Twists

Zock, H.J.

H.J. Zock
zockhugo@gmail.com

Twists

Bachelor thesis

July 4, 2022

Thesis supervisor: prof.dr. R.M. van Luijk

Leiden University
Mathematical Institute

Contents

1 Introduction

Mathematical objects often come with an associated base field k. Examples include vector spaces over k, algebras over k, schemes over k, and elliptic curves over k. If K/k is a field extension and X is an object over k, then we say that an object Y over k is a K/k-twist of X if X and Y "become isomorphic" over K. If Y is in addition not isomorphic to X over the base field k, then we say that Y is a nontrivial twist of X. By studying such twists we can get a grip on the arithmetic of the base field k.

Example 1.1. Consider the conic $C \subset \mathbb{P}^2_{\mathbb{R}}$ given by the equation $x^2 + y^2 + z^2 = 0$ over the field of real numbers $\mathbb{R}$. After extending our base field from the real numbers to the field of complex numbers $\mathbb{C}$, the conic C has a point over the base field, which implies that C is isomorphic to the complex projective line $\mathbb{P}^1_{\mathbb{C}}$. The field $\mathbb{R}$ fails to provide us with a point on C, and so C is a nontrivial twist of the real projective line $\mathbb{P}^1_{\mathbb{R}}$.

The goal of this thesis is to understand the K/k-twists of a given object X over k, when K/k is a Galois extension, using the theory of Galois cohomology introduced in sections 2 and 3. For many classes of objects, we can parameterize the K/k-twists in terms of the first cohomology set of $\mathrm{Gal}(K/k)$ with coefficients in $\mathrm{Aut}_K(X)$, denoted $H^1(K/k, \mathrm{Aut}_K(X))$. Theorem 5.5 makes this precise. One should also think of $H^1(K/k, \mathrm{Aut}_K(X))$ as the object that contains the obstruction preventing K-isomorphisms from descending to isomorphisms over k, and so this gives information about the arithmetic of k.

The "general principle" of parameterizing K/k-twists of a k-object X in terms of $H^1(K/k, \mathrm{Aut}_K(X))$ is well known. See, for instance, [Ser97, Chapter 3] or [Bru09]. Our treatment of the subject differs from these texts, as we build a general framework in which such a parameterization is possible. This is done through the notion of a base extension introduced in Section 4.

In Section 6 we apply the theory of twists to study Severi-Brauer varieties; these are twists of projective spaces. We have already seen an example above. Section 7 treats central simple algebras, which are twists of matrix algebras. These objects share a close connection, because the automorphism groups of $M_n(K)$ and $\mathbb{P}^{n-1}_K$, with $n > 0$ an integer, coincide. Specifically, this group is $\mathrm{PGL}_n(K)$. The parameterization of these objects in terms of $H^1(K/k, \mathrm{PGL}_n(K))$ will give us a correspondence between Severi-Brauer varieties and central simple algebras.

This thesis is concluded with the introduction of the Brauer group in Section 8. This group contains information regarding central simple algebras and Severi-Brauer varieties. Using Galois cohomology, we will derive some basic results and perform some calculations about Brauer groups.

From the reader we expect familiarity with basic algebra, in particular (infinite) Galois theory (see, for instance, [Lan02, Chapter VI]). Basic scheme theory is used in sections 4 and 6, as can for instance be found in [Har10, Chapter 2]. Familiarity with only the basic theory of varieties (over fields which are perhaps not algebraically closed), as in [Sil13, Chapter 1], will be sufficient if the reader is fine with taking some results in Section 4 for granted. Knowledge of category theory including limits and adjunctions, as can be found in [Rie17], is assumed. To build up the theory of Galois cohomology in sections 2 and 3, we make extensive use of the

material in Appendix A on homological algebra. We take a rather abstract approach to Galois cohomology, using the theory of derived functors. This is not only "the correct approach", but will also be crucial for calculations in Section 8. However, much of the material in sections 4 through 7 only depends on Section 3.4 on nonabelian cohomology, which can be read independently from the other material on Galois cohomology, if the reader does not mind a lack of motivation behind the definitions and results.

2 Cohomology of groups

Much of the material in this section is based on [Wei13, Chapter 6] and [Mil20, Chapter 2]. Throughout this section we fix a group G.

2.1 The category of G-modules

Definition 2.1 (G-modules)**.** *A G-module is an abelian group A equipped with a G-action $G \to \mathrm{Aut}(A)$. A G-map, or a map of G-modules, is a homomorphism $\varphi\colon A \to B$ such that φ is G-equivariant: we have*

$$\varphi(\sigma a) = \sigma\varphi(a)$$

for all $\sigma \in G$ and $a \in A$. The category of G-modules is denoted G-Mod.

Note that providing an abelian group with a G-action, is the same as providing it with the structure of a $\mathbb{Z}G$-module, where $\mathbb{Z}G$ is the group ring given by

$$\mathbb{Z}G = \left\{ \sum_{\sigma\in G} c_\sigma \sigma \quad : \quad c_\sigma \in \mathbb{Z} \text{ zero for all but finitely many } \sigma \in G \right\},$$

with evident addition and multiplication. The categories G-Mod and $\mathbb{Z}G$-mod are isomorphic, and so the category of G-modules is abelian. In particular, the category of G-modules has enough projective and injective objects (see Example A.21 and Proposition A.23).

Example 2.2. *(i) Any abelian group is a G-module if G is the trivial group.*

(ii) $\mathbb{Z}$ is a G-module by letting G act trivially on $\mathbb{Z}$.

(iii) Suppose G is the group $\mathbb{Z}^\times = \{\pm 1\}$. For any integer $n \geq 1$ we equip $\mathbb{Z}/n\mathbb{Z}$ with a G-action by setting $\sigma \cdot a = \sigma a$ for $\sigma \in \{\pm 1\}$ and $a \in \mathbb{Z}/n\mathbb{Z}$.

There is an evident forgetful functor

$$G\text{-Mod} \to \mathrm{Ab}.$$

This functor admits a right adjoint given by $\mathrm{Hom}_{\mathrm{Ab}}(\mathbb{Z}G, -)$ (see [Wei13, Proposition 2.6.3]); if M is an abelian group, then G acts on $\mathrm{Hom}_{\mathrm{Ab}}(\mathbb{Z}G, M)$ by

$$(\sigma\varphi)(x) = \varphi(x\sigma),$$

for $\sigma \in G$ and $\varphi \in \mathrm{Hom}_{\mathrm{Ab}}(\mathbb{Z}G, M)$. We abreviate the functor $\mathrm{Hom}_{\mathrm{Ab}}(\mathbb{Z}G, -)$ with the following definition.

Definition 2.3. *We define the functor* $\mathrm{ind}^G\colon \mathrm{Ab} \to G\text{-Mod}$ *by* $\mathrm{ind}^G = \mathrm{Hom}_{\mathrm{Ab}}(\mathbb{Z}G, -)$. *If M is an abelian group, then we call* $\mathrm{ind}^G M$ *a G-induced module, or simply an induced module.*

In the above definition, we often omit the superscript G from ind^G and simply write ind.

Remark 2.4. What we call induced modules are often referred to as coinduced modules in the literature, where the word "induced module" is reserved for modules of the form $M \otimes_{\mathbb{Z}} \mathbb{Z}G$. When G is finite these notions actually coincide. See [Wei13, Lemma 6.3.4].

Proposition 2.5. *The functor* ind *is exact and preserves injective objects.*

Proof. Exactness follows from the fact that $\mathbb{Z}G$ is free as an abelian group. The functor ind preserves injectives, because it is a right adjoint to the exact forgetful functor $G\text{-Mod} \to \mathrm{Ab}$. ■

2.2 Cohomology groups

Fix a G-module A. We denote the subset of A of elements invariant under the action of G by

$$A^G = \{a \in A : \sigma a = a \text{ for all } \sigma \in G\}.$$

It is straightforward to check that A^G is a subgroup of A. Any map of G-modules induces a map on invariants by restriction. In this way we get a functor

$$(-)^G\colon G\text{-Mod} \to \mathrm{Ab}.$$

Remark 2.6. Equip $\mathbb{Z}$ with the trivial G-action. We note that there is an isomorphism $(-)^G \simeq \mathrm{Hom}_G(\mathbb{Z}, -)$, given on G-modules A by sending $a \in A^G$ to the map $\mathbb{Z} \to A, 1 \mapsto a$.

By the above remark and Proposition A.8 we immediately get the following result.

Proposition 2.7. *The functor $(-)^G$ is left exact.*

In general, $(-)^G$ need not be right exact.

Example 2.8. Let G be the group of order 2 and equip $\mathbb{Z}/n\mathbb{Z}$ with the G-action of Example 2.2. We consider the short exact sequence of G-modules

$$0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{\cdot 4} \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to 0.$$

Taking invariants yields the exact sequence

$$0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{\cdot 4} 4\mathbb{Z}/8\mathbb{Z} \xrightarrow{0} 2\mathbb{Z}/4\mathbb{Z},$$

which is clearly not short exact.

Since the category of G-modules has enough injectives, it is now sensible to consider the right derived functors of $(-)^G$ (see Section A.5), which is precisely how we define our cohomology groups.

Definition 2.9 (cohomology groups)**.** *For all integers $n \geq 0$ we define the functor $H^n(G;-)\colon G\text{-Mod} \to \text{Ab}$ by*

$$H^n(G;-) = R^n(-)^G,$$

the n-th right derived functor of $(-)^G$. We call $H^n(G;A)$ the n-th cohomology group of G with coefficients in A.

Example 2.10. Suppose G is the trivial group. Then taking invariants is simply the identity functor. As a result we have

$$H^n(1;-) = 0$$

for $n > 0$.

Lemma 2.11. *Let M be an abelian group. We have a natural isomorphism $M \simeq (\operatorname{ind} M)^G$ of abelian groups given by*

$$\begin{aligned} M &\xrightarrow{\simeq} (\operatorname{ind} M)^G \\ m &\mapsto (\sigma \mapsto m). \end{aligned}$$

Proof. Clearly this is an injective map of abelian groups. Let $\varphi \in (\operatorname{ind} M)^G$. Then for all $\sigma \in G$ we have

$$\varphi(\sigma) = (\sigma\varphi)(1) = \varphi(1),$$

and hence the map described in the lemma is surjective. Naturality is straightforward. ∎

Proposition 2.12 (cohomology of induced modules)**.** *Suppose A is an induced G-module. Then*

$$H^n(G;A) = 0$$

for $n > 0$.

Proof. Let M be an abelian group such that $A = \operatorname{ind} M$. Let $0 \to M \to I^*$ be an injective resolution in Ab. Then $0 \to A \to \operatorname{ind} I^*$ is an injective resolution for A by Proposition 2.5. The group of invariants of $\operatorname{ind} I^i$ under G is naturally isomorphic to I^i by Lemma 2.11, and so for $n > 0$ we find

$$H^n(G;A) = H^n((\operatorname{ind} I^*)^G) = H^n(I^*) = 0.$$

∎

Remark 2.13. Proposition 2.12 is a special case of a more general statement, known as Shapiro's lemma. See [Wei13, Lemma 6.3.2].

Proposition 2.14. *Suppose G is finite. Then $H^n(G;A)$ is torsion for all $n > 0$.*

Proof. Let A_0 be A considered as an abelian group. Consider the maps

$$\begin{aligned} A &\to \operatorname{ind} A_0, \\ a &\mapsto (\varphi_a\colon x \mapsto xa) \end{aligned}$$

and

$$\begin{aligned} \operatorname{ind} A_0 &\to A \\ \varphi &\mapsto \sum_{\sigma} \sigma(\varphi(\sigma^{-1})). \end{aligned}$$

These maps are G-equivariant. The composition $A \to \operatorname{ind} A_0 \to A$ is multiplication by $\#G$. The induced map on cohomology is then also multiplication by $\#G$. This map factors through $H^n(G; \operatorname{ind} A_0)$, which is zero by Proposition 2.12. We conclude that $H^n(G; A)$ is annihilated by $\#G$, and hence it is torsion. ■

By Remark 2.6, we see that $H^n(G; -) = \operatorname{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, -)$. In combination with Example A.33 this gives us more flexibility in computing cohomology groups.

Example 2.15 (cohomology of infinite cyclic groups)**.** Suppose G is infinite cyclic. Notice that $\mathbb{Z}G = \mathbb{Z}[\sigma, \sigma^{-1}]$. We have a projective resolution of $\mathbb{Z}$ as a trivial G-module given by

$$0 \to \mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}G \to \mathbb{Z} \to 0,$$

where the first map is multiplication by $\sigma - 1$ and the second sends 1 to 1; indeed, localisation is exact, and we obtain the above sequence by localising the clearly exact sequence

$$0 \to \mathbb{Z}[\sigma] \xrightarrow{\sigma-1} \mathbb{Z}[\sigma] \to \mathbb{Z} \to 0$$

of $\mathbb{Z}[\sigma]$-modules at σ. Applying the contravariant functor $\operatorname{Hom}(-, A)$ to the sequence

$$0 \to \mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}G$$

we find the complex

$$A \xrightarrow{\sigma-1} A \to 0.$$

Taking cohomology we find

$$H^n(G; A) = \operatorname{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A) \simeq \begin{cases} A^G & n = 0 \\ A/(\sigma - 1)A & n = 1 \\ 0 & n \geq 2. \end{cases}$$

Example 2.16 (cohomology of finite cyclic groups)**.** Suppose G is cyclic of order m. Notice that $\mathbb{Z}G = \mathbb{Z}[\sigma]/(\sigma^m - 1)$. Let $N = 1 + \sigma + \sigma^2 + \ldots + \sigma^{m-1}$. We will show that the sequence

$$\ldots \xrightarrow{N} \mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}G \to \mathbb{Z} \to 0 \tag{2.1}$$

is a projective resolution of $\mathbb{Z}$ as a trivial G-module. Exactness at $\mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}G \to \mathbb{Z}$ follows from the commutative diagram of abelian groups

$$\begin{array}{ccccc} \mathbb{Z}[s] & \xrightarrow{s-1} & \mathbb{Z}[s] & \longrightarrow & \mathbb{Z} \\ \downarrow & & \downarrow & & \downarrow{=} \\ \mathbb{Z}G & \xrightarrow{\sigma-1} & \mathbb{Z}G & \longrightarrow & \mathbb{Z} \\ \downarrow & & \downarrow & & \\ 0 & & 0 & & \end{array}$$

in which the top row and the columns are exact; here $\mathbb{Z}[s] \to \mathbb{Z}G$ sends s to σ.

We see that $N(\sigma-1) = (\sigma-1)N = 0$, and so the sequence in (2.1) is a complex. Suppose $a = \sum_k c_k \sigma^k$, with k ranging over $\mathbb{Z}/m\mathbb{Z}$, is such that $(\sigma-1)a = 0$. Then a is invariant under the action of G and so for any $g \in G$ we get

$$\sum c_k g\sigma^k = ga = a = \sum c_k \sigma^k.$$

Comparing coefficients, we see that the c_k are all equal, and so we have $a \in N\mathbb{Z}G$; hence, the sequence in (2.1) is exact at $\mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}$.

Now suppose $b = \sum d_k \sigma^k$ is such that $Nb = 0$. Then

$$0 = Nb = \sum d_k N\sigma^k = \sum d_k N = N\sum d_k,$$

and so $\sum d_k = 0$. It follows from exactness of $\mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}G \to \mathbb{Z}$ that $b \in (\sigma-1)\mathbb{Z}G$; hence, the sequence in (2.1) is exact at $\mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}G \xrightarrow{N} \mathbb{Z}G$. We conclude that the sequence in (2.1) is a projective resolution.

Applying $\mathrm{Hom}(-, A)$ to the sequence

$$\ldots \xrightarrow{N} \mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}G$$

we get the complex

$$A \xrightarrow{\sigma-1} A \xrightarrow{N} A \xrightarrow{\sigma-1} A \xrightarrow{N} A \to \ldots.$$

Taking cohomology we find

$$H^n(G;A) = \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A) \simeq \begin{cases} A^G & n = 0 \\ \{a \in A : Na = 0\}/(\sigma-1)A & n = 1,3,5,\ldots \\ A^G/NA & n = 2,4,6,\ldots. \end{cases}$$

Computing the long exact sequence of cohomology groups corresponding to the short exact sequence of Example 2.8 yields

$$\begin{aligned} 0 \to \mathbb{Z}/2\mathbb{Z} &\xrightarrow{\cdot 4} 4\mathbb{Z}/8\mathbb{Z} \xrightarrow{0} 2\mathbb{Z}/4\mathbb{Z} \\ &\xrightarrow{\simeq} \mathbb{Z}/2\mathbb{Z} \xrightarrow{0} \mathbb{Z}/2\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}/2\mathbb{Z} \\ &\xrightarrow{0} \mathbb{Z}/2\mathbb{Z} \xrightarrow{\simeq} 4\mathbb{Z}/8\mathbb{Z} \xrightarrow{0} 2\mathbb{Z}/4\mathbb{Z} \to \ldots. \end{aligned}$$

2.3 Cocycles and coboundaries

Examples 2.15 and 2.16 compute cohomology groups by finding a projective resolution of $\mathbb{Z}$ as a trivial G-module. We will do this more generally for any group G. For the rest of this section we fix a G-module A.

For $n \geq 0$ we define P_n to be the free abelian group on the $(n+1)$-tuples $(g_0, \ldots, g_n)$ of elements in G. We equip P_n with the G-action specified on basis elements by

$$\sigma(g_0, \ldots, g_n) = (\sigma g_0, \ldots, \sigma g_n)$$

for $\sigma \in G$. We define homomorphisms $f_n \colon P_n \to P_{n-1}$, given on basis elements by

$$f_n(g_0, \dots, g_n) = \sum_{i=0}^{n} (-1)^i (g_0, \dots, \hat{g_i}, \dots, g_n),$$

where the hat means "omit". It is easy to see that f_n is also G-equivariant.

