear how it's related to the Galois group directly. Despite this, the Galois group was critically important in understanding this correspondence, since the quasi-inverse to $V \rightsquigarrow V_K$ was $M \rightsquigarrow M^G$.

2.3 Alternate approach (Milne)

The next proof follows Milne's proof in Appendix A, A.64. He also only gives a proof for the case where K/k is finite Galois, and only really addresses that the functor is essentially surjective.

Definition 2.15. Let A, B be associative, unital rings (not necessarily commutative). Let S be an A-B-bimodule, which means A acts on S on the left, and B acts on S on the right, and the actions commute. Given a left B-module M, the tensor product

$$S \otimes_B M$$

is a left A-module via

$$A \times (S \otimes_B M) \to S \otimes_B M \qquad a(s \otimes m) = as \otimes m$$

So the assignement

$$\mathrm{LMod}(B) \to \mathrm{LMod}(A) \qquad M \rightsquigarrow S \otimes_B M$$

gives a covariant functor from the category of left B-modules to the category of left A-modules. If this functor is an equivalence of categories, we say that A and B are **Morita equivalent through** S.

Example 2.16. Let k be a field and let D be a finite dimensional division algebra over k. Let $A = M_n(D)$ be the matrix algebra over D. Let $S = D^n$, thought of as column vectors, and let $B = D$. A acts on S on the left by matrix multiplication, and $B = D$ acts on S on the right by right multiplication, and these two actions commute, so S is an A-B-bimodule.

From the theory of simple algebras we know that S is a simple A-module, and every (left) A-module is a direct sum of copies of S (up to isomorphism). Since D is a division algebra, every (left) D-module is direct sum of copies of D, so the functor

$$\mathrm{LMod}(D) \to \mathrm{LMod}(A) \qquad M \cong D^m \rightsquigarrow D^n \otimes_D D^m \cong D^{mn}$$

is essentially surjective. It is not too hard to see that it is fully faithful, so it is an equivalence of categories, which is to say, A and D are Morita equivalent through $S = D^n$.

Theorem 2.17 (A.64)**.** *Let K/k be a finite Galois extension with Galois group G. The functor $V \rightsquigarrow V_K$ gives a covariant equivalence of categories between k-vector spaces and continuous semilinear G-modules.*

Proof. We start by assuming K/k is a finite extension, and let $n = [K : k] = \dim_k K$. In this case, the proof is mostly just a special case of example 2.16 where $k = D$, and $S = K \cong k^n$. Let $A = M_n(k) \cong \mathrm{End}_k(K)$. By the example,

$$\mathrm{LMod}(k) \to \mathrm{LMod}(A) \qquad V \rightsquigarrow V_K = V \otimes_k K$$

is an equivalence of categories from the category of k-vector spaces to the category of left $\mathrm{End}_k(K)$-modules. Now let $K[G]$ be the K-algebra with K-basis given by elements of G, and multiplication given by

$$\left(\sum_{\sigma\in G} a_\sigma \sigma\right)\left(\sum_{\tau\in G} b_\tau \tau\right) = \sum_{\sigma,\tau\in G} a_\sigma \sigma(b_\tau)(\sigma\tau)$$

where $a_\sigma, b_\tau \in K$. The algebra $K[G]$ acts k-linearly on K by

$$K[G] \times K \to K \qquad \left(\sum_{\sigma\in G} a_\sigma \sigma\right) c = \sum_{\sigma\in G} a_\sigma \sigma(c)$$

By linear independence of characters, the homomorphism (of k-vector spaces)

$$K[G] \to \mathrm{End}_k(K) \cong M_{\dim_k K}(k)$$

is injective. Their dimensions over k are

$$\dim_k K[G] = (\dim_k K)|G| = [K : k]^2 = \dim_k M_{\dim_k K}(k) = \dim_k \mathrm{End}_k(K)$$

Since the dimensions are equal and finite and the map is injective, it is an isomorphism. Since $K[G] \cong \mathrm{End}_k(K)$, their respective categories of modules are equivalent. But obviously, the category of left $K[G]$-modules is precisely the category of continuous semilinear G-modules. This completes the proof. $\square$

2.4 Extending the result to K/k infinite

Corollary 2.18. *Theorem 2.13 holds when K/k is an infinite extension as well, provided that* Vec_k *only includes finite dimensional k-vector spaces and* Mod_G *only includes modules which are finite dimensional K-vector spaces.*

Proof. Let K/k be an infinite extension with Galois group $G = \mathrm{Gal}(K/k)$, and let M be a continuous semilinear G-module, which is finite-dimensional as a K-vector space. Let $n = \dim_K M$. Let $\{m_1, \ldots, m_n\}$ be a K-basis of M. For each i, define

$$G_i = \mathrm{stab}(m_i) = \{\sigma \in G : \sigma v_i = v_i\} \subset G$$

Since M is a continuous G-module, $G_i \subset G$ is an open subgroup (hence has finite index). Then define

$$H = \bigcap_{i=1}^{n} G_i$$

which is also an open, finite index subgroup of G. By construction, H acts trivially on M. Hence by the Galois correspondence, $H = \mathrm{Gal}(L/k)$ for some finite extension L/k. Then define

$$\widetilde{H} = \bigcap_{\sigma \in G} \sigma H \sigma^{-1}$$

which is also an open, finite index subgroup of G, which has fixed field $\widetilde{L}$, where $\widetilde{L}$ is the Galois closure of L. Since it is contained in H, $\widetilde{H}$ also acts trivially on H. The diagram below depicts the situation of the corresponding subgroups and fixed fields under the Galois correspondence.

$$\begin{tikzcd}
e = \mathrm{Gal}(k/k) \arrow[r, leftrightsquigarrow] \arrow[d, hook] & K = K^{\{e\}} \arrow[d, dash] \\
\widetilde{H} = \mathrm{Gal}(K/\widetilde{L}) \arrow[r, leftrightsquigarrow] \arrow[d, hook] & \widetilde{L} = K^{\widetilde{H}} \arrow[d, dash, "\text{finite, Galois over } k"] \\
H = \mathrm{Gal}(K/L) \arrow[r, leftrightsquigarrow] \arrow[d, hook, "\text{finite index}"'] & L = K^{H} \arrow[d, dash, "\text{finite, not necesarily Galois}"] \\
G = \mathrm{Gal}(K/k) \arrow[r, leftrightsquigarrow] & k = K^{\Gamma}
\end{tikzcd}$$

We can record roughly the same data in the following short exact sequence

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(K/\widetilde{L}) \arrow[r, hook] \arrow[d, equal] & \mathrm{Gal}(K/k) \arrow[r, two heads, "\mathrm{res}"] \arrow[d, equal] & \mathrm{Gal}(\widetilde{L}/k) \arrow[r] \arrow[d, equal] & 1 \\
& \widetilde{H} & G & G/\widetilde{H} &
\end{tikzcd}$$

As noted previously, $\widetilde{H}$ acts trivially on M, so the G-action factors through the quotient $G/\widetilde{H} = \mathrm{Gal}(\widetilde{L}/k)$. This puts us back in the situation of a finite Galois extension $\widetilde{L}/k$, where we have the equivalence of categories from the previous result.

That is to say, we know that M is isomorphic (as a continuous semilinear $\widetilde{H}$-module) to $V_{\widetilde{L}}$ for some k-vector space V, but then tensoring up to K gives an isomorphism $M \cong V_K$ as (continuous, semilinear) G-modules.

We are being a bit sloppy here and not writing down the natural isomorphisms, but this does at least show that $V \rightsquigarrow V_K$ is essentially surjective, which is interesting part of the extension to the infinite case. That this functor is faithful is relatively obvious, that it is full is less so but we omit it. $\square$

3 Descent for tensors of type (p, q)

3.1 Tensors

Fix a base field k.

Definition 3.1. Let V be a k-vector space. Fix $p, q \in \mathbb{Z}_{\geq 0}$. A **tensor of type (p, q)** on V is an element $\Phi \in \mathrm{Hom}_k(V^{\otimes q}, V^{\otimes p})$.

Example 3.2. If $q = 2$ and $p = 0$, then a tensor is just a k-linear map

$$\Phi : V \otimes V \to k = V^{\otimes 0}$$

which is to say, Φ is a bilinear form on V.

Example 3.3. If $q = 2$ and $p = 1$, then a tensor is just a k-linear map

$$\Phi : V \otimes V \to V$$

which is to say, Φ gives V the structure of a k-algebra (not necessarily unital or associative).

Remark 3.4 (CSAGC 2.3.1)**.** The setting of tensors is very broad and general, since it includes:

1. $\Phi = 0$ and (p, q) are arbitrary, which is the case where V is just a k-vector space without additional structure.

2. $(p, q) = (1, 1)$ which is the case where Φ is a k-linear endomorphism of V.

3. $(p, q) = (0, 2)$ which is where $\Phi : V \otimes_k V \to k$ is a bilinear form on V.

4. $(p, q) = (1, 2)$ which is where $\Phi : V \otimes_k V \to V$, which is to say, Φ can be thought of as a multiplication map for a k-algebra structure on V. This multiplication need not even be associative or unital, so this case contains the entire theory of k-algebras.

There is another way to think of tensors, which other people (e.g. CSAGC) seem to prefer, but seems excessively confusing to me. It starts with the following lemma.

Lemma 3.5 (CSAGC pg27)**.** *Let V, W be k-vector spaces. Then the map below is an isomorphism.*

$$V^* \otimes_k W \xrightarrow{\cong} \mathrm{Hom}_k(V, W) \qquad \alpha \otimes w \mapsto (v \mapsto \alpha(v)w)$$

where $V^* = \mathrm{Hom}_k(V, k)$ denotes the dual space.

Remark 3.6 (CSAGC pg27)**.** Let V be a k-vector space and $p, q \in \mathbb{Z}_{\geq 0}$. Using the previous lemma with $W = V^{\otimes p}$ and $V = V^{\otimes q}$, we get an isomorphism

$$V^{\otimes p} \otimes_k (V^*)^{\otimes q} \cong \mathrm{Hom}_k(V^{\otimes q}, V^{\otimes p})$$

Using this isomorphism along with the isomorphism

$$(V^*)^{\otimes q} \cong (V^{\otimes q})^*$$

we may think of a tensor of type (p, q) as an element $\Phi \in V^{\otimes p} \otimes_k (V^*)^{\otimes q}$.

3.2 k-objects and k-morphisms

Definition 3.7. Fix $p, q \in \mathbb{Z}_{\geq 0}$ and a field k. A ***k*-object** is a pair (V, Φ) where V is a k-vector space and $\Phi \in \mathrm{Hom}(V^{\otimes q}, V^{\otimes p})$ is a tensor of type (p, q) on V.

From now own, when we speak about k-objects, there are fixed integers $p, q \in \mathbb{Z}_{\geq 0}$ lying in the background.

Definition 3.8. Fix (p, q) and let (V, Φ) and (W, Ψ) be k-objects. A **morphism of *k*-objects** or ***k*-morphism** is a k-linear map $f : V \to W$ such that the following diagram commutes.

$$\begin{array}{ccc} V^{\otimes q} & \xrightarrow{f^{\otimes q}} & W^{\otimes q} \\ \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Psi} \\ V^{\otimes p} & \xrightarrow{f^{\otimes p}} & W^{\otimes p} \end{array}$$

As one would expect, k-objects with their morphisms form a category. We denote this category $\mathcal{C}_k^{(p,q)}$ or just $\mathcal{C}_k$ if (p, q) are understood from context.

Definition 3.9. If there is an isomorphism of k-objects $(V, \Phi) \cong (W, \Psi)$, we say they are ***k*-isomorphic** and call such an isomorphism a ***k*-isomorphism**.

Remark 3.10 (CSAGC pg28)**.** In terms of thinking of tensors as elements of $V^{\otimes p} \otimes_k (V^*)^{\otimes q}$, a morphism is a k-linear map $f : V \to W$ such that the induced map

$$f^{\otimes p} \otimes \left((f^*)^{-1}\right)^{\otimes q} : V^{\otimes p} \otimes_k (V^*)^{\otimes q} \to W^{\otimes p} \otimes_k (W^*)^{\otimes q}$$

takes Φ to Ψ.

3.3 Extension of scalars

Fix (p, q). All k-objects will be those with a tensor of type (p, q).

Definition 3.11. Let (V, Φ) be a k-object and let K/k be a field extension. We want to define an associated K-object (V_K, Φ_K). For the vector space, we just tensor with K.

$$V_K = V \otimes_k K$$

For the tensor, we just tensor with the identity function. That is, given

$$\Phi : V^{\otimes q} \to V^{\otimes p}$$

we form the tensor

$$\Phi_K : (V_K)^{\otimes q} \to (V_K)^{\otimes p}$$

We try to describe this as concretely as possible. Given a simple tensor

$$x_1 \otimes \cdots \otimes x_q = (v_1 \otimes \lambda_1) \otimes \cdots \otimes (v_q \otimes \lambda_q) \in (V_K)^{\otimes q}$$

where $x_i \in V_K, v_i \in V, \lambda_i \in K$, the tensor Φ_K acts on it by

$$\Phi_K\Big((v_1 \otimes \lambda_1) \otimes \cdots \otimes (v_q \otimes \lambda_q)\Big) = \lambda_1 \cdots \lambda_q \Phi(v_1 \otimes \cdots \otimes v_q)$$

This doesn't cover everything, since not every element of $V^{\otimes q}$ is of this form, but every element is a K-linear combination of such elements, so we then extend Φ_K by K-linearity.

