A Specific Construction of a Versal Torsor under a Finite Group G

by

Zhaowei Zeng

A thesis submitted in partial fulfillment of the requirements for the degree of

Master of Science

in

Mathematics

Department of Mathematical and Statistical Sciences
University of Alberta

Abstract

Versal torsors arise as an important tool in algebraic groups and algebraic geometry for the universal perspective they provide on the behaviour and properties of other torsors under the same group. Two classic examples of versal torsors are constructed from general linear groups and affine spaces, respectively, described in lecture notes of Jean-Pierre Serre. The objective of this thesis is to find an algebraic proof for the second construction under finite groups without the use of heavy machinery from Galois cohomology.

The content of the different chapters is as follows:

Chapter 1 is an introduction to the goals of the thesis.

Chapter 2 is dedicated to give the readers a comprehensive introduction to étale algebras and Galois algebras.

Chapter 3 and 4 are general discussions on quotients of varieties and torsors, respectively, followed by their behaviour in our special case.

Chapter 5 presents two classic constructions of versal torsors under finite groups and lastly gives a new proof for the construction from affine spaces.

Acknowledgements

I would like to express my deepest gratitude to my supervisors Dr. Jochen Kuttler and Dr. Stefan Gille for all the time they have spent and the insight they have provided. This work would be impossible without their guidance and invaluable advice.

I am also grateful to my family, especially my partner, Jiatong Sun, for her selfless support and continuing understanding.

I would be remiss in not mentioning my friends, Wen Rui Sun and Tomasz Szczepanski, for their presence and precious friendship.

Lastly, I would like to thank the University of Alberta and the Department of Mathematical and Statistical Sciences, especially the faculty members whom I had the pleasure to work with.

Table of Contents

Chapter 1

Introduction

1.1 Background

The notion of versal torsors [1] arises in the theory of algebraic groups and becomes an important tool in many areas. In Galois cohomology for instance, one can show that two cohomological invariants are equal if and only if they agree on a versal torsor, cf. [5] Part I Theorem 12.3. Using this result, Serre computed the cohomological invariants of $H^1(\_, G)$ for some algebraic groups G, cf. [5] Part I Chapter VI.

Versal torsors are also related to Noether's problem. Let G be a finite group and k a field. Noether's problem asks whether the following statement is true: there exists an embedding $G \hookrightarrow \mathbf{GL}_n(k)$ for some n such that, if K is the subfield of $k(x_1, \cdots, x_n)$ fixed by the induced G-action, then K is k-rational (i.e., is a purely transcendental extension of k).

For this, one may consider whether there exists a versal G-torsor $X \to Y$ such that Y is a smooth and irreducible k-variety and its function field K is k-rational. If an embedding $G \hookrightarrow \mathbf{GL}_n(k)$ in Noether's problem exists, then the second construction of versal G-torsors sketched in Section 1.3 gives such a versal torsor. As a corollary, Noether's problem turns out to have a negative answer over $\mathbb{Q}$ for some finite groups, e.g., any group with a 2-Sylow subgroup which is cyclic of order ≥ 8, cf. [5] Part I Theorem 33.16.

[1] Unless otherwise stated, the term "torsor" refers to a right torsor in this thesis, though a left torsor can be defined analogously.

1.2 Torsors and Galois algebras

The primary objective of the first part of this thesis is to examine the various descriptions of torsors and explore how they are connected.

Let G be a finite group. We fix a base field k and a separable closure k_s of k, and denote by Γ the Galois group $\mathrm{Gal}(k_s/k)$. The first notion of torsors is developed within the category of finite Γ-sets and Γ-maps, cf. [17] I.5.2.

Definition 1.2.1 (Definition 2.2.1)**.** An *étale* k-algebra is a finite direct product of finite separable field extensions of k.

Let Γ act trivially on G.

Definition 1.2.2 (Definition 2.3.7)**.** A *G-torsor over Γ* is a Γ-set X endowed with a simply transitive right G-action such that the G-action is commutative with the Γ-action.

Together with Γ- and G-maps, these G-torsors form a category. This category will be demonstrated to be equivalent to the category of Galois G-algebras over k and G-algebra homomorphisms.

Definition 1.2.3 (Definition 2.3.1)**.** Suppose G is a finite group. A *Galois G-algebra over k* is an étale k-algebra L on which G acts faithfully by automorphisms such that the G-action on $L(k_s) := \mathrm{Hom}_{k\text{-alg}}(L, k_s)$ by composing on the right is simply transitive. A G-algebra homomorphism is a G-equivariant k-algebra homomorphism.

It is readily seen by definition that we can assign to a given Galois G-algebra L over k the G-torsor $L(k_s)$, see Subsection 2.3.1 for the details.

Example 1.2.4. Let $L = k[G]$ denote the set of maps from G to k. It is a k-algebra if endowed with point-wise addition, multiplication and scalar multiplication. As a k-algebra, it is nothing but a direct product of $|G|$ copies of k; hence an étale k-algebra. $L(k_s)$ is the set of the $|G|$ natural projections onto k followed by the embedding $k \hookrightarrow k_s$. If we let Γ act on $L(k_s)$ by composing on the left, then $L(k_s)$ is a finite Γ-set.

Now we define a left faithful G-action on $k[G]$ as follows:

$$\begin{aligned} G \times k[G] &\to k[G] \\ (h, f) &\mapsto \big(g \mapsto f(gh)\big). \end{aligned}$$

This gives a right G-action on $L(k_s)$: for any $\tau \in L(k_s)$, $g \in G$, $f \in k[G]$,

$$(\tau \cdot g)(f) = \tau(g \cdot f).$$

Together with the Γ-action above, it makes $L(k_s)$ a G-torsor over Γ.

An alternative notion of torsors can be found in the category of schemes that plays an important role in a wider scope, cf. [12]. III.4. This perspective is particularly useful when one considers schemes over an arbitrary base S.

Definition 1.2.5 (Definition 4.1.5)**.** Suppose G is an fppf group scheme over S. A *G-torsor over S* is an fppf S-scheme X with a right G-action such that there is an fppf base change $S' \to S$ such that $X_{S'}$ with the right $G_{S'}$-action is isomorphic to $G_{S'}$ with right translation $G_{S'}$-action. A morphism of G-torsors over S is a G-equivariant S-morphism.

The connection between these two definitions may not be obvious at first sight. However, if G is (the constant group scheme associated to) a finite group, which is the case we focus on in this thesis, then G-torsors in Definition 1.2.5 are precisely the spectra of Galois G-algebras. In this way, Definition 1.2.5 can be viewed as a generalization of the set-theoretic G-torsors introduced in Definition 1.2.2, as expounded in Section 4.2.

There are several intermediate approaches that could also be discussed such as those in [18] 2.1.1 and [13] 2.66. These approaches, however, are also reduced to Galois G-algebras due to the assumption that G is finite, so beginning with Chapter 4 we will exclusively use Definition 1.2.5 for its generality and applicablity.

Galois cohomology is briefly introduced in Section 2.1. The classification of torsors under finite groups is done in Subsection 2.3.2 with respect to Definition 1.2.2, though it could also be done purely in the category of schemes in a more general setting.

In Chapter 3, we discuss quotients of varieties and find an explicit example of torsors to be the quotient map under a free group action. This particular example will be essential in the subsequent constructions of versal torsors.

1.3 Versal torsors

The second part of the thesis is about a very special type of torsors, called versal torsors. Roughly speaking, a versal torsor is a torsor that is locally isomorphic to every other torsor under the same group. More precisely, any G-torsor can be obtained by pulling back a versal G-torsor along some rational points.

We fix a base field k_0 and a finite group G for the rest of the section.

Definition 1.3.1 (Definition 5.1.1)**.** A *versal G-torsor* over a k_0-scheme S is a G-torsor Q over S such that for every extension k of k_0 with k infinite, every G-torsor T over k, and every non-empty open subset U of S, there exists $x \in U(k)$ whose fiber Q_x is isomorphic to T as a G-torsor.

There are two classic constructions of versal torsors described in the lecture notes of Jean-Pierre Serre, c.f. [5] Part I Section I.5, briefly sketched as follows:

1. Choose an embedding of G into the general linear group $\mathbf{GL}_n$ defined over k_0 for some n. The quotient map $\mathbf{GL}_n \to \mathbf{GL}_n/G$ is a versal G-torsor.

2. Choose an embedding of G into the general linear group $\mathbf{GL}_n$ defined over k_0 for some n. Let V be the affine n-space (hence G acts on V) and V' the G-stable open subset of V with $\ker(g-1)$ removed for all $1 \neq g \in G$. The quotient map $V' \to V'/G$ is a versal G-torsor.

The classical proofs rely on the applications of Galois cohomology. Additionally, 2 is regarded as a corollary of 1, see Section 5.1.

We present a new proof showing directly that $V' \to V'/G$ above is a versal G-torsor. Notably, this approach differs from the traditional Galois cohomology method and we outline the basic idea as follows:

1. Given a G-torsor T (which must be the spectrum of some Galois G-algebra L) over a field extension k of k_0 with k infinite, to find a k-point x that realizes T, it suffices to find a surjective G-algebra homomorphism $\mathcal{O}(V) \to \mathcal{O}(T) = L$.

2. Consider the k-vector space $(L \otimes_k V_k)^G$, denoted by H. It is canonically in bijection with the set of G-algebra homomorphisms $\mathcal{O}(V) \to L$.

3. We show that there is an element in H that corresponds to a surjection using the fact that there are only finitely-many G-stable sub-k-algebras of L, which proves the existence of a k-point x that realizes T.

4. We show that such k-points must be dense in V'/G due to the density of the orbit of x under the action of $\mathbf{GL}_n(k_0)$.

Chapter 2

Étale algebras and Galois algebras

The goal of this chapter is to give a general discussion of étale and Galois algebras. We start with some main results in Galois cohomology. It studies how properties of objects defined over a Galois extension[2] of a base field "descend" to those of objects defined over the base field by studying the actions of Galois groups. In particular, Galois cohomology is used to classify objects defined over a base field that become isomorphic over some Galois extension.

Étale algebras over a field k can be thought as a generalization of finite separable field extensions of k such that finite (co)products exist in the enlarged category. They are characterized by being isomorphic to split étale algebras over some Galois extension of k, namely the direct product of copies of the underlying field. We show they are equivalent to finite sets with continuous actions of the absolute Galois group, and the isomorphism classes of étale algebras of dimension n over k are in bijection with $H^1(k, S_n)$ by Galois descent.

Let G be a finite group. Galois G-algebras over k are a generalization of finite Galois field extensions of k. They become isomorphic to the split Galois G-algebras after base change to some Galois extension. Galois G-algebras are equivalent to torsors for G, and their isomorphism classes are in bijection with

[2]In this article, the term "Galois extension" refers to a field extension that is Galois and we refer to "Galois ring extensions" as Galois algebras.

the first cohomology set $H^1(k, G)$.

2.1 Galois descent

2.1.1 First cohomology sets

The mail goal of this section is to introduce to the readers the first cohomology set. Although in general, the first cohomology sets could be defined for so-called profinite groups, the only profinite groups in this thesis will be Galois groups.

In this thesis, we fix a bask field throughout, and denote it by k unless otherwise specified.

Definition 2.1.1. Let Ω be a (not necessarily finite) Galois extension of k. The *Krull topology* on $\mathrm{Gal}(\Omega/k)$ is the group topology defined by taking as a basis of open neighborhoods of 1 the family of subgroups

$$\{\mathrm{Gal}(\Omega/L)\colon L/k \text{ is a finite Galois subextension of } \Omega/k\}.$$

Unless specified otherwise, all Galois groups in this thesis are endowed with the Krull topology. Note that the Krull topology on any finite Galois group is the same as the discrete topology.

Let Γ be a Galois group (endowed with the Krull topology).

Definition 2.1.2. Let A be a discrete topological space with a left Γ-action. We say the action is *continuous* if the following equivalent conditions hold:

1. The map of the action
$$\begin{aligned} \Gamma \times A &\to A \\ (\sigma, a) &\mapsto {}^{\sigma}a \end{aligned}$$
is continuous.

2. For any $a \in A$, the Γ-stabilizer of a is open in Γ.

Definition 2.1.3. A (left) Γ-*set* is a discrete topological space with a continuous left Γ-action. A (left) Γ-*group* is a Γ-set if Γ acts by group automorphisms.

A *morphism of* Γ*-sets* (resp. Γ-groups) is a Γ-equivariant map (resp. group homomorphism).

Let A be a Γ-group.

Definition 2.1.4. A *1-cocycle* (or simply *cocycle*) of Γ with values in A is a continuous map $\alpha\colon \Gamma \to A, \sigma \mapsto \alpha_\sigma$ satisfying the *cocycle condition*

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

We denote by $Z^1(\Gamma, A)$ the set of all 1-cocycles of Γ with values in A. The constant map 1 is clearly a cocycle, called the *trivial cocycle*.

Note that the cocycle condition implies that any cocycle maps 1 to 1.

Definition 2.1.5. A *pointed set* is a pair (X, x) of a set X and an element x in X, often denoted by only X when the choice of x is clear from the context. The element x is called the *base point*. A *morphism of pointed sets* is map preserving the base point (so an *isomorphism of pointed sets* is nothing but a bijection preserving the base point).

Example 2.1.6. The set $Z^1(\Gamma, A)$ is a pointed set with the base point being the trivial cocycle.

Remark 2.1.7. If Γ acts on A trivially, then a cocycle is nothing but a continuous group homomorphism from Γ to A.