Lemma 2.17. *The following sequence*

$$\dots \xrightarrow{f_3} P_2 \xrightarrow{f_2} P_1 \xrightarrow{f_1} P_0 \xrightarrow{f_0} \mathbb{Z} \to 0, \tag{2.2}$$

where the map f_0 sends all g to 1, is a projective resolution of $\mathbb{Z}$ as a trivial G-module.

Proof. We see that P_n is free as a $\mathbb{Z}G$-module on the basis consisting of elements of the form $(1, g_1, \dots, g_n)$, so P_n is projective. We verify that $f_{n-1} \circ f_n = 0$.

We define a map $h_n \colon P_{n-1} \to P_n$ given on basis elements by $(g_1, \dots, g_n) \mapsto (1, g_1, \dots, g_n)$. For $n = 0$ we define $h_0 \colon \mathbb{Z} \to P_0$ by $1 \mapsto 1$. We now compute

$$f_{n+1} \circ h_n + h_{n-1} \circ f_n = \mathrm{id}.$$

For $x \in \ker f_n$ we get $f_{n+1}(h_n(x)) = x$, and so $x \in \operatorname{im} f_{n+1}$. We conclude that the sequence in (2.2) is exact, and hence it is a projective resolution of $\mathbb{Z}$ as a trivial G-module. ∎

By remark A.33 we now get

$$H^n(G; A) = \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A) = H^n(\mathrm{Hom}(P_*, A)).$$

There is a more convenient complex, which is isomorphic to $\mathrm{Hom}(P_*, A)$, and is often used in practice. Define

$$C^n(G; A) = \{\varphi \colon G^n \to A \text{ a function}\}.$$

This is a group under pointwise addition. We define a homomorphism

$$\partial^n \colon C^n(G; A) \to C^{n+1}(G; A)$$

by

$$\begin{aligned} \partial^n \varphi(g_1, \dots, g_{n+1}) = g_1 \varphi(g_2, \dots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i \varphi(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) \\ + (-1)^{n+1} \varphi(g_1, \dots, g_n). \end{aligned} \tag{2.3}$$

Proposition 2.18. *The sequence $C^*(G; A)$ is a complex, and it is isomorphic to* $\mathrm{Hom}(P_*, A)$.

Proof. The group $\mathrm{Hom}(P_n, A)$ can be identified with the abelian group of G-equivariant maps $G^{n+1} \to A$. We define

$$\begin{aligned} \mathrm{Hom}(P_n, A) &\to C^n(G, A) \\ \varphi &\mapsto ((g_1, \dots, g_n) \mapsto \varphi(1, g_1, g_1 g_2, \dots, g_1 \dots g_n)). \end{aligned}$$

An inverse to this map is given by

$$\begin{aligned} C^n(G,A) &\to \mathrm{Hom}(P_n, A) \\ \psi &\mapsto ((1, g_1, \ldots, g_n) \mapsto \psi(g_1, g_1^{-1}g_2, g_2^{-1}g_3, \ldots, g_{n-1}^{-1}g_n)). \end{aligned}$$

It is straightforward to check that these maps commute with the coboundary maps. As a result, $C^*(G;A)$ is a complex and isomorphic to $\mathrm{Hom}(P_*, A)$. ■

Definition 2.19. *We define subgroups $Z^n(G;A)$ and $B^n(G;A)$ of $C^n(G;A)$ by*

$$\begin{aligned} Z^n(G;A) &= \ker \partial^n, \\ B^n(G;A) &= \begin{cases} \mathrm{im}\, \partial^{n-1} & n > 1 \\ 0 & n = 0, \end{cases} \end{aligned}$$

called the group of n-cocycles with coefficients in A and the group of n-coboundaries of G with coefficients in A, respectively.

Corollary 2.20. *We have a natural isomorphism*

$$H^n(G;A) \simeq \frac{Z^n(G;A)}{B^n(G;A)}.$$

2.3.1 The first cohomology group

Of special importance in this thesis is the first cohomology group. By Corollary 2.20, we have a natural isomorphism

$$H^1(G;A) \simeq \frac{Z^1(G;A)}{B^1(G;A)} = \frac{\{\varphi \colon G \to A \mid \forall \sigma, \tau \in G \colon \varphi(\sigma\tau) = \varphi(\sigma) + \sigma\varphi(\tau)\}}{\{\varphi \colon G \to A \mid \exists a \in A \forall \sigma \in G \colon \varphi(\sigma) = \sigma a - a\}}. \tag{2.4}$$

As a demonstration, we prove a classical theorem known as Hilbert's Theorem 90.

Proposition 2.21. *Let K/k be a finite Galois extension. Then $H^1(\mathrm{Gal}(K/k); K^\times) = 0$.*

Proof. Write $G = \mathrm{Gal}(K/k)$. Let $\varphi \colon G \to K^\times$ be a 1-cocycle. We will prove that there exists $a \in K^\times$ such that for all $\tau \in G$ we have $\varphi(\tau) = a/\tau(a)$, and hence that φ is the 1-coboundary associated to a^{-1}. Let $b \in K^\times$ be such that

$$a = \sum_{\sigma \in G} \varphi(\sigma)\sigma(b)$$

is nonzero. Such a b always exists by independence of characters (see [Lan02, Chapter VI, Theorem 4.1]). For all $\tau \in G$ we find

$$\begin{aligned} \tau(a) &= \sum_{\sigma \in G} \tau(\varphi(\sigma))\tau(\sigma b) \\ &= \sum_{\sigma \in G} \varphi(\tau)^{-1}\varphi(\tau\sigma)(\tau\sigma)(b) \\ &= \varphi(\tau)^{-1} a, \end{aligned}$$

and so $\varphi(\tau) = a/\tau(a)$. ■

In section 3 we will develop a more specialized cohomology theory of Galois groups, for which an analog of Proposition 2.21 will be true for infinite Galois extensions.

3 Galois cohomology

We assume knowledge of Galois theory, which can be found, for instance, in [Lan02, Chapter VI]. Much of the material in sections 3.1 through 3.3 is based on [Wei13, Chapter 6] and [NSW, Chapter I]. The material on nonabelian cohomology in Section 3.4 is based on [Ser97, §I.5].

3.1 Profinite groups

In this section, I will always denote a partially ordered directed set; that is, I is a partially ordered set such that any two elements have a common upper bound. We write TopGrp for the category of topological groups. We view I as a category. An *inverse system* of topological groups indexed by I is a functor $I^{\mathrm{opp}} \to \mathrm{TopGrp}$. The *inverse limit* of such a system is defined to be the limit of this functor and will be denoted $\varprojlim_{i\in I} G_i$, where we write G_i for the image of $i \in I$. This is well defined, because limits exist in the category of topological groups by [Sta22, Tag 0B20].

Definition 3.1. *We call a topological group G profinite if it is isomorphic to an inverse limit $\varprojlim_{i\in I} G_i$, with G_i a finite discrete topological group for all $i \in I$.*

Remark 3.2. We can view the inverse limit $\varprojlim_{i\in I} G_i$ as the closed subgroup of $\prod_{i\in I} G_i$ given by

$$\left\{ (x_i)_{i\in I} \in \prod_{i\in I} G_i : f_j^i(x_i) = x_j \text{ for } j \le i \right\},$$

where we write $f_j^i \colon G_i \to G_j$ for the map induced by $j \le i$.

Example 3.3.

1. Any discrete finite group is profinite.
2. The group of p-adic integers $\mathbb{Z}_p = \varprojlim_{n\ge 1} \mathbb{Z}/p^n\mathbb{Z}$ is a profinite group by definition.

The most important class of examples (and in fact every example by [Wat74]) are the Galois groups.

Example 3.4 (Galois groups are profinite)**.** Let K/k be a Galois extension. We have an isomorphism of topological groups

$$\mathrm{Gal}(K/k) \simeq \varprojlim \mathrm{Gal}(F/k),$$

with the direct limit taken over the finite Galois extensions F/k with F contained in K, by [Lan02, Chapter VI, Theorem 14.1]. In particular, $\mathrm{Gal}(K/k)$ is profinite, because $\mathrm{Gal}(F/k)$ is discrete if F/k is finite Galois.

Proposition 3.5. *Let G be a profinite group. Then G is*

(i) Hausdorff,

(ii) compact,

(iii) totally disconnected.

Proof. Let $G = \varprojlim_{i \in I} G_i$ be a profinite group, and embed G into the product $\prod_{i \in I} G_i$ as in remark 3.2. Products of discrete finite groups have the above properties, so G is Hausdorff and totally disconnected, because it is a subspace of a space with these properties. Compactness of G follows from the fact that G is a closed subspace of the compact Hausdorff space $\prod_{i \in I} G_i$. ■

Corollary 3.6. *Finite profinite groups are always discrete.*

Proof. Finite Hausdorff spaces are discrete. ■

Corollary 3.7. *If $U \subset G$ is an open subgroup of G, then U has finite index in G.*

Proof. The cosets of U cover G, and G is compact. ■

Remark 3.8. As it turns out, the converse of Proposition 3.5 is also true, as shown in [Ser97, Chapter 1, Proposition 0], giving us a different characterization of profinite groups.

3.2 The category of discrete G-modules

Fix a profinite group G.

Definition 3.9. *We call a G-module A discrete if the multiplication map*

$$G \times A \to A$$

is continuous when A is equipped with the discrete topology. The category of discrete G-modules is the full subcategory of the category of G-modules on the discrete G-modules. We denote this category by dG-Mod.

The following proposition gives a slightly more concrete condition for a G-module to be discrete.

Proposition 3.10. *A G-module A is discrete if and only if we have an equality*

$$A = \bigcup A^U$$

taken over all open subgroups $U \subset G$.

Proof. Suppose A is a discrete G-module. Let $a \in A$. We have a composition of continous maps

$$G \simeq G \times \{a\} \hookrightarrow G \times A \to A.$$

The inverse image of $\{a\}$ under this map is the open subgroup $\mathrm{Stab}_G(a) = \{\sigma \in G : \sigma a = a\}$. In particular, a is fixed by $\mathrm{Stab}_G(a)$.

Conversely, suppose $A = \bigcup A^U$. Let $a \in A$ and consider the inverse image X of $\{a\}$ under the multiplication map. Consider a pair $(\sigma, b) \in X$. There exists an open subgroup $U \subset A$ such that $b \in A^U$, by assumption. We now have an open neighbourhood $\sigma U \times \{b\}$ of (σ, b) in X. So X is open, and hence $G \times A \to A$ is continuous. ■

Example 3.11. (i) If G is finite, then any G-module A is a discrete G-module.

(ii) For any Galois extension K/k, the unit group $K^\times$ is a discrete $\mathrm{Gal}(K/k)$-module by Proposition 3.10: for $\alpha \in K^\times$ we have $\alpha \in (K^\times)^{\mathrm{Gal}(K/k(\alpha))}$, and $\mathrm{Gal}(K/k(\alpha)) \subset \mathrm{Gal}(K/k)$ is open, because its index is finite by Galois theory.

Proposition 3.12. *The category* dG-Mod *is abelian.*

Proof. The category dG-Mod contains 0. Finite direct sums, kernels and cokernels all inherit continuous actions. ∎

Consider the evident inclusion functor $i : \text{dG-Mod} \hookrightarrow \text{G-Mod}$.

Lemma 3.13. *The functor i admits a right adjoint $\cup(-)^U \colon$ G-Mod $\to$ dG-Mod sending a G-module A to $\cup A^U$, with the union taken over all open subgroups $U \subset G$.*

Proof. Let A be a discrete G-module, and B a G-module. Then $\cup B^U$ is a G-module: it is clearly closed under addition, and for any $x \in B^U$ and any $\sigma \in G$, the element σx is fixed by the open subgroup $\sigma U \sigma^{-1}$. The module $\cup B^U$ is discrete by Proposition 3.10. The action of $\cup(-)^U$ on maps is clear. We have a natural isomorphism

$$\mathrm{Hom}_{\text{G-Mod}}(A, B) \xrightarrow{\simeq} \mathrm{Hom}_{\text{dG-Mod}}(A, \cup B^U)$$

sending $f : A \to B$ to $\tilde{f} : A \to \cup B^U, x \mapsto f(x)$, and so we have an adjunction $i \dashv \cup(-)^U$. ∎

Proposition 3.14. *The category* dG-Mod *has enough injectives.*

Proof. Let A be a discrete G-module. Then there exists a G-module I and an embedding $A \hookrightarrow I$, because G-Mod has enough injectives. This gives an embedding

$$A \hookrightarrow \cup I^U.$$

The functor $\cup(-)^U$ is a right adjoint to an exact functor by Lemma 3.13, so by the same argument as in the proof of Proposition A.23 we see that $\cup I^U$ is injective. ∎

3.3 Cohomology of profinite groups

In this section fix a profinite group G and a discrete G-module A. As in the case of G-modules, we consider the functor taking invariants under the action of G

$$(-)^G \colon \text{dG-Mod} \to \text{Ab}.$$

This is, again, a left exact functor. By Proposition 3.14 the following definition now makes sense.

Definition 3.15. *For all integers $n \geq 0$ we define the functor $H^n_{cont}(G; -) : \text{dG-Mod} \to \text{Ab}$ by*

$$H^n_{cont}(G; -) = R^n(-)^G,$$

the n-th right derived functor of $(-)^G$. We call $H_{cont}(G; A)$ the n-th (continuous) cohomology group of G with coefficients in A.

Usually the subscript "cont" will be dropped. Unless otherwise specified, this definition then supersedes definition 2.9.

Notation 3.16. If K/k is a Galois extension, then the functors $H^n(\mathrm{Gal}(K/k);-)$ will often be denoted $H^n(K/k;-)$ for the sake of brevity. If $K = k^s$ is a separable closure of k, then we will simply write $H^n(k,-)$.

Remark 3.17. Suppose G is finite. Then G is discrete by Corollary 3.6, and so the continuous cohomology groups are the same as the ordinary cohomology groups.

3.3.1 Continuous cocycles and coboundaries

We can give a description of $H^n(G;A)$ similar to the one in Section 2.3. It is, however, reasonable to expect that the topology of G should be taken into account for this. This motivates us to consider the following. We define $C^n_{\mathrm{cont}}(G;A)$ to be the abelian group of continous maps $G^n \to A$. As before, the subscript "cont" will usually be dropped. This yields an additive functor

$$C^n(G;-)\colon \text{dG-Mod} \to \text{Ab}.$$

With the same coboundary maps as in (2.3) we can extend this to a functor

$$C^*(G;-)\colon \text{dG-Mod} \to \text{Ch}_{\text{Ab}},$$

with values in the category of chain complexes of abelian groups. Define

$$T^n(G;-) = H^n(C^*(G;-))\colon \text{dG-Mod} \to \text{Ab}.$$

We will want to turn the collection $T^*(G;-) = (T^n(G;-))$ into a δ-functor.

Lemma 3.18. *The functor $C^*(G;-)$ is exact.*

Proof. For this it suffices to prove that $C^n(G;-)$ is exact. Left exactness of this functor follows as in the proof of Proposition A.8. We will show that $C^n(G;-)$ preserves surjections to show right exactness. Let $g\colon B \to C$ be a surjective map of discrete G-modules. Let $\varphi\colon G^n \to C$ be a continuous map. Let $\{U_i\}$ be an open cover of G^n such that φ is constant on each U_i, and the U_i are pairwise disjoint. Such a cover exists by discreteness of C. Define $\psi\colon G^n \to B$ by sending $x \in U_i$ to an element $b_i \in B$ such that $g(b_i) = \varphi(x)$. Then ψ is continuous, because it is locally constant, and we have $g\psi = \varphi$. ∎

If $U \subset U'$ are open normal subgroups of G, then there is a map

$$C^*(G/U';A^{U'}) \to C^*(G/U;A^U)$$

given by sending a function $\varphi : (G/U')^n \to A^{U'}$ in $C^n(G/U';A^{U'})$ to the composition

$$(G/U)^n \to (G/U')^n \xrightarrow{\varphi} A^{U'} \hookrightarrow A^U,$$

where the map $(G/U)^n \to (G/U')^n$ is induced by the quotient map $G/U \to G/U'$. These maps concatenate into a direct system $\{C^*(G/U;A^U)\}$ indexed by the open normal subgroups $U \subset G$.

Lemma 3.19. *We have a natural isomorphism*

$$C^*(G;A) = \varinjlim_{U \subset G} C^*(G/U; A^U),$$

taken over all open normal subgroups $U \subset G$.

Proof. We refer to [NSW, Proposition 1.2.6]. ∎

By Lemma 3.18, given a short exact sequence $0 \to A \to B \to C \to 0$ in dG-Mod, we get a short exact sequence

$$0 \to C^*(G;A) \to C^*(G;B) \to C^*(G;C) \to 0$$

of complexes. By the "Zigzag Lemma" from homological algebra (see [Lee, Lemma 13.17]) we find maps

$$\delta^n \colon T^n(G;C) \to T^{n+1}(G;A),$$

making $T^*(G;-) = (T^n(G;-))$ a δ-functor.

Theorem 3.20. *The δ-functors $T^*(G;-)$ and $H^*(G;-)$ are isomorphic.*

Proof. It is sufficient to show that $T^0(G;-) = H^0(G;-)$ and that $T^*(G;-)$ is universal. The first statement can easily be checked. For the second statement we apply Proposition A.30. Let I in dG-Mod be an injective object, then I^U is an injective G/U-module, because $(-)^U$ is right adjoint to $\mathrm{res}^{G/U}_G$, which is an exact functor. We have $H^n(G/U; I^U) = 0$ for all $n \geq 1$, because G/U is finite (Corollary 3.7) and ordinary group cohomology vanishes on injective objects. By Lemma 3.19,

$$\begin{aligned} T^n(G;I) &= H^n(C^*(G;I)) \\ &= H^n(\varinjlim C^*(G/U; I^U)) \\ &= \varinjlim H^n(G/U; I^U) = 0. \end{aligned}$$

∎

Analogously to Definition 2.19 we have the following definition.