Definition 3.12. Let $f : (V, \Phi) \to (W, \Psi)$ be a k-morphism, and let K/k be a field extension. Then we get an associated K-morphism $f_K : (V_K, \Phi_K) \to (W_K, \Psi_K)$, which is just

$$f_K = f \otimes \mathrm{Id}_K : V_K \to W_K \qquad f_K(v \otimes \lambda) = f(v) \otimes \lambda$$

We need to verify that f_K makes the following diagram commute.

$$\begin{tikzcd}
(V_K)^{\otimes q} \arrow[r, "(f_K)^{\otimes q}"] \arrow[d, "\Phi_K"] & (W_K)^{\otimes q} \arrow[d, "\Psi_K"] \\
(V_K)^{\otimes p} \arrow[r, "(f_K)^{\otimes p}"] & (W_K)^{\otimes p}
\end{tikzcd}$$

This is relatively obvious from the definitions, but we include it to be sure. Let $v_1, \ldots, v_q \in V$ and $\lambda_1, \ldots, \lambda_q \in K$. Then

$$\begin{aligned}
(f_K)^{\otimes p} \circ \Phi_K\Big((v_1 \otimes \lambda_1) \otimes \cdots \otimes (v_q \otimes \lambda_q)\Big) &= (f_K)^{\otimes p}\Big(\lambda_1 \cdots \lambda_q \Phi(v_1 \otimes \cdots \otimes v_q\Big) \\
&= \lambda_1 \cdots \lambda_q f^{\otimes p} \circ \Phi(v_1 \otimes \cdots \otimes v_q) \\
&= \lambda_1 \cdots \lambda_q \Psi \circ f^{\otimes q}(v_1 \otimes \cdots \otimes v_q) \\
&= \lambda_1 \cdots \lambda_q \Psi\Big(f(v_1) \otimes \cdots \otimes f(v_q)\Big) \\
&= \Psi_K\Big(\big(f(v_1) \otimes \lambda_1\big) \otimes \cdots \otimes \big(f(v_q) \otimes \lambda_q\big)\Big) \\
&= \Psi_K\Big(f_K(v_1 \otimes \lambda_1) \otimes \cdots \otimes f_K(v_q \otimes \lambda_q)\Big) \\
&= \Psi_K \circ (f_K)^{\otimes q}\Big((v_1 \otimes \lambda_1) \otimes \cdots \otimes (v_q \otimes \lambda_q)\Big)
\end{aligned}$$

As before we note that not every element of $(V_K)^{\otimes q}$ is of this form, but having the same value on such elements forces $(f_K)^{\otimes p} \circ \Phi_K = \Psi_K \circ (f_K)^{\otimes q}$ because of K-linearity.

Remark 3.13. The previous two definition give us a covariant functor

$$\mathcal{C}_k^{(p,q)} \to \mathcal{C}_K^{(p,q)} \qquad (V, \Phi) \mapsto (V_K, \Phi_K), f \mapsto f_K$$

3.4 Twisted forms

Definition 3.14. Let (V, Φ) and (W, Ψ) be k-objects. We say they are ***K*-isomorphic** or **become isomorphic over** K if there is a K-isomorphism $(V_K, \Phi_K) \cong (W_K, \Psi_K)$. In such a situation, we say that (W, Ψ) is a ***K*/*k*-twisted form** of (V, Φ), or just a **twisted form** of (V, Φ).

Fixing a k-object (V, Φ), we may consider all K/k-twisted forms of (V, Φ). A k-isomorphism $(V, \Phi) \cong (W, \Psi)$ induces a K-isomorphism $(V_K, \Phi_K) \cong (W_K, \Psi_K)$, so we want to consider K/k-twisted forms of (V, Φ) which are not already k-isomorphic. That is, we want to consider two such forms the same if they are already k-isomorphic. We denote the set of k-isomorphism classes of K/k-twisted forms of (V, Φ) by

$$\boldsymbol{TF_K(V, \Phi)}$$

This is a pointed set, with distinguished point given by the class of (V, Ψ) itself.

Definition 3.15. Let (V, Φ) be a k-object and K/k an extension. We denote the set of K-automorphisms of (V_K, Φ_K) by $\mathbf{Aut}_{\boldsymbol{K}}\boldsymbol{(\Phi)}$. That is, $\mathrm{Aut}_K(\Phi)$ is the set of K-isomorphisms $(V_K, \Phi_K) \xrightarrow{\cong} (V_K, \Phi_K)$. It forms a group under composition.

Remark 3.16. We are finally in a position to discuss our original motivating questions with the right definitions in hand, and more precisely reformulate them. We fix (p, q) and an extension K/k.

1. Given a K-object (W, Ψ), when is it in the essential image of the functor of extension by scalars, $\mathcal{C}_k \to \mathcal{C}_K, (V, \Phi) \mapsto (V_K, \Phi_K)$? That is, when is there a k-object (V, Φ) such that $(V_K, \Phi_K) \cong (W, \Psi)$? (For answer, see proposition 3.26.)

2. Given k-objects (V, Φ) and (W, Ψ) and a K-morphism $g : (V_K, \Phi_K) \to (W_K, \Psi_K)$, when does this morphism come from a k-morphism? That is, when is there a k-morphism $f : (V, \Phi) \to (W, \Psi)$ such that $f_K = g$? (For answer, see proposition 3.23.)

3. Given two k-objects (V, Φ) and (W, Ψ), when is there a K-isomorphism $(V_K, \Phi_K) \cong (W_K, \Psi_K)$? It may be that there is a K-isomorphism even if they are not k-isomorphic.

4. How can we describe the set of all K/k forms of a k-object (V, Φ)? (For answer, see theorem 3.40.)

5. In the case when K/k is Galois, how are the above questions related to the Galois group $\mathrm{Gal}(K/k)$ and various associated cohomology groups?

Although the questions are well-posed even when K/k is not Galois, we do not attempt any answers except when it is. The fact that these questions have meaningful answers in this scenario is precisely where the name "Galois descent" comes from, especially the first two questions.

We think of extension of scalars $(V, \Phi) \rightsquigarrow (V_K, \Phi_K)$ as "ascending," and the reverse process as "descending." As we have already described, ascent is not very hard - you just tensor everything with K. The hard part is descent, hence the name for the subject. The heart of the theory is deciding, based on interactions with the Galois group $\mathrm{Gal}(K/k)$, when a morphism or object in $\mathcal{C}_K^{(p,q)}$ "descends" to an object in $\mathcal{C}_k^{(p,q)}$.

We will give full and descriptive answers to questions 1,2, and 5. Questions 3 and 5 are less concrete, although they motivate a lot of what happens. In particular, the answer to question 5 is not so much any particular result, but in the fact that in answering questions 1,2,5 all the answers involved the Galois group $\mathrm{Gal}(K/k)$ acting on some set and associated cohomology groups.

Remark 3.17. Let's take a moment to revisit remark 2.14 in light of our more precise phrasings of questions above. That remark, and the previous big result, covered the case where $\Phi = 0$ is the trivial tensor, or alternatively the case where $(p, q) = 0$ and all tensors are trivial, and the extension K/k is Galois (even infinite Galois).

1. The functor of extension by scalars is essentially surjective, so every K-object descends.

2. The functor of extension by scalars is fully faithful, so every K-morphism descends.

3. Two k-objects are k-isomorphic if and only if they are K-isomorphic after extension by scalars.

4. The set of k-isomorphism classes of twisted K/k-forms of (V, Φ) is a set with only one element.

5. The most significant relationship between $\mathrm{Gal}(K/k)$ and the above questions is that it provides the means of a quasi-inverse functor to ascent. That is, the method of descending from a K-object M to the associated k-object is just by taking G-invariants, which is to say, the cohomology group $H^0(G, M)$.

3.5 Galois action on K-morphisms

Definition 3.18. Let V be a k-vector space and K/k a Galois extension. Given $\sigma \in \mathrm{Gal}(K/k)$, there is an induced map

$$1 \otimes \sigma : V_K \to V_K \qquad v \otimes \lambda \mapsto v \otimes \sigma(\lambda)$$

where $v \in V, \lambda \in K$. We sometimes abuse notation and denote this map also by $\sigma : V_K \to V_K$. Note that an arbitrary element of V_K is not of the form $v \otimes \lambda$. However, if we fix a k-basis $\{e_i\}$ of V, then we get a K-basis $\{e_i \otimes 1\}$ of V_K, so every element of V_K can be uniquely written as a K-linear combination

$$y = \sum_i \lambda_i (e_i \otimes 1) = \sum_i e_i \otimes \lambda_i$$

where $\lambda_i \in K$. Then $1 \otimes \sigma$ acts on such an element as

$$(1 \otimes \sigma)(y) = (1 \otimes \sigma) \sum_i e_i \otimes \lambda_i = \sum_i e_i \otimes \sigma\lambda_i$$

Remark 3.19. Let (V, Φ) be a k-object, and K/k a Galois extension. We claim that $1 \otimes \sigma : V_K \to V_K$ is a K-morphism. We just need to verify that the following diagram commutes.

$$\begin{array}{ccc} (V_K)^{\otimes q} & \xrightarrow{(1\otimes\sigma)^{\otimes q}} & (V_K)^{\otimes q} \\ \Big\downarrow{\scriptstyle \Phi_K} & & \Big\downarrow{\scriptstyle \Phi_K} \\ (V_K)^{\otimes p} & \xrightarrow{(1\otimes\sigma)^{\otimes p}} & (V_K)^{\otimes p} \end{array}$$

The following calculations verifies this commutativity.

$$\begin{aligned}
(1 \otimes \sigma)^{\otimes p} \circ \Phi_K\Big((v_1 \otimes \lambda_1) \otimes \cdots \otimes (v_q \otimes \lambda_q)\Big) &= (1 \otimes \sigma)^{\otimes p}\Big(\lambda_1 \cdots \lambda_q \Phi(v_1 \otimes \cdots \otimes v_q\Big) \\
&= \sigma(\lambda_1 \cdots \lambda_q)\Phi(v_1 \otimes \cdots \otimes v_q) \\
&= \sigma(\lambda_1) \cdots \sigma(\lambda_q)\Phi(v_1 \otimes \cdots \otimes v_q) \\
&= \Phi_K\Big(\big(v_1 \otimes \sigma(\lambda_1)\big) \otimes \cdots \otimes \big(v_q \otimes \sigma(\lambda_q)\big)\Big) \\
&= \Phi_K \circ (1 \otimes \sigma)^{\otimes q}\Big((v_1 \otimes \lambda_1) \otimes \cdots \otimes (v_q \otimes \lambda_q)\Big)
\end{aligned}$$

where $v_i \in V, \lambda_i \in K, \sigma \in G$. Remember that elements of this form are not all of $(V_K)^{\otimes q}$, but they generate $(V_K)^{\otimes q}$ in K-linear combinations so this is sufficient.

Definition 3.20. Let K/k be a Galois extension, and let V, W be k-vector spaces. Then we define a group action of G on $\mathrm{Hom}_K(V_K, W_K)$ [3] as follows.

$$\begin{aligned}
G \times \mathrm{Hom}_K(V_K, W_K) &\to \mathrm{Hom}_K(V_K, W_K) \\
(\sigma, f) &\mapsto \sigma(f) = (1 \otimes \sigma) \circ f \circ (1 \otimes \sigma^{-1}) = \sigma \circ f \circ \sigma^{-1}
\end{aligned}$$

For obvious reasons, we call this the **conjugation action** of the Galois group. To spell it out in more detail, $\sigma(f)$ acts on a simple tensor $v \otimes \lambda \in V_K$ by

$$v \otimes \lambda \mapsto (1 \otimes \sigma) \circ f \circ (1 \otimes \sigma^{-1})(v \otimes \lambda) = (1 \otimes \sigma) \circ f(v \otimes \sigma^{-1}\lambda)$$

where $v \in V, \lambda \in K$. Note that if f is an isomorphism, $\sigma(f)$ is an isomorphism.

Remark 3.21. We claim that the above action also gives an action of G on morphisms of K-objects. That is, if (V, Φ) and (W, Ψ) are k-objects, and $f : V_K \to W_K$ is a K-morphism, then $\sigma(f)$ is a K-morphism. This is immediate from remark 3.19, since $\sigma(f)$ is the composition

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

and the outer maps are K-morphisms from remark 3.19. Hence we have an action of $G = \mathrm{Gal}(K/k)$ on $\mathrm{Hom}_{\mathcal{C}_K^{(p,q)}}(V_K, W_K)$.

[3] By $\mathrm{Hom}_K(V_K, W_K)$ we just mean K-linear maps, which need not be morphisms of K-objects.

Remark 3.22. Since the G-action described above takes isomorphisms to isomorphisms, we have a G-action on K-automorphisms of (V_K, Φ_K). Furthermore, this action interacts favorably with composition in $\mathrm{Aut}_K(\Phi)$. Given $\sigma \in G$, $f, g \in \mathrm{Aut}_K(\Phi)$, we have

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

That is to say, G acts by automorphisms on $\mathrm{Aut}_K(\Phi)$, so it is a G-group. Hence we may consider its nonabelian cohomology $H^1(G, \mathrm{Aut}_K(\Phi))$.

Proposition 3.23. *Fix (p, q), let K/k be a Galois extension, and let $(V, \Phi), (W, \Psi)$ be k-objects. Let $g : (V_K, \Phi_K) \to (W_K, \Psi_K)$ be a K-morphism. The following are equivalent.*

1. *There exists a k-morphism $f : V \to W$ such that $f_K = g$.*

2. *$\sigma(g) = g$ for all $\sigma \in G$. That is,*

$$g \in \mathrm{Hom}_{\mathcal{C}_K}(V_K, W_K)^G = H^0\Big(G, \mathrm{Hom}_{\mathcal{C}_K}(V_K, W_K)\Big)$$

3. *The map $g : V_K \to W_K$ is a morphism of G-modules, which is to say, for every $\sigma \in G$, the following diagram commutes.*

$$\begin{tikzcd} V_K \arrow[r, "g"] \arrow[d, "1\otimes\sigma"] & W_K \arrow[d, "1\otimes\sigma"] \\ V_K \arrow[r, "g"] & W_K \end{tikzcd}$$

Proof. (1) $\implies$ (2) If $g = f_K$ and $\sigma \in G$, then

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

Hence $\sigma(g) = g$.

(2) $\implies$ (3) Take the equality $\sigma(g) = g$, and compose on the right by $1 \otimes \sigma$.

$$(1 \otimes \sigma) \circ g \circ (1 \otimes \sigma^{-1}) = g \implies (1 \otimes \sigma) \circ g = g \circ (1 \otimes \sigma)$$

So the diagram commutes. (Similarly we could prove (3) $\implies$ (2) by composing on the right by $1 \otimes \sigma^{-1}$.)

(3) $\implies$ (1) If $x \in (V_K)^G$, then for $\sigma \in G$,

$$(1 \otimes \sigma) \circ g(x) = g \circ (1 \otimes \sigma)(x) = g(x)$$

That is to say, the commutative diagram in (3) implies that restricting g to $(V_K)^G$ lands in $(W_K)^G$, where G acts on V_K and W_K as in definition 2.3. So we get

$$g : (V_K)^G \to (W_K)^G$$

By lemma 2.4, we make the identifications $(V_K)^G = V$ and $(W_K)^G = W$. So we have a k-linear map $f = g|_{(V_K)^G} : V \to W$. But then since g is a K-morphism, f is a k-morphism. (Think through the commutative diagrams, this is not terribly complicated.) And also $g = f_K$ is clear. $\square$

Remark 3.24. The previous proposition gives a fairly complete answer to question 2 of remark 3.16. It tells us that the K-morphisms $(V_K, \Phi_K) \to (W_K, \Psi_K)$ which come from k-morphisms are precisely the fixed points of the Galois group acting on morphisms by conjugation.