Lemma 2.1.8. *Let α be a cocycle of Γ with values in A and let $a \in A$. The map*

$$\begin{aligned} \alpha'\colon \Gamma &\to A \\ \sigma &\mapsto a^{-1}\alpha_\sigma{}^\sigma a \end{aligned}$$

is again a cocycle of Γ with values in A.

Proof. See [3] Lemma II.3.9. □

Definition 2.1.9. We define a relation $\sim$ in $Z^1(\Gamma, A)$ as follows: $\alpha \sim \alpha'$ if there exists an $a \in A$ such that $\alpha' = a^{-1}\alpha^\sigma a$. In this case, we say α and α' are

cohomologous. It is easy to see that this relation is reflexive, symmetric and transitive; hence an equivalence relation in $Z^1(\Gamma, A)$. We denote by $H^1(\Gamma, A)$ the quotient set

$$H^1(\Gamma, A) := Z^1(\Gamma, A)/\sim,$$

called *the first cohomology set of* Γ *with coefficients in* A. It is a pointed set with the base point being the equivalence class of the trivial cocycle. If α is a cocycle, we denote by $[\alpha]$ its equivalence class, called the *cohomology class* of α.

2.1.2 Galois descent for vector spaces

We first introduce the notion of semi-linear actions. Let Ω be a Galois extension of k with Galois group G.

Definition 2.1.10. Let W be a vector space[3] over Ω. A G-action on W is called *semi-linear* if it is k-linear and

$$\forall w \in W, \forall g \in G, \forall s \in \Omega\colon\ g(s \cdot w) = g(s) \cdot g(w).$$

For any G-set X, we denote by X^G the set of fixed points of X under the G-action. Very often X^G has some additional structure induced from some structure on X.

Theorem 2.1.11. *Let V be a (possibly infinite-dimensional) k-vector space on which G acts trivially. Then $\Omega \otimes_k V$ endowed with the diagonal G-action is a Ω-vector space and the G-action is semi-linear. Furthermore, the map*

$$V \to (\Omega \otimes_k V)^G$$
$$v \mapsto 1 \otimes_k v.$$

is an isomorphism of k-vector spaces.

Proof. The first assertion is clear. Choose a k-basis B of V. Then we have a k-vector space isomorphism $V \simeq \oplus_{i \in B} k$. Now it follows from Galois theory

[3]In this article, all modules are assumed to be left modules unless specified otherwise.

that the map $k \to (\Omega \otimes_k k)^G, x \mapsto 1 \otimes x$ is a k-vector space isomorphism. Thus, the map in question is again a k-vector space isomorphism as it respects direct sums. $\square$

Theorem 2.1.12. *Let W be a (possibly infinite-dimensional) Ω-vector space with a semi-linear G-action. Then W^G is a k-vector space with the trivial G-action. Furthermore, there is a G-equivariant isomorphism of Ω-vector spaces*

$$\begin{aligned} f \colon \Omega \otimes_k W^G &\to W \\ s \otimes_k w &\mapsto s \cdot w, \end{aligned}$$

where $\Omega \otimes_k W^G$ is endowed with the diagonal G-action.

Proof (taken from [9] Lemma 18.1). It is routine to show that the map f is Ω-linear and G-equivariant. To see it is injective, suppose $x = \sum_{i=1}^m s_i \otimes w_i \in \ker f$, where $s_i \in \Omega$ and $w_i \in W^G$ for all i. And we have $f(x) = \sum_{i=1}^m s_i \cdot w_i = 0$. We may assume WLOG that w_i's are linearly independent over k since W^G is a k-vector space. Then it amounts to show that $s_i = 0$ for all i, namely w_i's are linearly independent over Ω.

Assume towards a contradiction that there are $m \in \mathbb{N}$ and $w_1, \cdots, w_m \in W^G$ such that these w_i's are linearly independent over k but not over Ω. Let m be the minimum of such natural numbers. Then there are non-zero $t_1, \cdots, t_m \in \Omega$ such that $\sum_{i=1}^m t_i \cdot w_i = 0$. Renaming $t_1^{-1} t_i$ to t_i if necessary, we may assume that $t_1 = 1$. By assumption not all t_i's belong to k, say $t_2 \in \Omega \setminus k$. Then there is a $g \in G = \mathrm{Gal}(\Omega/k)$ such that $g(t_2) \neq t_2$. Therefore, the equation $\sum_{i=2}^m (g(t_i) - t_i) \cdot w_i = 0$ gives a linear relation among $w_2, \cdots, w_m$ over Ω, which contradicts the minimality of m.

As for the surjectivity of f, consider an arbitrary $x \in W$. Suppose that $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ is a basis for Ω over k, and $G = \{g_i \colon i = 1, \cdots, n\}$ with $g_1 = \mathrm{id}$. Define $y_j = \sum_{i=1}^n g_i(\alpha_j) \cdot g_i(x)$ for $j = 1, \cdots, n$. Since G acts semi-linearly on W, we have $y_j \in W^G$ for all j. By Dedekind's lemma, g_i's are linearly independent over Ω as endomorphisms of Ω, so the $n \times n$ matrix $\{g_i(\alpha_j)\}$ is invertible. In particular, $x = g_1(x)$ can be written as a Ω-linear combination of $y_1, \cdots, y_n$; hence lies in the image of f. $\square$

Corollary 2.1.13. *There is an equivalence of categories*

$$\begin{aligned} \{k\text{-vector spaces}\} &\leftrightarrow \{\Omega\text{-vector spaces with semi-linear } G\text{-actions}\} \\ V &\mapsto V_\Omega \\ W^G &\hookleftarrow W. \end{aligned}$$

One can use the previous theorem to prove the Hilbert's Theorem 90.

Let $\mathbf{GL}_N$ denote the general linear group of degree $N > 0$ defined over k. The functoriality of $\mathbf{GL}_N$ induces a continuous action of $\mathrm{Gal}(\Omega/k)$ on $\mathbf{GL}_N$, so we may consider the pointed set $H^1(\mathrm{Gal}(\Omega/k), \mathbf{GL}_N(\Omega))$.

Theorem 2.1.14 (Hilbert's Theorem 90)**.** *The first cohomology set of* $\mathrm{Gal}(\Omega/k)$ *with coefficients in* $\mathbf{GL}_N(\Omega)$ *is trivial, i.e.,* $H^1(\mathrm{Gal}(\Omega/k), \mathbf{GL}_N(\Omega)) = 1$.

Proof. The continuity of the $\mathrm{Gal}(\Omega/k)$-action on $\mathbf{GL}_N$ follows from the fact that $\mathbf{GL}_N$ is representable, as shown in [3] Lemma III.7.16. The main theorem is proved in [3] Proposition III.8.24. □

2.1.3 Galois descent for algebras

Suppose K is a field extension of k. For any k-algebra L, we write the tensor product $K \otimes_k L$ simply as L_K when the base field k is understood.

Let A be a finite-dimensional algebra over k.

Definition 2.1.15. A k-algebra A' is called a K/k*-twisted form* of A if they become isomorphic over K as K-algebras, i.e.,

$$K \otimes_k A \simeq K \otimes_k A'.$$

Example 2.1.16. The complex numbers $\mathbb{C}$ is a $\mathbb{C}/\mathbb{R}$-twisted form of $\mathbb{R} \times \mathbb{R}$.

In descent theory, one can show that K/k-twisted forms of A correspond to so-called descent data on A_K, which then relates to the first cohomology set. We give some results here that will be used later.

Definition 2.1.17. Let $R \to S$ be a morphism of k-algebras. Let $\mathrm{Aut}_{R\text{-alg}}(S)$ be the group of automorphisms of the R-algebra S.

For any k-algebra R, we define

$$\mathbf{Aut}_{k\text{- alg}}(A)(R) = \mathrm{Aut}_{R\text{- alg}}\left(R \otimes_k A\right).$$

If $\iota\colon R \to S$ is a morphism of k-algebras, we define the map

$$\begin{aligned}\mathbf{Aut}_{k\text{- alg}}(A)(\iota)\colon\ \mathrm{Aut}_{R\text{- alg}}\left(R \otimes_k A\right) &\to \mathrm{Aut}_{S\text{- alg}}\left(S \otimes_k A\right)\\ f &\mapsto \mathrm{id}_S \otimes_R f\end{aligned}$$

under the identification $S \otimes_R R \otimes_k A \simeq S \otimes_k A$. Thus, we have a functor $\mathbf{Aut}_{k\text{-alg}}(A)$ from the category of k-algebras to the category of groups.

If Ω is a Galois (field) extension of k, then the functoriality of $\mathbf{Aut}_{k\text{-alg}}(A)$ induces a $\mathrm{Gal}(\Omega/k)$-action on $\mathbf{Aut}_{k\text{- alg}}(A)(\Omega)$. More explicitly, this action is give by the map

$$\begin{aligned}\mathrm{Gal}(\Omega/k) \times \mathbf{Aut}_{k\text{- alg}}(A)(\Omega) &\to \mathbf{Aut}_{k\text{- alg}}(A)(\Omega)\\ (\sigma, f) &\mapsto {}^{\sigma}f := \sigma \circ f \circ \sigma^{-1}.\end{aligned} \tag{2.1}$$

This action is continuous by [3] Lemma III.8.13 and the setup in [3] III.9.1, so we may consider the pointed set $H^1(\mathrm{Gal}(\Omega/k), \mathbf{Aut}_{k\text{-alg}}(A)(\Omega))$.

Note that the set of k-algebra isomorphism classes of Ω/k-twisted forms of A is naturally a pointed set with the base point being the isomorphism class of A.

Theorem 2.1.18. *Let Ω be a Galois extension of k. There is an isomorphism of pointed sets*

$$\frac{\{\Omega/k\text{-twisted forms of } A\}}{k\text{-algebra isomorphism}} \leftrightarrow H^1(\mathrm{Gal}(\Omega/k), \mathbf{Aut}_{k\text{-alg}}(A)(\Omega))$$

defined as follows. Given a k-algebra A' such that there is an Ω-algebra isomorphism $f\colon A'_\Omega \simeq A_\Omega$, it corresponds to the cohomology class of the cocycle

$$\begin{aligned}\alpha\colon\ \mathrm{Gal}(\Omega/k) &\to \mathbf{Aut}_{k\text{-alg}}(A)(\Omega)\\ \sigma &\mapsto f \circ {}^{\sigma}(f^{-1}).\end{aligned}$$

Conversely, given $[\alpha] \in H^1(\mathrm{Gal}(\Omega/k), \mathbf{Aut}_{k\text{-alg}}(A)(\Omega))$*, it corresponds to the isomorphism class of the* k*-algebra*

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

whose k*-algebra structure is given by the restriction of the algebra structure of* A_Ω*.*

Under this correspondence, the isomorphism class of A *corresponds to the cohomology class of the trivial cocycle.*

Proof. See the discussion before [3] Proposition III.9.1. □

2.1.4 Galois descent for algebras with group actions

If A has further structure, a group action for example, descent formalism often works similarly with respect to the structure on A. Throughout this subsection, let G be a group.

Definition 2.1.19. A *G-algebra over k* is a k-algebra A on which G acts faithfully by automorphisms, i.e., there is an injective embedding $G \hookrightarrow \mathrm{Aut}(A)$. [4] A homomorphism (resp. isomorphism) of G-algebras over k is a G-equivariant k-algebra homomorphism (resp. isomorphism).

Without loss of generality, G can be identified with a subgroup of $\mathrm{Aut}(A)$, namely the image of the defining embedding.

Let A be a finite-dimensional G-algebra over k and K a field extension of k.

Definition 2.1.20. A G-algebra A' over k is called a K/k-twisted form of A if they become isomorphic over K as G-algebras.

Definition 2.1.21. Let $R \to S$ be a homomorphism of G-algebras over k. Let $\mathrm{Aut}_{G\text{-alg}/R}(S)$ be the group of automorphisms of an G-algebra S over R. One can define as before a functor $\mathbf{Aut}_{G\text{-alg}}(A)$ from the category of G-algebras

[4] Here we understand that by a G-algebra in general it is not necessary that $G \hookrightarrow \mathrm{Aut}(A)$.

over k to the category of groups given by

$$\mathbf{Aut}_{G\text{-alg}}(A)(R) = \mathrm{Aut}_{G\text{-alg}/R}\left(R \otimes_k A\right),$$

where G acts on the second component of $R \otimes_k A$. Let Ω be a Galois extension of k. It can be seen similarly that the functoriality of $\mathbf{Aut}_{G\text{-alg}}(A)$ gives a continuous action of $\mathrm{Gal}(\Omega/k)$ on $\mathbf{Aut}_{G\text{-alg}}(A)(\Omega)$.

Note that the set of G-algebra isomorphism classes of Ω/k-twisted forms of A is naturally a pointed set with the base point being the isomorphism class of A.

Theorem 2.1.22. *Let Ω be a Galois extension of k. There is an isomorphism of pointed sets*

$$\frac{\{\Omega/k\text{-twisted forms of } A\}}{G\text{-algebra isomorphism over } k} \leftrightarrow H^1(\mathrm{Gal}(\Omega/k), \mathbf{Aut}_{G\text{-alg}}(A)(\Omega)).$$

defined as follows. Given a G-algebra A' over k such that there is an G-algebra isomorphism $f\colon A'_\Omega \simeq A_\Omega$ over Ω, it corresponds to the cohomology class of the cocycle

$$\begin{aligned} \alpha\colon \mathrm{Gal}(\Omega/k) &\to \mathbf{Aut}_{G\text{-alg}}(A)(\Omega) \\ \sigma &\mapsto f \circ {}^{\sigma}(f^{-1}). \end{aligned}$$

Conversely, given $[\alpha] \in H^1(\mathrm{Gal}(\Omega/k), \mathbf{Aut}_{G\text{-alg}}(A)(\Omega))$, it corresponds to the isomorphism class of the G-algebra

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

whose G-algebra structure is given by the restriction of the G-algebra structure of A_Ω.