Definition 3.21. *We define abelian groups $Z^n(G;A)$ (or $Z_{cont}(G;A)$) and $B^n(G;A)$ (or $B_{cont}(G;A)$) by*

$$\begin{aligned} Z^n(G;A) &= \ker(\partial^n \colon C^n(G;A) \to C^{n+1}(G;A)), \\ B^n(G;A) &= \begin{cases} \mathrm{im}(\partial^{n-1} \colon C^{n-1}(G;A) \to C^n(G;A)) & n > 0 \\ 0 & n = 0, \end{cases} \end{aligned}$$

called the group of (continuous) n-cocycles and n-coboundaries, respectively.

Corollary 3.22. *We have isomorphisms*

$$H^n(G;A) \simeq \frac{Z^n(G;A)}{B^n(G;A)}.$$

Corollary 3.23. *For all $n > 0$ the group $H^n(G;A)$ is torsion.*

Proof. By Proposition 2.14 and Corollary 3.7 we have that $H^n(G;A)$ is a direct limit of torsion groups, and hence is itself torsion. ■

We can now give a generalization of Proposition 2.21.

Proposition 3.24. *Let K/k be a Galois extension. Then*

$$H^1(K/k;K^\times) = 0.$$

Proof. By Lemma 3.19 and Proposition 2.21 we find

$$H^1(K/k;K^\times) = \varinjlim H^1(F/k;(K^\times)^{\mathrm{Gal}(K/F)}) = \varinjlim H^1(F/k;F^\times) = 0,$$

where the direct limit is taken over all finite Galois extensions F/k such that $F \subset K$. ■

3.4 Nonabelian cohomology

We again fix a profinite group G. Thus far, discrete G-modules have been abelian groups equipped with some continuous G-action. In this thesis, we will encounter many non-commutative groups with continuous G-actions. A more primitive version of our cohomology is applicable in this situation.

Let A be a (perhaps noncommutative) group with a continuous G-action $G \times A \to A$. We will still refer to A as a *discrete G-module*, and we will sometimes add the prefix *noncommutative* if A is not abelian. We denote the action of $\sigma \in G$ on $x \in A$ by ${}^\sigma x$. As in Proposition 3.10, continuity of this action is equivalent to the equality

$$A = \bigcup A^U,$$

where this union is taken over all open subgroups $U \subset G$. We define $H^0(G;A)$ to be the subgroup of A consisting of elements invariant under the action of G.

We call a continuous function $c\colon G \to A$ a *cocycle*, or *1-cocycle*, if for all $\sigma, \tau \in G$ we have

$$c_{\sigma\tau} = c_\sigma {}^\sigma c_\tau.$$

We define $Z^1(G;A)$ to be the set of 1-cocycles $G \to A$. We say that cocycles (c_σ) and (d_σ) are *cohomologous*, and write $(c_\sigma) \sim (d_\sigma)$, if there exists $a \in A$ such that for all $\sigma \in G$ we have

$$d_\sigma = a^{-1} c_\sigma {}^\sigma a.$$

This defines an equivalence relation on $Z^1(G;A)$ and we define *the first cohomology set of G with coefficients in A* by

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

Compare this to (2.4). The set $H^1(G;A)$ no longer has the structure of a group, but still has the structure of a pointed set with the basepoint being the class of the trivial cocycle sending everything in G to $1 \in A$. Note that the constructions of H^0 and H^1 are functorial. If $G = \mathrm{Gal}(K/k)$ is a Galois group, then we often simply write $H^0(K/k;-)$ and $H^1(K/k;-)$. When $K = k^s$ is a separable closure of k, then we write $H^0(k;-)$ and $H^1(k;-)$.

Analogously to Proposition 3.19, we have the following statement.

Proposition 3.25. *We have*

$$H^1(G;A) = \varinjlim H^1(G/U;A^U),$$

with the direct limit taken over all open normal subgroups U of G.

The existence of long exact sequences of cohomology groups has the following analogy in the noncommutative case.

Proposition 3.26. *Suppose we have an exact sequence*

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

of (perhaps noncommutative) discrete G-modules, then we get an exact sequence

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

of pointed sets, in the sense that the image of a map is the inverse image of the basepoint. If, in addition, A lies in the center of B, then this sequence can be extended by a map $H^1(G;C) \xrightarrow{\Delta} H^2(G;A)$ such that the resulting sequence is exact.

We only give the connecting map. See [Ser79, Appendix: Non-abelian Cohomology, propositions 1 and 2] for a complete proof.

Sketch of proof. For $x \in H^0(G;C)$, let $y \in B$ be such that $y \mapsto x$. Define $c_\sigma = y^{-1\sigma} y$ for $\sigma \in G$. The elements c_σ get mapped to 1 under the map $B \to C$, because x is invariant under the action of G. As a result, the elements c_σ can be viewed as elements of A, since A is the kernel of the map $B \to C$. The collection $c = (c_\sigma)$ defines a 1-cocycle $G \to A$ whose class is independent of the choice of y. We set $\delta(x) = [c]$. This defines a pointed function $\delta\colon H^0(G;C) \to H^1(G;A)$.

Suppose that A lies in the center of B. For a 1-cocycle $(d_\sigma) \in H^1(G;C)$, let $b_\sigma \in B$ be such that $b_\sigma \mapsto d_\sigma$ for all $\sigma \in G$. For all $\sigma, \tau \in G$ define $a_{\sigma,\tau} = b_\sigma{}^\sigma b_\tau b_{\sigma\tau}^{-1}$. By a similar argument as above we can view the elements $a_{\sigma,\tau}$ in A. Then $a = (a_{\sigma,\tau})$ defines a 2-cocycle $G \times G \to A$ whose class is independent of the choice of lifts b_σ. We set $\Delta([d]) = [a]$. This defines a pointed function $\Delta\colon H^1(G;C) \to H^2(G;A)$. ■

4 Galois descent

Mathematical objects often have an associated *base field*. For example, if k is a field, then we can consider vector spaces over k, algebras over k, schemes over k, elliptic curves over k, etc. If K/k is a field extension, then there is often a natural way to *extend* objects over k to objects over K. An example of this is given in the introduction. Given an object X over K, it is not necessarily true that there exists an object x over k such that x extends to X. If this is the case, then we say that X *descends* to x. In this section we will prove that if K/k is finite Galois, then certain objects X over K can be descended to objects over k by giving an action of the Galois group $\mathrm{Gal}(K/k)$ on the object X satisfying certain properties. Roughly speaking, we call descent through this method *Galois descent*. The notion of a *base extension*, introduced in Section 4.1, makes this precise.

For the rest of this section we fix a finite Galois extension K/k with group G.

4.1 Base extensions

Let

$$(-)_K \colon \mathscr{C}_k \to \mathscr{C}_K \quad \text{and} \quad \mathrm{res} \colon \mathscr{C}_K \to \mathscr{C}_k$$

be functors, with res faithful. We think of the categories $\mathscr{C}_k$ and $\mathscr{C}_K$ as categories of *objects over* k and K, respectively. We will, for example, write Hom_k and $\simeq_k$ to indicate Hom-sets and isomorphisms in the category $\mathscr{C}_k$, and similarly for $\mathscr{C}_K$. The functor $(-)_K$ *extends* objects X over k to objects X_K over K, and the functor res *restricts* objects Y over K to objects $\mathrm{res}\, Y$ over k.

For $\sigma \in G$ and $X, Y \in \mathscr{C}_K$ we let

$$\mathrm{Hom}_\sigma(X,Y) \subset \mathrm{Hom}_k(\mathrm{res}\, X, \mathrm{res}\, Y)$$

be a subset of $\mathrm{Hom}_k(\mathrm{res}\, X, \mathrm{res}\, Y)$ such that the collection of these subsets satisfies

- for $X, Y \in \mathscr{C}_K$ we have
$$\mathrm{Hom}_{\mathrm{id}}(X,Y) = \mathrm{Hom}_K(X,Y), \tag{4.1}$$
where we view $\mathrm{Hom}_K(X,Y)$ as a subset of $\mathrm{Hom}_k(\mathrm{res}\, X, \mathrm{res}\, Y)$ via res (which we had assumed to be faithful);
- for $\sigma, \tau \in G$ and $X, Y, Z \in \mathscr{C}_K$ composition induces a map
$$\mathrm{Hom}_\sigma(X,Y) \times \mathrm{Hom}_\tau(Y,Z) \to \mathrm{Hom}_{\tau\sigma}(X,Z). \tag{4.2}$$

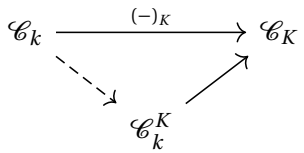
We refer to the set $\mathrm{Hom}_\sigma(X,Y)$ as the set of σ*-twisted*, or σ*-linear*, maps $X \to Y$.

If X is an object over K and $S \colon G \to \mathrm{Aut}_k(\mathrm{res}\, X)$ is a homomorphism, then we say that S is a *semi-linear*, or *Galois*, action if for all $\sigma \in G$ we have $S(\sigma) \in \mathrm{Hom}_\sigma(X,X)$. We will often abreviate $S(\sigma)$ to σ. We write $\mathscr{C}_k^K$ for the category whose objects are objects over K with Galois action, and whose morphisms are G-equivariant morphisms: K-maps $f \colon X \to Y$ such that for all $\sigma \in G$ the diagram

$$\begin{array}{ccc} \mathrm{res}\, X & \xrightarrow{\mathrm{res}\, f} & \mathrm{res}\, Y \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} \\ \mathrm{res}\, X & \xrightarrow{\mathrm{res}\, f} & \mathrm{res}\, Y \end{array}$$

commutes.

Notice that there is an evident forgetful functor $\mathscr{C}_k^K \to \mathscr{C}_K$. For the above data to define a base extension, we require a factorization of $(-)_K$ via this forgetful functor.



We sumarize in the definition below.

Definition 4.1. *A base extension consists of*

- *functors* $(-)_K\colon \mathscr{C}_k \to \mathscr{C}_K$ *and* $\mathrm{res}\colon \mathscr{C}_K \to \mathscr{C}_k$*, with* res *faithful;*
- *sets* $\mathrm{Hom}_\sigma(X,Y) \subset \mathrm{Hom}_k(\mathrm{res}\, X, \mathrm{res}\, Y)$ *for all* $\sigma \in G$ *and* $X, Y \in \mathscr{C}_K$ *such that the conditions in* (4.1) *and* (4.2) *are satisfied;*
- *a factorization of* $(-)_K$ *via the forgetful functor* $\mathscr{C}_k^K \to \mathscr{C}_K$*, where the category* $\mathscr{C}_k^K$ *is defined as above.*

We say that such a base extension satisfies Galois descent if the induced functor $\mathscr{C}_k \xrightarrow{\simeq} \mathscr{C}_k^K$ *is an equivalence of categories.*

A base extension will often be denoted just $(-)_K\colon \mathscr{C}_k \to \mathscr{C}_K$, leaving the other data implicit. In the future, restricting objects or morphisms will often be done implicitly; the restriction of an object X over K will simply be denoted X if no confusion can arise.

We have the following examples of base extensions, but this list can certainly be extended (see [Bru09] and [Jah00]).

Example 4.2. (i) If F is a field, then we write Vect_F for the category of vector spaces over F. We define the functor $(-)_K\colon \mathrm{Vect}_k \to \mathrm{Vect}_K$ by $V \mapsto V \otimes_k K$. The functor $\mathrm{res}\colon \mathrm{Vect}_K \to \mathrm{Vect}_k$ is defined to be the evident restriction functor.

For vector spaces W and W' over K, and $\sigma \in G$, we write $\mathrm{Hom}_\sigma(W,W')$ for the set of k-linear maps $f\colon W \to W'$ such that for all $a \in K$ and $x \in W$ we have

$$f(ax) = \sigma(a) f(x).$$

The sets $\mathrm{Hom}_\sigma(W,W')$ then satisfy the conditions in (4.1) and (4.2).

Define the category Vect_k^K as above. If V is a vector space over k, then we can equip $V_K = V \otimes_k K$ with a semi-linear G-action by letting $\sigma \in G$ act as $\mathrm{id} \otimes \sigma$. A map of k-vector spaces $f\colon V \to V'$ then gives a G-equivariant map $f_K\colon V_K \to V'_K$. We see that the functor $(-)_K$ factors via the forgetful functor $\mathrm{Vect}_k^K \to \mathrm{Vect}_K$, and hence that we have defined a base extension.

(ii) If F is a field, then we write Alg_F for the category of algebras over F. We define the functor $(-)_K\colon \mathrm{Alg}_k \to \mathrm{Alg}_K$ by $A \mapsto A \otimes_k K$. The functor $\mathrm{res}\colon \mathrm{Alg}_K \to \mathrm{Alg}_k$ is defined to be the evident restriction functor.

For K-algebras B and B', and $\sigma \in G$, we write $\mathrm{Hom}_\sigma(B,B')$ for the set of k-maps $f\colon B \to B'$ such that the diagram

$$\begin{array}{ccc} B & \xrightarrow{f} & B' \\ \uparrow & & \uparrow \\ K & \xrightarrow{\sigma} & K \end{array}$$

commutes. The sets $\mathrm{Hom}_\sigma(B,B')$ then satisfy the conditions in (4.1) and (4.2).

Define the category Alg_k^K as above. If A is an algebra over k, then we can equip $A_K = A \otimes_k K$ with a semi-linear G-action by letting $\sigma \in G$ act as $\mathrm{id} \otimes \sigma$. A map of k-algebras

$f\colon A \to A'$ then gives a G-equivariant map $f_K\colon A_K \to A'_K$. We see that the functor $(-)_K$ factors via the forgetful functor $\mathrm{Alg}_k^K \to \mathrm{Alg}_K$, and hence that we have defined a base extension.

(iii) If F is a field, then we write Sch_F for the category of schemes over F. We define the functor $(-)_K\colon \mathrm{Sch}_k \to \mathrm{Sch}_K$ by $X \mapsto X \times_{\mathrm{Spec}\, k} \mathrm{Spec}\, K$. The functor res$\colon \mathrm{Sch}_K \to \mathrm{Sch}_k$ is defined by sending a K-scheme $X \to \mathrm{Spec}\, K$ to $X \to \mathrm{Spec}\, K \to \mathrm{Spec}\, k$.

For K-schemes Y and Y', and $\sigma \in G$, we write $\mathrm{Hom}_\sigma(Y, Y')$ for the set of k-maps $f : Y \to Y'$ such that the diagram

$$\begin{array}{ccc} Y & \xrightarrow{f} & Y' \\ \downarrow & & \downarrow \\ \mathrm{Spec}\, K & \xrightarrow{(\sigma^{-1})^*} & \mathrm{Spec}\, K \end{array}$$

commutes. Then the conditions in (4.1) and (4.2) are satisfied; indeed, (4.1) is clear, and for $\sigma, \tau \in G$, $f\colon Y \to Y'$ a map in $\mathrm{Hom}_\sigma(Y, Y')$ and $g\colon Y' \to Y''$ a map in $\mathrm{Hom}_\tau(Y', Y'')$ we have a commutative diagram

$$\begin{array}{ccccc} Y & \xrightarrow{f} & Y' & \xrightarrow{g} & Y'' \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Spec}\, K & \xrightarrow{(\sigma^{-1})^*} & \mathrm{Spec}\, K & \xrightarrow{(\tau^{-1})^*} & \mathrm{Spec}\, K, \end{array} \qquad \text{with } ((\tau\sigma)^{-1})^* : \mathrm{Spec}\, K \to \mathrm{Spec}\, K,$$

which shows that the condition in (4.2) holds.

Define the category Sch_k^K as above. If X is a k-scheme, then we let $\sigma \in G$ act on X_K by the map induced by $(\sigma^{-1})^*$ via the universal property of the fiber product, $\mathrm{id} \times_{\mathrm{Spec}\, k} (\sigma^{-1})^*$. This equips X_K with a Galois G-action, and if $f\colon X \to X'$ is a map of k-schemes, then $f_K\colon X_K \to X'_K$ is G-equivariant. We see that the functor $(-)_K\colon \mathrm{Sch}_k \to \mathrm{Sch}_K$ factors via the forgetful functor $\mathrm{Sch}_k^K \to \mathrm{Sch}_K$, and hence that we have defined a base extension.

Suppose we have a base extension $(-)_K\colon \mathscr{C}_k \to \mathscr{C}_K$. Let X and Y be objects over K with Galois G-action and let $g\colon X \to Y$ be a K-map. By (4.1) and (4.2), the compostition $\sigma g \sigma^{-1}$ is a again a K-map for $\sigma \in G$. In this way we define an action of G on $\mathrm{Hom}_K(X, Y)$ given by

$$^\sigma f = \sigma f \sigma^{-1}, \tag{4.3}$$

for all $\sigma \in G$ and $f \in \mathrm{Hom}_K(X, Y)$. Note that the G-equivariant maps $X \to Y$ are precisely the maps invariant under this action. This action is compatible with composition in the sense that if X, Y and Z are K-objects with Galois G-action, and $g : X \to Y$ and $h : Y \to Z$ are maps of K-objects, then we have

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

In particular, this turns $\mathrm{Aut}_K(X)$ into a (perhaps noncommutative) G-module. This fact is exploited in the next section.

In the rest of this section we will show that (i) and (ii) of Example 4.2 satisfy Galois descent. We will also show that the example in part (iii) satisfies Galois descent if we restrict to the full subcategory of quasi-projective schemes.