3.6 Galois action on tensors

Definition 3.25. Let V be a k-vector space, and K/k a Galois extension with Galois group $G = \mathrm{Gal}(K/k)$. Fix (p, q). Let $H = \mathrm{Hom}_K((V_K)^{\otimes q}, (V_K)^{\otimes p})$ be the set of tensors of type (p, q) on V_K. We define an action of G on H as follows.

$$G \times H \to H \qquad (\sigma, \Psi) = \sigma(\Psi) = (1 \otimes \sigma)^{\otimes p} \circ \Psi \circ (1 \otimes \sigma^{-1})^{\otimes q}$$

We will call this the **conjugation action**. Hopefully it will be clear from context which conjugation we are talking about, since this is an action on a different (but related) set than the conjugation action in definition 3.20.

Proposition 3.26. *Fix (p, q). Let K/k be a Galois extension with Galois group $G = \mathrm{Gal}(K/k)$, let V be a k-vector space, and let Ψ be a tensor of type (p, q) on V_K. The following are equivalent.*

1. *There exists a tensor Φ of type (p, q) on V such that $\Phi_K = \Psi$.*
2. *$\sigma(\Psi) = \Psi$ for all $\sigma \in G$. That is,*

$$\Psi \in \mathrm{Hom}_K((V_K)^{\otimes q}, (V_K)^{\otimes p})^G = H^0(G, \mathrm{Hom}_K\Big((V_K)^{\otimes q}, (V_K)^{\otimes p}\Big)$$

3. *For every $\sigma \in G$, the following diagram commutes.*

$$\begin{tikzcd}
(V_K)^{\otimes q} \arrow[r, "\Psi"] \arrow[d, "(1\otimes\sigma)^{\otimes q}"'] & (V_K)^{\otimes p} \arrow[d, "(1\otimes\sigma)^{\otimes p}"] \\
(V_K)^{\otimes q} \arrow[r, "\Psi"] & (V_K)^{\otimes p}
\end{tikzcd}$$

Proof. (1) $\implies$ (2) Suppose $\Phi_K = \Psi$, and let $\sigma \in G$. Basically, since Φ_K only acts on the V part and $1 \otimes \sigma$ only acts on the K part, they commute. We include the details below.

$$\begin{aligned}
\sigma(\Phi_K)\Big((v_1 \otimes \lambda_1) \otimes \cdots \otimes (v_q \otimes \lambda_q)\Big) &= (1 \otimes \sigma)^{\otimes p} \circ \Phi_K \circ (1 \otimes \sigma^{-1})^{\otimes q}\Big((v_1 \otimes \lambda_1) \otimes \cdots \otimes (v_q \otimes \lambda_q)\Big) \\
&= (1 \otimes \sigma)^{\otimes p} \circ \Phi_K\Big((v_1 \otimes \sigma^{-1}\lambda_1) \otimes \cdots \otimes (v_q \otimes \sigma^{-1}\lambda_q)\Big) \\
&= (1 \otimes \sigma)^{\otimes p}\Big((\sigma^{-1}\lambda_1) \cdots (\sigma^{-1}\lambda_q)\Phi(v_1 \otimes \cdots \otimes v_q)\Big) \\
&= (\sigma\sigma^{-1}\lambda_1) \cdots (\sigma\sigma^{-1}\lambda_q)\Phi(v_1 \otimes \cdots \otimes v_q) \\
&= \lambda_1 \cdots \lambda_q \Phi(v_1 \otimes \cdots \otimes v_q) \\
&= \Phi_K\Big((v_1 \otimes \lambda_1) \otimes \cdots (v_q \otimes \lambda_q)\Big)
\end{aligned}$$

The previous calculation shows that $\sigma(\Phi_K) = \Phi_K$.

(2) $\implies$ (3) Take the equality $\sigma(\Psi) = \Psi$ and compose on each side by $(1 \otimes \sigma)^{\otimes q}$.

$$\sigma(\Psi) = (1 \otimes \sigma)^{\otimes p} \circ \Psi \circ (1 \otimes \sigma)^{\otimes q} = \Psi \implies (1 \otimes \sigma)^{\otimes p} \circ \Psi = \Psi \circ (1 \otimes \sigma)^{\otimes q}$$

So the diagram commutes. (Similarly we could easily prove (3) $\implies$ (2) by composing with $(1 \otimes \sigma^{-1})^{\otimes q}$.)

(3) $\implies$ (1) Recall that G acts on V_K on the K-part.

$$G \times V_K \to V_K \qquad \sigma(v \otimes \lambda) = v \otimes (\sigma\lambda)$$

So we also get an action of G on $(V_K)^{\otimes q}$ (or replace q with p).

$$G \times (V_K)^{\otimes q} \to (V_K)^{\otimes q} \qquad \sigma(x_1 \otimes \cdots \otimes x_n) = (\sigma x_1) \otimes \cdots \otimes (\sigma x_n)$$

By lemma 2.6, we identify the fixed points of this action with $V^{\otimes q}$. The commutative diagram in (3) implies that restricting Ψ to the fixed points $V^{\otimes q} = ((V_K)^{\otimes q})^G$ always outputs fixed points. So we obtain a tensor of type (p, q) on V, which we call Φ.

$$\Phi = \Psi|_{((V_K)^{\otimes q})^G} : V^{\otimes q} \to V^{\otimes p}$$

The manner of the identification $V^{\otimes q} \cong ((V_K)^{\otimes q})^G$ then makes it clear that $\Phi_K = \Psi$. $\square$

Remark 3.27. In particular, in the implication (3) $\implies$ (1), the proof constructs the tensor Φ as just the restriction of Ψ to fixed points.

Remark 3.28. The previous proposition answers question 1 of remark 3.16. Given a K-object (W, Ψ), we know that there is always a k-vector space V such that $V_K \cong W$ (isomorphism of K-vector spaces, or even of Γ-modules using Theorem 2.17). Then the proposition gives the criterion that (V_K, Ψ) descends to a k-object (V, Φ) if and only if Ψ is fixed by the conjugation action of $\mathrm{Gal}(K/k)$ on tensors.

3.7 Classifying twisted forms via cohomology

Throughout this whole section, we fix the following notation: K/k is a finite Galois extension with Galois group $G = \mathrm{Gal}(K/k)$. We fix $p, q \in \mathbb{Z}_{\geq 0}$, and a k-object (V, Φ). The group of K-automorphisms of (V, Φ) is $A = \mathrm{Aut}_K(\Phi)$. The twisted K/k-forms of (V, Φ) are $TF_K(V, \Phi)$.

3.7.1 Going from twisted forms to cohomology classes

Definition 3.29. Let (W, Ψ) be a K/k-twisted form of (V, Φ). Let B be the set of K-isomorphisms $(V_K, \Phi_K) \to (W_K, \Psi_K)$. We describe a map

$$\beta : B \to Z^1(G, A)$$

Given a K-isomorphism g, the image is the cocycle

$$a = \beta(g) : G \to A \qquad \sigma \mapsto a_\sigma = (g^{-1})^\sigma g = g^{-1} \circ \sigma(g)$$

We can verify this is a cocycle, as follows. For all $\sigma, \tau \in G$, a satisfies

$$a_{\sigma\tau} = g^{-1} \circ \sigma(\tau(g)) = g^{-1} \circ \sigma(g) \circ \sigma(g^{-1}) \circ \sigma(\tau(g)) = a_\sigma \circ \sigma(g^{-1} \circ \tau(g)) = a_\sigma{}^\sigma a_\tau$$

hence a is a 1-cocycle, $a \in Z^1(G, A)$.

Lemma 3.30. *Let (W, Ψ) be a K/k-twisted form of (V, Φ), and let β be the map above.*

1. *If $g, h \in B$, then $\beta(g)$ and $\beta(h)$ are cohomologous. That is, $\operatorname{im} \beta$ is contained in a single cohomology class.*
2. *If $a, b \in Z^1(G, A)$ are cohomologous and $a \in \operatorname{im} \beta$, then $b \in \operatorname{im} \beta$.*
3. *The image of β is precisely one cohomology class in $Z^1(G, A)$.*

Proof. (1) Let $g, h \in B$, and let $a = \beta(g), b = \beta(h)$.

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

Then let $c = h^{-1} g \in A$, and compute

$$c^{-1} b_\sigma{}^\sigma c = (h^{-1}g)^{-1} b_\sigma{}^\sigma (h^{-1}g) = g^{-1} h h^{-1} \sigma(h) \sigma(h)^{-1} \sigma(g) = g\sigma(g) = a_\sigma$$

Thus a, b are cohomologous.

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

$$b_\sigma = c^{-1} a_\sigma{}^\sigma c = c^{-1} g^{-1} \circ \sigma(g)^\sigma c = ((gc)^{-1})^\sigma gc$$

hence $b = \beta(gc)$.

(3) This is just a rephrasing of the combination of (1) and (2). $\square$

Definition 3.31. Let $\beta : B \to Z^1(G, A)$ be the map above. We now describe a map

$$\widetilde{\beta} : TF_K(V, \Phi) \to H^1(G, A)$$

Given a K/k-twisted form (W, Ψ) of (V, Φ), we want to obtain a cocycle class in $H^1(G, A)$. Given (W, Ψ), choose a K-isomorphism $g \in B$, then let $a = \beta(g)$. Then define

$$\widetilde{\beta}(W, \Psi) = [a] = [\beta(g)]$$

By the previous lemma, the choice of isomorphism g does not affect the cohomology class of $\beta(g)$, so this assignment rule does not depend on g, only on the twisted form (W, Ψ). Note that the cocycle $a = \beta(g)$ is dependent on g, only the cohomology class is independent of the choice of g.

Remark 3.32. Both $TF_K(V, \Phi)$ and $H^1(G, A)$ are pointed sets. The basepoint in $TF_K(V, \Phi)$ is the k-isomorphism class of (V, Φ) itself, and the basepoint in $H^1(G, A)$ is the cohomology class of the unit cocycle. We claim that under the map above, the basepoint is sent to the basepoint.

We are free to choose any isomorphism $(V_K, \Phi_K) \cong (V_K, \Phi_K)$, so we may choose the identity $g = \mathrm{Id} : V_K \to V_K$. Then for $\sigma \in G$,

$$a_\sigma = \mathrm{Id}^{-1} \circ \sigma(\mathrm{Id}) = \mathrm{Id} \circ \mathrm{Id} = 1 \in A$$

That is, a is the unit cocycle. Thus under our map, (V, Φ) gets sent to the cohomology class of the unit cocycle, which is the basepoint of $H^1(G, A)$.

Actually, we don't even need to choose the identity map on V_K. As long as we choose any k-morphism $(V, \Phi) \to (V, \Phi)$ and then tensor it up to a K-morphism $(V_K, \Phi_K) \to (V_K, \Phi_K)$, it will commute with $\sigma \in G$, and we will get the unit cocycle.

3.7.2 Going from cohomology classes to twisted forms

Our next major goal is to prove that the map $TF_K(V,\Phi) \to H^1(G,A)$ is an isomorphism (of pointed sets). Since we already know it preserves basepoints, this is just a fancy way of saying it is a bijection. We'll get there by constructing the inverse map, using twisted actions.

Remark 3.33. We have actions of G and A on V_K, and an action of G on A, and these are compatible actions, as we now verify. The actions are

$$\begin{aligned} G \times V_K \to V_K \qquad & \sigma \cdot x = (1 \otimes \sigma)(x) \\ A \times V_K \to V_K \qquad & f \cdot x = f(x) \\ G \times A \to A \qquad & \sigma \cdot f = (1 \otimes \sigma) \circ f \circ (1 \otimes \sigma^{-1}) \end{aligned}$$

For $\sigma \in G, f \in A, x \in V_K$,

$$(\sigma \cdot f) \cdot (\sigma \cdot x) = (1 \otimes \sigma) \circ f \circ (1 \otimes \sigma^{-1}) \circ (1 \otimes \sigma)(x) = (1 \otimes \sigma) \circ f(x) = \sigma \cdot (f \cdot x)$$

Thus the actions are compatible.

Definition 3.34. Let $\alpha \in H^1(G,A)$, and choose a representative cocycle $a \in Z^1(G,A)$, so $\alpha = [a]$. Since G, A act compatibly on V_K, we can form the twisted action of definition 1.36.

$$G \times {}_aV_K \to {}_aV_K \qquad \sigma * x = a_\sigma(\sigma x)$$

Let $W = ({}_aV_K)^G$ be the G-invariants of this action.

$$W = ({}_aV_K)^G = \{x \in V_K : \sigma * x = x, \forall \sigma \in G\} = \{x \in V_K : a_\sigma(\sigma x) = x, \forall \sigma \in G\}$$

For any $\sigma \in G$, both a_σ and σ act on A as k-linear maps, so W is a k-vector subspace of V_K. (It is not necessarily a K-vector subspace, since σ is not K-linear.) We call W the **twisted form of (V, Φ) associated to α**.

Remark 3.35. It is not clear at this point if W depends on the choice of a (and not just on α), or that W is a twisted form of (V, Φ), so our next priority is to address these issues. Regarding the second issue, the question doesn't even make sense at this point since we haven't defined a tensor on W.

Remark 3.36. Let α, a, W be as above. Let's consider the following map from lemma 2.11.

$$f : W_K = \left(({}_aV_K)^G\right)_K \xrightarrow{\cong} V_K \qquad x \otimes \lambda \mapsto \lambda x$$

The lemma says that the map f above gives an isomorphism of G-modules IF we replace the V_K on the right by ${}_aV_K$, but since V_K and ${}_aV_K$ have different actions, our map f is NOT necessarily a morphism of G-modules.

In fact, f should only be a morphism of G-modules when the twisting cocycle a is trivial. Let's do some calculations to try and understand this. Given $\sigma \in G$, let's compare f and ${}^\sigma f$.