Under this correspondence, the isomorphism class of A corresponds to the cohomology class of the trivial cocycle.

Proof. See the discussion before [3] Proposition III.9.7. □

2.2 Étale algebras

2.2.1 Definition and first properties

In the category of field extensions of k, (finite) products and coproducts do not exist. For example, $\mathbb{C} \times \mathbb{C}$ and $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ are no longer fields. Étale algebras over k can be thought of as an enlargement of the category of finite separable field extensions of k such that this problem is fixed.

From now on, we fix a separable closure k_s of k and an embedding $k \hookrightarrow k_s$, and write Γ for the Galois group $\mathrm{Gal}(k_s/k)$ for short.

Definition 2.2.1. A k-algebra L is called *étale* if L can be written as a finite direct product of finite separable field extensions of k. A morphism of étale algebras over k is a k-algebra homomorphism.

Étale algebras over k and k-algebra homomorphisms form a subcategory of the category of k-algebras and k-algebra homomorphisms, denoted by $\mathbf{Ét}_k$ or simply $\mathbf{Ét}$ if the base field k is understood from the context. We will show that products and coproducts exist in $\mathbf{Ét}$ and are given by direct products and tensor products, respectively.

There is a geometric interpretation of étale algebras. We recall étale morphisms of schemes before we proceed.

Definition 2.2.2.

- A local homomorphism of local rings $f\colon A \to B$ with maximal ideals $\mathfrak{m}_A$ and $\mathfrak{m}_B$ is *unramified* if $f(\mathfrak{m}_A)B = \mathfrak{m}_B$ and $B/\mathfrak{m}_B$ is a finite separable extension of $A/\mathfrak{m}_A$.

- Let $f\colon X \to Y$ be a morphism of schemes. Then f is *unramified*[5] *at* $x \in X$ if f is locally of finite presentation at x and the natural map $\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ is an unramified homomorphism of local rings. We say f is *unramified* if it is unramified at every point $x \in X$.

[5]Some authors call such a property "G-unramified" and reserve the term "unramified" for morphisms not necessarily locally of finite presentation but locally of finite type.

- Let $f\colon X \to Y$ be a morphism of schemes. Then f is *flat at* $x \in X$ if $\mathcal{O}_{X,x}$ is flat as an $\mathcal{O}_{Y,f(x)}$-module. We say f is *flat* if it is flat at every point $x \in X$.

- Let $f\colon X \to Y$ be a morphism of schemes. Then f is *étale at* $x \in X$ if it is flat at x and unramified at x. We say f is *étale* if it is étale at every point $x \in X$.

Theorem 2.2.3. *Let L be a k-algebra. The following are equivalent:*

1. *L is étale;*

2. *The morphism of schemes $\operatorname{Spec} L \to \operatorname{Spec} k$ is finite and étale.*

Proof. If L is étale, then $L = L_1 \times \cdots \times L_m$ for some finite separable field extensions L_i/k for $i = 1, \cdots, m$. The morphism $\operatorname{Spec} L \to \operatorname{Spec} k$ is finite and flat since L is finite-dimensional as a k-vector space. To see it is unramified, it then suffices to notice that the local homomorphisms are given by finite separable field extensions $k \hookrightarrow L_i$.

Conversely, if the morphism of schemes $\operatorname{Spec} L \to \operatorname{Spec} k$ is finite and étale, then for any maximal ideal $\mathfrak{m} \subset L$, the natural homomorphism $k \hookrightarrow L_{\mathfrak{m}}$ of local rings is unramified. This means that $\mathfrak{m}L_{\mathfrak{m}} = 0 \cdot L_{\mathfrak{m}} = 0$, so $L_{\mathfrak{m}}$ is a finite separable field extension of k. In particular, L has no non-zero nilpotent. Since prime ideals of L that are contained in $\mathfrak{m}$ are in one-to-one correspondence with the prime ideals of $L_{\mathfrak{m}}$, no prime ideal of L is contained properly in $\mathfrak{m}$. This implies that $\dim \operatorname{Spec} L = 0$. Noticing that L is a finitely generated k-algebra, L is Noetherian; hence an Artin ring by [1] Theorem 8.5. Let $\mathfrak{m}_1, \cdots, \mathfrak{m}_n$ be the distinct maximal ideals of L. Then

$$\cap_{i=1}^{n} \mathfrak{m}_i \subseteq \operatorname{nil}(L) = \{0\},$$

where $\operatorname{nil}(L) = \{x \in L\colon \exists n, x^n = 0\}$ is the nilradical of L. Also $\mathfrak{m}_i$ and $\mathfrak{m}_j$ are coprime whenever $i \neq j$. By the Chinese remainder theorem (see e.g. [1]

Proposition 1.10), the natural map

$$\begin{aligned} L &\to \prod_{i=1}^{n} L/\mathfrak{m}_i \simeq \prod_{i=1}^{n} L_{\mathfrak{m}_i} \\ x &\mapsto (x+\mathfrak{m}_i)_i \end{aligned}$$

is a k-algebra isomorphism. Thus, L is written as a finite product a finite separable field extensions of k and is étale. □

Let L be an étale algebra over k. By a k_s-point of L we mean a k-algebra homomorphism from L to k_s. The set of k_s-points of L is denoted by $L(k_s)$. Then there is a canonical Γ-action on the k_s-points $L(k_s) = \mathrm{Hom}_{k\text{-alg}}(L, k_s)$:

$$\begin{aligned} \Gamma \times L(k_s) &\to L(k_s) \\ (\sigma, \tau) &\mapsto {}^{\sigma}\tau := \sigma \circ \tau. \end{aligned}$$

Notably, this Γ-action is continuous when $L(k_s)$ is endowed with the discrete topology and makes $L(k_s)$ a finite Γ-set. Indeed, let $l_1, \cdots, l_m$ be generators of L over k as a k-algebra. For any $\tau \in L(k_s)$, $\sigma \in \mathrm{Stab}_\Gamma(\tau)$ if and only if σ acts trivially on the finite field extension $K = k[\tau(l_1), \cdots, \tau(l_m)]$. This implies that $\mathrm{Stab}_\Gamma(\tau) = \mathrm{Gal}(k_s/K)$, an open subgroup in Γ. Hence the Γ-action is continuous by Definition 2.1.2.

Example 2.2.4. If L is a direct product of m copies of k viewed as a k-algebra, namely $L = k^m$ endowed with component-wise addition, multiplication and scalar multiplication, then L is an étale k-algebra called the *split* (or *trivial*) *étale k-algebra of dimension m*. We denote it simply by k^m when no confusion is possible.

The k_s-points of k^m are exactly the m natural projections followed by the embedding $k \hookrightarrow k_s$ on which Γ acts trivially.

Example 2.2.5. If L is a finite separable field extension of k with a primitive element $\gamma \in L$, then $L(k_s)$ is in bijection with all roots of the minimal polynomial of γ over k. In particular, we have $\dim_k L = |L(k_s)|$. If, furthermore, L is Galois, then $L(k_s)$ is in bijection with $\mathrm{Gal}(L/k)$, a quotient of Γ by a clopen subgroup.

Lemma 2.2.6. *Suppose L_i is an étale algebra over k for all $i = 1, \cdots, m$. Then the k_s-points of the direct product of L_i's canonically correspond to the disjoint union of the k_s-points of individual L_i's. More precisely, the map*

$$\coprod_{i=1}^{m} L_i(k_s) \simeq \left(\prod_{i=1}^{m} L_i\right)(k_s)$$
$$\tau \in L_i(k_s) \mapsto \tau \circ p_i$$

is a bijective morphism of Γ-sets, where p_i is the canonical projection from $\prod_{i=1}^{m} L_i$ onto L_i and $\amalg$ denotes the disjoint union operation.

Proof. Put $L = \prod_{i=1}^{m} L_i$. For any $i = 1, \cdots, m$, $L_i(k_s)$ is a Γ-set and the map

$$f_i \colon L_i(k_s) \to L(k_s)$$
$$\tau \mapsto \tau \circ p_i$$

is Γ-equivariant. These maps induce a Γ-map

$$f \colon \coprod_{i=1}^{m} L_i(k_s) \to L(k_s).$$

It is clearly injective. For any $\tau \in L(k_s)$, note that τ maps idempotents to idempotents. Denote by e_i the idempotent in L with the ith factor being 1 and other factors being 0. Because τ is a k-algebra homomorphism, we have $\tau(\sum e_i) = 1$ and $\tau(e_i \cdot e_j) = 0$ for any $i \neq j$. Thus, there is a unique e_i mapped to 1 for some i and others are mapped to 0. Say $\tau(e_1) = 1$. Then $\tau_1 \colon L_1 \to k_s, x \mapsto \tau(x, 0, \cdots, 0)$ lies in $L_1(k_s)$ and $\tau = f_1(\tau_1)$, so f is surjective. □

Remark 2.2.7. For the rest of this section we identify these two Γ-sets: $L(k_s)$ and $\coprod_{i=1}^{m} L_i(k_s)$, though they are not the same set strictly speaking.

Corollary 2.2.8. *If L is an étale algebra over k, then $|L(k_s)| = \dim_k L$.*

Corollary 2.2.9. *Suppose L is an étale k-algebra. Then L is a field if and only if Γ acts transitively on $L(k_s)$, and L is split if and only if Γ acts trivially on $L(k_s)$.*

Finite Γ-sets and Γ-maps form a category, denoted by $\mathbf{FinSet}_\Gamma$. Our discussion above gives a contravariant functor α from $\mathbf{\acute{E}t}_k$ to $\mathbf{FinSet}_\Gamma$. It assigns to each étale algebra L over k the finite Γ-set $\alpha(L) = L(k_s)$. Suppose we have a k-algebra homomorphism $f\colon L_1 \to L_2$, then α assigns to f the Γ-map $\alpha(f)\colon L_2(k_s) \to L_1(k_s), \tau \mapsto \tau \circ f$. It respects the identity morphism and composition of morphisms, so α is indeed a functor.

It turns out the k_s-points of an étale algebra L determine L completely. To see this, we give a contravariant functor $\beta\colon \mathbf{FinSet}_\Gamma \to \mathbf{\acute{E}t}_k$ that is an inverse of α.

Given a finite Γ-set X, the set of Γ-maps from X to k_s, denoted by $\mathrm{Map}_\Gamma(X, k_s)$, has a k-algebra structure, namely point-wise addition, multiplication and scalar multiplication.

Lemma 2.2.10. *Let X be a finite Γ-set. Then $\mathrm{Map}_\Gamma(X, k_s)$ is an étale k-algebra.*

Proof. Consider the Γ-orbit decomposition $X = \coprod_{i=1}^m X_i$. Then it is clear that the map

$$\prod_{i=1}^m \mathrm{Map}_\Gamma(X_i, k_s) \simeq \mathrm{Map}_\Gamma(X, k_s)$$
$$(\tau_1, \cdots, \tau_m) \mapsto \big(x \in X_i \mapsto \tau_i(x)\big)$$

is a k-algebra isomorphism. So it suffices to prove the statement in the case that Γ acts transitively on X. Pick any $x \in X$. Then a Γ-map from X to k_s is determined by where it maps x. Since Γ acts continuously on X, the stabilizer $\mathrm{Stab}(x)$ is an open subgroup of Γ. The homomorphism

$$f\colon \mathrm{Map}_\Gamma(X, k_s) \to k_s^{\mathrm{Stab}(x)}$$
$$\tau \mapsto \tau(x)$$

is an isomorphism of k-algebras. Indeed, if $\tau(x) = 0$, then the transitivity of the Γ-action on X implies that $\tau = 0$ and f is injective. To see it is surjective, note that for any $c \in k_s^{\mathrm{Stab}(x)}$, there is a unique Γ-map from X to k_s sending x to c. By the fundamental theorem of (infinite) Galois theory (see e.g. [14] Theorem 17.8), $k_s^{\mathrm{Stab}(x)}$ is a finite separable field extension of k, which

completes the proof. □

Remark 2.2.11. If one chooses a different element $x' \in X$, say $x' = {}^{\sigma}x$ for some $\sigma \in \Gamma$, then $\mathrm{Stab}(x') = \sigma \,\mathrm{Stab}(x)\sigma^{-1}$, so $\sigma(k_s^{\mathrm{Stab}(x)}) = k_s^{\mathrm{Stab}(x')}$ by Galois theory. In particular, they are isomorphic.

Now let β assign to each finite Γ-set X the étale k-algebra $\mathrm{Map}_\Gamma(X, k_s)$. Suppose $g\colon X \to Y$ is a Γ-map between finite Γ-sets. Let β assign to g the k-algebra homomorphism $\beta(g)\colon \mathrm{Map}_\Gamma(Y, k_s) \to \mathrm{Map}_\Gamma(X, k_s), \tau \mapsto \tau \circ g$. It respects the identity morphism and composition of morphisms, so β is indeed a functor.

Theorem 2.2.12 ([9] Theorem 18.4)**.** *There is an anti-equivalence of categories between* $\mathbf{\acute{E}t}_k$ *and* $\mathbf{FinSet}_\Gamma$ *given by the contravariant functors* α *and* β*.*

Proof. Suppose L is an étale algebra over k. By Lemma 2.2.6, we may assume without loss of generality that L is a finite separable field extension of k. Then we have k-algebra isomorphisms

$$\mathrm{Map}_\Gamma(L(k_s), k_s) \simeq k_s^{\mathrm{Stab}(\tau)} = k_s^{\mathrm{Aut}(k_s/\tau(L))} = \tau(L) \simeq L$$

for any $\tau \in L(k_s)$, where the first isomorphism is shown in the proof of Lemma 2.2.10.