4.2 Descent of vector spaces

We consider the base extension $(-)_K\colon \mathrm{Vect}_k \to \mathrm{Vect}_K$ described in (i) of Example 4.2. Since the isomorphism class of a vector space is entirely determined by its dimension, and the tensor product preserves dimension, all vector spaces descend. It will, however, turn out to be very useful to still describe a category Vect_k^K and an equivalence of categories $\mathrm{Vect}_k \simeq \mathrm{Vect}_k^K$.

Given an object W in Vect_k^K, the set of fixed points under the action of G, denoted W^G, has the structure of a k-vector space. A map $f\colon W \to W'$ in Vect_k^K restricts to a map $f^G\colon W^G \to W'^G$ of k-vector spaces. This yields a functor

$$(-)^G\colon \mathrm{Vect}_k^K \to \mathrm{Vect}_k\,.$$

By the following theorem, the base extension $(-)_K : \mathrm{Vect}_k \to \mathrm{Vect}_K$ satisfies Galois descent.

Theorem 4.3. *There is an equivalence of categories*

$$\begin{aligned} \mathrm{Vect}_k &\simeq \mathrm{Vect}_k^K \\ V &\mapsto V \otimes_k K \\ W^G &\mathrel{\reflectbox{$\mapsto$}} W. \end{aligned}$$

Our proof of this theorem uses the following lemma.

Lemma 4.4. *Given a vector space W over K with a semilinear G-action, the map*

$$\begin{aligned} \varphi\colon W^G \otimes_k K &\to W \\ x \otimes a &\mapsto ax \end{aligned}$$

is an isomorpism of K-vector spaces compatible with G-actions.

Proof. We follow the proof from [Bru09, Lemma 6.4]. Let $(\alpha_1, \dots, \alpha_n)$ be a k-basis for K. Write $G = \{\sigma_1, \dots, \sigma_n\}$. For $w \in W$ we consider

$$v_j = \sum_{i=1}^{n} \sigma_i(\alpha_j w) = \sum_{i=1}^{n} \sigma_i(\alpha_j)\sigma_i(w) \in W^G,$$

for $j = 1, \dots, n$. By independence of characters, the matrix $(\sigma_i(\alpha_j))_{i,j}$ is invertible. In particular, we can express $w = \mathrm{id}(w)$ as a K-linear combination of the v_j, hence w is in the image of φ and φ is surjective.

We will show that φ is injective. Let $(e_i)_i$ be a k-basis for W^G, then $(e_i \otimes 1)_i$ is a K-basis for $W^G \otimes_k K$.

Suppose that $v = \sum_i a_i(e_i \otimes 1) \in \ker\varphi$, with $a_i \in K$, is a nonzero element with minimal number of nonzero coefficients. By rescaling and reordering we can assume that $a_1 = 1$. If all coefficients a_i are in k, then

$$v = \left(\sum_i a_i e_i\right) \otimes 1 = \varphi(v) \otimes 1 = 0,$$

which contradicts $v \neq 0$, so we can assume that $a_2 \notin k$. By the fact that K/k is Galois, there exists $\sigma \in G$ such that $\sigma(a_2) \neq a_2$. It follows that $\sigma(v) - v \neq 0$. We compute

$$\varphi(\sigma(v) - v) = \varphi(\sigma(v)) - \varphi(v) = \sigma(\varphi(v)) = 0,$$

and so $\sigma(v) - v \in \ker\varphi$. However, $\sigma(v) - v$ has fewer nonzero coefficients than v, because $a_1 = 1$. This is a contradiction. We conlude that $\ker\varphi = 0$, and hence that φ is injective. ■

proof of Theorem 4.3. An isomorphism $(-)_K \circ (-)^G \simeq \mathrm{id}$ is described by Lemma 4.4. Clearly, $(-)^G \circ (-)_K \simeq \mathrm{id}$. ■

4.3 Descent of algebras

We consider the base extension $(-)_K : \mathrm{Alg}_k \to \mathrm{Alg}_K$ described in (ii) of Example 4.2.

Example 4.5. Let $n > 0$ be an integer. Consider the k-algebra $M_n(k)$ of $n \times n$-matrices over k. Its base extension is given by

$$A_K = A \otimes_k K = M_n(K).$$

The Galois group G simply acts on the coefficients of a matrix.

If B is a K-algebra equipped with a semi-linear G-action, then the elements of B invariant under this action form a k-algebra, which we denote B^G. If $f\colon B \to B'$ is a map compatible with G-actions, then it restricts to a map of k-algebras $f^G\colon B^G \to B'^G$. We see that we have a functor

$$(-)^G\colon \mathrm{Alg}_k^K \to \mathrm{Alg}_k\,.$$

By the following theorem, the base extension $(-)_K\colon \mathrm{Alg}_k \to \mathrm{Alg}_K$ satisfies Galois descent.

Theorem 4.6. *There is an equivalence of categories*

$$\begin{aligned} \mathrm{Alg}_k &\simeq \mathrm{Alg}_k^K \\ A &\mapsto A \otimes_k K \\ B^G &\mapsfrom B. \end{aligned}$$

Proof. Lemma 4.4 also works for algebras. The proof of this theorem is then completely analogous to that of Theorem 4.3. ■

4.4 Descent of quasi-projective schemes

We consider the base extension $(-)_K : \mathrm{Sch}_k \to \mathrm{Sch}_K$ described in (iii) of Example 4.2.

Example 4.7. (i) Suppose $k = \mathbb{Q}$ and $K = \mathbb{Q}(\zeta)$ with ζ a seventeenth root of unity. Let X be the affine $\mathbb{Q}$-scheme $X = \operatorname{Spec}\mathbb{Q}[x,y]/(x^2+y^2-1)$. The extension of X to $\mathbb{Q}(\zeta)$ is given by

$$\begin{aligned} X_{\mathbb{Q}(\zeta)} = X \times_{\operatorname{Spec}\mathbb{Q}} \operatorname{Spec}\mathbb{Q}(\zeta) &= \operatorname{Spec}(\mathbb{Q}[x,y]/(x^2+y^2-1) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta)) \\ &= \operatorname{Spec}\mathbb{Q}(\zeta)[x,y]/(x^2+y^2-1). \end{aligned}$$

The action of the map $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ given by $\zeta \mapsto \zeta^5$ on $X_{\mathbb{Q}(\zeta)}$ is induced by the $\mathbb{Q}$-algebra map

$$\begin{aligned} \mathbb{Q}(\zeta)[x,y]/(x^2+y^2-1) &\to \mathbb{Q}(\zeta)[x,y]/(x^2+y^2-1) \\ x &\mapsto x, y \mapsto y, \zeta \mapsto \zeta^7. \end{aligned}$$

On coefficients this map is the inverse of σ.

(ii) Let $n \geq 0$ be an integer, and consider projective n-space $\mathbb{P}^n_k = \operatorname{Proj} k[x_0,\ldots,x_n]$ over k. We find the unsurprising expression

$$(\mathbb{P}^n_k)_K = \mathbb{P}^n_K.$$

An element $\sigma \in G$ acts on $\mathbb{P}^n_K$ as the map induced by the map of graded rings

$$K[x_0,\ldots,x_n] \to K[x_0,\ldots,x_n]$$

sending $a \in K$ to $\sigma^{-1}(a)$ and x_i to x_i. Recall that K-points $\operatorname{Spec} K \to \mathbb{P}^n_K$ correspond to tuples $[a_0 : a_1 : \ldots : a_n]$, with $a_i \in K$ not all zero, modulo multiplication by elements of $K^\times$ (see [Har10, §II.7]). Equation (4.3) gives us an action on K-points by

$${}^{\sigma}[a_0 : a_1 : \ldots : a_n] = [\sigma a_0 : \sigma a_1 : \ldots : \sigma a_n],$$

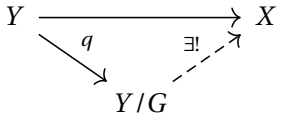
with $\sigma \in G$ and $[a_0 : \ldots : a_n] \in \mathbb{P}_K(K)$.

If F is a field, then we write QPSch_F for the category of quasi-projective schemes over F. By Example 4.7(ii), and the fact that both open and closed immersions are stable under base change, we can define a base extension $(-)_K \colon \mathrm{QPSch}_k \to \mathrm{QPSch}_K$. All other data in this base extension is defined analogously to Example 4.2. We will show that this base extension satisfies Galois descent.

Definition 4.8. *Given an object $Y \in \mathrm{QPSch}_k^K$ and a map of k-schemes $f \colon Y \to X$, we call f a G-invariant map if for all $\sigma \in G$ we have*

$$f \circ \sigma = f.$$

Proposition 4.9. *Given an object $Y \in \mathrm{QPSch}_k^K$, there exists a quasi-projective k-scheme Y/G and a G-invariant map of k-schemes $q \colon Y \to Y/G$ such that for any G-invariant map of k-schemes $Y \to X$ there exists a unique map of k-schemes $Y/G \to X$ making the following diagram commute.*



Sketch of proof. We only roughly sketch the construction of quotients. We refer to [Bru09, Theorem 12.1] for a complete proof.

If $Y = \operatorname{Spec} B$ is taken to be affine with B a K-algebra, then B is equipped with a semi-linear G-action from Y, and the quotient is given by the map $\operatorname{Spec} B \to \operatorname{Spec} B^G$ induced by the inclusion $B^G \hookrightarrow B$. In the general case we cover Y by open affines U_i stable under the action of G and construct the quotient of Y by glueing the quotients U_i/G and U_j/G together along $(U_i \cap U_j)/G = U_i/G \cap U_j/G$. The reason we can always cover Y by G-stable open affines is by the assumption that Y is quasi-projective (see [Jah00, Lemma 2.10]). ■

Notice that quotients are unique up to canonical isomorphism.

Definition 4.10. *In the above proposition, we refer to $q\colon Y \to Y/G$ as the quotient of Y by the action of G.*

Given objects $Y, Y' \in \mathrm{QPSch}_k^K$ and a map $f\colon Y \to Y'$ in QPSch_k^K, let $q'\colon Y' \to Y'/G$ be the quotient of Y' by G. The composition $q' \circ f$ is a G-invariant map:

$$q' \circ f \circ \sigma = q' \circ \sigma \circ f = q' \circ f,$$

and hence we get a natural map $f/G\colon Y/G \to Y'/G$ of k-schemes. In this way we obtain a functor

$$(-)/G\colon \mathrm{QPSch}_k^K \to \mathrm{QPSch}_k.$$

The following theorem shows that the base extension $(-)_K\colon \mathrm{QPSch}_k \to \mathrm{QPSch}_K$ satisfies Galois descent.

Theorem 4.11. *There is an equivalence of categories*

$$\begin{aligned} \mathrm{QPSch}_k &\simeq \mathrm{QPSch}_k^K \\ X &\mapsto X \times_{\operatorname{Spec} k} \operatorname{Spec} K \\ Y/G &\mapsfrom Y. \end{aligned}$$

Proof. Let X be a quasi-projective scheme over k. If X is affine, the natural map $X_K \to X$ is a quotient by Theorem 4.6. The general case then follows by glueing; hence, we have $(-)/G \circ (-)_K \simeq \mathrm{id}$.

Given $Y \in \mathrm{QPSch}_k^K$. If Y is affine, we get that $(Y/G)_K \simeq Y$ by Theorem 4.6. In the general case we proceed as in the proof of Proposition 4.9 and cover Y by G-stable open affines $\{U_i\}$. Then $(Y/G)_K$ can be constructed by glueing $(U_i/G)_K = U_i$, which gives $(Y/G)_K \simeq Y$; hence, we have $(-)_K \circ (-)/G \simeq \mathrm{id}$. ■

5 Twists

We use the same notation and terminology as in Section 4.

Suppose K/k is a field extension and $(-)_K\colon \mathscr{C}_k \to \mathscr{C}_K$ is a functor. For an object X over k, it is interesting to consider the so called K/k-*twists* of X: objects over k to which X_K descends. Explicitly, we define

$$T_{K/k}(X) = \{Y \in \mathscr{C}_k : Y_K \simeq_K X_K\}/\simeq_k. \tag{5.1}$$

We endow $T_{K/k}(X)$ with a basepoint given by the class of the *trivial twist*, X. When $K = k^s$ is a separable closure of k, we simply refer to k^s/k-twists as *twists*. In this case we also write $T(X)$ instead of $T_{k^s/k}(X)$.

For the rest of this section we fix a finite Galois extension K/k with group G, a base extension $(-)_K \colon \mathscr{C}_k \to \mathscr{C}_K$ satisfying Galois descent, and an object X over k. The functor $(-)_K$ can be viewed as a functor $\mathscr{C}_k \to \mathscr{C}_k^K$ by the definition of a base extension, where the category $\mathscr{C}_k^K$ is defined as in Section 4. We let $F \colon \mathscr{C}_k^K \to \mathscr{C}_k$ be a functor such that $F(-)_K \simeq \mathrm{id}$ and $(-)_K F \simeq \mathrm{id}$, which exists by Galois descent. Equation (4.3) provides us with an action of G on $\mathrm{Aut}_K(X_K)$, turning it into a (perhaps noncommutative) G-module. Theorem 5.5 describes a bijection between $T_{K/k}(X)$ and the first cohomology set $H^1(G; \mathrm{Aut}_K(X_K))$.

Let Y be a K/k-twist of X, and let $\varphi \colon X_K \to Y_K$ be a K-isomorphism. For every $\sigma \in G$ we define $c_\sigma \in \mathrm{Aut}_K(X_K)$ by

$$c_\sigma = \varphi^{-1} \circ {}^\sigma\varphi. \tag{5.2}$$

This defines a function $c \colon G \to \mathrm{Aut}_K(X_K), \sigma \mapsto c_\sigma$, which essentially measures to which extent φ is not a G-equivariant map. In particular, if φ *is* G-equivariant, then c sends all $\sigma \in G$ to the identity map $1 \colon X_K \to X_K$.

The function c is a cocycle: for $\sigma, \tau \in G$ we have

$$\begin{aligned} c_{\sigma\tau} &= \varphi^{-1} \circ {}^{\sigma\tau}\varphi \\ &= \varphi^{-1} \circ {}^\sigma\varphi \circ ({}^\sigma\varphi)^{-1} \circ {}^{\sigma\tau}\varphi \\ &= c_\sigma \circ {}^\sigma(\varphi^{-1} \circ {}^\tau\varphi) \\ &= c_\sigma \circ {}^\sigma c_\tau. \end{aligned}$$

Example 5.1. Suppose the Galois extension K/k is $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$, and let X be the conic over $\mathbb{Q}$ given by the equation $x^2 + y^2 = 3z^2$. The conic X is a $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$-twist of the projective line over $\mathbb{Q}$: the base extension of X to $\mathbb{Q}(\sqrt{3})$ is the conic over $\mathbb{Q}(\sqrt{3})$ given by the same equation, and we have an isomorphism

$$\begin{aligned} \varphi \colon \mathbb{P}^1_{\mathbb{Q}(\sqrt{3})} &\xrightarrow{\simeq} X_{\mathbb{Q}(\sqrt{3})} \\ [s:t] &\mapsto \left[\frac{s^2 - t^2}{2} : st : \frac{s^2 + t^2}{2\sqrt{3}}\right]. \end{aligned}$$

We compute the cocycle associated to φ. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$ be such that $\sigma \neq 1$. We find

$$[s:t] \xmapsto{{}^\sigma\varphi} \left[\frac{s^2 - t^2}{2} : st : \frac{-s^2 - t^2}{2\sqrt{3}}\right] \xmapsto{\varphi^{-1}} [-t:s].$$

We conclude that $c_\sigma = \varphi^{-1} \circ {}^\sigma\varphi$ is the projective transformation given by the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

The choice of K-isomorphism $\varphi \colon X_K \to Y_K$ is not canonical, but the resulting cocycle class is, as shown by the following proposition.

Proposition 5.2. *Let Y be an object over k such that $[Y] \in T_{K/k}(X)$, and let $Z \in \mathscr{C}_k$ be such that $Y \simeq_k Z$. Let $\varphi\colon X_K \to Y_K$ and $\psi\colon X_K \to Z_K$ be K-isomorphisms. Consider the cocycles associated to φ and ψ given by $c_\sigma = \varphi^{-1} \circ {}^\sigma\varphi$ and $d_\sigma = \psi^{-1} \circ {}^\sigma\psi$, respectively. Then the cocycles c and d are cohomologous.*

Proof. Let $f\colon Z \to Y$ be a k-isomorphism. The map f_K is a morphism in $\mathscr{C}_k^K$, and so it is invariant under the action of G. Define the K-automorphism $a = \varphi^{-1} \circ f_K \circ \psi$. We compute

$$\begin{aligned} d_\sigma &= \psi^{-1} \circ {}^\sigma\psi \\ &= a^{-1} \circ \varphi^{-1} \circ f_K \circ {}^\sigma(f_K^{-1} \circ \varphi \circ a) \\ &= a^{-1} \circ \varphi^{-1} \circ {}^\sigma\varphi \circ {}^\sigma a \\ &= a^{-1} \circ c_\sigma \circ {}^\sigma a, \end{aligned}$$

and so c and d are cohomologous. ∎

The above proposition allows us to speak of the cocycle class associated to the k-isomorphism class of a K/k-twist. We now get a well-defined function

$$\theta\colon T_{K/k}(X) \to H^1(G; \mathrm{Aut}_K(X_K)) \tag{5.3}$$

sending the class of a K/k-twist to its associated coycle class. The class of the trivial twist gets sent to the class of the trivial cocycle, so this is a map of pointed sets. We intend to construct an inverse to this map, so that θ^{-1} will give us a parameterization of the K/k-twists of X.