Let's fix a k-basis $\{e_i\}$ for V. We obtain the associated K-basis $\{e_i \otimes 1\}$ for V_K. We want to write an arbitrary element of W_K in terms of this basis. Let's also fix a k-basis $\{w_j\}$ for W, which gives us a K-basis $\{w_j \otimes 1\}$ of W_K. By lemma 2.7 and remark 2.12, we can choose the basis $\{w_i\}$ so that it is also a K-basis of V_K.

We want to write an arbitrary element of W_K in terms of the e_i's. We can write each $w_j \in W \subset V_K$ uniquely in terms of the K-basis $\{e_i \otimes 1\}$.

$$w_j = \sum_i \lambda_{ij}(e_i \otimes 1) = \sum_i e_i \otimes \lambda_{ij}$$

where $\lambda_{ij} \in K$. That is, (λ_{ij}) is the transition matrix from the K-basis $\{w_j\}$ of V_K to the K-basis $\{e_i \otimes 1\}$ also of V_K. We can now write an arbitrary $x \in W_K$ in terms of the K-basis $\{w_i \otimes 1\}$.

$$x = \sum_j x_j(w_j \otimes 1) = \sum_j w_j \otimes x_j$$

where $x_j \in K$. Then we can rewrite x as

$$x = \sum_j \left(\sum_i e_i \otimes \lambda_{ij} \right) \otimes x_j$$

Applying f to x in this form, we get

$$\begin{aligned} f(x) &= f\left(\sum_j \left(\sum_i e_i \otimes \lambda_{ij} \right) \otimes x_j \right) \\ &= \sum_j x_j \sum_i e_i \otimes \lambda_{ij} \\ &= \sum_{i,j} e_i \otimes x_j \lambda_{ij} \end{aligned}$$

Now we try applying ${}^\sigma f$ to x.

$$\begin{aligned} {}^\sigma f(x) &= (\mathrm{Id}_V \otimes \sigma) \circ f \circ (\mathrm{Id}_W \otimes \sigma^{-1}) \left(\sum_j \left(\sum_i e_i \otimes \lambda_{ij} \right) \otimes x_j \right) \\ &= (\mathrm{Id}_V \otimes \sigma) \circ f \left(\sum_j \left(\sum_i e_i \otimes \lambda_{ij} \right) \otimes \sigma^{-1}(x_j) \right) \\ &= (\mathrm{Id}_V \otimes \sigma) \left(\sum_{i,j} e_i \otimes \lambda_{ij} \sigma^{-1}(x_j) \right) \\ &= \sum_{i,j} e_i \otimes \sigma(\lambda_{ij} \sigma^{-1} x_j) \\ &= \sum_{i,j} e_i \otimes \sigma(\lambda_{ij}) x_j \end{aligned}$$

Comparing these, we see that $f(x) = {}^\sigma f(x)$ if and only if, when written in terms of this basis, all the elements λ_{ij} are fixed by σ. That is to say, $f = {}^\sigma f$ for every σ if and only if every $\lambda_{ij} \in k$, which is to say, there is a basis $\{e_i\}$ of V such that $\{e_i \otimes 1\}$ is a k-basis of W.

Now le'ts try to understand f^{-1} and ${}^\sigma(f^{-1})$. We can write each $e_i \otimes 1$ in terms of the K-basis $\{w_j\}$ of V_K.

$$e_i \otimes 1 = \sum_j \gamma_{ij} w_j$$

That is, $(\gamma_{ij}) = (\lambda_{ij})^{-1}$ is the transition matrix from the K-basis $\{e_i \otimes 1\}$ to the basis $\{w_j\}$. We write an arbitrary $y \in V_K$ in terms of the K-basis $\{e_i \otimes 1\}$.

$$y = \sum_i e_i \otimes y_i = \sum_i y_i(e_i \otimes 1) = \sum_i y_i \left(\sum_j \gamma_{ij} w_j \right) = \sum_{i,j} y_i \gamma_{ij} w_j$$

with $y_i \in K$. Then

$$f^{-1}(y) = \sum_{i,j} f^{-1}(y_i \gamma_{ij} w_j) = \sum_{i,j} w_j \otimes y_i \gamma_{ij}$$

Being a bit more sloppy with notation, we can write this as

$$f^{-1}(e_i) = f^{-1}(e_i \otimes 1) = \sum_j w_j \otimes \gamma_{ij}$$

With ${}^\sigma(f^{-1})$, we get

$$\begin{aligned}
{}^\sigma(f^{-1})(y) &= (\mathrm{Id}_W \otimes \sigma) \circ f^{-1} \circ (\mathrm{Id}_V \otimes \sigma^{-1})(y) \\
&= (\mathrm{Id}_W \otimes \sigma) \circ f^{-1} \circ (\mathrm{Id}_V \otimes \sigma^{-1}) \left(\sum_i e_i \otimes y_i \right) \\
&= (\mathrm{Id}_W \otimes \sigma) \circ f^{-1} \left(\sum_i e_i \otimes \sigma^{-1} y_i \right) \\
&= (\mathrm{Id}_W \otimes \sigma) \circ f^{-1} \left(\sum_{i,j} \sigma^{-1}(y_i) \gamma_{ij} w_j \right) \\
&= (\mathrm{Id}_W \otimes \sigma) \left(\sum_{i,j} w_j \otimes \sigma^{-1}(y_i) \gamma_{ij} \right) \\
&= \sum_{i,j} w_j \otimes y_i \sigma(\gamma_{ij})
\end{aligned}$$

Using a bit more sloppy notation, we can write this as

$${}^\sigma(f^{-1})(e_i) = \sum_j \sigma(\gamma_{ij}) w_j$$

This is analogous to what happened with f, since it also demonstrates that $f^{-1} = {}^\sigma(f^{-1})$ for all σ if and only if all of the coefficients γ_{ij} are in k. But since $(\gamma_{ij}) = (\lambda_{ij})^{-1}$ (this equality is in $\mathrm{GL}_n(k)$ where $n = \dim_k V$), this is equivalent to all the λ_{ij} lying in k.

Definition 3.37. Let α, a, W be as above. Our goal is to define a tensor Ψ on W to make it a k-object. Using lemma 2.11, the following is an isomorphism of K-vector spaces.

$$f : W_K = \left(({}_aV_K)^G\right)_K \xrightarrow{\cong} V_K \qquad x \otimes \lambda \mapsto \lambda x$$

Keep in mind the previous remark, which tells us that f is not generally a morphism of G-modules.

We have the tensor Φ_K on V_K, so using the above isomorphism we can transfer it to a tensor $\widetilde{\Phi}_K$ on W_K in such a way that $f : (W_K, \Phi_K) \to (V_K, \Phi_K)$ is a morphism of K-objects. To be more concrete, set

$$\widetilde{\Phi}_K = (f^{-1})^{\otimes p} \circ \Phi_K \circ f^{\otimes q}$$

which then immediately makes the required diagram commute for f to be a morphism of K-objects.

$$\begin{tikzcd}
(W_K)^{\otimes q} \arrow[r, "f^{\otimes q}"] \arrow[d, dashed, "\widetilde{\Phi}_K"'] & (V_K)^{\otimes q} \arrow[d, "\Phi_K"] \\
(W_K)^{\otimes p} \arrow[r, "f^{\otimes p}"] & (V_K)^{\otimes p}
\end{tikzcd}$$

So we have a K-object $(W_K, \widetilde{\Phi}_K)$, which we would like to say descends to a k-object (W, Ψ). By the criterion in proposition 3.26, this happens precisely if Φ_K is fixed by the action of G. For a proof of this, see a very long and hard to follow calculation in the appendix, proposition 5.1.

Assuming the lemma, $\widetilde{\Phi}_K$ is fixed by G, so by proposition 3.23 it descends to a k-tensor Ψ on W. To be more specific, using the remark following proposition 3.23, the tensor Ψ is just the restriction of Φ to W. So we have a k-object (W, Ψ). Following the terminology in definition 3.34, we call (W, Ψ) the **twisted form of (V, Φ) associated to α**.

Lemma 3.38. *Let $\alpha \in H^1(G, A)$ and let (W, Ψ) the associated twisted form of (V, Φ). Then*

1. *(W, Ψ) is a twisted K/k-form of (V, Φ).*
2. *The k-isomorphism class of (W, Ψ) does not depend on the choice of cocycle a, only on the cohomology class $\alpha \in H^1(G, A)$.*

Proof. (1) This is immediate from the construction of Ψ. To be more precise, in definition 3.37, the map

$$f : W_K \to V_K \qquad x \otimes \lambda \mapsto \lambda x$$

was an isomorphism of K-vector spaces, and by construction of Ψ, we have $\Psi_K = \widetilde{\Phi}_K$, and by construction of $\widetilde{\Phi}_K$, $f : (W_K, \widetilde{\Phi}_K) \to (V_K, \Phi_K)$ is an isomorphism of K-objects. Hence (W, Ψ) is a twisted K/k-form of (V, Φ).

(2) Let $a, b \in Z^1(G, A)$ both be cocycles representing $\alpha \in H^1(G, A)$, and let (W^a, Ψ^a) and (W^b, Ψ^b) be the respective associated twisted forms of (V, Φ).

$$W^a = ({}_aV_K)^G$$
$$W^b = ({}_bV_K)^G$$

We need to give a k-isomorphism $(W^a, \Psi^a) \cong (W^b, \Psi^b)$. By definition, $[a] = [b] = \alpha$ means that there exists $c \in A = \mathrm{Aut}_K(\Phi)$ such that

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

for all $\sigma \in G$. We can rewrite this as

$$b_\sigma {}^\sigma c = c a_\sigma$$

Then we claim that $c : V_K \to V_K$ restricts to a map $W^a \to W^b$. If $x \in W^a$, then $a_\sigma \sigma x = x$ for all $\sigma \in G$. Then

$$b_\sigma \sigma(cx) = b_\sigma \sigma c \sigma^{-1} \sigma x = b_\sigma {}^\sigma c \sigma x = c a_\sigma \sigma x = cx$$

for all $\sigma \in G$, hence $cx \in W^b$, so $c : W^a \to W^b$ as claimed. Hence $c : W^a \to W^b$ is a bijective k-linear map. It just remains to verify that it is a morphism of k-objects. Since $c : V_K \to V_K$ is a K-morphism, the following diagram commutes.

$$\begin{tikzcd}
({}_aV_K)^{\otimes q} \arrow[r, "c^{\otimes q}"] \arrow[d, "\Phi_K"] & ({}_bV_K)^{\otimes q} \arrow[d, "\Phi_K"] \\
({}_aV_K)^{\otimes p} \arrow[r, "c^{\otimes p}"] & ({}_bV_K)^{\otimes p}
\end{tikzcd}$$

Then restricting to G-invariants we obtain

$$\begin{tikzcd}
(W^a)^{\otimes q} \arrow[r, "c^{\otimes q}"] \arrow[d, "\Psi^a"] & (W^b)^{\otimes q} \arrow[d, "\Psi^b"] \\
(W^b)^{\otimes p} \arrow[r, "c^{\otimes p}"] & (W^b)^{\otimes p}
\end{tikzcd}$$

hence $c : W^a \to W^b$ is the needed k-isomorphism. $\square$

Remark 3.39. As a consequence of the previous lemma, we have a well defined map

$$H^1(G, A) \to TF_K(V, \Phi) \qquad [a] \mapsto \big(({}_aV_K)^G, \Psi\big)$$

3.7.3 Main correspondence

Theorem 3.40 (CSAGC 2.3.3)**.** *Let (V, Φ) be a k-object and K/k a finite Galois extension with Galois group $G = \mathrm{Gal}(K/k)$, and let $A = \mathrm{Aut}_K(\Phi)$. The maps defined above*

$$TF_K(V, \Phi) \to H^1(G, A) \qquad (W, \Psi) \mapsto [a]$$
$$H^1(G, A) \to TF_K(V, \Phi) \qquad [a] \mapsto \big(({}_aV_K)^G, \Psi\big)$$

are mutual inverses, so they give a basepoint-preserving bijection.

Proof. We already know the map preserves basepoints, by remark 3.32. We just need to verify that the two compositions are the respective identity maps.

First, start with a twisted K/k-form (W, Ψ). We choose a K-isomorphism $f : W_K \to V_K$, and obtain the associated cocycle $b = \beta(f^{-1}) \in Z^1(G, A)$,

$$b : G \to A \qquad b_\sigma = f^\sigma(f^{-1})$$

Then the associated cohomology class is $[b] \in H^1(G, A)$. To return to twisted forms, we set $W^b = ({}_bV_K)^G$, and get a tensor Ψ^b on W^b by restricting Φ_K to W^b. So we have obtained a twisted K/k-form (W^b, Ψ^b). We need to verify that (W^b, Ψ^b) is k-isomorphic to (W, Ψ). Consider the composition

$$W^b = ({}_bV_K)^G \hookrightarrow V_K \xrightarrow{f^{-1}} W_K$$

Clearly this is a K-morphism. We claim that the image is precisely $(W_K)^G$. If $x \in W^b$, then for every $\sigma \in G$,

$$x = \sigma * x = b_\sigma \sigma x = (f)^\sigma(f^{-1})\sigma x = f\sigma f^{-1}\sigma^{-1}\sigma x = f\sigma f^{-1}x \implies f^{-1}x = \sigma f^{-1}x$$

Thus $f^{-1}x \in (W_K)^G$. Since W^b and $(W_K)^G$ have equal k-dimension, the image is precisely $(W_K)^G$. Thus f^{-1} restricts to an isomorphism of k-vector spaces $W^b \to (W_K)^G$. Using lemma 2.4 we identify $(W_K)^G$ with W using the isomorphism

$$(W_K)^G \to W \qquad w \otimes 1 \mapsto w$$

hence f^{-1} gives an isomorphism of k-vector spaces $W^b \to W$. Since Ψ^b is just the restriction of Φ_K to W^b and f^{-1} takes Φ_K to Ψ_K (since f^{-1} is a K-morphism), the restriction of f^{-1} to W^b is a k-morphism, that is, f^{-1} gives the needed k-isomorphism $(W^b, \Psi^b) \to (W, \Psi)$. Hence the composition

$$TF_K(\Phi) \to H^1(G, A) \to TF_K(\Phi)$$

is the identity.