Conversely, suppose given a finite Γ-set X. We may assume without loss of generality that Γ acts on X transitively. Then the isomorphism $\mathrm{Map}_\Gamma(X, k_s) \simeq k_s^{\mathrm{Stab}(x)}$ induces

$$\mathrm{Map}_\Gamma(X, k_s)(k_s) \simeq k_s^{\mathrm{Stab}(x)}(k_s) \tag{2.2}$$

for any $x \in X$. The latter is isomorphic to the cosets of $\mathrm{Stab}(x)$ in Γ by Galois theory; hence isomorphic to X by the orbit-stabilizer theorem. □

Remark 2.2.13. One can also write down the general isomorphisms explicitly:

- For any étale k-algebra L, we have the canonical k-algebra isomorphism given by the functor $\beta \circ \alpha$ (which is naturally isomorphic to the identity

functor on $\mathbf{\acute{E}t}_k$)

$$L \simeq \mathrm{Map}_\Gamma(L(k_s), k_s)$$
$$l \mapsto \big(\tau \mapsto \tau(l)\big).$$

- For any finite Γ-set X, we have the canonical Γ-set isomorphism given by the functor $\alpha \circ \beta$ (which is naturally isomorphic to the identity functor on $\mathbf{FinSet}_\Gamma$)

$$X \simeq \mathrm{Map}_\Gamma(X, k_s)(k_s)$$
$$x \mapsto \big(\tau \mapsto \tau(x)\big).$$

Corollary 2.2.14. *Let X be a finite Γ-set. Then*

$$\dim_k \mathrm{Map}_\Gamma(X, k_s) = |X|.$$

Proof. This follows from the isomorphism (2.2) and Corollary 2.2.8. □

This theorem gives a categorial interpretation of Lemma 2.2.6. Also, it implies that the tensor product of étale k-algebras corresponds to the direct product of the corresponding Γ-sets.

It is worth mentioning that being étale is stable under base change. Suppose K is field extension of k.

Proposition 2.2.15. *Let L be an étale algebra over k. Then $K \otimes_k L$ is an étale algebra over K.*

Proof. Suppose $L = \prod_{i=1}^m L_i$ for some finite separable extensions L_i's. Since $K \otimes_k L = \prod_{i=1}^m (K \otimes_k L_i)$, we reduce to the case where L is a finite separable extension of k. Let α be a primitive element of L over k with minimal polynomial $f \in k[x]$. Then $L \simeq k[x]/(f)$ and we have

$$K \otimes_k L \simeq K \otimes_k k[x]/(f) \simeq K[x]/(f) \simeq \prod_{i=1}^n K[x]/(f_i),$$

where $f = \prod_{i=1}^n f_i$ is a decomposition of f into distinct irreducibles in $K[x]$. For each $i = 1, \cdots, n$, $K[x]/(f_i)$ is a finite separable field extension of K, so $K \otimes_k L$ is étale over K. □

We finish this subsection with the following fact that will be used later.

Proposition 2.2.16. *Any étale k-algebra has only finitely many subalgebras*[6] *over k.*

Proof. Let $L = \prod_{i=1}^{m} L_i$ be an étale k-algebra, where L_i's are finite separable field extensions of k. We use induction on $m \geq 1$.

The base case $m = 1$ is the statement of the primitive element theorem.

Assume it is true for $m = k$ for some $k \geq 1$. Then we need to verify that if $L = \prod_{i=1}^{k+1} L_i$ is an étale k-algebra, where L_i's are finite separable field extensions of k, then L has only finitely many subalgebras over k. By the inductive hypothesis, the étale k-algebra $\prod_{i=1}^{k+1} L_i$, denoted by A, has only finitely many subalgebras over k. In fact, Goursat's Lemma, cf. [10] Lemma 4.5, states that there is a bijection between the set of subalgebras of $L = A \times L_{k+1}$ and the set of 5-tuples (B, C, I, J, φ) with the following properties

- B is a subalgebra of A over k;
- C is a subalgebra of L_{k+1} over k;
- $I \leq B$ is an ideal of B;
- $J \leq C$ is an ideal of C;
- $\varphi\colon B/I \to C/J$ is an isomorphism of k-algebras;

given by $(B, C, I, J, \varphi) \mapsto \{(b, c) \in B \times C\colon \varphi(\bar{b}) = \bar{c}\}$, where $\bar{b}$ denotes the image of b under $B \to B/I$ and $\bar{c}$ denotes the image of c under $C \to C/J$.

We have only finitely many choices for B and C, which is guaranteed by the hypothesis and the base case. Now that L_{m+1} is a field, J must be either 0 or (1). If $J = (1)$, then $I = (1)$ and φ must be the trivial map. If $J = 0$, then the number of choices for φ equals $|\operatorname{Aut}_k(L_{k+1})|$ which is finite. Furthermore, I must be a maximal ideal of B since $B/I = L_{k+1}$ is a field. Since the inclusion $B \hookrightarrow A$ is integral, B has only finitely many maximal ideals due to the finiteness of maximal ideals of A. To summarize, the set of such 5-tuples is finite, and so is the number of subalgebras of L. □

[6] By a subalgebra of a k-algebra L, we refer to a subset of L that contains $1 \in L$ and is closed under addition, multiplication and scalar multiplication.

2.2.2 A cohomological interpretation

Theorem 2.2.17. *Let L be a finite-dimensional commutative k-algebra. The following are equivalent:*

1. *L is étale;*
2. *L is a k_s/k-twisted form of the split étale k-algebra, i.e., $L_{k_s} \simeq k_s^n$, where $n = \dim_k L$.*

Proof. $1 \Rightarrow 2$ follows immediately from the proof of 2.2.15. For the other direction we refer to [4] Theorem 4, p.V.34. □

Remark 2.2.18. In the case above, L is a K/k-twisted form for some *finite* field extension K/k. For example, one may take K to be a normal closure of the compositum of the factors of L.

This theorem suggests that one can use Galois descent to classify the isomorphism classes of étale algebras over k. Let $[\mathbf{\acute{E}t}_n]$ denote the pointed set of the isomorphism classes of étale algebras over k with the base point being the isomorphism class of the split étale k-algebra of dimension n. It follows from Theorem 2.1.18 that $[\mathbf{\acute{E}t}_n]$ is classified by $H^1(k, \mathrm{Aut}_{k_s\text{-alg}}(k_s^n))$. Our next goal is to compute this automorphism group.

Definition 2.2.19 ([11], Proposition 21.8 and Exercise 21.2)**.** Let R be a nonzero commutative ring and $e \in R$ a nonzero idempotent. We say e is a *primitive idempotent* if the following equivalent conditions hold:

1. The ring Re is connected, i.e., it has no non-trivial idempotent;
2. The idempotent e admits no decomposition $e = \alpha + \beta$ such that α and β are nonzero idempotents and $\alpha \cdot \beta = 0$;
3. The idempotent e is minimal with respect to the partial order: $e' \leq e$ if and only if $e \cdot e' = e'$.

Example 2.2.20. Let $L = L_1 \times \cdots \times L_m$ for some finite separable field extensions L_i/k, $i = 1, \cdots m$. It is easy to see that L has exactly m primitive

idempotents given by

$$e_i := (\delta_{ij})_{j=1}^m, \text{ where } \delta_{ij} = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}.$$

Lemma 2.2.21. *Let K be a field and K^n the split étale K-algebra of dimension n. There is a group isomorphism*

$$\mathrm{Aut}_{K\text{-alg}}\, K^n \simeq S_n.$$

Proof. Consider the canonical homomorphism

$$\begin{aligned} S_n &\to \mathrm{Aut}_{K\text{-alg}}\, K^n \\ \sigma &\mapsto \big((x_i)_{i=1}^n \mapsto (x_{\sigma^{-1}(i)})_{i=1}^n\big). \end{aligned}$$

It is clearly injective. To see it is surjective, for any K-algebra automorphism $\gamma\colon K^n \to K^n$, we note that γ maps primitive idempotents to primitive idempotents, and hence corresponds to a permutation $\sigma \in S_n$ such that $\gamma(e_i) = e_{\sigma(i)}$ for all i. Then this permutation is mapped to γ. □

Via this isomorphism, the Γ-action on the automorphism group defined in (2.1) induces a trivial Γ-action on S_n. Thus, $H^1(k, S_n)$ is the set of cohomology classes of continuous group homomorphisms from Γ to S_n.

Theorem 2.2.22 ([3] Proposition V.13.5)**.** *There is an isomorphism of pointed sets*

$$[\mathbf{\acute{E}t}_n] \leftrightarrow H^1(k, S_n).$$

Under this correspondence, the isomorphism class of the n-dimensional split étale k-algebra corresponds to the cohomology class of the trivial cocycle.

2.3 Galois algebras

2.3.1 Definition and first properties

Let G be a finite group and L an étale G-algebra over k. Then G acts on the k_s-points $L(k_s)$ of L by composing on the right:

$$\begin{aligned} L(k_s) \times G &\to L(k_s) \\ (\tau, g) &\mapsto \tau \cdot g := \tau \circ g. \end{aligned}$$

Definition 2.3.1. A G-algebra L over k is called *Galois* if it is étale and the G-action on $L(k_s)$ is simply transitive, i.e.,

$$\forall \tau_1, \tau_2 \in L(k_s), \exists! g \in G, \tau_1 \cdot g = \tau_2.$$

A morphism of Galois G-algebras is a morphism of G-algebras. The Galois G-algebras over k form a subcategory of $\mathbf{Ét}_k$, denoted by $G\text{-}\mathbf{Gal}_k$ or simply $G\text{-}\mathbf{Gal}$ if the base field k is understood.

First, we will examine the two simplest cases: when L is a field and when L is split.

Example 2.3.2. Suppose L is a finite Galois extension of k. Then L is a Galois $\mathrm{Gal}(L/k)$-algebra over k. Indeed, we have seen in Example 2.2.5 that $L(k_s)$ is in bijection with $\mathrm{Gal}(L/k)$ and the action of $\mathrm{Gal}(L/k)$ is given by right composition; hence simply transitive.

Proposition 2.3.3. *Suppose L is a field extension of k. Then L is a Galois G-algebra over k for some finite group G if and only if L/k is a finite Galois extension and $G \simeq \mathrm{Gal}(L/k)$.*

Proof. It remains to show the "only if" part of the statement. Fix a $\tau \in L(k_s)$ and consider the following maps

- $f_1 \colon \mathrm{Aut}(L/k) \to L(k_s)$ that maps σ to $\tau \circ \sigma$;
- $f_2 \colon L(k_s) \to G$ that maps τ' to the unique g such that $\tau' = \tau \circ g$;

- $f_3 \colon G \to \mathrm{Aut}(L/k)$, the defining injective homomorphism of the G-algebra L.

By construction, their composite $f_3 \circ f_2 \circ f_1$ is the identity map on $\mathrm{Aut}(L/K)$. By definition f_2 is bijective and f_3 is injective, so they are all bijective. In particular, $|\mathrm{Aut}(L/k)| = |L(k_s)| = \dim_k L$, so L/k is a Galois extension, and f_3 gives the group isomorphism $G \simeq \mathrm{Gal}(L/k)$. □

This proposition could be misleading because the structure of G is not intrinsic to a Galois G-algebra L over k in general.

Example 2.3.4. Let $L = k^4$ be the split étale algebra over k of dimension 4. Define

$$G_1 = \mathbb{Z}/4\mathbb{Z} \simeq \langle (1234) \rangle \leq S_4$$

and

$$G_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \{(1), (12)(34), (13)(24), (14)(23)\} \leq S_4.$$

Then L has a Galois G_i-algebra structure for both $i = 1, 2$. These two groups have the same cardinality (which is a must by Corollary 2.2.8) but are not isomorphic. This example explains why the group G should be specified in advance when we talk about Galois algebras.

Given a finite group G, we have a unique (up to isomorphism) Galois G-algebra over k that is split.

Example 2.3.5. Let $L = \mathrm{Map}(G, k)$ denote the set of maps from G to k endowed with point-wise addition, multiplication, scalar multiplication and a left G-action as follows

$$\begin{aligned} G \times L &\to L \\ (h, f) &\mapsto \big(g \mapsto f(gh)\big). \end{aligned}$$

It is easy to see that L has an underlying split étale k-algebra structure of

dimension $|G|$ and the maps $e_g, g \in G$ defined by

$$e_g(h) = \begin{cases} 1 & \text{if h = g} \\ 0 & \text{otherwise} \end{cases}$$

are exactly the $|G|$ primitive idempotents of L and generate L as a k-algebra. It is worth mentioning that G acts on the primitive idempotents by

$$h \cdot e_g = e_{gh^{-1}}.$$

The k_s-points of L are exactly the evaluations at $|G|$ elements of G followed by the embedding $k \hookrightarrow k_s$, so G acts simply transitively on $L(k_s)$. We call this Galois G-algebra L the *split* (or *trivial*) *Galois G-algebra over k*, denoted by $k[G]$. Sometimes we denote elements $\big(g \mapsto x_g\big)$ of $k[G]$ simply by $(x_g)_{g\in G}$.