Let $\varphi\colon X_K \to Y_K$ be as before. The map φ is not G-equivariant if c is not the trivial cocycle, but it will be if we let $\sigma \in G$ act on X_K by the k-automorphism $c_\sigma\sigma$ instead: we have a commutative diagram

$$\begin{array}{ccc} X_K & \xrightarrow{\varphi} & Y_K \\ \downarrow{\scriptstyle c_\sigma\sigma} & & \downarrow{\scriptstyle \sigma} \\ X_K & \xrightarrow{\varphi} & Y_K. \end{array}$$

Using the fact that c is a cocycle, we show that this actually defines an action on X_K. Indeed, for $\sigma, \tau \in G$ we have

$$\begin{aligned} c_{\sigma\tau} \circ (\sigma\tau) &= c_\sigma \circ {}^\sigma c_\tau \circ \sigma \circ \tau \\ &= c_\sigma \circ \sigma \circ c_\tau \circ \sigma^{-1} \circ \sigma \circ \tau \\ &= (c_\sigma\sigma) \circ (c_\tau\tau). \end{aligned}$$

This action is also Galois by (4.1) and (4.2), because $c_\sigma \in \mathrm{Hom}_K(X_K, X_K) = \mathrm{Hom}_{\mathrm{id}}(X_K, X_K)$.

Definition 5.3. *Let $c = (c_\sigma)$ be a cocycle $G \to \mathrm{Aut}_K(X_K)$. We define the action of G twisted by c on X_K by letting $\sigma \in G$ act on X_K as the k-automorphism $c_\sigma \circ \sigma$. We write ${}_cX_K$ for X_K equipped with this action.*

Proposition 5.4. *Let $c = (c_\sigma)$ and $d = (d_\sigma)$ be cocycles $G \to \mathrm{Aut}_K(X_K)$. If c and d are cohomologous, then ${}_cX_K$ and ${}_dX_K$ are isomorphic in $\mathscr{C}_k^K$.*

Proof. Let $a \in \mathrm{Aut}_K(X_K)$ be such that $c_\sigma = a^{-1} d_\sigma {}^\sigma a$ for all $\sigma \in G$. We have a commutative diagram

$$\begin{array}{ccc} X_K & \xrightarrow{a} & X_K \\ \downarrow{\scriptstyle c_\sigma \sigma} & & \downarrow{\scriptstyle d_\sigma \sigma} \\ X_K & \xrightarrow{a} & X_K. \end{array}$$

It follows that a defines an isomorphism ${}_cX_K \simeq {}_dX_K$ in $\mathscr{C}_k^K$. ∎

Given a cocycle $c\colon G \to \mathrm{Aut}_K(X_K)$, the object $F({}_cX_K)$ over k is a K/k-twist of X, because of the equivalence $F\colon \mathscr{C}_k^K \rightleftarrows \mathscr{C}_k : (-)_K$ and the fact that ${}_cX_K$ and X_K are the same when viewed as K-objects. By the above proposition we now have a well-defined function

$$\begin{aligned} \eta\colon H^1(G;\mathrm{Aut}_K(X_K)) &\to T_{K/k}(X) \\ [c] &\mapsto [F({}_cX_K)]. \end{aligned} \tag{5.4}$$

The trivial cocycle class gets mapped to the class of the trivial twist, so this is a map of pointed sets. The following result states that the maps θ and η, defined in (5.3) and (5.4), are inverse to each other.

Theorem 5.5 (Main result on twists)**.** *There is an isomorphism of pointed sets*

$$\begin{aligned} T_{K/k}(X) &\xrightarrow{\simeq} H^1(G;\mathrm{Aut}_K(X_K)) \\ \theta\colon [Y] &\mapsto [(\varphi^{-1} \circ {}^\sigma\varphi)_{\sigma\in G}] \\ [F({}_cX_K)] &\mapsfrom [c] : \eta, \end{aligned}$$

where $\varphi\colon X_K \to Y_K$ is some K-isomorphism.

Proof. Let $[Y]$ be the class of a K/k-twist Y of X, let $\varphi\colon X_K \to Y_K$ be a K-isomorphism, and let $c = (c_\sigma) = (\varphi^{-1} \circ {}^\sigma\varphi)$ be its associated cocycle. The map φ defines an isomorphism ${}_cX_K \to Y_K$ in $\mathscr{C}_k^K$ (see the paragraph above Definition 5.3). Applying F we get a k-isomorphism $F({}_cX_K) \xrightarrow{\simeq} F(Y_K) \simeq Y$. We find $\eta \circ \theta = \mathrm{id}$.

Let $[c] = [(c_\sigma)] \in H^1(G;\mathrm{Aut}_K(X_K))$ be the cohomology class of a cocycle c. There exists an isomorphism $\varphi\colon {}_cX_K \to F({}_cX_K)_K$ of objects in $\mathscr{C}_k^K$. We now have a commutative diagram

$$\begin{array}{ccc} X_K & \xrightarrow{\varphi} & (F({}_cX_K))_K \\ \downarrow{\scriptstyle c_\sigma \sigma} & & \downarrow{\scriptstyle \sigma} \\ X_K & \xrightarrow{\varphi} & (F({}_cX_K))_K. \end{array}$$

It follows that $\varphi^{-1} \circ {}^\sigma\varphi = c_\sigma$. Thus, the cocycle class associated to $F({}_cX_K)$ is equal to $[c]$, and hence we find $\theta \circ \eta = \mathrm{id}$. ∎

Example 5.6. Suppose K/k is the Galois extension $\mathbb{C}/\mathbb{R}$. Let A be the $\mathbb{R}$-algebra $\mathbb{R} \times \mathbb{R} \simeq \mathbb{R}[x]/(x^2 - 1)$. The extension of A to $\mathbb{C}$ is given by

$$A_{\mathbb{C}} = A \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C}[x]/(x^2 - 1) \simeq \mathbb{C} \times \mathbb{C}.$$

The group $\mathrm{Aut}_{\mathbb{C}}(A_{\mathbb{C}})$ is of order 2. As a result, $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ must act trivially on $\mathrm{Aut}_{\mathbb{C}}(A_{\mathbb{C}})$, and so we find

$$H^1(\mathbb{R};\mathrm{Aut}_{\mathbb{C}}(A_{\mathbb{C}})) = \mathrm{Hom}(\mathrm{Gal}(\mathbb{C}/\mathbb{R}),\mathrm{Aut}_{\mathbb{C}}\, A_{\mathbb{C}}).$$

This set consists of only two elements, and so by Theorem 5.5 the algebra A has only one non-trivial twist up to $\mathbb{R}$-isomorphism. It is given by $A' = \mathbb{C}$; indeed, we have

$$A'_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C} \simeq A_{\mathbb{C}},$$

and A' is not isomorphic to A, because A is not a field.

In terms of affine schemes: the scheme $X = \mathrm{Spec}\,\mathbb{R} \sqcup \mathrm{Spec}\,\mathbb{R}$ only has one non-trivial twist given by the $\mathbb{R}$-scheme $\mathrm{Spec}\,\mathbb{C} = \mathrm{Spec}\,\mathbb{R}[x]/(x^2+1)$.

Corollary 5.7. *Let L/ℓ be a Galois extension, and $n \geq 0$ an integer. We have an action of $\mathrm{Gal}(L/\ell)$ on $\mathrm{GL}_n(L)$ by acting on the coefficients of a matrix. This turns $\mathrm{GL}_n(L)$ into a discrete $\mathrm{Gal}(L/\ell)$-module, and we have*

$$H^1(L/\ell;\mathrm{GL}_n(L)) = 0.$$

Proof. Notice that $\mathrm{GL}_n(L)$ is the automorphism group of the L-vector space L^n. If L/ℓ is finite, the result follows from Theorem 5.5, and the fact that twists of a vector space are always trivial. Continuity of the action in the general case is clear, and we find

$$\begin{aligned} H^1(L/\ell;\mathrm{GL}_n(L)) &= \varinjlim H^1(F/\ell;\mathrm{GL}_n(L)^{\mathrm{Gal}(L/F)}) \\ &= \varinjlim H^1(F/\ell;\mathrm{GL}_n(F)) = 0, \end{aligned}$$

by Proposition 3.25, with the direct limit taken over the finite Galois extensions F/ℓ such that $F \subset L$. ∎

Notice that we retrieve Proposition 3.24 from Corollary 5.7 by taking n equal to 1. For this reason, the above corollary is often referred to as the *generalized Hilbert's Theorem 90*.

6 Severi-Brauer varieties

This section will look at a geometric application of the theory of twists, so called Severi-Brauer varieties. The theory of twists will yield a parametrization of all Severi-Brauer varieties. Throughout this section we fix a field k with a separable closure k^s. Many of the results in this section can also be found in [Jah00, §4], but in our case they follow more readily from Section 5.

If L/ℓ is a field extension, and X is scheme over ℓ, then we write X_L for the fiber product $X \times_{\mathrm{Spec}\,\ell} \mathrm{Spec}\,L$.

Definition 6.1. *Let X be a k-scheme. We call X a Severi-Brauer variety (over k) of dimension r, if there is an isomorphism $X_{k^s} \simeq \mathbb{P}^r_{k^s}$.*

In other words, the Severi-Brauer varieties over k of dimension r are precisely the twists of $\mathbb{P}^r_k$. In agreement with our notation for twists, the set of k-isomorphism classes of Severi-Brauer varieties of dimension r is denoted $T(\mathbb{P}^r_k)$, and a Severi-Brauer variety is called *trivial* if it is isomorphic to $\mathbb{P}^r_k$.

To be able to parameterize Severi-Brauer varieties as twists using the results from Section 5, we need to be able to apply Galois descent as in Section 4.4, and so we need to know that Severi-Brauer varieties are at least quasi-projective. This turns out to be true, as shown by the following proposition.

Proposition 6.2. *Let X be a Severi-Brauer variety, then X is projective.*

Proof. We refer to [Jah00, Lemma 2.12]. ■

Remark 6.3. Severi-Brauer varieties have many more nice properties. For example, they are integral and of finite type. See [Jah00, Lemma 2.12]. This justifies the use of the word "variety" in Definition 6.1, but we will not need any of these properties.

It turns out to be sufficient to consider finite Galois extensions when working with Severi-Brauer varieties, as shown by the following proposition.

Proposition 6.4. *Let X be a Severi-Brauer variety of dimension r. Then there exists some finite Galois extension ℓ/k such that we have an isomorphism $X_\ell \simeq_\ell \mathbb{P}^r_\ell$.*

Proof. Let $\varphi\colon \mathbb{P}_{k^s} \to X_{k^s}$ be a k^s-isomorphism. Then φ is of finite type. As a result, only a finite number of coefficients in k^s are needed to describe φ. Considering the field extension over k generated by these coefficients, and embedding it in a finite Galois extension, we obtain a finite Galois extension ℓ of k over which X_ℓ and $\mathbb{P}^r_\ell$ are isomorphic. ■

In the above proposition, we refer to ℓ as a *splitting field* of X and say that X is *split by* ℓ. To adhere to our notation for twists, we write $T_{\ell/k}(\mathbb{P}^r_k)$ for the set of Severi-Brauer varieties of dimension r split by ℓ. As a result of the above proposition, we obtain the expression

$$T(\mathbb{P}^r_k) = \varinjlim T_{\ell/k}(\mathbb{P}^r_k), \tag{6.1}$$

with the direct limit running over the finite Galois extensions ℓ/k with $\ell \subset k^s$. The transition maps are given by the natural inclusion maps; if X is split by ℓ and $\ell \subset \ell'$, then X is also split by ℓ':

$$X_{\ell'} = (X_\ell)_{\ell'} \simeq (\mathbb{P}^r_\ell)_{\ell'} = \mathbb{P}^r_{\ell'},$$

where the last equality is by Example 4.7(ii).

Example 6.5. The conic X over $\mathbb{Q}$ given by the equation $x^2 + y^2 = 3z^2$ is an example of a Severi-Brauer variety over $\mathbb{Q}$ of dimension 1, as shown in Example 5.1. To see that this is a non-trivial Severi-Brauer variety, note that the curve $x^2 + y^2 = 3z^2$ admits no $\mathbb{Q}$-rational points. To prove this, we can show that the equation admits no solutions in integers by considering it modulo 4.

At the end of this section we will see that the existence of a rational point is actually enough to prove triviality of a Severi-Brauer variety. For smooth conics this is a well known basic fact from geometry.

We recall (see, for instance, [Har10, Chapter 2, Example 7.1.1]) that the ℓ-automorphism group of $\mathbb{P}^r_\ell$, with ℓ a field, is the group $\mathrm{PGL}_{r+1}(\ell)$ defined by the exact sequence of groups

$$1 \to \ell^\times \to \mathrm{GL}_{r+1}(\ell) \to \mathrm{PGL}_{r+1}(\ell) \to 1, \tag{6.2}$$

where the map $\ell^\times \to \mathrm{GL}_{r+1}(\ell)$ is given by sending a scalar to that scalar times the $(r+1)\times(r+1)$-identity matrix. Explicitly, a matrix $A = (a_{ij}) \in \mathrm{PGL}_{r+1}(\ell)$ acts on an ℓ-point $[a_0 : \ldots : a_n] \in \mathbb{P}^r_\ell(\ell)$ by viewing it as a column vector and multiplying it on the left by A.

If ℓ/k is finite Galois, then the action of $\mathrm{Gal}(\ell/k)$ on $\mathrm{PGL}_{r+1}(\ell)$ given by acting on coordinates corresponds to the action defined in (4.3). In particular, this turns the sequence in (6.2) into an exact sequence of $\mathrm{Gal}(\ell/k)$-modules.

Corollary 6.6. *Let ℓ/k be a finite Galois extension, and Let $r \geq 0$ be an integer. We have an isomorphism of pointed sets*

$$\begin{aligned} T_{\ell/k}(\mathbb{P}^r_\ell) &\xrightarrow{\simeq} H^1(\ell/k, \mathrm{PGL}_{r+1}(\ell)) \\ X &\mapsto [(\varphi^{-1} \circ {}^\sigma\varphi)_\sigma], \end{aligned}$$

where $\varphi\colon \mathbb{P}^r_\ell \to X_\ell$ is an isomorphism. This isomorphism is natural in ℓ.

Proof. This isomorphism is the one obtained from Theorem 5.5. Naturality is straightforward. ∎

We similarly equip $\mathrm{PGL}_{r+1}(k^s)$ with a $\mathrm{Gal}(k^s/k)$-action by acting on the coordinates of a matrix. This action is then continuous. Taking $\mathrm{Gal}(k^s/\ell)$-invariants of the sequence

$$1 \to (k^s)^\times \to \mathrm{GL}_{r+1}(k^s) \to \mathrm{PGL}_{r+1}(k^s) \to 1,$$

we get the exact sequence of $\mathrm{Gal}(\ell/k)$-modules

$$1 \to \ell^\times \to \mathrm{GL}_{r+1}(\ell) \to \mathrm{PGL}_{r+1}(k^s)^{\mathrm{Gal}(k^s/\ell)} \to 1,$$

by Proposition 3.26, because of the equality $H^1(k, (k^s)^\times) = 0$ from Corollary 5.7. It follows that $\mathrm{PGL}_{r+1}(k^s)^{\mathrm{Gal}(k^s/\ell)} = \mathrm{PGL}_{r+1}(\ell)$ as $\mathrm{Gal}(\ell/k)$-modules. By Proposition 3.25 we now find

$$H^1(k, \mathrm{PGL}_{r+1}(k^s)) = \varinjlim H^1(\ell/k, \mathrm{PGL}_{r+1}(\ell)), \tag{6.3}$$

with the direct limit runing over the finite Galois extensions ℓ/k with $\ell \subset k^s$.

Theorem 6.7. *Let $r \geq 0$ be an integer. We have an isomorphism of pointed sets*

$$\begin{aligned} T(\mathbb{P}^r_k) &\xrightarrow{\simeq} H^1(k; \mathrm{PGL}_{r+1}(k^s)) \\ X &\mapsto [(\varphi^{-1} \circ {}^\sigma\varphi)_\sigma], \end{aligned}$$

where $\varphi\colon \mathbb{P}^r_{k^s} \to X_{k^s}$ is an isomorphism.

Proof. By Corollary 6.6 we have natural isomorphisms

$$\theta_{\ell/k}\colon T_{\ell/k}(\mathbb{P}^r_k) \xrightarrow{\simeq} H^1(\ell/k;\mathrm{PGL}_{r+1}(\ell)),$$

for all finite Galois extensions $k \subset \ell \subset k^s$. These isomorphisms concatenate into an isomorphism

$$(T_{\ell/k}(\mathbb{P}^r_k)) \xrightarrow{\simeq} (H^1(\ell/k;\mathrm{PGL}_{r+1}(\ell)))$$

of direct systems, and hence

$$T(\mathbb{P}^r_k) = \varinjlim T_{\ell/k}(\mathbb{P}^r_k) \simeq \varinjlim H^1(\ell/k;\mathrm{PGL}_{r+1}(\ell)) = H^1(k;\mathrm{PGL}_{r+1}(k^s)),$$

where the first equality is by (6.1) and the last equality is by (6.3). That this isomorphism is given by the map in the theorem is now not hard to see.

■

The following theorem shows that determining whether a Severi-Brauer variety is trivial, is equivalent to determining whether it has a rational point over k. This is important information about the arithmetic of k.

Theorem 6.8. *Let X be a Severi-Brauer variety, then X is trivial if and only if X has a k-rational point.*

Proof. This proof is inspired by [Jah00, Proposition 4.8]. If X is trivial, then clearly X has a rational point. Now suppose X has a k-rational point $Q \in X(k)$. Let $\varphi\colon \mathbb{P}^r_{k^s} \to X_{k^s}$ be an isomorphism. The k-point Q induces a k^s-point Q_{k^s}, and by composing with an automorphism of $\mathbb{P}^r_{k^s}$ we can assume that $\varphi(P) = Q_{k^s}$, where P is the point $[1:0:\ldots:0] \in \mathbb{P}^r_{k^s}(k^s)$. We consider the cocycle $c = (c_\sigma = \varphi^{-1} \circ {}^\sigma\varphi)$ associated to φ. To show triviality of X, it suffices to prove that $[c] = 0$ in $H^1(k;\mathrm{PGL}_{r+1}(k^s))$ by Theorem 6.7.