Now we consider the other composition. Start with a cohomology class $\alpha \in H^1(G, A)$, and choose a representative cocycle $a \in Z^1(G, A)$. We then obtain the associated twisted form (W^a, Ψ^a) where $W^a = ({}_aV_K)^G$ and Ψ is the restriction of Φ_K to W. This process comes via a K-isomorphism $f_a : W^a_K \to V_K$, as in definition 3.37. To return to cohomology classes (as in definition 3.31), we use the isomorphism f_a^{-1} to obtain a cocycle $b = \beta(f_a^{-1}) \in Z^1(G, A)$.

$$b : G \to A \qquad b_\sigma = {f_a}^\sigma(f_a^{-1})$$

We just need to prove that a and b are cohomologous. Let $W^b = ({}_bV_K)^G$ be the twisted form of (V, Φ) associated to the cocycle b. Using the previous case, under the composition

$$W^b \hookrightarrow V_K \xrightarrow{f_a^{-1}} W^a_K$$

the image of f_a^{-1} is precisely $(W^a_K)^G$, which we identify with W^a using the isomorphism from lemma 2.11.

$$(W^a_K)^G \to W^a \qquad x \mapsto x \otimes 1$$

By the previous case, f_a^{-1} then gives a k-isomorphism $W^b \to W^a$. So we have the following commutative diagram.

$$\begin{tikzcd}
{}_bV_K \arrow[r, "f_a^{-1}"] & W_K^a = \left(({}_aV_K)^G\right)_K \arrow[r, "\epsilon", "x\otimes\lambda\mapsto\lambda x"'] & {}_aV_K \\
W^b = ({}_bV_K)^G \arrow[u, hook] \arrow[rr, "f_a^{-1}"] & & W^a = ({}_aV_K)^G \arrow[u, hook]
\end{tikzcd}$$

with the ϵ map coming from Speiser's lemma 2.11. That is to say, ϵf_a^{-1} commutes with the G-actions, since it descends to a k-morphism (using proposition 3.23). Let $c = \epsilon f_a^{-1}$[4]. The fact that c commutes with G-actions means that for all $x \in {}_aV_K$,

$$c(\sigma * x) = \sigma * (cx) \implies cb_\sigma \sigma x = a_\sigma \sigma cx \implies cb_\sigma \sigma = a_\sigma \sigma c \implies b_\sigma = c^{-1} a_\sigma {}^\sigma c$$

Thus a, b are cohomologous cocycles. This proves that the composition

$$H^1(G, A) \to TF_K(\Phi) \to H^1(G, A)$$

is the identity. □

3.8 Families of tensors

This section is based on Remark 2.3.10 of CSAGC, which says that we can generalize theorem 3.40 to the situation of a family of tensors.

Definition 3.41. Let V be a k-vector space. Let $\{\Phi_i\}$ be a family of tensors of type (p_i, q_i) on V. The pair (V, Φ_i) is a **generalized k-object**.

Definition 3.42. A **morphism of generalized k-objects** is a k-linear map $V \to W$ which preserves all the tensors, which is to say, each tensor makes the appropriate diagram commute.

Remark 3.43. Why would we need more than one tensor to track the structure on V? Well, for example, suppose we wanted to study algebras of a particular type. A tensor Φ_1 of type $(p_1, q_1) = (1, 2)$ gives V the structure of a k-algebra, but does not say anything about the properties of this multiplication map.

If we want to also require that the algebras be associative, unital, central, or simple, we can encode whatever property in some appropriate commutative diagrams, and turn that data into some kind of tensor on V. Then our morphisms of k-objects will have to respect all the structural properties of our algebras.

Remark 3.44. Given our definitions of generalized k-objects and their morphisms, the rest of the development of the theory generalizes immediately. Extension of scalars, twisted forms, Galois actions, and K-automorphism groups are defined as one would expect.

Theorem 3.45 (Generalized theorem 3.40)**.** *Let (V, Φ_i) be a generalized k-object and K/k a finite Galois extension with Galois group $G = \mathrm{Gal}(K/k)$, and let $A = \mathrm{Aut}_K(\Phi_i)$. The maps*

$$\begin{aligned} TF_K(V, \Phi_i) &\to H^1(G, A) \qquad & (W, \Psi_i) &\mapsto [a] \\ H^1(G, A) &\to TF_K(V, \Phi_i) \qquad & [a] &\mapsto \left(({}_aV_K)^G, \Psi_i\right) \end{aligned}$$

are mutual inverses, so they give a basepoint-preserving bijection.

[4]I'm not exactly sure why $c \in \mathrm{Aut}_K(\Phi)$, but it feels like it really should be. I don't have the energy to figure out why right now.

3.9 Infinite extensions

The main correspondence generalizes to case where K/k is an infinite Galois extension. The basic gist of this is that $G = \mathrm{Gal}(K/k)$ acts on $A = \mathrm{Aut}_K(\Phi)$ continuously, so it always acts through a finite quotient. So the profinite cohomology group $H^1(G, A)$ is not a scary or complicated as it could be.

Alternatively, one can try to obtain the finite case from the infinite case by using direct and inverse limits. There is some discussion of this in Platonov-Rapinchuk, but the details there are not particularly spelled out, nor do I feel the need to work them out myself and record them here.

4 Examples and applications

In this section, we consider what the main corespondence says in a few special cases with small p, q values. Sometimes we can compute $H^1(G, A)$, and it tells us about twisted forms. Sometimes we can describe the twisted forms, and it tells us about $H^1(G, A)$.

4.1 Revisiting vector spaces $(p, q) = 0$

When $(p, q) = (0, 0)$ a k-object (V, Φ) is just the vector space V with no additional structure, and morphisms $(V, \Phi) \to (W, \Psi)$ of k-objects are merely k-linear maps. We have already fully described what happens in this case in proposition 2.13, remark 2.14, and remark 3.17.

To reiterate those remarks, in this situation $TF_K(\Phi)$ is just a single point set containing the k-isomorphism class of (V, Φ) itself. So by the main correspondence 3.40, $H^1(G, A)$ is only one cohomology class. That is to say, every cocycle is cohomologous to the trivial cocycle.

Also, because every K-automorphism $(V_K, \Phi_K) \to (V_K, \Phi_K)$ comes from a k-automorphism $(V, \Phi) \to (V, \Phi)$, it is fixed by every $\sigma \in G$. That is to say, G acts trivially on $A = \mathrm{Aut}_K(\Phi)$. So

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

4.2 $(p, q) = (1, 0)$

In this case, Φ is a k-linear map $k \to V$. Since Φ is determined by $\Phi(1)$, a k-object (V, Φ) is really just a vector space V with a distinguished element $v_0 = \Phi(1)$. We may as well assume Φ is nonzero, although we won't actually need this assumption. Then Φ is just an embedding of k into V, and the image is a 1-dimensional subspace spanned by v_0.

A k-morphism $f : (V, \Phi) \to (V', \Phi')$ is a k-linear map $f : V \to V'$ such that $f\Phi = \Phi'$. In other words, if we let $v_0 = \Phi(1)$ and $v_0' = \Phi'(1)$, then $f(v_0) = v_0'$.

$$\begin{array}{ccc} k & \xrightarrow{f^{\otimes 0} = \mathrm{Id}} & k \\ \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Phi'} \\ V & \xrightarrow{f} & V' \end{array}$$

Suppose (W, Ψ) is a twisted K/k-form of (V, Φ), so we get a K-isomorphism $g : V_K \to W_K$. This just means g is K-linear and $g(v_0 \otimes 1) = w_0 \otimes 1$.

$$\begin{array}{ccc} K & \xrightarrow{\mathrm{Id}} & K \\ \downarrow{\scriptstyle \Phi_K} & & \downarrow{\scriptstyle \Psi_K} \\ V_K & \xrightarrow{g} & W_K \end{array}$$

We know that g descends to a k-linear map $f : V \to W$ where $f_K = g$, though f may not be a morphism of k-objects.

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle v\mapsto v\otimes 1}\downarrow & & \downarrow{\scriptstyle w\mapsto w\otimes 1} \\ V_K & \xrightarrow[g=f_K]{} & W_K \end{array}$$

This implies

$$f(v_0) \otimes 1 = f_K(v_0 \otimes 1) = g(v_0 \otimes 1) = w_0 \otimes 1$$

But this implies $f(v_0) = w_0$, which is to say, f is a k-morphism. Thus every K-isomorphism from V_K descends to a k-isomorphism, meaning $TF_K(\Phi)$ is trivial. Hence $H^1(G, A)$ is also trivial.

4.3 $(p, q) = (0, 1)$

In this case, Φ is a k-linear map $V \to k$. That is, Φ is a linear functional on V, an element of the dual space V^*. A k-morphism $f : (V, \Phi) \to (V', \Phi')$ is just a k-linear map $f : V \to V'$ such that $\Phi' f = \Phi$.

$$\begin{array}{ccc} V & \xrightarrow{f} & V' \\ \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Phi'} \\ k & \xrightarrow{\text{Id}} & k \end{array}$$

Example 4.1. Let $k = \mathbb{R}, K = \mathbb{C}, V = \mathbb{R}^2$. Let $\Phi : \mathbb{R}^2 \to \mathbb{R}$ be the projection onto the first coordinate.

$$\Phi : \mathbb{R}^2 \to \mathbb{R} \qquad (x_1, x_2) \mapsto x_1$$

We have isomorphisms (of $\mathbb{C}$-vector spaces)

$$\begin{array}{ccccc} \mathbb{R}^2 \otimes_{\mathbb{R}} \mathbb{C} & \xrightarrow{\cong} & (\mathbb{R} \otimes_{\mathbb{R}} \mathbb{C}^2) & \xrightarrow{\cong} & \mathbb{C}^2 \\ (x_1, x_2) \otimes z & \longmapsto & (x_1 \otimes z, x_2 \otimes z) & \longmapsto & (x_1 z, x_2 z) \end{array}$$

How to describe $\Phi_{\mathbb{C}}$? It is

$$\Phi_{\mathbb{C}} : \mathbb{R}^2 \otimes_{\mathbb{R}} \mathbb{C} \to \mathbb{R} \otimes_{\mathbb{R}} \mathbb{C} \qquad (x_1, x_2) \otimes z \mapsto x_1 \otimes z$$

Using the previous isomorphisms, we can write it more usefully as the projection map onto the first coordinate.

$$\Phi_{\mathbb{C}} : \mathbb{C}^2 \to \mathbb{C} \qquad (z_1, z_2) \mapsto z_1$$

The Galois group is $G = \mathbb{Z}/2\mathbb{Z}$ with complex conjugation being the lone nontrivial element. We denote it by σ, and just write $\sigma(z) = \overline{z}$. A K-automorphism of V is a $\mathbb{C}$-linear map $g : \mathbb{C}^2 \to \mathbb{C}^2$ such that the diagram below commutes.

$$\begin{array}{ccc} \mathbb{C}^2 & \xrightarrow{g} & \mathbb{C}^2 \\ \downarrow{\scriptstyle \Phi_{\mathbb{C}}} & & \downarrow{\scriptstyle \Phi_{\mathbb{C}}} \\ \mathbb{C} & \xrightarrow{\text{Id}} & \mathbb{C} \end{array}$$

That is to say, g acts as the identity on the first component of $\mathbb{C}$. So we can write it as

$$g : \mathbb{C}^2 \to \mathbb{C}^2 \qquad g(z_1, z_2) = (z_1, \lambda_g z_2)$$

for some $\lambda_g \in \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times$. Any $\lambda_g \in \mathbb{C}^\times$ gives rise to such a g, so we may identify $A = \mathrm{Aut}_{\mathbb{C}}(\Phi)$ with $\mathbb{C}^\times$. To describe the G-action on this, it suffices to describe what complex conjugation does. Given $(z_1, z_2) \in \mathbb{C}^2$ and $g \in A$,

$${}^\sigma g(z_1, z_2) = \sigma g \sigma(z_1, z_2) = \sigma g(\overline{z}_1, \overline{z}_2) = \sigma(\overline{z}_1, \lambda_g \overline{z}_2) = \big(z_1, \overline{\lambda_g \overline{z}_2}\big) = \big(z_1, \overline{\lambda}_g z_2\big)$$

So G acts on $A = \mathbb{C}^\times$ as you would expect, just restricting the usual action of the Galois group on $\mathbb{C}$. So the fixed points are $\lambda_g \in \mathbb{C}^\times$ which are fixed by complex conjugation, which is to say,

$$H^0(G, A) = \mathbb{R}^\times$$

By Hilbert's theorem 90, $H^1(G, \mathbb{C}^\times) = 0$. By our main correspondence, this tells us that every twisted $\mathbb{C}/\mathbb{R}$-form of (V, Φ) is already $\mathbb{R}$-isomorphic to (V, Φ).

Example 4.2. Let $k = \mathbb{R}, K = \mathbb{C}, V = \mathbb{R}^2$. Let $\Phi : \mathbb{R}^2 \to \mathbb{R}$ be the usual multiplication map of $\mathbb{R}$.

$$\Phi : \mathbb{R}^2 \to \mathbb{R} \qquad \Phi(x, y) = xy$$

After extending scalars to $\mathbb{C}$, we see that $\Phi_{\mathbb{C}}$ is the multiplication map for $\mathbb{C}$.

$$\Phi_{\mathbb{C}} : \mathbb{C}^2 \to \mathbb{C} \qquad \Phi_{\mathbb{C}}(w, z) = wz$$

Thus the group $\mathrm{Aut}_K(\Phi)$ is the group of $\mathbb{C}$-linear automorphisms of $V_{\mathbb{C}} = \mathbb{C}^2$ which preserve this multiplication.

$$\begin{tikzcd} \mathbb{C}^2 \arrow[r, "g"] \arrow[d, "\Phi_{\mathbb{C}}"] & \mathbb{C}^2 \arrow[d, "\Phi_{\mathbb{C}}"] \\ \mathbb{C} \arrow[r, "\mathrm{Id}"] & \mathbb{C} \end{tikzcd}$$

Since g is $\mathbb{C}$-linear, we can think of it as an element of $\mathrm{GL}_2(\mathbb{C})$. So if $g = (g_{ij})$,

$$g(w, z) = (g_{11} w + g_{12} z, g_{21} w + g_{22} z)$$

The diagram above says that if $g = (g_{ij})$ and $(w, z) \in \mathbb{C}^2$, then

$$wz = \Phi(w, z) = \Phi g(w, z) = (g_{11}w + g_{12}z)(g_{21}w + g_{22}z) = g_{11}g_{21}w^2 + (g_{11}g_{22} + g_{12}g_{21})wz + g_{12}g_{22}z^2$$

Since this holds for all $w, z \in \mathbb{C}$, this implies

$$g_{11}g_{12} = g_{12}g_{22} = 0 \qquad g_{11}g_{22} + g_{12}g_{21} = 1$$

Since $g \in \mathrm{GL}_2(\mathbb{C})$, we also know $g_{11}g_{22} - g_{12}g_{21} \neq 0$. The first equations above say that g has a zero in each row. Then the second equation says that $g_{11}g_{22} = 1$ or $g_{12}g_{21} = 1$, whichever is nonzero. So g has one of the following forms.

$$\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}, \begin{pmatrix} 0 & x \\ x^{-1} & 0 \end{pmatrix} \qquad x \in \mathbb{C}^\times$$

So the automorphism group $\mathrm{Aut}_K(\Phi)$ is identified with this subgroup of $\mathrm{GL}_2(\mathbb{C})$.

$$\mathrm{Aut}_K(\Phi) \cong \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}, \begin{pmatrix} 0 & x \\ x^{-1} & 0 \end{pmatrix} : x \in \mathbb{C}^\times \right\}$$

The Galois group acts on these entrywise. Perhaps there would be more I could say at this point if I knew the classification of real bilinear forms better.