Proposition 2.3.6. *Let G be a group of cardinality n and L a split étale k-algebra of dimension n on which G acts faithfully. Then L is a Galois G-algebra over k if and only if $L \simeq k[G]$ as G-algebras.*

Proof. It remains to show the "only if" part. Pick any primitive element of L and denote it by e_1. Then for all $g \in G$, put $e_g := g^{-1} \cdot e_1$ and denote the factors $e_g \cdot L \simeq k$ of L by L_g. Since G acts simply transitively on $L(k_s)$, this indexing process is well-defined and the map

$$\begin{aligned} L = \prod_{g\in G} L_g &\to k[G] \\ (l_g)_{g\in G} &\mapsto \big(g \mapsto l_g\big) \end{aligned}$$

is a G-algebra isomorphism. □

Next, we consider Galois G-algebras in the correspondence $\mathbf{Ét}_k \leftrightarrow \mathbf{FinSet}_\Gamma$. If L is a Galois G-algebra over k, then the corresponding Γ-set $L(k_s)$ is a G-torsor over Γ.

Definition 2.3.7 (Following [17] I.5.2)**.**

- Suppose G is a Γ-group. A (right) *G-torsor over* Γ is a Γ-set X on which G acts simply transitively on the right, and the G-action is compatible with the Γ-action, namely

$$^{\sigma}(x \cdot g) = {}^{\sigma}x \cdot {}^{\sigma}g, \ \forall x \in X, \forall g \in G, \forall \sigma \in \Gamma.$$

- Suppose G is a Γ-group. G-torsors over Γ and G- and Γ-equivariant maps form a subcategory of $\mathbf{FinSet}_{\Gamma}$, denoted by G-$\mathbf{Tor}_{\Gamma}$ or simply G-$\mathbf{Tor}$ when Γ is understood from the context. Note that G itself endowed with right multiplication is a G-torsor over Γ, called the *trivial G-torsor over* Γ.

Example 2.3.8. Suppose L is a Galois G-algebra over k and Γ acts trivially on G,[7] then $L(k_s)$ is a G-torsor over Γ. Indeed, G acts simply transitively on $L(k_s)$ by definition. The left Γ-action and the right G-action are compatible because for any $g \in G, \tau \in L(k_s), \sigma \in \Gamma$, we have

$$^{\sigma}(\tau \cdot g) = \sigma \circ \tau \circ g = {}^{\sigma}\tau \cdot g = {}^{\sigma}\tau \cdot {}^{\sigma}g.$$

In fact, any G-torsor over Γ is given by some Galois G-algebra. More precisely, if P is a G-torsor over Γ, then we can make $\beta(X) = \mathrm{Map}_{\Gamma}(P, k_s)$ an étale G-algebra over k by letting G acts by

$$\begin{aligned} G \times \mathrm{Map}_{\Gamma}(P, k_s) &\to \mathrm{Map}_{\Gamma}(P, k_s) \\ (g, f) &\mapsto g(f), \end{aligned}$$

where $g(f)$ is defined by

$$(g(f))(\tau) = f(\tau \cdot g), \ \forall \tau \in P.$$

Theorem 2.3.9 ([9] Theorem 18.19)**.** *There is an anti-equivalence of categories between G-$\mathbf{Gal}_k$ and G-$\mathbf{Tor}_{\Gamma}$ given by the restrictions of α and β in Theorem 2.2.12.*

[7] A deeper reason why we let Γ act trivially on G is given in Lemma 2.3.16.

Proof. We first check that the restriction of β is also well-defined. Suppose that P is a G-torsor over Γ. We verify that the étale k-algebra $\mathrm{Map}_\Gamma(P, k_s)$ with the G-action above is Galois, namely the G-action on $\mathrm{Map}_\Gamma(P, k_s)(k_s)$ is simply transitive. To see this, it suffices to check that the Γ-set isomorphism given in Remark 2.2.13

$$P \to \mathrm{Map}_\Gamma(P, k_s)(k_s)$$
$$\tau \mapsto \big(f \mapsto f(\tau)\big)$$

is G-equivariant. Indeed, for any $\tau \in P$ and any $g \in G$, $(\beta \circ \alpha)(\tau \cdot g)$ and $(\beta \circ \alpha)(\tau) \cdot g$ both map any $f \in \mathrm{Map}_\Gamma(P, k_s)$ to $f(\tau \cdot g) \in k_s$. Because the G-action on P is simply transitive, so is the G-action on $\mathrm{Map}_\Gamma(P, k_s)(k_s)$.

This also shows that $\beta \circ \alpha$ is naturally isomorphic to the identity functor on G-$\mathbf{Tor}_\Gamma$. For similar reasons, $\alpha \circ \beta$ also respects the G-action and hence is naturally isomorphic to the identity functor on G-$\mathbf{Gal}_k$. □

The following theorem describes the structure of Galois G-algebras.

Theorem 2.3.10. *Every Galois G-algebra L over k can be written as a direct product of Galois extensions of k that are isomorphic as field extensions of k.*

Proof. Since L is étale over k, we may assume that $L = \prod_{i=1}^m L_i$ for some finite separable field extensions L_i of k. We will have shown that all L_i's are Galois and isomorphic as field extensions of k.

We have seen in Section 2.2 the Γ-orbit decomposition $L(k_s) = \coprod_{i=1}^m L_i(k_s)$. Pick a k_s-point $\tau \in L_1(k_s) \subseteq L(k_s)$ and consider the map

$$\rho\colon G \to L(k_s)$$
$$g \mapsto \tau \cdot g.$$

The assumption that L is Galois implies this map is bijective. Let H denote the stabilizer of the idempotent $e_1 \in L$, as in Example 2.2.20, under the G-action. Then $\rho(g) \in L_1(k_s)$ if and only if $\rho(g)(e_1) = 1$, if and only if g fixed e_1, so $\rho(H) = L_1(k_s)$. Therefore, L_1 is a Galois H-algebra by Theorem 2.3.9 as H acts simply transitively on $\rho(H) = L_1(k_s)$; hence a Galois extension of k with Galois group H by Corollary 2.2.9.

Furthermore, the right cosets of H in G are mapped to $L_i(k_s)$ for $i \neq 1$. In fact, if $f \in G \setminus H$, say $f(e_i) = e_1$ for some $i \neq 1$, then $\rho(hf)(e_i) = \rho(h)(e_1) = 1$ for any $h \in H$. Thus, $\rho(Hf) \subseteq L_i(k_s)$. On the other hand, if $\rho(f') \in L_i(k_s)$, then $\rho(f'f^{-1})(e_1) = \rho(f')(e_i) = 1$, so $f'f^{-1} \in H$ and $L_i(k_s) \subseteq \rho(Hf)$. Therefore, $\rho(Hf) = L_i(k_s)$, which implies that f maps $L_i(k_s)$ bijectively onto $L_1(k_s)$ and gives an isomorphism $L_i \to L_1$ of field extensions of k. In particular, each L_i is a Galois extension of k with Galois group isomorphic to H. $\square$

Remark 2.3.11. We will later see in Proposition 2.3.21 that L can be recovered as the Galois G-algebra induced from the Galois H-algebra L_1.

Products and coproducts do not exist in the category G-**Gal** by dimension considerations. Indeed, every Galois G-algebra over k has dimension equal to the cardinality of G. But base change still makes sense.

Suppose K is a field extension of k with defining homomorphism $\iota\colon k \to K$ and fix an embedding $e\colon K \to K_s$.

Proposition 2.3.12. *Let L be a Galois G-algebra over k. Then $K \otimes_k L$ is a Galois G-algebra over K with G acting on the second component.*

Proof. Since being étale is stable under base change (Proposition 2.2.15), the tensor product L_K is étale over K. The group G acts faithfully on L and so it does on L_K. By definition of Galois algebras, it remains to show that the G-action on $L_K(K_s)$ is simply transitive. Let $\tilde{\iota}\colon k_s \to K_s$ be an extension of $\iota\colon k \to K$; that is, the diagram

$$\begin{array}{ccc} k_s & \xrightarrow{\tilde{\iota}} & K_s \\ \uparrow & & \uparrow{\scriptstyle e} \\ k & \xrightarrow{\iota} & K \end{array}$$

commutes. Such an extension always exists, see e.g. [3] Corollary I.1.20. Now consider the map

$$\begin{aligned} L(k_s) = \mathrm{Hom}_{k\text{-alg}}(L, k_s) &\to \mathrm{Hom}_{K\text{-alg}}(L_K, K_s) = L_K(K_s) \\ \tau &\mapsto e \otimes (\tilde{\iota} \circ \tau). \end{aligned}$$

If τ_1 and τ_2 have the same image, then in particular, for any $l \in L$ we have

$$(e \otimes (\tilde{\iota} \circ \tau_1))(1 \otimes l) = (\tilde{\iota} \circ \tau_1)(l) = (\tilde{\iota} \circ \tau_2)(l) = (e \otimes (\tilde{\iota} \circ \tau_2))(1 \otimes l),$$

which implies $\tau_1(l) = \tau_2(l)$, so $\tau_1 = \tau_2$ and the map is injective. Notice that

$$|L(k_s)| = \dim_k L = \dim_K L_K = |L_K(K_s)| < \infty.$$

Thus, this map is bijective. Furthermore, since the G-action on L_K is induced by the G-action on L, this correspondence is G-equivariant, so G acts on $L_K(K_s)$ simply transitively because it acts on $L(k_s)$ simply transitively. Therefore, L_K is Galois over K. □

Remark 2.3.13. Galois G-algebras over k also have a geometric interpretation. They are equivalent to scheme-theoretic G-torsors over k, which we will discuss in Section 4.2.

2.3.2 A cohomological interpretation

Let G be a finite group. This subsection is devoted to give a cohomological interpretation of Galois G-algebras. We start with the following lemma.

Lemma 2.3.14. *Let G be a finite group acting on a k-vector space V faithfully and linearly, and K/k a field extension. Then G acts naturally on the extension of scalars $V_K = K \otimes_k V$ by acting on the second component and we have*

$$(V^G)_K = (V_K)^G.$$

Proof. The inclusion $(V^G)_K \subset (V_K)^G$ is straightforward. For the other direction, we need to show the implication

$$\sum_i (g \cdot v_i - v_i) \otimes_k x_i = 0,\ \forall g \in G \Rightarrow g \cdot v_i - v_i = 0,\ \forall i,\ \forall g \in G,$$

for which it suffices to show

$$\sum_i v_i \otimes_k x_i = 0 \Rightarrow v_i = 0,\ \forall i,$$

where $x_i \in K$ are linearly independent over k and $v_i \in V$. This follows immediately from the natural isomorphisms of k-vector spaces

$$V \otimes_k (\oplus_i k x_i) \simeq \oplus_i (V \otimes_k k x_i) \simeq \oplus_i V$$
$$0 = \sum_i v_i \otimes_k x_i \longmapsto (v_i)_i = 0$$

□

Theorem 2.3.15. *Let L be an étale G-algebra over k. The following are equivalent:*

1. *L is Galois;*
2. *L is a k_s/k-twisted form of the split Galois G-algebra, i.e., $L_{k_s} \simeq k_s[G]$ as G-algebras over k_s;*
3. *$L^G = k$ and $|G| = \dim_k L$.*

Proof. The implication $1 \Rightarrow 2$ follows immediately from Proposition 2.3.12, Proposition 2.3.6 and Theorem 2.2.17.

To see $2 \Rightarrow 3$, note that by Lemma 2.3.14,

$$(L^G)_{k_s} = (L_{k_s})^G \simeq (k_s[G])^G \simeq k_s,$$

which implies that L^G is of dimension 1 as a vector space over k; hence equal to k. Also $\dim_k L = \dim_{k_s} L_{k_s} = |G|$.

For the implication $3 \Rightarrow 1$, assume towards a contradiction that the G-action on $L(k_s)$ is not simply transitive. Since $|G| = \dim_k L = |L(k_s)|$ by assumption, the G-orbit decomposition of $L(k_s)$ is non-trivial. Consider the G-algebra isomorphism

$$L \simeq \mathrm{Map}_\Gamma(L(k_s), k_s)$$
$$l \mapsto \big(\tau \mapsto \tau(l)\big).$$

It restricts to a G-algebra isomorphism on the G-invariants

$$L^G \simeq (\mathrm{Map}_\Gamma(L(k_s), k_s))^G = \mathrm{Map}_\Gamma(L(k_s)/G, k_s),$$

where $L(k_s)/G$ denotes the set of the G-orbits of $L(k_s)$ (this is again a Γ-set since on $L(k_s)$ the Γ-action commutes with the G-action). By Corollary 2.2.14, $\dim_k \mathrm{Map}_\Gamma(L(k_s)/G, k_s) \geq 2$, so the dimension of L^G as a k-vector space must be at least two, leading to a contradiction. □

This theorem suggests Galois G-algebras are k_s/k-twisted forms of the split Galois G-algebra $k[G]$. Let $[G\text{-}\mathbf{Gal}_k]$ denote the pointed set of the isomorphism classes of Galois G-algebras over k with the base point being the isomorphism class of the split Galois G-algebra, so one can use $H^1(k, \mathrm{Aut}_{G\text{-alg}\,/k_s}(k_s[G]))$ to classify $[G\text{-}\mathbf{Gal}_k]$ by Theorem 2.1.22.

We now compute this automorphism group.