The points Q_{k^s} and P are invariant under the action of $\mathrm{Gal}(k^s/k)$, as both are induced by k-points, and so we find

$$\begin{aligned} c_\sigma(P) &= \varphi^{-1\sigma}\varphi(P) \\ &= \varphi^{-1\sigma}\varphi({}^\sigma P) \\ &= \varphi^{-1\sigma}(\varphi(P)) \\ &= \varphi^{-1\sigma}(Q_{k^s}) \\ &= \varphi^{-1}(Q_{k^s}) = P. \end{aligned}$$

As a result c_σ lies in the stabilizer of P under $\mathrm{PGL}_{r+1}(k^s)$. This stabilizer is equal to

$$S_P = \left\{ \begin{pmatrix} * & * & \ldots & * \\ 0 & * & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \ldots & * \end{pmatrix} \in \mathrm{PGL}_{r+1}(k^s) \right\}.$$

The subgroup S_P is, in fact, a $\mathrm{Gal}(k^s/k)$-submodule of $\mathrm{PGL}_{r+1}(k^s)$, and so we can view the cocycle class of c in $H^1(k, S_P)$. Considering its image under the map induced by the inclusion $S_P \hookrightarrow \mathrm{PGL}_{r+1}(k^s)$, we obtain the cocycle class of c in $H^1(k, \mathrm{PGL}_{r+1}(k^s))$. We now have a commutative diagram of $\mathrm{Gal}(k^s/k)$-modules

$$\begin{array}{ccc} & & \mathrm{GL}_{r+1}(k^s) \\ & \nearrow & \downarrow \\ S_P & \hookrightarrow & \mathrm{PGL}_{r+1}(k^s), \end{array}$$

where the dashed arrow is given by scaling the top left coefficient to 1. Considering the induced maps on H^1, we obtain the diagram

$$\begin{array}{ccc} & H^1(k; \mathrm{GL}_{r+1}(k^s)) & \\ \nearrow & & \searrow \\ H^1(k; S_P) & \longrightarrow & H^1(k; \mathrm{PGL}_{r+1}(k^s)). \end{array}$$

By Corollary 5.7, we find that $H^1(k; \mathrm{GL}_{r+1}(k^s)) = 0$, and so the map $H^1(k; S_P) \to H^1(k; \mathrm{PGL}_{r+1}(k^s))$ is zero. We conclude that $[c] = 0$ in $H^1(k; \mathrm{PGL}_{r+1}(k^s))$, and hence that there exists an isomorphism $X \simeq_k \mathbb{P}^r_k$ by the pointed isomorphism in Theorem 6.7. ■

7 Central simple algebras

This section considers an algebraic application of the theory of twists. Using Theorem 5.5 we will give a parametrization of so called *central simple algebras*. We will also show the existence of a one-to-one correspondence between central simple algebras and the Severi-Brauer varieties from Section 6. This correspondence will be made explicit for one-dimensional Severi-Brauer varieties. Many of the results in the first part of this section can also be found in [Jah00, §3] and [GS17, Chapter 2]. Throughout this section we fix a field k with a separable closure k^s.

If A is an ℓ-algebra, and L/ℓ is a field extension, then we write A_L for the L-algebra $A \otimes_\ell L$.

Definition 7.1. *Let A be a finite-dimensional algebra over k. We call A central if the center of A equals k. We call A simple if A has no non-trivial two-sided ideals.*

Example 7.2. Let $r \geq 1$ be an integer. The algebra of $r \times r$-matrices over k, denoted $M_r(k)$, is a central simple algebra of dimension r^2 over k. See [GS17, Example 2.1.2].

The example above turns out to be crucial, as shown by the following theorem: the central simple algebras are precisely the twists of $M_r(k)$ with r ranging over the positive integers.

Proposition 7.3. *Let A be a k-algebra. Then A is a central simple algebra if and only if there exists an isomorphism $A_{k^s} \simeq M_r(k^s)$ for some $r \geq 1$.*

Proof. We refer to [GS17, Proposition 2.2.5]. ∎

In particular, every central simple algebra has dimension equal to a square by the above proposition.

Proposition 7.3 can be rephrased in the language of twists by saying that the central simple algebras are precisely the twists of $M_r(k)$ with r ranging over the positive integers. In line with this interpretation, we denote the set of k-isomorphism classes of r^2-dimensional central simple algebras by $T(M_r(k))$, and call a central simple algebra *trivial* if it is isomorphic to $M_r(k)$.

Analogously to Proposition 6.4 we have the following statement.

Proposition 7.4. *Let A be a central simple algebra over k of dimension r^2, then there exists a finite Galois extension ℓ/k such that $A_\ell \simeq M_r(\ell)$.*

In the above proposition we refer to ℓ as a *splitting field* of A and say that A is *split by* ℓ. As with twists, we write $T_{\ell/k}(M_r(k))$ for the set of k-isomorphism classes of central simple algebras of dimension r^2 split by ℓ. Analogously to (6.1) we obtain the following expression

$$T(M_r(k)) = \varinjlim T_{\ell/k}(M_r(k)),$$

with the direct limit running over the finite Galois extensions ℓ/k with $\ell \subset k^s$. To parameterize central simple algebras of dimension r^2 over k as twists, we need to understand the automorphism group of $M_r(k)$. To this end we state the following proposition.

Proposition 7.5 (Skölem-Noether)**.** *Let $r \geq 1$ be an integer, and let F be a field. We have an isomorphism*

$$\begin{aligned} \mathrm{PGL}_r(F) &\xrightarrow{\sim} \mathrm{Aut}_F(M_r(F)) \\ B &\mapsto (A \mapsto BAB^{-1}). \end{aligned}$$

Proof. We refer to [GS17, Corollary 2.4.2]. ∎

If ℓ/k is a finite Galois extension, then the induced action of $\mathrm{Gal}(\ell/k)$ on $\mathrm{PGL}_r(\ell)$ from (4.3) is given by acting on the coefficients of a matrix. Analogously to Corollary 6.6 and Theorem 6.7 we obtain the following results.

Corollary 7.6. *Let $r \geq 1$ be an interger, and let ℓ/k be a finite Galois extension. Then we have an isomorphism*

$$\begin{aligned} T_{\ell/k}(M_r(k)) &\xrightarrow{\simeq} H^1(\ell/k, \mathrm{PGL}_r(\ell)) \\ [A] &\mapsto [(\varphi^{-1} \circ {}^\sigma\varphi)], \end{aligned}$$

with $\varphi\colon M_r(\ell) \to A_\ell$ an isomorphism. This isomorphism is natural in ℓ.

Theorem 7.7. *Let $r \geq 1$ be an integer. Then we have an isomorphism*

$$\begin{aligned} T(M_r(k)) &\xrightarrow{\simeq} H^1(k^s/k; \mathrm{PGL}_r(k^s)) \\ [A] &\mapsto [(\varphi^{-1} \circ {}^\sigma\varphi)], \end{aligned}$$

with $\varphi\colon M_r(k^s) \to A_{k^s}$ an isomorphism.

Let $r \geq 1$ be an integer. By composing the isomorphisms in theorems 6.7 and 7.7 we obtain an isomorphism of pointed sets

$$T(M_r(k)) \simeq T(\mathbb{P}_k^{r-1}). \tag{7.1}$$

Corollary 7.8. *Let A be a central simple algebra. Then A is trivial if and only if the Severi-Brauer variety associated to A (up to k-isomorphism) has a rational point.*

Proof. This follows from Theorem 6.8 ■

7.1 Quaternion algebras and associated conics

This section is inspired by [Ser97, §3.1.4, Exercise 3]. We assume $\mathrm{Char}(k) \neq 2$ unless otherwise specified. We consider central simple algebras of dimension $2^2 = 4$ over k. Given units $a, b \in k^\times$, let $\mathbb{H}(a,b)$ be the k-algebra generated by i and j satisfying the relations

$$i^2 = a, j^2 = b, ij = -ji.$$

We call $\mathbb{H}(a,b)$ the *quaternion algebra corresponding to the pair* (a,b). The algebra $\mathbb{H}(a,b)$ is a central simple algebra of dimension 4 split by $k(\sqrt{a})$. An isomorphism is given by

$$\mathbb{H}(a,b) \otimes_k k(\sqrt{a}) \xrightarrow{\simeq} M_2(k(\sqrt{a}))$$
$$i \mapsto \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}, j \mapsto \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}.$$

By the following proposition, the quaternion algebras exhaust all central simple algebras of dimension 4.

Proposition 7.9. *Let A be a central simple algebra of dimension 4, then there exist $a, b \in k^\times$ such that $A \simeq_k \mathbb{H}(a,b)$.*

Proof. We refer to [GS17, Proposition 1.1.7 and Proposition 1.2.1]. ■

By (7.1), we obtain a correspondence between the quaternion algebras and Severi-Brauer varieties of dimension 1. In particular, by the following theorem and the above proposition, this correspondence shows that the Severi-Brauer varieties of dimension 1 are precisely the smooth conics over k.

Theorem 7.10. *The isomorphism of pointed sets*

$$T(\mathbb{P}_k^1) \xrightarrow{\simeq} T(M_2(k))$$

of (7.1) sends the k-isomorphism class of a conic in $\mathbb{P}_k^2$ given by the equation $ax^2 + by^2 = z^2$ with $a, b \in k^\times$, to the k-isomorphism class of $\mathbb{H}(a,b)$.

We refer to the conic given by the equation $ax^2 + by^2 = z^2$ as the *conic associated to the pair* (a,b).

Proof. Let $a, b \in k^\times$. Let X be the conic in $\mathbb{P}^2_k$ given by the equation $ax^2 + by^2 = z^2$. A splitting field for this conic is given by $k(\sqrt{a})$. Indeed, over $k(\sqrt{a})$ we have that $X_{k(\sqrt{a})}$ is isomorphic to the conic $x^2 + by^2 = z^2$, which has a rational point, $[1:0:1]$, and hence it is isomorphic to $\mathbb{P}^1_{k(\sqrt{a})}$. An isomorphism $\varphi\colon \mathbb{P}^1_{k(\sqrt{a})} \to X_{k(\sqrt{a})}$ is given by

$$[s:t] \mapsto \left[\frac{bs^2 - t^2}{2\sqrt{a}} : st : \frac{t^2 + bs^2}{2}\right].$$

Let $\sigma \in \mathrm{Gal}(k(\sqrt{a})/k)$ with $\sigma \neq 1$. We compute the cocycle c associated to φ:

$$c_\sigma = \varphi^{-1} \circ {}^\sigma\varphi = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix} \in \mathrm{PGL}_2(k(\sqrt{a})).$$

We consider the action twisted by c of $\mathrm{Gal}(k(\sqrt{a})/k)$ on $M_2(k(\sqrt{a}))$ by letting σ act as $c_\sigma\sigma$. Explicitly, σ acts on matrices as

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix} \begin{pmatrix} \sigma(\alpha) & \sigma(\beta) \\ \sigma(\gamma) & \sigma(\delta) \end{pmatrix} \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}^{-1}.$$

The k-isomorphism class in $T(M_2(k))$ associated to the cocycle class of c is the class of the algebra ${}_cM_2(k(\sqrt{a}))^{\mathrm{Gal}(k(\sqrt{a})/k)}$. This algebra consists of matrices of the form

$$\begin{pmatrix} \alpha_1 + \alpha_2\sqrt{a} & \alpha_3 + \alpha_4\sqrt{a} \\ \alpha_3 b - \alpha_4 b\sqrt{a} & \alpha_1 - \alpha_2\sqrt{a} \end{pmatrix},$$

with $\alpha_i \in k$. As a result, it is generated as a k-vector space by

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}, J = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}, IJ = \begin{pmatrix} 0 & \sqrt{a} \\ -b\sqrt{a} & 0 \end{pmatrix}.$$

The relations $I^2 = a, J^2 = b, IJ = -JI$ are now easily computed and it is clear that no further relations can exist. We obtain an isomorphism ${}_cM_2(k(\sqrt{a}))^{\mathrm{Gal}(k(\sqrt{a})/k)} \simeq_k \mathbb{H}(a,b)$. ∎

Corollary 7.11. *The quaternion algebra $\mathbb{H}(a,b)$ with $a, b \in k^\times$ is isomorphic to $M_2(k)$ if and only if the associated conic $ax^2 + by^2 = z^2$ has a rational point.*

Proof. By Theorem 7.10 this is a special case of Corollary 7.8. ∎

Remark 7.12. Suppose that the characteristic of k is 2. Let $a, b \in k^\times$ and let $\mathbb{H}(a,b)$ be the algebra generated over k by i and j, with the relations $i^2 + i = a, j^2 = b, ji = ij + j$. We refer to $\mathbb{H}(a,b)$ as the *quaternion algebra corresponding to the pair* (a,b). The correspondence $T(\mathbb{P}^1_k) \simeq T(M_2(k))$ is given by sending the class of the conic X given by the equation $x^2 + xy + ay^2 + bz^2 = 0$ to the the class of the algebra $\mathbb{H}(a,b)$. See [Ser97, §3.1.4, Exercise 3]. We refer to X as the conic associated to the pair (a,b).

As in Corollary 7.11, the algebra $\mathbb{H}(a,b)$ is isomorphic to $M_2(k)$ if and only if the conic associated to the pair (a,b) has a rational point.

Remark 7.13. The statement that two quaternion algebras are isomorphic if and only if their associated conics are isomorphic is a theorem of Witt. A direct proof, without the theory of twists, can be found in [GS17, Theorem 1.4.2].

8 The Brauer group

In this section we parameterize all central simple algebras over a field (or Severi-Brauer varieties over a field), regardless of dimension, under an appropriate notion of equivalence, using Galois cohomology. Much of the material in this section is based on [GS17, §4.4]. Throughout this section we fix a field k with a separable closure k^s, and a finite Galois extension ℓ/k. The letters m and n will always denote positive integers.

By the isomorphism $M_n(k) \otimes_k M_m(k) \simeq M_{nm}(k)$, we get a map

$$\begin{aligned} T_{\ell/k}(M_n(k)) &\to T_{\ell/k}(M_{nm}(k)) \\ [A] &\mapsto [A \otimes_k M_m(k)] = [M_m(A)]. \end{aligned} \tag{8.1}$$

This gives a direct system $(T_{\ell/k}(M_n(k)))_{n\geq 1}$ and we define the set $\mathrm{Br}(\ell/k)$ by

$$\mathrm{Br}(\ell/k) = \varinjlim_{n\geq 1} T_{\ell/k}(M_n(k)).$$

We intend to provide $\mathrm{Br}(\ell/k)$ with a group structure. Let A and B be central simple algebras of dimension n^2 and m^2, respectively. If A and B are split by ℓ, then the tensor product $A \otimes_k B$ is again a central simple algebra split by ℓ:

$$(A \otimes_k B) \otimes_k \ell = (A \otimes_k \ell) \otimes_\ell (B \otimes_k \ell) \simeq M_n(\ell) \otimes_\ell M_m(\ell) \simeq M_{nm}(\ell).$$

As a result, we can define a map

$$\begin{aligned} T_{\ell/k}(M_n(\ell)) \times T_{\ell/k}(M_m(\ell)) &\to T_{\ell/k}(M_{nm}(\ell)) \\ ([A],[B]) &\mapsto [A \otimes_k B]. \end{aligned} \tag{8.2}$$

It is straightforward to show that this is compatible with the maps in (8.1). This yields an operation on $\mathrm{Br}(\ell/k)$.

Theorem 8.1. *The set* $\mathrm{Br}(\ell/k)$ *is an abelian group under the operation described in (8.2) with unit [k].*

Proof. Associativity, commutativity and the fact that $[k]$ is unital for this operation is clear from basic properties of the tensor product. We need only show that $\mathrm{Br}(\ell/k)$ has inverses. Let A be a central simple algebra of dimension n^2 split by ℓ/k. Let $\varphi\colon M_n(\ell) \to A \otimes_k \ell$ be an ℓ-isomorphism. Consider the opposite algebra A^{opp}. This algebra is A as a vector space over k, but with multiplication defined by $x \cdot_{A^{\mathrm{opp}}} y = yx$. We have an isomorphism

$$\varphi^{\mathrm{opp}}\colon M_n(\ell)^{\mathrm{opp}} \to (A \otimes_k \ell)^{\mathrm{opp}} = A^{\mathrm{opp}} \otimes_k \ell.$$

The map $M_n(\ell) \to M_n(\ell)^{\mathrm{opp}}, M \mapsto M^t$, with M^t the transpose of M, is an isomorphism, and hence A^{opp} is a central simple algebra split by ℓ/k. Consider the map of k-algebras

$$\begin{aligned} A \otimes_k A^{\mathrm{opp}} &\to \mathrm{End}_k(A) \\ a \otimes b &\mapsto (x \mapsto axb), \end{aligned}$$

with $\mathrm{End}_k(A) \simeq M_{n^2}(k)$ the algebra of k-linear endomorphisms of A. This map is nonzero, and hence injective by simplicity of $A \otimes_k A^{\mathrm{opp}}$. Comparing dimensions, we see that it must also be surjective. We conclude that $[A^{\mathrm{opp}}]$ is the inverse of $[A]$. ∎

Definition 8.2. *We define the Brauer group of ℓ/k to be the group* $\mathrm{Br}(\ell/k)$.

If F/k and F'/k are finite Galois extensions, both contained in k^s, then there is an evident group homomorphism $\mathrm{Br}(F/k) \to \mathrm{Br}(F'/k)$. In this way we obtain a direct system $(\mathrm{Br}(F/k))_F$ of abelian groups with F ranging over the finite galois extensions F/k such that $F \subset k^s$.