Example 4.3. [5] We generalize the previous example. Let L/K be a quadratic extension in char $\neq 2$, so $L = K(\sqrt{c})$ for some non-square $c \in K^\times$. Let $\Gamma = \mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$ with generator/unique nontrivial element τ. Let $V = K^2$, and let Φ be the quadratic form on K just given by multiplication.

$$\Phi : V \to K \qquad (x, y) \mapsto xy$$

Then $V_L = L^2$ with Φ_L also just given by multiplication. Rather than describe the group of L-automorphisms of V_L, we just construct a nontrivial twisted form of (V, Φ) using a particular cocycle. Let $A = \mathrm{Aut}_L(V_L)$, and define a cocycle $b \in Z^1(\Gamma, A)$ by

$$b : \Gamma \to A \qquad b_e = \mathrm{Id} \qquad b_\tau = \Big((x, y) \mapsto (y, x) \Big)$$

The regular action of Γ on V_L is just acting by Γ on each entry of $V_L = L^2$. The twisted action is

$$\Gamma \times {}_bV_L \to {}_bV_L \qquad \sigma * v = b_\sigma(\sigma v)$$

In the case of the nontrivial element τ, it acts as

$$\tau * v = \tau * (v_1, v_2) = (\tau v_2, \tau v_2)$$

To get a twisted form of V, we take the Γ-fixed points of the twisted action. Since τ is the only nontrivial element, the Γ-fixed points are just points fixed by τ.

$$W = ({}_bV_L)^\Gamma = \big\{ (x, y) \in V_L = L^2 : (x, y) = (\tau y, \tau x) \big\} = \big\{ (x, \tau x) \in L^2 : x \in L \big\}$$

Projecting onto the first component, we can identify W with L. However, W is not necessarily isomorphic to L as a K-algebra, because the "multiplication" in W is

$$(x, \tau x) \mapsto x \cdot \tau x = \mathrm{Nm}_K^L(x)$$

To summarize: we have the K-algebra $V = K^2$ viewed as a K-algebra with the tensorΦ being the usual multiplication in K. We constructed the K-algebra W which is identified with L as a set, but the tensor on W captures the field norm Nm_K^L. To be even more concrete,

$$\begin{aligned} V \to K \qquad & (x, y) \mapsto xy \\ W \to K \qquad & x + y\sqrt{c} \mapsto x^2 - cy^2 \end{aligned}$$

Although V, W are isomorphic as K-vector spaces (both are 2-dimensional) they are not isomorphic as K-algebras.

[5] Inspired by example 2 on page 69 of Platonov-Rapinchuk.

4.4 Vector space with fixed endomorphism $(p, q) = (1, 1)$

In this case, Φ is just a k-linear map $V \to V$. A k-morphism $(V, \Phi) \to (V', \Phi')$ is a linear map $f : V \to V'$ such that $\Phi' f = f\Phi$.

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "\Phi"] & V' \arrow[d, "\Phi'"] \\ V \arrow[r, "f"] & V \end{tikzcd}$$

The group of K-automorphisms is

$$A = \mathrm{Aut}_K(\Phi) = \{f \in \mathrm{GL}(V_K) : f\Phi = \Phi f\}$$

So A is just the centralizer of Φ in $\mathrm{GL}(V)$. Note that Φ may itself not be in $\mathrm{GL}(V)$, but it is at least in $\mathrm{End}_K(V)$.

Example 4.4. Let $k = \mathbb{R}, K = \mathbb{C}, V = \mathbb{R}^2$. Fix $\theta \in \mathbb{R}$, and let $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$ be the rotation through a angle θ about the origin, and assume $\theta \neq 0$ and $\theta \neq \pi$. That is, Φ is given by the following matrix in the standard basis $\{e_1 = (1, 0), e_2 = (0, 1)\}$ of $\mathbb{R}^2$.

$$\Phi = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \qquad \Phi\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{pmatrix}$$

Then $\Phi_{\mathbb{C}} : \mathbb{C}^2 \to \mathbb{C}^2$ is given by the same matrix in terms of the $\mathbb{C}$-basis $\{(1 \otimes 1, 0), (0, 1 \otimes 1)\}$ for $V_{\mathbb{C}}$. However, if instead we use the basis $\{e_1 \otimes 1 + e_2 \otimes i, e_1 \otimes 1 - e_2 \otimes i\}$ for $V_{\mathbb{C}}$, in terms of this basis $\Phi_{\mathbb{C}}$ has the matrix

$$\Phi_{\mathbb{C}} = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$$

(For an explicit calculation of this, see example 4.20 of my notes for my summer class on algebraic groups with Rajesh Kulkarni.) In these terms, a K-automorphism of (V, Φ) is $g \in \mathrm{GL}_2(\mathbb{C})$ which commutes with Φ. A quick calculation shows that the matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$$

commute if and only if $be^{i\theta} = be^{-i\theta}$ and $ce^{i\theta} = ce^{-i\theta}$. This only happens when $\theta = 0$ or $\theta = \pi$ or $b = c = 0$. Since we ruled out the first two to start, $b = c = 0$, which is to say, $g \in \mathrm{GL}_2(\mathbb{C})$ is a diagonal matrix. So we have an identification of A with $\mathbb{C}^{\times 2}$. Again, $\sigma \in G$ acts as usual on the $\mathbb{C}$-parts of A, so

$$H^0(G, A) = \mathbb{R}^{\times 2}$$

and using additivity of cohomology and Hilbert 90,

$$H^1(G, A) = H^1(G, \mathbb{C}^{\times 2}) = H^1(G, \mathbb{C}^\times) \oplus H^1(G, \mathbb{C}^\times) = 0 \oplus 0 = 0$$

I'm not sure if this is right.

4.5 Bilinear forms $(p, q) = (0, 2)$

In this case, Φ is a bilinear form $V \otimes V \to k$.

Example 4.5. Assume k does not have characteristic 2. Let $n = \dim V$ and Φ be a nondegenerate symmetric bilinear form on V. The $\mathrm{Aut}_K(\Phi)$ is the group $O_n(K)$ of orthogonal matrices with respect to Φ, and the correspondence says that there is a bijection

$$TF_K(V, \Phi) \cong H^1(G, O_n(K))$$

According to CSAGC example 2.3.5, "this bijection is important for the classification of quadratic forms."

Example 4.6. Let $k = \mathbb{R}, K = \mathbb{C}, V = \mathbb{R}^n$. The Galois group is $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. Let Φ be the usual dot product on $\mathbb{R}^n$.

$$\Phi : \mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{R}^n \to \mathbb{R} \qquad \Phi\left((x_1, \ldots, x_n) \otimes (y_1, \ldots, y_n)\right) = \sum_{i=1}^n x_i y_i$$

The extension of Φ to $\Phi_{\mathbb{C}} : \mathbb{C}^n \otimes_{\mathbb{C}} \mathbb{C}^n \to \mathbb{C}$ has the same formula as the above. The automorphism group $\mathrm{Aut}_{\mathbb{C}}(V, \Phi)$ is the orthogonal group $O_n(\mathbb{C})$.

$$O_n(\mathbb{C}) = \left\{x \in \mathrm{GL}_n(\mathbb{C}) : xx^t = 1\right\}$$

From the correspondence,

$$TF_{\mathbb{R}}(V, \Phi) \cong H^1(\mathbb{Z}/2\mathbb{Z}, O_n(\mathbb{C}))$$

It is known that over $\mathbb{C}$, all nondegenerate symmetric bilinear forms are equivalent to Φ. Hence the nondegenerate symmetric bilinear forms on $\mathbb{R}^n$ are classified by the cohomology group $H^1(G, O_n(\mathbb{C}))$.

4.6 Algebras $(p, q) = (1, 2)$

In this case, Φ is a multiplication map for a (possibly nonassociative) algebra on V.

$$\Phi : V \otimes V \to V$$

This is where our generalization to a family of tensors starts to play a useful role. Instead of arbitrary algebras, we would like to consider associative, unital, central, simple algebras. Therefore, in addition to the multiplication map, we need to include some other tensors on V which encode these properties. For the moment, we suppress any details of how to do this, but perhaps it will be included later. For now, we just assume that we can encode all of this data into a family of tensors without much trouble.

Example 4.7. Let K/k be a Galois extension with Galois group G. For this example, assume all algebras are associative, unital, central, and simple.

Let (V, Φ_i) be the k-algebra $M_n(k)$, where Φ_i includes a structure map for multiplication, along with some tensors to encode the fact that it is an associative, unital, central, simple algebra. Over K, it is $(V_K, (\Phi_i)_K) = M_n(K)$. So $TF_K(V, \Phi_i)$ is the k-isomorphism classes of central simple k-algebras which become isomorphic to $M_n(K)$ after tensoring up to K. These are precisely the central simple k-algebras of dimension n^2 which become isomorphic to $M_n(K)$ after extending scalars.

The automorphism group $\mathrm{Aut}_K(\Phi_i)$ is K-algebra automorphisms of $M_n(K)$. By the Skolem-Noether theorem, all such automorphisms are inner, so we may realize each such automorphism with an element of $\mathrm{GL}_n(K)$, which then acts on $M_n(K)$ by conjugation. Since any scalar matrix is central and acts trivially, this action factors through the quotient $\mathrm{PGL}_n(K)$. That is, $\mathrm{Aut}_K(\Phi_i) \cong \mathrm{PGL}_n(K)$. Using our main correspondence, we get

$$TF_K(V, \Phi_i) \cong H^1(G, \mathrm{PGL}_n(K))$$

This is used, for example in CSAGC, as motivation and construction of the relative Brauer group $\mathrm{Br}(K/k)$, and its identification with $H^2(G, K^\times)$. Without proof, we mention that

$$\mathrm{Br}(K/k) \cong H^1(G, \mathrm{PGL}_\infty)$$

This is mostly useful in the situation where $K = k^{\mathrm{sep}}$ is the separable closure, in which case we obtain the absolute Brauer group.

$$\mathrm{Br}(k) = \mathrm{Br}(k^{\mathrm{sep}}/k) \cong H^1(G, \mathrm{PGL}_\infty) \cong H^2(G, (k^{\mathrm{sep}\,\times}))$$

Note that here we are using profinite cohomology.

Example 4.8. Let k be a field with trivial Brauer group, for example, $k = \mathbb{F}_q$ a finite field with q elements. Let K/k be a Galois extension with Galois group G. Since $\mathrm{Br}(k) = 0$, the relative Brauer group $\mathrm{Br}(K/k)$ is also trivial. Let (V, Φ) be the k-algebra $M_n(k)$, where Φ encodes the multiplication map, and the fact that it is central simple (and unital and associative).

From the previous example, $TF_K(V, \Phi)$ consists of k-isomorphism classes of central simple k-algebras of dimension n^2, which represent Brauer classes of the relative Brauer group $\mathrm{Br}(K/k)$. Since this group is trivial, all such algebras are Brauer equivalent. Since they also all have the same dimension, they are all already k-isomorphic. So $TF_K(V, \Phi)$ is just one point. Using the correspondence, this tells us that

$$H^1(G, \mathrm{PGL}_n(K))$$

is trivial.

Example 4.9. For this entire example, all algebras are assumed to be associative, unital, central, and simple. Let $k = \mathbb{R}, K = \mathbb{C}$. Let (V, Φ) be the $\mathbb{R}$-algebra $M_2(\mathbb{R})$, and let (W, Ψ) be the Hamilton quaternion algebra. That is, $W = \mathbb{R}^4$ with basis $\{1, i, j, ij\}$ and multiplication

$$i^2 = j^2 = -1 \qquad ij = -ji$$

We know from the theory of central simple algebras and Brauer groups that after tensoring up to the separable closure $\mathbb{C}$, these algebras are isomorphic. That is to say, (W, Ψ) is a twisted $\mathbb{C}/\mathbb{R}$-form of (V, Φ). We also know that they are NOT isomorphic $\mathbb{R}$-algebras. Hence (W, Ψ) is a nontrivial twisted form of (V, Φ). So we know to expect $H^1(G, A) \neq 0$.

Let's try to describe $\mathrm{Aut}_K(\Phi)$. A K-automorphism of (V, Φ) is a $\mathbb{C}$-algebra automorphism of $M_2(\mathbb{C})$. By the Skolem-Noether theorem, every such automorphism is inner, which is to say, is of the form

$$M_2(\mathbb{C}) \to M_2(\mathbb{C}) \qquad x \mapsto gxg^{-1}$$

for some $g \in \mathrm{GL}_2(\mathbb{C})$. Since any scalar $g \in \mathrm{GL}_2(\mathbb{C})$ acts trivially, the action factors through the quotient $\mathrm{PGL}_2(\mathbb{C})$, hence we identity A with $\mathrm{PGL}_2(\mathbb{C})$. The Galois group $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}\langle\sigma\rangle$ acts on $M_2(\mathbb{C})$ entry-wise, so given $g \in \mathrm{GL}_2(\mathbb{C})$, ${}^\sigma g$ is the automorphism

$${}^\sigma g : M_2(\mathbb{C}) \to M_2(\mathbb{C}) \qquad x \mapsto \overline{g\overline{x}g^{-1}} = \overline{g}x\overline{g}^{-1}$$

Thus ${}^\sigma g = \overline{g}$, which is to say, G acts entry-wise on $A = \mathrm{PGL}_2(\mathbb{C})$. Now the question is, what can we say about $H^1(G, A)$ or $TF_K(V, \Phi)$? There is a relatively easy calculation of $H^1(G, A)$ in the case where G is cyclic and A is abelian, but in our situation A is not abelian.