Lemma 2.3.16. *Let K be a field. There is a group isomorphism*

$$\mathrm{Aut}_{G\text{-alg}\,/K}\,(K[G]) \simeq G.$$

Proof. Let $(e_g)_{g\in G}$ be the primitive idempotents of $K[G]$. The map

$$\begin{aligned} G &\to \mathrm{Aut}_{G\text{-alg}}\,(K[G]) \\ g &\mapsto \big((x_h)_{h\in G} \mapsto (x_{gh})_{h\in G}\big) \end{aligned}$$

is an injective group homomorphism. Notice that the image of g maps the primitive idempotents e_h to $e_{g^{-1}h}$ for all $h \in G$. To see it is surjective, suppose $f \in \mathrm{Aut}_{G\text{-alg}}\,(K[G])$. Then $f(e_1) = e_g$ for some $g \in G$. For any $h \in G$, we have

$$f(e_h) = f(h^{-1} \cdot e_1) = h^{-1} \cdot f(e_1) = h^{-1} \cdot e_g = e_{gh},$$

which shows that g^{-1} is mapped to f. □

Via this isomorphism, the Γ-action on the automorphism group defined in (2.1) induces a trivial Γ-action on G, so $H^1(k, G)$ is the set of cohomology classes of continuous group homomorphism from Γ to G.

Theorem 2.3.17 ([3] Proposition V.14.13)**.** *There is an isomorphism of pointed sets*

$$[G\text{-}\mathbf{Gal}_k] \leftrightarrow H^1(k, G).$$

Under this correspondence, the isomorphism class of the split Galois G-algebra over k corresponds to the cohomology class of the trivial cocycle.

Remark 2.3.18. There is an isomorphism between $[G\text{-}\mathbf{Tor}_\Gamma]$, the pointed set of isomorphism classes of G-torsors over Γ with the base point being the class of the trivial torsor, and the pointed set $H^1(\mathrm{Gal}(k_s/k), G)$

$$\lambda\colon [G\text{-}\mathbf{Tor}_\Gamma] \to H^1(\mathrm{Gal}(k_s/k), G)$$

defined as follows: If P is a G-torsors over $\mathrm{Gal}(k_s/k)$, pick an $x \in P$. We define a cocycle α by associating to each $\sigma \in \mathrm{Gal}(k_s/k)$ the unique element $\alpha_\sigma \in G$ such that $\sigma \cdot x = x \cdot \alpha_\sigma$ and define λ by taking $\lambda[P]$ to be the cohomology class of α. This is well-defined, base-point-preserving and bijective, as shown in [17], Proposition I.33.

In summary, we now have the following diagram connecting $H^1(k, G)$, $[G\text{-}\mathbf{Tor}_\Gamma]$ and $[G\text{-}\mathbf{Gal}_k]$.

$$\begin{array}{ccc} [G\text{-}\mathbf{Gal}_k] & \xrightarrow{\sim} & H^1(k, G) \\ \wr\uparrow & \nearrow_{\lambda} & \\ [G\text{-}\mathbf{Tor}_\Gamma] & & \end{array}$$

Straightforward calculation shows that this triangle is commutative, see [3], Lemma V.14.16 for the details.

2.3.3 Induced Galois algebras

Let G be a finite group and $H \subseteq G$ a subgroup. Suppose M is a Galois H-algebra over k. There is a natural way to construct a Galois G-algebra out of M.

Definition 2.3.19. The *induced G-algebra of M* is the set $\mathrm{Map}_H(G, M)$ of H-equivariant maps of sets from G to M, denoted by $\mathrm{Ind}_H^G M$, where H acts on G by left multiplication and G acts on $\mathrm{Ind}_H^G M$ by

$$(g(f))(g') = f(g'g),\ \forall g, g' \in G,\ \forall f \in \mathrm{Ind}_H^G M.$$

It is a k-algebra with point-wise addition, multiplication and scalar multiplication. For any $1 \neq g \in G$, there is an $f \in \operatorname{Ind}_H^G M$ such that $f \neq g(f)$. Indeed, one could take f to be

$$f(g') = \begin{cases} c & \text{if } g' \in H \\ 0 & \text{otherwise} \end{cases},$$

where we take

$$c = \begin{cases} 1 & \text{if } g \notin H \\ \text{any element of } M \text{ that is not fixed by } g & \text{if } g \in H \end{cases}.$$

This shows that the G-action is faithful and $\operatorname{Ind}_H^G M$ is indeed a G-algebra.

Let e denote the identity element of G. Then the map $e\colon \operatorname{Ind}_H^G M \to M$, $f \mapsto f(e)$ is H-equivariant because f is. Indeed, for any $h \in H$,

$$e(h(f)) = (h(f))(e) = f(h) = h \cdot f(e) = h \cdot e(f).$$

This induced algebra has the following universal property:

$$\begin{array}{ccc} & & X \\ & \overset{F}{\swarrow} & \downarrow{\scriptstyle f} \\ \operatorname{Ind}_H^G M & \xrightarrow{\ e\ } & M \end{array}$$

For any G-algebra X and H-equivariant homomorphism $f\colon X \to M$, there exists a unique G-equivariant homomorphism $F\colon X \to \operatorname{Ind}_H^G M$ such that the diagram above commutes. Indeed, for any $x \in X$, one has $F(x)\colon G \to M$ given by $g \mapsto f(g \cdot x)$.

Proposition 2.3.20. *The G-algebra $\operatorname{Ind}_H^G M$ is Galois over k.*

Proof. Let $Hg_1, \cdots, Hg_r$ be the distinct right cosets of H in G. Consider the map

$$\begin{aligned} \operatorname{Ind}_H^G M &\to M^r \\ f &\to (f(g_1), \cdots, f(g_r)), \end{aligned}$$

where M^r is the direct product of r copies of M with component-wise addition, multiplication and scalar multiplication. Notice that every H-equivariant map $f \in \mathrm{Map}_H(G, M)$ is uniquely determined by how it maps $g_1, \cdots, g_m$, so this is a k-algebra isomorphism and hence $\mathrm{Ind}_H^G M$ is étale over k.

Furthermore, if $f \in \mathrm{Ind}_H^G M$ is G-fixed, then it is constant. But because f is H-equivariant, the image lies in M^H. By Theorem 2.3.15, $M^H = k$, so f is a k-valued constant map and $(\mathrm{Ind}_H^G M)^G = k$. Also we have $|G| = r|H| = \dim_k M^r = \dim_k \mathrm{Ind}_H^G M$. Therefore, $\mathrm{Ind}_H^G M$ is Galois. □

Proposition 2.3.21. *Let $L = L_1 \times \cdots \times L_r$ be a Galois G-algebra over k where L_i's are Galois field extensions of k with Galois group isomorphic to $H \leq G$. The projection $L \to L_1$ induces a G-algebra isomorphism $L \to \mathrm{Ind}_H^G L_1$. In particular, every Galois algebra is induced by a field.*

Proof. The projection $p_1 \colon L \to L_1$ induces a G-equivariant homomorphism $P \colon L \to \mathrm{Ind}_H^G L_1$ by the universal property of induced algebras. This map P is injective because for distinct $x_1, x_2 \in L$, there exists a $g \in G$ such that $p_1(g \cdot x_1) \neq p_1(g \cdot x_2)$. Then P is an isomorphism because $\dim_k \mathrm{Ind}_H^G L_1 = |G| = \dim_k L$, as shown in the proof of last proposition. □

Chapter 3

Quotients of Varieties

This chapter serves as justification for the construction of versal torsors in the following chapters. We show that the quotient of a k-variety X under a G-action exists in the category of k-varieties when G is finite. Furthermore, when G acts freely on X, the quotient map is an étale morphism.

We start with a clarification on what we mean by actions on varieties and in what sense an action is free in a general viewpoint, though our main interests lie in actions of finite groups. So in the second section, we restrict ourselves to group varieties associated to finite groups and sketch a proof due to Mumford for the existence of quotients under finite groups. In the end of the chapter, we present several examples of quotients.

3.1 Generalities

Definition 3.1.1. Let $\mathcal{C}$ be a category where finite products[8] exist. A *group object* in $\mathcal{C}$ is an object G in $\mathcal{C}$ with morphisms $m\colon G \times G \to G$, $i\colon G \to G$ and $e\colon \bullet \to G$, where $\bullet$ is the terminal object in $\mathcal{C}$, that makes the following diagrams commute.

[8]In this article, by saying finite products exist, we explicitly assume an empty product exists, which is the same thing as a terminal object.

$$\begin{array}{ccc} G\times G\times G & \xrightarrow{\mathrm{id}_G\times m} & G\times G \\ {\scriptstyle m\times\mathrm{id}_G}\downarrow & & \downarrow{\scriptstyle m} \\ G\times G & \xrightarrow{\quad m\quad} & G \end{array} \qquad \text{(associativity)}$$

$$\begin{array}{ccccc} \bullet\times G & \xrightarrow{e\times\mathrm{id}_G} & G\times G & \xleftarrow{e\times\mathrm{id}_G} & \bullet\times G \\ & \searrow & \downarrow{\scriptstyle m} & \swarrow & \\ & & G & & \end{array} \qquad \text{(identity)}$$

$$\begin{array}{ccc} G\times G & \xrightarrow{i\times\mathrm{id}_G} & G\times G \\ \downarrow & & \downarrow{\scriptstyle m} \\ \bullet & \xrightarrow{\quad e\quad} & G \end{array} \qquad \begin{array}{ccc} G\times G & \xrightarrow{\mathrm{id}_G\times i} & G\times G \\ \downarrow & & \downarrow{\scriptstyle m} \\ \bullet & \xrightarrow{\quad e\quad} & G \end{array} \qquad \text{(inverse)}$$

Example 3.1.2. If $\mathcal{C}$ is the category **Sets** of sets and maps of sets, then the group objects in $\mathcal{C}$ are (abstract) groups. In fact, the terminal object in $\mathcal{C}$ is a one-point set (which is unique up to isomorphism). For any group G, the morphism m is the multiplication, i is the inverse operation, and e is the map from a one-point set to the neutral element of G. The diagrams above are commutative due to the axioms of groups.

We assume that the readers are familiar with the definition and first properties of schemes. For a complete introduction, we refer to [8] Chapter II.

From now on, we fix an algebraic closure of the base field k and denote it by $\bar{k}$.

Definition 3.1.3. Let S be a k-scheme. We say S is *geometrically reduced* if $S_{\bar{k}}$ is reduced.

Definition 3.1.4. An *(algebraic) variety over a field* k is a separated and geometrically reduced scheme of finite type over $\operatorname{Spec} k$. A morphism between two varieties over k is a k-morphism of schemes. A *group variety over* k is a group object in the category of varieties over k.

Remark 3.1.5. If $G = \operatorname{Spec} R$ is an affine group variety over k, then the defining morphisms m, i, e correspond to k-algebra homomorphisms satisfying the

opposite diagrams

$$\begin{aligned} M\colon R \to R \otimes_k R \quad & \text{(comultiplication)} \\ I\colon R \to R \quad & \text{(coinverse)} \\ E\colon R \to k \quad & \text{(augmentation)}, \end{aligned}$$

which, together with the k-algebra structure of R, makes R a *Hopf algebra* over k.

We now define actions of group varieties on algebraic varieties, which is analogous to actions of groups on sets.

Definition 3.1.6. A (right) action of a group variety G over k on a variety X over k is a morphism $\varphi\colon X \times_k G \to X$ that makes the following diagrams commute.

1. The identity of G acts trivially on X:

$$\begin{array}{ccc} X \times \bullet & & \\ {\scriptstyle \mathrm{id}_X \times e}\downarrow & \searrow & \\ X \times_k G & \xrightarrow[\varphi]{} & X \end{array}$$

2. The action is associative with the multiplication on G:

$$\begin{array}{ccc} X \times_k G \times_k G & \xrightarrow{\mathrm{id}_X \times m} & X \times_k G \\ {\scriptstyle \varphi \times \mathrm{id}_G}\downarrow & & {\scriptstyle \varphi}\downarrow \\ X \times_k G & \xrightarrow{\varphi} & X \end{array}$$

We say G *acts freely* on X if for any scheme S over k, the induced group action of $G(S)$ on the set $X(S)$ is free.

Remark 3.1.7. One can define group schemes and actions of group schemes similarly in the category of schemes.

Remark 3.1.8. If G acts freely on X, the G-action on the underlying set $|X|$ of prime ideals of X need not be free. For example, let the generator g of $G = \mathbb{Z}/2\mathbb{Z}$ act on the 1-dimensional affine space $X = \mathbb{A}^1_{\mathbb{R}}$ over $\mathbb{R}$ by $g\colon \mathbb{R}[x] \to \mathbb{R}[x], f(x) \mapsto f(-x)$. Then G acts freely on $X \setminus \{0\}$ but the ideal $(x^2 + c)$ is fixed by g for any $c > 0$.

Proposition 3.1.9. *With the setting above, the following are equivalent:*

1. *The G-action on X is free;*
2. *The G-action on X is geometrically free, i.e., the induced $G_{\bar{k}}$-action on $X_{\bar{k}}$ is free;*
3. *The natural morphism*

$$\begin{aligned} X \times_k G &\to X \times_k X \\ (x, g) &\mapsto (x \cdot g, x) \end{aligned}$$

is a monomorphism of k-schemes.

Proof.

$1 \Leftrightarrow 3$: Note that G acts on X freely if and only if the natural map $G(S) \times X(S) \to X(S) \times X(S)$ is injective (monomorphic) for any k-scheme S. What we desire then follows from Yoneda's lemma.

$1 \Rightarrow 2$: This is clear as $G_{\bar{k}}(S) = G(S)$ and $X_{\bar{k}}(S) = X(S)$ for any $\bar{k}$-scheme S.

$2 \Rightarrow 1$: This follows from the fact that monomorphism fpqc descends.

□

In this thesis, we will use fpqc descent and some fpqc descending properties of schemes that we now explain.