Definition 8.3. *The absolute Brauer group of k, or simply the Brauer group of k, is defined to be*

$$\mathrm{Br}(k) = \varinjlim \mathrm{Br}(F/k),$$

with the direct limit taken over the finite Galois extensions F/k such that $F \subset k^s$.

8.1 The Brauer group in terms of a cohomology group

In this subsection we will give a more tangible characterization of the Brauer group in terms of the second cohomology group the discrete $\mathrm{Gal}(\ell/k)$-module $\ell^\times$. This will also allow for much easier computations.

Given an ℓ-automorphism $\varphi\colon \ell^n \to \ell^n$, tensoring with $\mathrm{id}\colon \ell^m \to \ell^m$ yields an automorphism $\varphi \otimes \mathrm{id}\colon \ell^{nm} \to \ell^{nm}$. This gives a map $\mathrm{GL}_n(\ell) \to \mathrm{GL}_{nm}(\ell)$ of G-modules, which passes to $\mathrm{PGL}_n(\ell) \to \mathrm{PGL}_{nm}(\ell)$. The induced map on H^1 is given by

$$\begin{aligned} H^1(\ell/k;\mathrm{PGL}_n(\ell)) &\to H^1(\ell/k;\mathrm{PGL}_{nm}(\ell)) \\ [(c_\sigma)] &\mapsto [(c_\sigma \otimes \mathrm{id})]. \end{aligned} \tag{8.3}$$

We obtain a direct system $(H^1(\ell/k,\mathrm{PGL}_n(\ell)))_{n\geq 1}$. The isomorphisms $T_{\ell/k}(M_n(k)) \simeq H^1(\ell/k;\mathrm{PGL}_n(\ell))$ obtained from Corollary 7.6 are compatable with the maps in (8.1) and (8.3), and hence concatenate into an isomorphism of direct systems. This yields an isomorphism of pointed sets

$$\mathrm{Br}(\ell/k) \simeq \varinjlim_{n\geq 1} H^1(\ell/k;\mathrm{PGL}_n(\ell)). \tag{8.4}$$

By the exact sequence in (6.2), Proposition 3.26 and Corollary 5.7, we obtain an exact sequence of pointed sets

$$0 = H^1(\ell/k;\mathrm{GL}_n(\ell)) \to H^1(\ell/k;\mathrm{PGL}_n(\ell)) \xrightarrow{\delta_n} H^2(\ell/k;\ell^\times). \tag{8.5}$$

Explicitly, δ_n sends the class of the 1-cocycle $[c = (c_\sigma)]$ to the class of the 2-cocycle $a\colon G \times G \to \ell^\times$ given by

$$a_{\sigma,\tau} = {b_\sigma}^\sigma b_\tau b_{\sigma\tau}^{-1}, \quad \sigma,\tau \in G,$$

where b_σ is a lift of c_σ to $\mathrm{GL}_n(\ell)$.

The maps δ_n are compatible with the maps in (8.3); hence, by (8.4), we get a map

$$\delta\colon \mathrm{Br}(\ell/k) \to H^2(\ell/k;\ell^\times). \tag{8.6}$$

Lemma 8.4. *The map $\delta\colon \mathrm{Br}(\ell/k) \to H^2(\ell/k;\ell^\times)$ defined in (8.6) is a group isomorphism, which is natural in ℓ.*

We only outline the proof. A complete proof is given in [GS17, Theorem 4.4.5].

Sketch of proof. Showing that δ is a homomorphism is a direct computation with cocycles.

Injectivity follows from the fact that all the maps δ_n have trivial kernel by the exact sequence in (8.5), and the fact that δ is a group homomorphism.

It can be shown directly that δ_m, with m equal to $[\ell : k]$, is surjective, and hence that δ is surjective.

Naturality is verified from the definitions. ■

Theorem 8.5. *There are isomorphisms*

$$\mathrm{Br}(\ell/k) \simeq H^2(\ell/k; \ell^\times), \quad \textit{and} \quad \mathrm{Br}(k) \simeq H^2(k; (k^s)^\times).$$

Proof. The first isomorphism is given by Lemma 8.4, the second isomorphism is obtained by taking a direct limit, applying Lemma 3.19. ■

Corollary 8.6. *The groups* $\mathrm{Br}(\ell/k)$ *and* $\mathrm{Br}(k)$ *are torsion.*

Proof. This follows from Theorem 8.5 and the fact that Galois cohomology groups in degree greater than 0 are torsion by Corollary 3.23. ■

Using Theorem 8.5 we can now explicitly compute some Brauer groups.

Example 8.7 ($\mathrm{Br}(\mathbb{R})$)**.** Let $N\colon \mathbb{C}^\times \to \mathbb{R}^\times$ be the norm map. Using Example 2.16, we compute the Brauer group of $\mathbb{R}$ to be

$$\mathrm{Br}(\mathbb{R}) \simeq H^2(\mathbb{R}; \mathbb{C}^\times) \simeq (\mathbb{C}^\times)^{\mathrm{Gal}(\mathbb{C}/\mathbb{R})}/N(\mathbb{C}^\times) = \mathbb{R}^\times/\mathbb{R}_{>0} \simeq \mathbb{Z}/2\mathbb{Z}.$$

The nontrivial element of $\mathrm{Br}(\mathbb{R})$ is given by the class of Hamilton's quaternion algebra $\mathbb{H} = \langle i, j \mid i^2 = -1, j^2 = -1, ij = -ji\rangle$. Indeed, the conic given by the equation $x^2 + y^2 + z^2 = 0$ has no $\mathbb{R}$-points, so we conclude that the associated algebra is non-trivial by Corollary 7.11.

Example 8.8 ($\mathrm{Br}(\mathbb{F}_q)$)**.** Let n be a positive integer and q a prime power. Let $N\colon \mathbb{F}_{q^n}^\times \to \mathbb{F}_q$ be the norm map. By (2.1) we have an exact sequence

$$\begin{aligned} \mathbb{F}_{q^n}^\times \xrightarrow{N} \mathbb{F}_{q^n}^\times &\to \mathbb{F}_{q^n}^\times \\ x &\mapsto x^{-1}\sigma(x), \end{aligned}$$

where σ is the Frobenius automorphism $x \mapsto x^q$. Since $x \in \mathbb{F}_{q^n}^\times$ is in $\mathbb{F}_q^\times$ if and only if $\sigma(x) = x$, we find $N(\mathbb{F}_{q^n}^\times) = \mathbb{F}_q^\times$. Using Example 2.16, we compute

$$\mathrm{Br}(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq H^2(\mathbb{F}_{q^n}/\mathbb{F}_q; \mathbb{F}_{q^n}^\times) \simeq (\mathbb{F}_{q^n}^\times)^{\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)}/N(\mathbb{F}_{q^n}^\times) = \mathbb{F}_q^\times/N(\mathbb{F}_{q^n}^\times) = 0.$$

By taking a direct limit we find that $\mathrm{Br}(\mathbb{F}_q)$ is trivial.

As a corollary, we obtain Wedderburns little theorem, which states that every finite division algebra (equivalently, every finite domain) is a field, as shown below. Let D be a finite division algebra, and let p be its characteristic. Writing $Z(D)$ for the center of D, we have $Z(D) \simeq \mathbb{F}_{p^n}$

for some integer $n > 0$, and so D is a central algebra over $\mathbb{F}_{p^n}$. Simplicity follows from the fact that D is a division algebra. By the fact that $\mathrm{Br}(\mathbb{F}_q) = 0$, we find that there exists an integer m such that $D \simeq M_m(\mathbb{F}_{p^n})$. Since this is only a domain for $m = 1$, we conclude that $D \simeq \mathbb{F}_{p^n}$ is a field.

We also state the following results. Their proofs fall outside the scope of this thesis. See [Ser79, §X.7, Examples of Fields with Non-zero Brauer Group].

- Let p be a prime and let $\mathbb{Q}_p$ denote the p-adic numbers. There is an isomorphism $\mathrm{Br}(\mathbb{Q}_p) \simeq \mathbb{Q}/\mathbb{Z}$.
- There exists a short exact sequence

$$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_p \mathrm{Br}(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z} \to 0,$$

  where the direct sum ranges over the primes and 0, and we set $\mathbb{Q}_0 = \mathbb{R}$.

A Notions from homological algebra

This appendix assumes knowledge of basic concepts from category theory (see, for instance, [Rie17]). This appendix is largely based on [Wei13, chapter 1 and 2]. Given a ring R, we write R-Mod for the category of left R-modules.

A.1 Abelian categories and additive functors

Definition A.1 (Ab-category)**.** *An* Ab*-category is a (locally small) category $\mathscr{C}$ such that for all $C, C' \in \mathscr{C}$ the set* $\mathrm{Hom}(C, C')$ *has the structure of an abelian group, and composition is linear with respect to this structure:*

$$a \circ (b + c) \circ d = a \circ b \circ d + a \circ c \circ d.$$

Definition A.2 (abelian category)**.** *Let $\mathscr{A}$ be an* Ab*-category. We call $\mathscr{A}$ abelian if $\mathscr{A}$ has a zero object (an object that is both initial and terminal), $\mathscr{A}$ has all finite products and coproducts, $\mathscr{A}$ has all kernels and cokernels*[1]*, every monic map is the kernel of its cokernel, and every epic map is the cokernel of its kernel.*

Example A.3. (i) The category of modules over a fixed ring R is abelian. In particular, the category Ab of abelian groups is abelian.

(ii) For any category $\mathscr{A}$, its opposite $\mathscr{A}^{\mathrm{opp}}$ is again abelian.

Remark A.4. When working with abelian categories, it is often useful to imagine a category of modules over a ring. The Freyd-Mitchell embedding justifies this by stating that every small abelian category can be embedded in a category of modules over a ring. See [Wei13, Theorem 1.6.1].

[1] The kernel of $f\colon A \to A'$ is defined to be the equalizer of f and the zero map $0\colon A \to A'$. Cokernels are defined dually.

Definition A.5 (additive functor)**.** *Let $F\colon \mathscr{A} \to \mathscr{B}$ be a functor between* Ab*-categories. We call F additive if for all $A, A' \in \mathscr{A}$ the map*

$$\mathrm{Hom}(A, A') \to \mathrm{Hom}(FA, FA')$$

is a homomorphism of abelian groups.

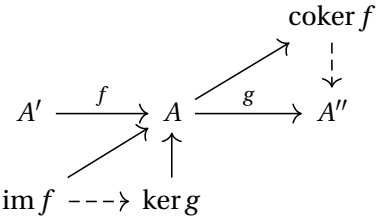
Example A.6. (i) For every object A in an abelian category $\mathscr{A}$, the functors $\mathrm{Hom}(A, -)\colon \mathscr{A} \to \mathrm{Ab}$ and $\mathrm{Hom}(-, A)\colon \mathscr{A}^{\mathrm{opp}} \to \mathrm{Ab}$ are additive.

(ii) Fix a commutative ring R and a module M over R. The functor $M \otimes_R (-)\colon R\text{-Mod} \to R\text{-Mod}$ is additive.

As in Ab, in general abelian categories the notion of an exact sequence makes sense. More specifically, let $\mathscr{A}$ be an abelian category and suppose we have a sequence

$$A' \xrightarrow{f} A \xrightarrow{g} A'' \tag{A.1}$$

of objects and maps in $\mathscr{A}$ such that the composition gf is the zero map. We write $\mathrm{im}\, f$ for the object $\ker(A \to \mathrm{coker}\, f)$. The composition $\mathrm{im}\, f \to A \xrightarrow{g} A''$ is zero, because g factors via the cokernel of f; hence, $\mathrm{im}\, f \to A$ must factor via the kernel of g. This is illustrated in the diagram below.



We say that the sequence in (A.1) is *exact* if the induced map $\mathrm{im}\, f \to \ker g$ is an isomorphism. The notion of exactness naturally extends to longer sequences of objects and maps in $\mathscr{A}$. An exact sequence of the form

$$0 \to A' \xrightarrow{f} A \xrightarrow{g} A'' \to 0$$

is called *short exact*. Since f and g are monic and epic, respectively, this means that f defines a kernel of g and g defines a cokernel of f (by the definition of an abelian category). In the category of abelian groups (or any category of modules over a ring), we retrieve the usual notion of an exact sequence.

Definition A.7 (exact functor)**.** *Given an additive functor $F\colon \mathscr{A} \to \mathscr{B}$ between abelian categories, we call F left exact if for any short exact sequence*

$$0 \to A' \to A \to A'' \to 0$$

in $\mathscr{A}$ we get an exact sequence

$$0 \to FA' \to FA \to FA''$$

in $\mathscr{B}$. Analogously, we define right exact functors. An additive functor that is both left exact and right exact is called exact.

Proposition A.8 (left-exactness of hom)**.** *For A an object in an abelian category $\mathscr{A}$, the functor* $\mathrm{Hom}(A,-)$ *is left exact.*

Proof. Let

$$0 \to B'' \xrightarrow{\alpha} B \xrightarrow{\beta} B' \to 0,$$

be an exact sequence in $\mathscr{A}$. Consider the sequence

$$0 \to \mathrm{Hom}(A,B'') \xrightarrow{\alpha_*} \mathrm{Hom}(A,B) \xrightarrow{\beta_*} \mathrm{Hom}(A,B')$$

in Ab. Exactness at $\mathrm{Hom}(A,B'')$ follows immediately from the fact that α is monic. Clearly $\alpha_*\beta_* = (\alpha\beta)_* = 0$. Let $f\colon A \to B$ be a map such that $\beta f = 0$. The map α is the kernel of β, and hence there must exist $g\colon A \to B''$ such that $\alpha g = f$. We conclude that the sequence is also exact at $\mathrm{Hom}(A,B)$. ∎

Remark A.9. Dually, $\mathrm{Hom}_{\mathscr{A}}(-,A)$ as a functor $\mathscr{A}^{\mathrm{opp}} \to \mathrm{Ab}$ is left exact.

A.2 Chain complexes

What follows can be done more generally in abelian categories, but we restrict ourselves to the category of abelian groups (which serves as a sort of "base category").

Definition A.10 (chain complexes)**.** *A (chain) complex is a collection of maps of abelian groups $(\partial^n : A^n \to A^{n+1})_{n\in\mathbb{Z}}$ such that $\partial^n \circ \partial^{n-1} = 0$ for all $n \in \mathbb{Z}$. Such a complex will frequently be denoted A^*. A map of chain complexes $f\colon A^* \to B^*$ is a collection of maps $f_n\colon A^n \to B^n$ such that we have a commutative diagram*

$$\begin{array}{ccc} A^n & \xrightarrow{\partial^n} & A^{n+1} \\ \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n+1}} \\ B^n & \xrightarrow{\partial^n} & B^{n+1} \end{array}$$

for all $n \in \mathbb{Z}$. This constitutes an abelian category, which will be denoted $\mathrm{Ch}_{\mathrm{Ab}}$*, or simply* Ch.

Notation A.11. Often, parts of a complex will be omited. These objects and maps should then be read as zero.

Remark A.12. A sequence of maps in Ch is exact, if and only if at every index the induced sequence of objects in Ab is exact.

Example A.13. Set $A^n = \mathbb{Z}/4\mathbb{Z}$ in Ab for all $n \in \mathbb{Z}$, and define $\partial^n\colon A^n \to A^{n+1}$ to be multiplication by 2 for n even, and the zero map for n odd. The resulting sequence

$$\ldots \xrightarrow{0} \mathbb{Z}/4\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/4\mathbb{Z} \xrightarrow{0} \mathbb{Z}/4\mathbb{Z} \xrightarrow{\cdot 2} \ldots$$

is a chain complex.

Definition A.14 (cohomology)**.** *Given a chain complex A^*, we define the n-th cohomology group of A^* to be*

$$H^n(A^*) = \ker \partial^n / \operatorname{im} \partial^{n-1}.$$

Maps of chain complexes naturally induce maps of cohomology groups, which gives an additive functor

$$H^n \colon \mathrm{Ch} \to \mathrm{Ab}.$$

Example A.15. *Letting A^* be the complex of Example A.13, we find*

$$H^n(A^*) = \mathbb{Z}/2\mathbb{Z},$$

for all $n \in \mathbb{Z}$.

In algebraic topology, if there exists a homotopy between two continuous maps, these maps will give rise to the same maps on (co)homology. A similar notion exists in homological algebra.

Definition A.16 (homotopy)**.** *Given two complexes A^* and B^* in* Ch *and a map $f \colon A^* \to B^*$, we say that f is null homotopic if there exist maps $h_n \colon A^{n+1} \to B^n$ such that*

$$f_n = h_n \partial^n + \partial^{n-1} h_{n-1}.$$

If $g \colon A^* \to B^*$ is another map, we say that f and g are homotopic if $f - g$ is null homotopic and write $f \simeq g$.

An easy computation shows that nullhomotopic maps induce zero maps on cohomology groups. By additivity of the H^n, this gives us a result analogous to what we see in algebraic topology:

Proposition A.17. *Let A^* and B^* in* Ch *be chain complexes, and let $f, g \colon A^* \rightrightarrows B^*$ be homotopic maps, then $H^n(f) = H^n(g)$.*

A.3 Projective and injective objects

Fix an abelian category $\mathscr{A}$. Hom functors form the central class of examples of left exact functors (see Proposition A.8). In general, the functor $\mathrm{Hom}(A, -)$ with $A \in \mathscr{A}$ is not exact, because $\mathrm{Hom}(A, -)$ need not preserve epimorphisms. As a simple example, consider the quotient map $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ in Ab, and apply $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, -)$. This then raises the question for which objects in a given abelian category these Hom functors are exact.

Definition A.18 (injective/projective objects)**.** *We call an object A in $\mathscr{A}$ injective if* $\mathrm{Hom}(-, A)$ *is an exact functor. Dually, we call A projective if* $\mathrm{Hom}(A, -)$ *is exact.*

Example A.19 (injectives/projectives in Ab)**.** In the category of abelian groups, all projective objects are free. The injective objects are precisely the divisible abelian groups. Examples of divisible abelian groups are $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$. See [Sta22, Tag 01D7].