Alternatively, perhaps we can use our knowledge of central simple algebras and the Brauer group to understand $TF_K(V, \Phi)$. A twisted form of $M_2(\mathbb{R})$ is a (unital, associative) central simple $\mathbb{R}$-algebra U such that $U \otimes_{\mathbb{R}} \mathbb{C} \cong M_2(\mathbb{C})$. Now we are in a position to use our full knowledge of the Brauer group. We know that $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$, which is to say, there are precisely two isomorphism classes of unital, associative, central $\mathbb{R}$-division algebras: $\mathbb{R}$ and the Hamilton quaternions. Combining this with Wedderburn's theorem, the only unital associative, central $\mathbb{R}$-algebras are $M_2(\mathbb{R})$ and the Hamilton quaternions. Hence $TF_K(V, \Phi)$ is a set with two elements, the distinct classes of (V, Φ) and (W, Ψ).

4.7 Descent for affine algebraic groups

4.7.1 Equivalence with Hopf algebras

The category of affine algebraic k groups is equivalent to the category of Hopf k-algebras, using spec.

$$\{\text{Hopf } k\text{-algebras}\} \xrightarrow{\text{spec}} \{\text{affine algebraic } k\text{-groups}\}$$

The quasi-inverse is given by taking global sections. Alternatively, thinking of affine algebraic k-groups as representable functors $\mathrm{Alg}_k \to \mathrm{Gp}$, every affine algebraic k-group has a representing algebra, and the multiplication and inversion maps induce a Hopf algebra structure on the representing algebra. Conversely, given a Hopf algebra A, the functor

$$G_A : \mathrm{Alg}_k \to \mathrm{Set} \qquad B \mapsto \mathrm{Hom}_k(A, B)$$

describes an algebraic k-group, using the Hopf algebra structure of A to make $\mathrm{Hom}_k(A, B)$ into a group.

4.7.2 Forms of algebraic groups

Definition 4.10. Let G be an affine algebraic k-group. Let K/k be an extension. A ***K/k*-form** of G is an algebraic group H such that $H_K \cong G_K$ as algebraic K-groups.

Definition 4.11. Let G be an affine algebraic k-group. The set of k-isomorphism classes of K/k-forms of G is denoted $TF_K(G)$.

4.7.3 Application of main correspondence

Let G be an affine algebraic k-group with representing Hopf k-algebra $\mathcal{O}_G$. Let K/k be a Galois extension (possibly infinite) with Galois group Γ. Let (V, Φ) be the Hopf algebra $\mathcal{O}_G$, where Φ is a family of tensors encoding multiplication, comultiplication, unit, counit, and antipode maps. Let $A = \mathrm{Aut}_K(\Phi)$. By the main correspondence, we have a basepoint preserving bijection

$$TF_K(\mathcal{O}_G) \cong H^1(\Gamma, A)$$

By our equivalence of categories, K-automorphisms of $(\mathcal{O}_G)_K$ which preserve Φ_K are in natural bijection with K-automorphisms of G_K as an algebraic K-group. Similarly, since the equivalence of categories commutes with extension of scalars, K/k-forms of $\mathcal{O}_G$ are in natural bijection with K/k-forms of G. So the bijection above turns into

$$TF_K(G) \cong H^1(\Gamma, \mathrm{Aut}_K(G_K))$$

There is probably some amount of details to check regarding how naturality supports this assertion, but this does not interest me at this time.

Example 4.12. Let K be a field with $\mathrm{char}\, K \neq 2$, and let L/K be a quadratic extension, so $L = K(\sqrt{c})$ for some non-square $c \in K^\times$. The Galois group is then $\Gamma = \mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$, and we let σ be the generator/unique nontrivial element. Let $G = \mathbb{G}_m$, viewed as an algebraic K-group. The twisted L/K forms of G are classified by cohomology using our main correspondence.

$$TF_L(G) \cong H^1\left(\Gamma, \mathrm{Aut}_L(G_L)\right)$$

The L-automorphisms of $G_L = (\mathbb{G}_m)_L = \mathbb{G}_m$ are just the power maps, so $\mathrm{Aut}_L(G_L) \cong \mathbb{Z}$. The Galois group action on this copy of $\mathbb{Z}$ is determined by how σ acts. The only possibilities are that it act by $+1$ or -1. I claim that σ acts as -1. Let $\alpha_n \in \mathrm{Aut}_L(G_L)$ be the nth power map, $x \mapsto x^n$. The Γ-action is given by by conjugating.

$$\sigma \cdot \alpha_n = (1 \otimes \sigma) \circ \alpha_n \circ (1 \otimes \sigma)^{-1} \in \mathrm{Aut}_L(G_L)$$

Let's just look at the action on K-points of G_L, which is $L^\times$. Let $x \in G_L(K) = L^\times$, and write x as $x = a + b\sqrt{c}$, with $a, b \in K$. Then $\sigma x = a - b\sqrt{c}$. Note that $\sigma = \sigma^{-1}$.

$$(\sigma \cdot \alpha_n)(x) = \sigma \alpha_n \sigma^{-1}(x) = \sigma \alpha_n (a - b\sqrt{c}) = \sigma (a - b\sqrt{c})^n = \sigma\left(a^n - a^{n-1} b\sqrt{c} + \cdots + (-1)^n b\sqrt{c}\right)$$

When σ is applied to this, it changes all of the $\sqrt{c}$ terms by a sign, but this does is not equal to $\alpha_n(x) = (a + b\sqrt{c})^n$, in general. So σ does not act as the identity, hence it must act as -1. So we get the cohomology group $H^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z})$ with nontrivial action. By a standard calculation of cohomology for cyclic groups, this is

$$H^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \cong \ker N / (\sigma - 1)\mathbb{Z}$$

where $N : \mathbb{Z} \to \mathbb{Z}$ is the norm map, which in this case is is the map $1 + \sigma = 0$, so

$$H^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$$

Thus there are precisely two K-isomorphism classes of twisted forms of $\mathbb{G}_m$. One is $\mathbb{G}_m$ itself. The other is the norm torus, which we describe more explicitly via twisting in the next example.

Example 4.13. [6] Let L/K be a quadratic extension in char $\neq 2$, $L = K(\sqrt{c}), \Gamma = \mathrm{Gal}(L/K)$ as above, with σ the generator (and only nontrivial element) of Γ. Let $G = \mathbb{G}_m$, viewed as a K-group. The extension of G to L is $(\mathbb{G}_m)_L$.

$$G_L = (\mathbb{G}_m)_L$$

The corresponding Hopf algebra is Laurent polynomials over K in one variable, and extending to L just gives Laurent polynomials over K.

$$\begin{aligned} \mathcal{O}_G &= K[t, t^{-1}] \\ \mathcal{O}_{G_L} &= L[t, t^{-1}] \end{aligned}$$

Let $V = \mathcal{O}_G, V_L = \mathcal{O}_{G_L}$ and let $A = \mathrm{Aut}_L(G_L) \cong \mathrm{Aut}_L(\mathcal{O}_{G_L})$. The Galois action of Γ on V_L is by acting on the L-coefficients.

$$\Gamma \times V_L \to V_L \qquad \tau\left(\sum a_n t^n\right) = \sum \tau(a_n) t^n \qquad \tau \in \Gamma$$

From the previous example, we know that $H^1(\Gamma, A)$ has exactly one nontrivial cohomology class, so let us describe it in terms of an explicit cocycle. Define a cocycle $a \in Z^1(\Gamma, A)$ by

$$a : \Gamma \to A \qquad a_e = \mathrm{Id} \qquad a_\sigma = \mathrm{Inv}$$

where Inv is the inversion map on G_L, or alternatively the map $t \mapsto t^{-1}$ on $\mathcal{O}_{G_L}$. Now let's construct the twisted algebra associated to the cocycle a. The twisted action of Γ on ${}_aV_L$ is

$$\Gamma \times {}_aV_L \to {}_aV_L \qquad \tau * f = a_\tau(\tau f)$$

This is only interesting when $\tau = \sigma$, so we describe that even more explicitly.

$$\sigma * f = a_\sigma(\sigma f) = \mathrm{Inv}(\sigma f) = \sigma f(t^{-1})$$

Then we take the Γ-invariants of the action to get our twisted form. To be fixed by Γ, it is enough to be fixed by σ.

$$\begin{aligned} W &= ({}_aV_L)^\Gamma \\ &= \left\{ f \in L[t, t^{-1}] : f(t) = \sigma * f(t) = \sigma f(t^{-1}) \right\} \\ &= \left\{ \sum_{n \in \mathbb{Z}} a_n t^n : a_n = \sigma(a_{-n}), \forall n \in \mathbb{Z} \right\} \end{aligned}$$

We can describe W even better than this using the following isomorphism. Recall that $L = K(\sqrt{c})$. Define

$$L[u, v] \to W \qquad u \mapsto \frac{t + t^{-1}}{2} \qquad v \mapsto \frac{t - t^{-1}}{2\sqrt{c}}$$

[6] Copied from example 1 on pages 69-69 of Platonov-Rapinchuk.

We claim this is a surjection of L-algebras whose kernel is the principal ideal $(u^2 - cv^2 - 1)$. There is nothing to check regarding being a map of L-algebras, since we have only defined it on L-algebra generators, and it clearly lands in W.

It's not hard to see that this is surjective, since W is generated by elements of the form $t + t^{-1}$ and $t - \sqrt{c}t^{-1}$, which are just scalar multiples of the images of u, v. The fact that $u^2 - cv^2 - 1$ lies in the kernel is just a calculation.

$$\begin{aligned}\left(\frac{t+t^{-1}}{2}\right)^2 - c\left(\frac{t-t^{-1}}{2\sqrt{c}}\right)^2 - 1 &= \left(\frac{t^2+2+t^{-2}}{4}\right) - c\left(\frac{t^2-2+t^{-2}}{4c}\right) - 1\\ &= \frac{t^2+2+t^{-2}-t^2+2-t^{-2}}{4} - 1 = \frac{4}{4} - 1 = 0\end{aligned}$$

We omit justification that the kernel is generated by $u^2 - cv^2 - 1$, but it is. Hence by the 1st isomorphism theorem, the mapping above induces an isomorphism (of L-algebras)

$$W \cong {}^{L[u,v]}\!\diagup_{(u^2 - cv^2 - 1)}$$

Remember what we were doing - we started with the algebraic K-group $\mathbb{G}_m$, translated to the associated Hopf algebra V, and extended scalars to V_L. Then we twisted the Γ-action and took Γ-invariants to obtain a twisted K-algebra W, which is an L/K-form of V. So if we translate the Hopf algebra W back to an algebraic K-group, we obtain a twisted L/K-form of $\mathbb{G}_m$. That is, we have the algebraic K-group

$$H = \operatorname{spec} W$$

which is an L/K-twisted form of $\mathbb{G}_m$. To be more precise, the K-points of H are the following subgroup of $\mathrm{SL}_2(L)$.

$$H(L) \cong \left\{ \begin{pmatrix} u & vc \\ v & u \end{pmatrix} : u, v \in L, u^2 - cv^2 = 1 \right\} \subset \mathrm{SL}_2(L)$$

The group H is better known as the norm torus $R_{L/K}\mathbb{G}_m$. As H is an L/K-twisted form of $\mathbb{G}_m$, the L-points of H are the same as the L-points of $\mathbb{G}_m$.

$$H(L) \cong \mathbb{G}_m(L) = L^\times$$

5 Appendix

5.1 A very long computational lemma

Lemma 5.1. *Let $K/k, G, (V, \Phi), \alpha, aW, f, \widetilde{\Phi}_K$ be as in definition 3.37. For $\sigma \in G$, $\sigma \cdot \widetilde{\Phi}_K = \widetilde{\Phi}_K$, hence it descends to a k-tensor Ψ on W.*

Proof. As in definition 3.36, fix a k-basis $\{e_i\}$ of V and a k-basis $\{w_j\}$ of W so that $\{w_j\}$ is also a K-basis of V_K. Let $\lambda_{ij}, \gamma_{ij}$ be as in that definition as well, that is, the transition coefficients between the K-bases $\{w_j\}$ and $\{e_i \otimes 1\}$ of V_K.

$$w_j = \sum_i e_i \otimes \lambda_{ij} \qquad e_i \otimes 1 = \sum_j \gamma_{ij} w_j$$

Also we know that $\Phi : V^{\otimes q} \to V^{\otimes p}$ is determined by the images of the basis elements $e_{i_1} \otimes \cdots \otimes e_{i_q}$. Let's just name the coefficients involved in the image. That is, for $(\ell_1, \ldots, \ell_p)$ with $1 \leq \ell_i \leq \dim_k V$, define $\phi_{(\ell_1,\ldots,\ell_p)} \in k$ by

$$\Phi(e_{i_1} \otimes \cdots \otimes e_{i_q}) = \sum_{(\ell_1,\ldots,\ell_p)} \phi_{(\ell_1,\ldots,\ell_p)}(e_{\ell_1} \otimes \cdots \otimes e_{\ell_p})$$

Let $\sigma \in G$. Then

$$\sigma \cdot \widetilde{\Phi}_K = (1 \otimes \sigma)^{\otimes p} \circ \widetilde{\Phi}_K \circ (1 \otimes \sigma^{-1})^{\otimes q} = (1 \otimes \sigma)^{\otimes p} \circ (f^{-1})^{\otimes p} \circ \Phi_K \circ f^{\otimes q} \circ (1 \otimes \sigma^{-1})^{\otimes q}$$

It suffices to verify that $\sigma \cdot \widetilde{\Phi}_K = \widetilde{\Phi}_K$ on simple tensors in $(W_K)^{\otimes q}$, so take such a simple tensor.

$$\widetilde{x} = x^1 \otimes x^2 \otimes \cdots \otimes x^q \in (W_K)^{\otimes q}$$

Write each x^k as

$$x^k = \sum_{j_k} \left(\sum_{i_k} e_{i_k} \otimes \lambda_{(i_k,j_k)} \right) \otimes x_{j_k}$$

Let's start by applying $\widetilde{\Phi}_K$ to $\widetilde{x}$.