Definition 3.1.10. A morphism of schemes $X \to Y$ is *fpqc* if it is faithfully flat and every quasi-compact[9] open subset of Y is the image of a quasi-compact open subset of X.

Example 3.1.11. Let $k \hookrightarrow \bar{k}$ be an embedding of k into an algebraic closure. The induced morphism of schemes $\operatorname{Spec} \bar{k} \to \operatorname{Spec} k$ is fpqc.

[9]In this article, a scheme is said to be *quasi-compact* if every open covering has a finite subcovering. We reserve the term "compact" for spaces that are both quasi-compact and Hausdorff.

Definition 3.1.12. Let $\mathcal{P}$ be a property of morphisms of schemes, $f\colon X \to S$ a morphism of schemes, and let $\tilde{f}\colon X_{S'} \to S'$ be the base extension of f by a fpqc morphism $S' \to S$. We say that $\mathcal{P}$ *fpqc descends* if $\tilde{f}$ has $\mathcal{P}$ implies that f has $\mathcal{P}$.

Example 3.1.13. The following properties of morphisms of schemes fpqc descend:

1. surjective (cf. [6] 2.6.1(i));
2. bijective (cf. [6] 2.6.1(iv));
3. isomorphism (cf. [6] 2.7.1(viii));
4. monomorphism (cf. [6] 2.7.1(ix));
5. finite (cf. [6] 2.7.1(xv));
6. étale (cf. [7] 17.7.3(ii)).

Example 3.1.14. Let G be a finite group and k a field. We can make G a group variety by considering the spectrum of $k[G]$, denoted by $\mathbf{G}$. The group structure of $\mathbf{G}$ is given by the comorphisms defined as follows

$$\begin{aligned} M\colon k[G] &\to k[G] \otimes_k k[G] \quad \text{(comultiplication)} \\ e_g &\mapsto \sum_{hh'=g} e_h \otimes e_{h'} \\ I\colon k[G] &\to k[G] \qquad\qquad\qquad \text{(coinverse)} \\ e_g &\mapsto e_{g^{-1}} \\ E\colon k[G] &\to k \qquad\qquad\qquad \text{(augmentation)} \\ f &\mapsto f(1) \end{aligned}$$

Intuitively, $\mathbf{G}$ is $\coprod_G \operatorname{Spec} k$, the disjoint union of $|G|$ copies of $\operatorname{Spec} k$. The multiplication, for instance, is then given by mapping g_1th $\operatorname{Spec} k$ and g_2th $\operatorname{Spec} k$ to the $(g_1 \cdot g_2)$th $\operatorname{Spec} k$.

Viewing $\mathbf{G}$ as a functor of points, for any field extension K of k, we have $\mathbf{G}(K) = \operatorname{Mor}_k(\operatorname{Spec} K, \mathbf{G}) = \operatorname{Hom}_{k\text{-alg}}(k[G], K) = G$. For this reason, $\mathbf{G}$ is called the *constant group scheme(variety)* associated to G over k.

3.2 Quotients of varieties by finite groups

From now on, we assume that G is a finite group and make no notational distinction between G and the constant group scheme associated to G over k when the field k is understood, though many propositions would still be valid in a more general setting.

We now introduce various notions of quotients of varieties, which have been the central objects in the geometric invariant theory.

Definition 3.2.1. Let X be an algebraic variety over k and G a finite group acting on X. A *categorial quotient* of X by G is a pair (Y, π), where Y is an algebraic variety with the trivial G-action and $\pi\colon X \to Y$ is a G-morphism, such that for any variety Z with the trivial G-action and any G-morphism $\pi'\colon X \to Z$, there exists a unique G-morphism $f\colon Y \to Z$ such that the diagram

$$\begin{array}{ccc} X & \xrightarrow{\pi'} & Z \\ \downarrow{\scriptstyle \pi} & \nearrow_{f} & \\ Y & & \end{array}$$

commutes. If there exists such a pair, it is unique up to canonical isomorphism by the universal property, so one may speak of *the* categorial quotient.

This definition of categorial quotients generalize the quotients of sets with group actions in the most general and simplest way. However, it is not very useful in practice as it gives no information of what the categorial quotients, if exist, should look like. A possible answer to this question lies in the notion of geometric quotients.

Definition 3.2.2 ([16] Definition 0.6)**.** Let X be an algebraic variety over k and G a finite group acting on X. A *geometric quotient* of X by G is a pair (Y, π), where Y is an algebraic variety with the trivial G-action and $\pi\colon X \to Y$ is a G-morphism, satisfying the following properties:

1. π is surjective and the fibers of π coincide with the G-orbits of X.
2. π is submersive, i.e., a subset $V \subset Y$ is open if and only if $\pi^{-1}(V)$ is open in X.

3. the natural morphism $\mathcal{O}_Y \to \pi_* (\mathcal{O}_X)^G$ is an isomorphism, where $\pi_* (\mathcal{O}_X)^G$ denotes the subsheaf of G-invariants of $\pi_* (\mathcal{O}_X)$ for the G-action.

Note that if a geometric quotient is to exist, then property 1 and 2 state that π is the quotient map for the G-action. Furthermore, one can show that a geometric quotient, if exists, is the categorial quotient, cf. [16] Proposition 0.1, so it is also unique up to isomorphism.

Due to the assumption that G is a finite group, the categorial quotient and geometric quotient both exist and coincide.

Theorem 3.2.3. *Let $X = \operatorname{Spec} A$ be an affine k-variety on which G acts. Denote by $\pi\colon X \to \operatorname{Spec} A^G$ the morphism induced by the inclusion $A^G \hookrightarrow A$. Then $(\operatorname{Spec} A^G, \pi)$ is the geometric quotient of X by G, denoted by X/G.*

Proof. See [16] Theorem 1.1 and Amplification 1.3. □

Lemma 3.2.4. *Let $X = \operatorname{Spec} A$ be an affine k-variety on which G acts and let $\pi\colon X \to \operatorname{Spec} A^G$ be the quotient map. The morphism π is finite, surjective and separable. Furthermore, if G acts freely on X, π is an étale morphism.*

Proof. The statement is proved in [15], II. 7 in the case that k is algebraically closed.

If k is not algebraically closed, we make a base change to $\bar{k}$ and obtain the morphism

$$\bar{\pi} = \mathrm{id}_{\bar{k}} \otimes \pi\colon \operatorname{Spec} A_{\bar{k}} \to \operatorname{Spec}(A^G)_{\bar{k}}.$$

Let G act on the second component of $A_{\bar{k}} = \bar{k} \otimes A$. Since $(A_{\bar{k}})^G = (A^G)_{\bar{k}}$ by Lemma 2.3.14, the morphism $\bar{\pi}$ is the quotient of $X_{\bar{k}}$ under the induced G-action. By the algebraically closed case, $\bar{\pi}$ is finite and surjective. These two properties fpqc descend, so π is also finite and surjective. If the G-action on X is free, then the induced G-action on $X_{\bar{k}}$ is also free by Proposition 3.1.9. This implies that π is étale as being étale also descends.

Finally, the G-action on A extends uniquely on $\operatorname{Frac}(A)$, the field of fractions of A. For any $a/b \in \operatorname{Frac}(A)^G, a, b \in A$ and $b \neq 0$, we have

$$\frac{a}{b} = \frac{a \prod_{g \neq e} g(b)}{\prod_{g \in G} g(b)}.$$

Then $a\prod_{g\neq e} g(b) \in A^G$, which implies $\mathrm{Frac}(A)^G = \mathrm{Frac}(A^G)$. Therefore, $\mathrm{Frac}(A^G)$ is a Galois field extension of $\mathrm{Frac}(A)$. In particular, π is separable. □

In general, X is not affine, but is covered by affine open subsets. Suppose that X is irreducible and for any $x \in X$, the orbit Gx of x is contained in a non-empty affine open subset of X. In this case, the existence of the quotient is also guaranteed and the previous lemma suggests that the quotient is locally given by the k-algebra of invariants.

Theorem 3.2.5. *Let X be an irreducible algebraic variety over k and G a finite group acting on X. Suppose that for any $x \in X$, the orbit Gx of x is contained in a non-empty affine open subset of X. Then the quotient (Y, π) exists and satisfies the following properties:*

1. *the map $\pi\colon X \to Y$ is the quotient map between the underlying topological spaces for the G-action;*
2. *the natural morphism $\mathcal{O}_Y \to \pi_*(\mathcal{O}_X)^G$ is an isomorphism, where $\pi_*(\mathcal{O}_X)^G$ denotes the subsheaf of G-invariants of $\pi_*(\mathcal{O}_X)$ for the G-action.*

The morphism π is finite, surjective and separable. Furthermore, if G acts freely on X, π is an étale morphism.

Proof. First, it suffices to show that the quotient topological space (Y, π) of X for the G-action, given the sheaf $\mathcal{O}_Y = \pi_*(\mathcal{O}_X)^G$, is an algebraic variety. Indeed, for any $x \in X$, there is an open affine subset $U_x \subset X$ containing the orbit Gx by the assumption. Substituting U_x by $\cap_{g\in G} gU_x$ (which is non-empty since X is irreducible and affine since X is separated) if needed, we may assume U_x is G-stable without loss of generality, so we obtain a G-stable open covering $\{U_x, x \in X\}$ of X. Suppose $\{X_i, i \in I\}$ is a finite subcovering. Then $\pi(X_i)$'s form a finite open covering of Y and $\mathcal{O}_Y|_{\pi(X_i)} = \pi_*(\mathcal{O}_{X_i})^G$, so each $\pi(X_i)$ is an affine variety by the previous theorem; hence Y is an algebraic variety. The other assertions follows immediately from the affine case. □

Example 3.2.6. For $N \geq 1$, let $\mathbf{GL}_N$ denote the general linear group over k, and let G be a finite group embedded in $\mathbf{GL}_N$. Then there is a morphism

$\pi\colon \mathbf{GL}_N \to \mathbf{GL}_N/G$ of affine varieties, where $\mathbf{GL}_N/G$ is the spectrum of the ring R_D^G of G-invariants in the localization of the affine N-space $R = \mathbb{A}_k^{N^2}$ at the determinant form $D = \det(X_{11}, \cdots, X_{NN})$.

Example 3.2.7. Let the generator g of $G = \mathbb{Z}/2\mathbb{Z}$ act on the 1-dimensional affine space $X = \mathbb{A}_{\mathbb{R}}^1$ over $\mathbb{R}$ by $g\colon \mathbb{R}[x] \to \mathbb{R}[x], f(x) \mapsto f(-x)$. Then $(\mathbb{R}[x])^G = \mathbb{R}[x^2]$ and $X/G \simeq \operatorname{Spec} \mathbb{R}[x^2]$, where we view $\mathbb{R}[x^2]$ as a subring of $\mathbb{R}[x]$.

Chapter 4

Torsors

This chapter revisits the notion of torsors in the category of schemes, generalizing the torsors discussed in section 2.3. The latter will be referred to as *set-theoretic torsors* from now on.

Geometrically, a torsor can be thought as a family of set-theoretic torsors. We discuss the definition of torsors and some first properties in the first section.

In the second section, we focus on the case when the base scheme is a field and the group is finite. In that case, torsors turn out to be relatively uncomplicated. Indeed, the category of G-torsors and G-equivariant morphisms is equivalent to that of set-theoretic G-torsors over $\mathrm{Gal}(k_s/k)$ and G-maps, and that of G-Galois algebras over k and G-equivariant homomorphisms as well.

4.1 Generalities

Throughout this section, we fix a base scheme S.

Definition 4.1.1. A morphism of schemes $X \to Y$ is *fppf* if it is faithfully flat and locally of finite presentation. We say an S-scheme is *fppf* if the defining morphism is fppf.

Remark 4.1.2. Both fppf and fpqc are French abbreviations: fppf stands for "fidèlement plat de présentation finie" and fpqc stands for "fidèlement plat quasi-compact".

Example 4.1.3. If the base scheme is a field K, then the faithful flatness is automatic. Since K is Noetherian, any K-scheme is fppf if and only if it is locally of finite type. In particular, any K-variety is fppf.

Proposition 4.1.4. *Let f be a morphism of schemes. Each of the following propositions implies the next:*

1. *f is surjective and étale;*
2. *f is fppf;*
3. *f is fpqc.*

Proof. The implication 1⇒2 follows immediately from the definition. For 2⇒3 we refer to [19] Proposition 2.35(iv). □

Definition 4.1.5 ([12]. III.4)**.** Let G be an fppf group scheme over S, i.e., the defining morphism $G \to S$ is fppf. A (right) *G-torsor* over S is an fppf S-scheme X with a right G-action $X \times_S G \to X$ such that the following equivalent conditions hold:

1. There exists an fppf base change $S' \to S$ such that $X_{S'}$ with the right $G_{S'}$-action is isomorphic to $G_{S'}$ with right translation $G_{S'}$-action.
2. The map
$$\begin{aligned} X \times_S G &\to X \times_S X \\ (x, g) &\mapsto (x, x \cdot g) \end{aligned} \tag{4.1}$$
is an isomorphism of S-schemes.

A morphism of G-torsors over S is a G-equivariant morphism of S-schemes.

Proof of equivalence. 2⇒1: Take $S' = X$. Then the map (4.1) gives an isomorphism $X_{S'} \simeq G_{S'}$ as S-schemes. It respects the $G_{S'}$-action as $x(gh) = (xg)h$ by the axioms of actions.