Definition A.20 (enough injectives/projectives)**.** *We say that $\mathscr{A}$ has enough injectives, if for any $A \in \mathscr{A}$, there exists a monomorphism $A \hookrightarrow I$ for some injective I in $\mathscr{A}$. Dually, $\mathscr{A}$ has enough projectives, if for any $A \in \mathscr{A}$ there exists an epimorphism $P \twoheadrightarrow A$.*

Example A.21. Any category of modules over a ring R has enough projectives, because for any module M over R we can create a surjection $R^{\oplus M} \twoheadrightarrow M$ sending the basis vector e_m corresponding to $m \in M$ to m. The module $R^{\oplus M}$ is projective, because it is free.

Proposition A.22. Ab *has enough injectives.*

Proof. Let A be an abelian group. Define the abelian group

$$I = \prod_{\mathrm{Hom}(A,\mathbb{Q}/\mathbb{Z})} \mathbb{Q}/\mathbb{Z}.$$

Being a product of injective objects (see Example A.19), I is injective by the universal property of the product: the functor

$$\mathrm{Hom}(-, I) = \prod \mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$$

is exact, because products preserve exact functors. There is an evident homomorphism $i\colon A \to I$ sending $x \in A$ to $(f(x))_f$ with f ranging over the maps $A \to \mathbb{Q}/\mathbb{Z}$. We will show that i is injective. Let $a \in A$ such that a is nonzero. Consider the subgroup $a\mathbb{Z}$ of A generated by a. If a is not a torsion element, then $a\mathbb{Z}$ is free and we can define a map $\varphi\colon a\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ sending a to $1/2$. If a has finite order n, then we define $\varphi\colon a\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ by sending a to $1/n$. In both cases, $\varphi(a)$ is nonzero. From the exact sequence

$$0 \to a\mathbb{Z} \to A$$

we obtain the exact sequence

$$\mathrm{Hom}(a\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z}) \to 0,$$

because $\mathbb{Q}/\mathbb{Z}$ is injective. Hence, φ can be extended to a map $A \to \mathbb{Q}/\mathbb{Z}$. It follows that $i(a)$ is nonzero, because $\varphi(a)$ is nonzero, and so i is injective. ∎

As a corollary to the above proposition, we find that every category of modules over a ring has enough injectives. To this end, we consider the forgetful functor

$$U\colon R\text{-Mod} \to \mathrm{Ab}.$$

By the tensor-hom adjunction (see [Wei13, Proposition 2.6.3]) U admits a right adjoint $V\colon \mathrm{Ab} \to R\text{-Mod}$ given by $VA = \mathrm{Hom}_{\mathbb{Z}}(R, A)$ with R-module structure given by $(r\varphi)(x) = \varphi(xr)$.

Proposition A.23. *The category of R-modules has enough injectives.*

Proof. Let M be a module over R and let M_0 denote the underlying abelian group. By Proposition A.19 there exists an injective abelian group I and an embedding $M_0 \hookrightarrow I$. We find that VI is again injective:

$$\mathrm{Hom}(-, VI) = \mathrm{Hom}(U-, I)$$

is the composition of two exact functors, and hence is exact. By left exactness of V, we find an embedding $VM_0 \hookrightarrow VI$. It now suffices to show that there exists an embedding $M \hookrightarrow VM_0$. Such an embedding is given by $m \mapsto (r \mapsto rm)$. ∎

Definition A.24 (injective/projective resolutions)**.** *Let $A \in \mathscr{A}$ an object. We call an exact sequence*

$$0 \to A \to I^0 \to I^1 \to \dots,$$

with $I^n \in \mathscr{A}$ injective, an injective resolution of $\mathscr{A}$. Dually, we call an exact sequence

$$\dots \to P_1 \to P_0 \to A \to 0,$$

with P_n projective in $\mathscr{A}$, a projective resolution of A.

Injective, respectively projective, resolutions need not exist in an arbitrary abelian category, but they do exist if there are enough injective, respectively projective, objects.

Proposition A.25 (existence of injective/projective resolutions)**.** *Suppose $\mathscr{A}$ has enough injective objects. Then every object $A \in \mathscr{A}$ has an injective resolution. Dually, if $\mathscr{A}$ has enough projectives, then every object $A \in \mathscr{A}$ has a projective resolution.*

The above propositon can be proved by constructing an injective/projective resolution inductively for any object in $\mathscr{A}$.

Although injective/projective resolutions are certainly not unique, they are up to homotopy, as shown by the following result.

Proposition A.26. *Let $f\colon A \to A'$ be a map in $\mathscr{A}$, and suppose we have injective resolutions $0 \to A \to I^*$ and $0 \to A' \to I'^*$, then there exist a map $\varphi\colon I^* \to I'^*$ of complexes, called a lift of f, such that*

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \longrightarrow & I^* \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \varphi} \\ 0 & \longrightarrow & A' & \longrightarrow & I'^* \end{array}$$

commutes. The map φ is unique up to homotopy. A dual statement holds for projective resolutions.

Proof. We refer to [Wei13, Theorem 2.3.7]. ∎

A particular case of interest is the case $A' = A$ and $f = \mathrm{id}$. We find that any two injective resolutions $0 \to A \to I^*$ and $0 \to A \to J^*$ are *homotopy equivalent*, in the sense that there exist chain maps $\varphi\colon I^* \to J^*$ and $\psi\colon J^* \to I^*$ such that $\varphi\psi \simeq \mathrm{id}$ and $\psi\varphi \simeq \mathrm{id}$.

A.4 δ-functors

Fix abelian categories $\mathscr{A}$ and $\mathscr{B}$.

Definition A.27 (δ-functor)**.** *A cohomological δ-functor, or simply a δ-functor, is a collection $(T^n\colon \mathscr{A}\to\mathscr{B})_{n\geq 0}$ of additive functors with maps $\delta^n : T^nC \to T^{n+1}A$ in $\mathscr{B}$, called connecting maps, for every short exact sequence*

$$0\to A\to B\to C\to 0$$

in $\mathscr{A}$, such that the sequence

$$\begin{aligned}0\to T^0A\to T^0B\to T^0C\\ \xrightarrow{\delta^0} T^1A\to T^1B\to T^1C\\ \xrightarrow{\delta^1} T^2A\to\dots\end{aligned}$$

is exact. Furthermore, we assume the connecting maps to be natural, in the sense that for every map of short exact sequences

$$\begin{array}{ccccccccc}0&\longrightarrow&A&\longrightarrow&B&\longrightarrow&C&\longrightarrow&0\\ &&\downarrow&&\downarrow&&\downarrow&&\\ 0&\longrightarrow&A'&\longrightarrow&B'&\longrightarrow&C'&\longrightarrow&0\end{array}$$

we get a map of long exact sequences

$$\begin{array}{ccccccccccccc}\dots&\longrightarrow&T^{n-1}C&\xrightarrow{\delta}&T^nA&\longrightarrow&T^nB&\longrightarrow&T^nC&\xrightarrow{\delta}&T^{n+1}A&\longrightarrow&\dots\\ &&\downarrow&&\downarrow&&\downarrow&&\downarrow&&\downarrow&&\\ \dots&\longrightarrow&T^{n-1}C'&\xrightarrow{\delta}&T^nA'&\longrightarrow&T^nB'&\longrightarrow&T^nC'&\xrightarrow{\delta}&T^{n+1}A'&\longrightarrow&\dots\end{array}$$

Let (S^n) be another δ-functor. A map of δ-functors $(T^n)\to(S^n)$ is a collection of natural transformations $(T^n\to S^n)$ that commute with the connecting maps. This constitutes a category of δ-functors from $\mathscr{A}$ to $\mathscr{B}$. We call (T^n) a universal δ-functor if it is initial among δ-functors (S^n) with a map $T^0\to S^0$.

Remark A.28. In particular, if (T^n) is a δ-functor, then T^0 is a left exact functor.

Remark A.29. Universal δ-functors are unique up to canonical isomorphism.

Proposition A.30. *Suppose $\mathscr{A}$ has enough injectives, and that we have a δ-functor $(T^n\colon \mathscr{A}\to\mathscr{B})$ such that $T^nI=0$ for all $n\geq 1$ and I in $\mathscr{A}$ injective. Then (T^n) is universal.*

Proof. We refer to [Wei13, Exercise 2.4.5]. ∎

A.5 Derived functors

Fix an abelian category $\mathscr{A}$ with enough injective objects. Let $F\colon \mathscr{A} \to \mathrm{Ab}$ be a left exact functor.

Example A.31. Let $\mathscr{A} = \mathrm{Ab}$, and suppose F is the additive functor $(-)_{\mathrm{tor}}$ sending an abelian group A to A_{tor}, its subgroup of torsion elements. Then F is a left exact functor, but not an *exact functor*, as shown by the short exact sequence

$$0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

By the above example, F need not be an exact functor. The so called *right derived functors* of F exist to rectify this problem. Let $A \in \mathscr{A}$ be an object. Let

$$0 \to A \to I^*$$

be an injective resolution of A. For $n \geq 0$ we define

$$R^n F(A) = H^n(F(I^*)).$$

By Proposition A.26 and Proposition A.17 we see that choosing a different injective resolution $0 \to A \to I'^*$ yields a canonical isomorphism $H^n(F(I^*)) = H^n(F(I'^*))$, showing that $R^n F(A)$ is well-defined up to canonical isomorphism. Let $A' \in \mathscr{A}$, $f\colon A \to A'$ a map, and $0 \to A' \to I'^*$ an injective resolution of A'. By Proposition A.26 we get an up to homotopy unique map $\varphi\colon I^* \to I'^*$ of complexes such that

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \longrightarrow & I^* \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \varphi} \\ 0 & \longrightarrow & A' & \longrightarrow & I'^* \end{array}$$

commutes. The map $F(\varphi)\colon F(I^*) \to F(I'^*)$ of complexes induces maps $R^n F(f)\colon R^n F(A) \to R^n F(A')$ on cohomology. Proposition A.17 shows that $R^n F(f)$ is independent of our choice of φ. The uniqueness statement in Proposition A.26 implies that this assignment is functorial, so we get functors $R^n F\colon \mathscr{A} \to \mathrm{Ab}$. The $R^n F$ are also additive: given a map $g\colon A \to A'$ and a lift $\psi\colon I^* \to I'^*$ to injective resolutions, we see that $\varphi + \psi$ is a lift for $f + g$. In combination with the fact that taking cohomology is additive, this yields $R^n F(f+g) = R^n F(f) + R^n F(g)$.

Definition A.32 (right derived functors)**.** *We call $R^n F$ the n-th right derived functor of F.*

Example A.33 (Ext)**.** Assume $\mathscr{A}$ also has enough projectives. Let A and B in $\mathscr{A}$. By Proposition A.8 the functors $\mathrm{Hom}(A,-)\colon \mathscr{A} \to \mathrm{Ab}$ and $\mathrm{Hom}(-,B)\colon \mathscr{A}^{\mathrm{opp}} \to \mathrm{Ab}$ are left exact. We can form the right derived functors of both. By [Wei13, Theorem 2.7.6], $R^n \mathrm{Hom}(A,-)(B)$ and $R^n \mathrm{Hom}(-,B)(A)$ are canonically isomorphic, and both are denoted $\mathrm{Ext}^n(A,B)$.

Example A.34. (i) Let $p \geq 1$ be an integer. We define an additive functor $(-)_p\colon \mathrm{Ab} \to \mathrm{Ab}$ sending an abelian group A to its subgroup of p-torsion elements $A_p = \{a \in A : pa = 0\}$.

Note that $(-)_p = \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, -)$ is a left exact functor by Proposition A.8. Let A be an abelian group. We have the following projective resolution of $\mathbb{Z}/p\mathbb{Z}$:

$$0 \to \mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0.$$

Note that this is an injective resolution in $\mathrm{Ab}^{\mathrm{opp}}$. Applying $\mathrm{Hom}(-, A)$ to this resolution, we get the following complex

$$A \xrightarrow{\cdot p} A \to 0.$$

Taking cohomology we find

$$R^n(-)_p(A) = \mathrm{Ext}^n(\mathbb{Z}/p\mathbb{Z}, A) = \begin{cases} A_p & n = 0 \\ A/pA & n = 1 \\ 0 & n \geq 2. \end{cases}$$

(ii) We now consider the torsion functor $(-)_{\mathrm{tor}}$ from Example A.31. Let A in Ab and note that $A_{\mathrm{tor}} = \varinjlim_{p \geq 1} A_p$. Let $0 \to A \to I^*$ be an injective resolution. We find

$$\begin{aligned} R^n(-)_{\mathrm{tor}}(A) &= H^n(I^*_{\mathrm{tor}}) \\ &= H^n(\varinjlim_{p \geq 1} I_p^*) \\ &= \varinjlim_{p \geq 1} H^n(I_p^*) = \begin{cases} A_{\mathrm{tor}} & n = 0 \\ \varinjlim_{p \geq 0} A/pA & n = 1 \\ 0 & n \geq 2. \end{cases} \end{aligned}$$

We can compute $R^1(-)_{\mathrm{tor}}(A)$ more explicitly as

$$R^1(-)_{\mathrm{tor}}(A) = \varinjlim_{p \geq 1} A/pA = \varinjlim_{p \geq 1} \tfrac{1}{p} A/A = (A \otimes \mathbb{Q})/A.$$

The main result about derived functors is the following theorem.

Theorem A.35. *The collection of functors $(R^n F)_{n \geq 0}$ forms a universal cohomological δ-functor.*

Proof. We refer to [Wei13, Theorem 2.4.7]. ■

Example A.36. Consider the short exact sequence

$$0 \to \tfrac{1}{2}\mathbb{Z} \xrightarrow{\cdot 2} \tfrac{1}{2}\mathbb{Z} \to \tfrac{1}{2}\mathbb{Z}/\mathbb{Z} \to 0.$$

We compute the long exact sequence induced by the δ-functor $(R^n(-)_{\mathrm{tor}})$

$$0 \to 0 \to 0 \to \tfrac{1}{2}\mathbb{Z}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Q}/\mathbb{Z} \to 0 \to 0 \to \dots,$$

using the results from Example A.34.

References

[Bru09] Eric Brussel. *Galois descent and Severi-Brauer varieties*. 2009. URL: http://www.mathcs.emory.edu/~brussel/Papers/galoisdescent.pdf.

[GS17] Philippe Gille and Tamás Szamuely. *Central Simple Algebras and Galois Cohomology*. eng. Vol. 165. Cambridge studies in advanced mathematics. Cambridge: University Press, 2017. ISBN: 978-1-107-15637-1. DOI: 10.1017/9781316661277.

[Har10] Robin Hartshorne. *Algebraic geometry*. eng. Graduate texts in mathematics 52. New York: Springer Science+Business Media, Inc, 2010. ISBN: 978-1-4757-3849-0.

[Jah00] Jörg Jahnel. *The Brauer-Severi variety associated with a central simple algebra: A Survey*. 2000. URL: https://www.math.uni-bielefeld.de/LAG/man/052.pdf.

[Lan02] S. Lang. *Algebra*. eng. Rev. Third edition. Graduate Texts in Mathematics, 211. New York, NY: Springer New York, 2002. ISBN: 978-1-4613-0041-0.

[Lee] John M. Lee. *Introduction to Topological Manifolds*. eng. Vol. 202. Graduate Texts in Mathematics. ISSN: 0072-5285. New York, NY: Springer New York. ISBN: 978-1-4419-7939-1. DOI: 10.1007/978-1-4419-7940-7.

[Mil20] J.S. Milne. *Class Field Theory (v4.03)*. 2020. URL: www.jmilne.org/math/.

[NSW] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. eng. Second Edition. Vol. 323. Grundlehren der mathematischen Wissenschaften. ISSN: 0072-7830. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 978-3-540-37888-4. DOI: 10.1007/978-3-540-37889-1.

[Poo17] Bjorn Poonen. *Rational points on varieties*. eng. Vol. 186. Graduate Studies in Mathematics. Providence, Rhode Island: American Mathematical Society, 2017. ISBN: 978-1-4704-3773-2.

[Rie17] Emily Riehl. *Category Theory in Context*. en. Google-Books-ID: 6B9MDgAAQBAJ. Courier Dover Publications, Mar. 2017. ISBN: 978-0-486-82080-4.

[Ser79] Jean-Pierre Serre. *Local fields*. eng. Graduate texts in mathematics 67. New York ; Berlin [etc.]: Springer-Verlag, 1979. ISBN: 978-0-387-90424-5.

[Ser97] Jean-Pierre Serre. *Galois cohomology*. eng. Springer Monographs in Mathematics. Berlin ; New York: Springer, 1997. ISBN: 978-3-642-59141-9.

[Sha72] Stephen S. Shatz. *Profinite groups, arithmetic, and geometry*. eng. Annals of mathematics studies ; no. 67. 831162228. Princeton, N.J.]: Princeton University Press, 1972. ISBN: 978-0-691-08017-8.

[Sil13] Joseph H. Silverman. *The arithmetic of elliptic curves*. eng. Vol. 106. Graduate texts in mathematics. Springer, 2013. ISBN: 978-0-387-96203-0.

[Sta22] The Stacks project authors. *The Stacks project*. https://stacks.math.columbia.edu. 2022.

[Wat74] William C. Waterhouse. “Profinite groups are Galois groups”. en. In: *Proceedings of the American Mathematical Society* 42.2 (1974). ISSN: 0002-9939, 1088-6826. DOI: 10.1090/S0002-9939-1974-0325587-3. URL: https://www.ams.org/proc/1974-042-02/S0002-9939-1974-0325587-3/.

[Wei13] Charles A. Weibel. *An Introduction to Homological Algebra*. eng. Vol. Series Number 38. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2013. ISBN: 978-0-521-55987-4.