$$\begin{aligned}
\widetilde{\Phi}_K(\widetilde{x}) &= (f^{-1})^{\otimes p} \circ \Phi_K \circ f^{\otimes q} \left(x^1 \otimes \cdots \otimes x^q\right) \\
&= (f^{-1})^{\otimes p} \circ \Phi_K \circ f^{\otimes q} \left(\cdots \otimes \left(\sum_{j_k} \left(\sum_{i_k} e_{i_k} \otimes \lambda_{(i_k,j_k)}\right) \otimes x_{j_k}\right) \otimes \cdots\right) \\
&= (f^{-1})^{\otimes p} \circ \Phi_K \left(\cdots \otimes \left(\sum_{i_k,j_k} e_{i_k} \otimes x_{j_k} \lambda_{(i_k,j_k)}\right) \otimes \cdots\right) \\
&= (f^{-1})^{\otimes p} \circ \Phi_K \left(\sum_{\substack{(i_1,\ldots,i_q)\\(j_1,\ldots,j_q)}} \left(\cdots \otimes \left(e_{i_k} \otimes x_{j_k} \lambda_{(i_k,j_k)}\right) \otimes \cdots\right)\right) \\
&= (f^{-1})^{\otimes p} \left(\sum_{\substack{(i_1,\ldots,i_q)\\(j_1,\ldots,j_q)}} \Phi_K \Big(\cdots \otimes \left(e_{i_k} \otimes x_{j_k} \lambda_{(i_k,j_k)}\right) \otimes \cdots\Big)\right) \\
&= (f^{-1})^{\otimes p} \left(\sum_{\substack{(i_1,\ldots,i_q)\\(j_1,\ldots,j_q)}} \left(\prod_{k=1}^{q} x_{j_k} \lambda_{(i_k,j_k)}\right) \Phi\Big(\cdots \otimes e_{i_k} \otimes \cdots\Big)\right) \\
&= (f^{-1})^{\otimes p} \left(\sum_{\substack{(i_1,\ldots,i_q)\\(j_1,\ldots,j_q)}} \left(\prod_{k=1}^{q} x_{j_k} \lambda_{(i_k,j_k)}\right) \sum_{(\ell_1,\ldots,\ell_p)} \phi_{(\ell_1,\ldots,\ell_p)}(\cdots \otimes e_{\ell_k} \otimes \cdots)\right) \\
&= (f^{-1})^{\otimes p} \left(\sum_{\substack{(i_1,\ldots,i_q)\\(j_1,\ldots,j_q)\\(\ell_1,\ldots,\ell_p)}} \left(\prod_{k=1}^{q} x_{j_k} \lambda_{(i_k,j_k)}\right) \phi_{(\ell_1,\ldots,\ell_p)}(\cdots \otimes e_{\ell_k} \otimes \cdots)\right) \\
&= \sum_{\substack{(i_1,\ldots,i_q)\\(j_1,\ldots,j_q)\\(\ell_1,\ldots,\ell_p)}} \left(\prod_{k=1}^{q} x_{j_k} \lambda_{(i_k,j_k)}\right) \phi_{(\ell_1,\ldots,\ell_p)} \left(\cdots \otimes \left(\sum_{m_k} w_{m_k} \otimes \gamma_{(\ell_k,m_k)}\right) \otimes \cdots\right)
\end{aligned}$$

$$= \sum_{\substack{(i_1,\dots,i_q)\\(j_1,\dots,j_q)\\(\ell_1,\dots,\ell_p)}} \left(\prod_{k=1}^{q} x_{j_k}\lambda_{(i_k,j_k)}\right)\phi_{(\ell_1,\dots,\ell_p)}\left(\sum_{(m_1,\dots,m_p)}\left(\cdots\otimes\left(w_{m_k}\otimes\gamma_{(\ell_k,m_k)}\right)\otimes\cdots\right)\right)$$

$$= \sum_{\substack{(i_1,\dots,i_q)\\(j_1,\dots,j_q)\\(\ell_1,\dots,\ell_p)\\(m_1,\dots,m_p)}} \left(\prod_{k=1}^{q} x_{j_k}\lambda_{(i_k,j_k)}\right)\phi_{(\ell_1,\dots,\ell_p)}\left(\cdots\otimes\left(w_{m_k}\otimes\gamma_{(\ell_k,m_k)}\right)\otimes\cdots\right)$$

$$= \sum_{\substack{(i_1,\dots,i_q)\\(j_1,\dots,j_q)\\(\ell_1,\dots,\ell_p)\\(m_1,\dots,m_p)}} \left(\prod_{k=1}^{q} x_{j_k}\lambda_{(i_k,j_k)}\gamma_{(\ell_k m_k)}\right)\phi_{(\ell_1,\dots,\ell_p)}\left(\cdots\otimes\left(w_{m_k}\otimes 1\right)\otimes\cdots\right)$$

On the other hand, when we apply $\sigma\cdot\widetilde{\Phi}_K$ to $\widetilde{x}$, we get something slightly different, with σ acting on some of the λ and γ coefficients.

$$\begin{aligned}
\sigma\cdot\widetilde{\Phi}_K(\widetilde{x}) &= (1\otimes\sigma)^{\otimes p}\circ(f^{-1})^{\otimes p}\circ\Phi_K\circ f^{\otimes q}\circ(1\otimes\sigma^{-1})^{\otimes q}\left(x^1\otimes\cdots\otimes x^q\right)\\
&= (1\otimes\sigma)^{\otimes p}\circ(f^{-1})^{\otimes p}\circ\Phi_K\circ f^{\otimes q}\left(\cdots\otimes\left(\sum_{j_k}\left(\sum_{i_k} e_{i_k}\otimes\lambda_{(i_k,j_k)}\right)\otimes\sigma^{-1}(x_{j_k})\right)\otimes\cdots\right)\\
&= (1\otimes\sigma)^{\otimes p}\circ(f^{-1})^{\otimes p}\circ\Phi_K\left(\cdots\otimes\left(\sum_{i_k,j_k} e_{i_k}\otimes\sigma^{-1}(x_{j_k})\lambda_{(i_k,j_k)}\right)\otimes\cdots\right)\\
&= (1\otimes\sigma)^{\otimes p}\circ(f^{-1})^{\otimes p}\circ\Phi_K\left(\sum_{\substack{(i_1,\dots,i_k)\\(j_1,\dots,j_k)}}\left(\cdots\otimes\left(e_{i_k}\otimes\sigma^{-1}(x_{j_k})\lambda_{(i_k,j_k)}\right)\otimes\cdots\right)\right)\\
&= (1\otimes\sigma)^{\otimes p}\circ(f^{-1})^{\otimes p}\left(\sum_{\substack{(i_1,\dots,i_q)\\(j_1,\dots,j_q)}}\Phi_K\Big(\cdots\otimes\left(e_{i_k}\otimes\sigma^{-1}(x_{j_k})\lambda_{(i_k,j_k)}\right)\otimes\cdots\Big)\right)\\
&= (1\otimes\sigma)^{\otimes p}\circ(f^{-1})^{\otimes p}\left(\sum_{\substack{(i_1,\dots,i_q)\\(j_1,\dots,j_q)}}\left(\prod_{k=1}^{q}\sigma^{-1}(x_{j_k})\lambda_{(i_k,j_k)}\right)\Phi\Big(\cdots\otimes e_{i_k}\otimes\cdots\Big)\right)\\
&= (1\otimes\sigma)^{\otimes p}\circ(f^{-1})^{\otimes p}\left(\sum_{\substack{(i_1,\dots,i_q)\\(j_1,\dots,j_q)}}\left(\prod_{k=1}^{q}\sigma^{-1}(x_{j_k})\lambda_{(i_k,j_k)}\right)\sum_{(\ell_1,\dots,\ell_p)}\phi_{(\ell_1,\dots,\ell_p)}(\cdots\otimes e_{\ell_k}\otimes\cdots)\right)
\end{aligned}$$

$$= (1 \otimes \sigma)^{\otimes p} \circ (f^{-1})^{\otimes p} \left(\sum_{\substack{(i_1,\ldots,i_q) \\ (j_1,\ldots,j_q) \\ (\ell_1,\ldots,\ell_p)}} \left(\prod_{k=1}^{q} \sigma^{-1}(x_{j_k}) \lambda_{(i_k,j_k)} \right) \phi_{(\ell_1,\ldots,\ell_p)}(\cdots \otimes e_{\ell_k} \otimes \cdots) \right)$$

$$= (1 \otimes \sigma)^{\otimes p} \left(\sum_{\substack{(i_1,\ldots,i_q) \\ (j_1,\ldots,j_q) \\ (\ell_1,\ldots,\ell_p)}} \left(\prod_{k=1}^{q} \sigma^{-1}(x_{j_k}) \lambda_{(i_k,j_k)} \right) \phi_{(\ell_1,\ldots,\ell_p)}(\cdots \otimes f^{-1} e_{\ell_k} \otimes \cdots) \right)$$

Recall from previous work that we can describe f^{-1} by

$$f^{-1}(e_{\ell_k}) = \sum_{m_k} w_{m_k} \otimes \gamma_{(\ell_k,m_k)}$$

So continuing our calculation,

$$\sigma \cdot \widetilde{\Phi}_K(\widetilde{x}) = (1 \otimes \sigma)^{\otimes p} \left(\sum_{\substack{(i_1,\ldots,i_q) \\ (j_1,\ldots,j_q) \\ (\ell_1,\ldots,\ell_p)}} \left(\prod_{k=1}^{q} \sigma^{-1}(x_{j_k}) \lambda_{(i_k,j_k)} \right) \phi_{(\ell_1,\ldots,\ell_p)}(\cdots \otimes f^{-1} e_{\ell_k} \otimes \cdots) \right)$$

$$= (1 \otimes \sigma)^{\otimes p} \left(\sum_{\substack{(i_1,\ldots,i_q) \\ (j_1,\ldots,j_q) \\ (\ell_1,\ldots,\ell_p)}} \left(\prod_{k=1}^{q} \sigma^{-1}(x_{j_k}) \lambda_{(i_k,j_k)} \right) \phi_{(\ell_1,\ldots,\ell_p)} \left(\cdots \otimes \left(\sum_{m_k} w_{m_k} \otimes \gamma_{(\ell_k,m_k)} \right) \otimes \cdots \right) \right)$$

$$= (1 \otimes \sigma)^{\otimes p} \left(\sum_{\substack{(i_1,\ldots,i_q) \\ (j_1,\ldots,j_q) \\ (\ell_1,\ldots,\ell_p)}} \left(\prod_{k=1}^{q} \sigma^{-1}(x_{j_k}) \lambda_{(i_k,j_k)} \right) \phi_{(\ell_1,\ldots,\ell_p)} \left(\sum_{(m_1,\ldots,m_p)} \left(\cdots \otimes \left(w_{m_k} \otimes \gamma_{(\ell_k,m_k)} \right) \otimes \cdots \right) \right) \right)$$

$$= (1 \otimes \sigma)^{\otimes p} \left(\sum_{\substack{(i_1,\ldots,i_q) \\ (j_1,\ldots,j_q) \\ (\ell_1,\ldots,\ell_p) \\ (m_1,\ldots,m_p)}} \left(\prod_{k=1}^{q} \sigma^{-1}(x_{j_k}) \lambda_{(i_k,j_k)} \right) \phi_{(\ell_1,\ldots,\ell_p)} \left(\cdots \otimes \left(w_{m_k} \otimes \gamma_{(\ell_k,m_k)} \right) \otimes \cdots \right) \right)$$

$$= \sum_{\substack{(i_1,\ldots,i_q)\\(j_1,\ldots,j_q)\\(\ell_1,\ldots,\ell_p)\\(m_1,\ldots,m_p)}} \left(\prod_{k=1}^{q} \sigma\sigma^{-1}(x_{j_k})\sigma(\lambda_{(i_k,j_k)})\right) \phi_{(\ell_1,\ldots,\ell_p)} \left(\cdots \otimes \left(w_{m_k} \otimes \sigma(\gamma_{(\ell_k,m_k)})\right) \otimes \cdots\right)$$

$$= \sum_{\substack{(i_1,\ldots,i_q)\\(j_1,\ldots,j_q)\\(\ell_1,\ldots,\ell_p)\\(m_1,\ldots,m_p)}} \left(\prod_{k=1}^{q} x_{j_k}\sigma(\lambda_{(i_k,j_k)})\right) \phi_{(\ell_1,\ldots,\ell_p)} \left(\cdots \otimes \left(w_{m_k} \otimes \sigma(\gamma_{(\ell_k,m_k)})\right) \otimes \cdots\right)$$

$$= \sum_{\substack{(i_1,\ldots,i_q)\\(j_1,\ldots,j_q)\\(\ell_1,\ldots,\ell_p)\\(m_1,\ldots,m_p)}} \left(\prod_{k=1}^{q} x_{j_k}\sigma(\lambda_{(i_k,j_k)}\gamma_{(\ell_k,m_k)})\right) \phi_{(\ell_1,\ldots,\ell_p)} \left(\cdots \otimes (w_{m_k} \otimes 1) \otimes \cdots\right)$$

Let's compare this side to side.

$$\widetilde{\Phi}_K(\widetilde{x}) = \sum_{\substack{(i_1,\ldots,i_q)\\(j_1,\ldots,j_q)\\(\ell_1,\ldots,\ell_p)\\(m_1,\ldots,m_p)}} \left(\prod_{k=1}^{q} x_{j_k}\lambda_{(i_k,j_k)}\gamma_{(\ell_k m_k)}\right) \phi_{(\ell_1,\ldots,\ell_p)} \left(\cdots \otimes (w_{m_k} \otimes 1) \otimes \cdots\right)$$

$$\sigma \cdot \widetilde{\Phi}_K(\widetilde{x}) = \sum_{\substack{(i_1,\ldots,i_q)\\(j_1,\ldots,j_q)\\(\ell_1,\ldots,\ell_p)\\(m_1,\ldots,m_p)}} \left(\prod_{k=1}^{q} x_{j_k}\sigma(\lambda_{(i_k,j_k)}\gamma_{(\ell_k,m_k)})\right) \phi_{(\ell_1,\ldots,\ell_p)} \left(\cdots \otimes (w_{m_k} \otimes 1) \otimes \cdots\right)$$

These are equal if σ acts trivially on the λ, γ coefficients. These lie in K, so in general this does not happen. However, recall that (λ_{ij}) and (γ_{ij}) are inverse transition matrices by definition, and in the sums/products above, we're basically multiplying those transition matrices together. Whether we apply σ before or after multiplying the transition matrices, the resulting matrix is the idenity, and all of the entries in that matrix are in k, hence fixed by σ. So the two expressions above should be equal, hence $\widetilde{\Phi}_K$ descends to a k-tensor on W. $\square$