1⇒2: Base change the map (4.1) to S' and composite with $X_{S'} \simeq G_{S'}$, we obtain
$$\begin{aligned} G_{S'} \times_{S'} G_{S'} &\to G_{S'} \times_S G_{S'} \\ (x, g) &\mapsto (x, x \cdot g), \end{aligned}$$

which is a translation isomorphism. Since $S' \to S$ is fppf; hence fpqc by Proposition 4.1.4. Since isomorphism fpqc descends, the map (4.1) is again an isomorphism. □

If S is a variety over a field k and G an fppf group scheme over k, we refer G_S-torsors X as G-torsors because $X \times_S G_S \simeq X \times_k G$ and fppf is stable under base change.

Remark 4.1.6. Being a G-torsor is stable under base change. More precisely, let X be a G-torsor over S. Then for any morphism $S' \to S$, the base change $X_{S'}$ is a $G_{S'}$-torsor over S'. Indeed, fppf is stable under base change, so we need only verify the torsor condition:

$$X_{S'} \times_{S'} X_{S'} \simeq S' \times_S (X \times_S X) \simeq S' \times_S (X \times_S G) \simeq X_{S'} \times_{S'} G_{S'}.$$

Before we proceed, we first prove the following lemma.

Lemma 4.1.7. *Let X_1 and X_2 be G-torsors over S_0. Suppose $f\colon X_1 \to X_2$ is a G-equivariant S_0-morphism. Then f is an isomorphism of G-torsors.*

Proof. By the definition of G-torsors, there exists fppf base changes $S_i \to S_0$ such that there are G_{S_i}-equivariant isomorphisms $S_i \times_{S_0} G \simeq S_i \times_{S_0} X_i$ for $i = 1, 2$. Taking $S = S_1 \times_{S_0} S_2$, one obtains the G_S-equivariant isomorphisms $S \times_{S_0} G \simeq S \times_{S_0} X_i$ for $i = 1, 2$.

Then the following diagram commutes for some G_S-equivariant morphism $t\colon G_S \to G_S$:

$$\begin{array}{ccc} S \times_{S_0} X_1 & \xrightarrow{\sim} & S \times_{S_0} G \\ \downarrow{\scriptstyle \mathrm{id}_S \times f} & & \downarrow{\scriptstyle t} \\ S \times_{S_0} X_2 & \xrightarrow{\sim} & S \times_{S_0} G \end{array}$$

Since t is G_S-equivariant, the following diagram also commutes:

$$\begin{array}{ccccc} G_S \simeq G_S \times_S S & \xrightarrow{\mathrm{id} \times e} & G_S \times_S G_S & \xrightarrow{\mathrm{id} \times t} & G_S \times_S G_S \\ & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle m} \\ & & G_S & \xrightarrow{\quad t \quad} & G_S \end{array}$$

where m and e are the defining morphisms of G_S as a group scheme over S, so t is given by a right translation by $t \circ e \in G(S)$ and hence an isomorphism. Therefore, $\mathrm{id}_S \times f$ is an isomorphism, so f is an isomorphism by fpqc descent. □

Corollary 4.1.8. *Let (S, π') be a G-torsor over S_0 and (T, π) a G-torsor over T_0. Suppose that the following diagram commutes*

$$\begin{array}{ccc} S & \xrightarrow{f} & T \\ \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} \\ S_0 & \xrightarrow{f_0} & T_0 \end{array}$$

where f is a G-equivariant morphism. Then $S \simeq T \times_{T_0} S_0$ as G-torsors over S_0.

Proof. The fiber product of f and π' is a G-equivariant morphism $(f, \pi') \colon S \to T \times_{T_0} S_0$ between G-torsors over S_0; hence an isomorphism by the previous lemma. □

4.2 Torsors under finite groups over fields

Now we come back to the case where G is a finite group and make no notational distinction between G and its associated constant group scheme over k.

Example 4.2.1. The group scheme G with the right translation is itself a G-torsor, called the *trivial G-torsor* over k, denoted by $\mathbf{G}$.

Example 4.2.2. Let L be a Galois G-algebra over k. Then $X = \operatorname{Spec} L$ is a G-torsor over $\operatorname{Spec} k$, because there is a finite field extension K of k such that $X_K = \operatorname{Spec}(L_K) \simeq \operatorname{Spec} K[G] \simeq \mathbf{G}_K$.

In fact, the G-torsors over k are equivalent to the set-theoretic torsors.

Proposition 4.2.3. *The G-torsors over k are precisely the spectra of G-Galois algebras over k. Furthermore, the category of G-torsors over k and morphisms*

of G-torsors is equivalent to the category of G-Galois algebras and the category of set-theoretic G-torsors over $\mathrm{Gal}(k_s/k)$.

$$\{G\text{-torsors over } k\} \equiv G\text{-}\mathbf{Gal}_k^{op} \equiv G\text{-}\mathbf{Tor}_{\mathrm{Gal}(k_s/k)}.$$

Thus, there is a bijection between pointed sets

$$\{\text{isomorphism classes of } G\text{-torsors over } k\} \leftrightarrow H^1(k, G),$$

where the isomorphism class of the trivial G-torsor corresponds to the cohomology class of the trivial cocycle.

Proof. The spectra of G-Galois algebras over k are G-torsors over k as discussed above.

Conversely, for any G-torsor X over k, we have $X_S \simeq \mathbf{G}_S$ for some fppf k-scheme S. Since $\mathbf{G}_S$ is finite and étale over S, by fpqc descent, so is X over k. Then $X = \operatorname{Spec} L$ for some étale k-algebra L by Theorem 2.2.3. And the isomorphism (4.1) implies that the induced action of $G(k_s) = G$ on $L(k_s)$ is simply transitive, so L is a Galois G-algebra over k. The rest then follows immediately from Theorem 2.3.9. □

Remark 4.2.4. This correspondence gives us an explicit way to compute the corresponding cohomology class of a G-torsor X over k. Namely, pick any element x in $X(k_s)$ (on which G acts simply transitively as X is given by some Galois k-algebra) and for any $\sigma \in \mathrm{Gal}(k_s/k)$, we define a_σ by ${}^\sigma x = x \cdot a_\sigma$. Then $a\colon \mathrm{Gal}(k_s/k) \to G$ is a cocycle representing X in $H^1(k, G)$.

The next proposition gives an example of G-torsors that is of crucial importance to us.

Proposition 4.2.5. *Let X be an algebraic variety over a field k and G act* freely *on X, and (Y, π) the quotient of X under the G-action. Then X is a G-torsor over Y.*

Proof. The morphism $G \to \operatorname{Spec} k$ is clearly fppf. Taking a base change to Y, we obtain that $G_Y \to Y$ is fppf. By Theorem 3.2.5, $\pi\colon X \to Y$ is surjective and étale; hence fppf.

We may assume without loss of generality that k is algebraically closed, otherwise we take a fpqc base change $Y \to Y_{\bar{k}}$ and then apply fpqc descent to the quotient map $\mathrm{id}_{\bar{k}} \times \pi \colon X_{\bar{k}} \to Y_{\bar{k}}$.

It remains to show that the map $\tau \colon X \times_Y G_Y \to X \times_Y X$, $(x, g) \mapsto (x, x \cdot g)$ is an isomorphism. Note that $X \times_Y G_Y \simeq X \times_k G$, and τ is the fiber product of étale morphisms $p_1 \colon X \times_k G \to X$, $(x, g) \mapsto x$ and $\mu \colon X \times_k G \to X$, $(x, g) \mapsto x \cdot g$, so τ is étale. Thus, it suffices to show that τ is bijective.

Since they are varieties over k, we need only check the bijectivity on closed points. As sets of prime ideals, we have

$$X \times_Y X \simeq \{(x, x', y, \mathfrak{p}) \colon y = \pi(x) = \pi(x') \text{ and } \mathfrak{p} \in \mathrm{Spec}(\mathbf{k}(x) \otimes_{\mathbf{k}(y)} \mathbf{k}(x'))\},$$

see e.g. [2] Lemma 26.17.5. Notice that only closed points are mapped to closed points via the finite morphism π and the residue field of any closed point $x \in X$ must be a finite field extension of k, so for any closed point $x, x' \in X$, we have $\mathbf{k}(x) = \mathbf{k}(x') = \mathbf{k}(y) = k$ because k is algebraically closed. Thus, the set of closed points of $X \times_Y X$ is in bijection with the set of pairs

$$\{(x, x') \colon \pi(x) = \pi(x'), x \text{ is a closed point in } X\},$$

and hence in bijection with the closed points of $X \times_k G$ via τ since π is the quotient map for the G-action. $\square$

Chapter 5

Versal Torsors

In this chapter, we denote by k_0 a base field and keep the assumption that G is a finite group throughout.

The goal of this chapter is to introduce versal torsors to the readers and present some specific constructions of versal torsors under finite groups. Intuitively, versal G-torsors are G-torsors in the category of S-schemes with the universal property that any G-torsor T over any infinite field $k \supseteq k_0$ can be obtained by pulling back a versal torsor along some k-points in S. So many properties of G-torsors are inherited by versal G-torsors, which motivates the study of versal torsors. For example, if a versal G-torsor is smooth, then so are all G-torsors by base change.

The first section of this chapter presents two classic ways of constructing a versal torsor under finite groups: from a general linear group scheme or from an affine space over k_0. In the second section, we provide a more direct proof of the second construction that avoids the use of Galois cohomology.

5.1 Two classic constructions

Definition 5.1.1. A *versal G-torsor* over a k_0-scheme S is a G-torsor Q over S such that for every extension k of k_0 with k infinite, every G-torsor T over k, and every non-empty open subset U of S, there exists $x \in U(k)$ whose fiber Q_x is isomorphic to T as a G-torsor.

A versal G-torsor Q over S is "universal" in the sense that any G-torsor T over any infinite field $k \supseteq k_0$ can be obtained by pulling back Q along some k-points in S. We say such a k-point *realizes* the G-torsor T.

The next theorem asserts that versal G-torsors exist for any finite group G and gives a specific construction out of general linear groups.

Theorem 5.1.2. *Suppose G is a finite group embedded into $\mathbf{GL}_N$ for some N over k_0. Let G act on $\mathbf{GL}_N$ by right multiplication. Then $\mathbf{GL}_N$ is a versal G-torsor over $\mathbf{GL}_N/G$.*

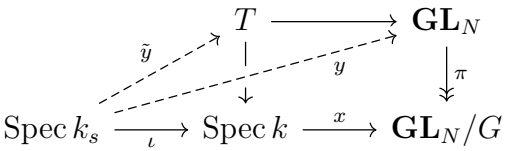
Proof. We have shown $\mathbf{GL}_N$ is a G-torsor over $\mathbf{GL}_N/G$ in Proposition 4.2.5. We now show that it is versal. By [17] Proposition I.36, the sequence of pointed sets

$$\begin{aligned} * \to H^0(k, G) \to H^0(k, \mathbf{GL}_N(k_s)) \to H^0(k, (\mathbf{GL}_N/G)(k_s)) \\ \xrightarrow{\delta} H^1(k, G) \to H^1(k, \mathbf{GL}_N(k_s)) \end{aligned} \tag{5.1}$$

is exact, where $H^0(k, A)$ is defined to be group of the invariants $A^{\mathrm{Gal}(k_s/k)}$ for any $\mathrm{Gal}(k_s/k)$-group A. It follows from Theorem 2.1.14 that $H^1(k, \mathbf{GL}_N(k_s))$ is trivial, so sequence (5.1) reduces to

$$* \to G \to \mathbf{GL}_N(k) \to (\mathbf{GL}_N/G)(k) \xrightarrow{\delta} H^1(k, G) \to * \tag{5.2}$$

Therefore, for any $t \in H^1(k, G)$, there exists an $x \in (\mathbf{GL}_N/G)(k)$ such that $\delta(x) = t$. Pick a $y \in \mathbf{GL}_N(k_s)$ such that the following diagram commutes.



Then $t = \delta(x)$ is represented by the cocycle $a_\sigma = y^{-1} \cdot {}^\sigma y$ for $\sigma \in \mathrm{Gal}(k_s/k)$.

On the other hand, put $T := \mathbf{GL}_N \times_{\mathbf{GL}_N/G} \operatorname{Spec} k$. Then T is a G-torsor over k by Remark 4.1.6. The fiber product $\tilde{y}$ of y and ι lies in $T(k_s)$, so by Remark 4.2.4, T is represented by the cocycle $a' \colon \mathrm{Gal}(k_s/k) \to G$ defined by

$${}^\sigma \tilde{y} = \tilde{y} \cdot a'_\sigma,$$

so $a'_\sigma = y^{-1} \cdot {}^\sigma y = a_\sigma$ and the class of T is represented by t.

Furthermore, the exactness of sequence (5.2) implies that the fiber of x for δ is identified with the orbit O_x of x under the action of $\mathbf{GL}_N(k)$ on $(\mathbf{GL}_N/G)(k)$ by [17] Corollary 1 (following Proposition I.36). Note that $\mathbf{GL}_N(k)$ is dense in $\mathbf{GL}_N$. In fact, since

$$\mathbf{GL}_N(k) = \mathrm{Mor}_{k_0}(\operatorname{Spec} k, \mathbf{GL}_N) \simeq \mathrm{Mor}_k(\operatorname{Spec} k, (\mathbf{GL}_N)_k) = \mathbf{GL}_{N,k}(k),$$

we may assume $k = k_0$ without loss of generality. Consider the closed points in the form $(X_{ij} - a_{ij})$ that have residue fields k where $a_{ij} \in k$. Assume there exists a non-zero $f \in R_D$ such that U_f contains no such point. Then f vanishes for all $a_{ij} \in k$. Since k is infinite, this is absurd. Next, π sends dense subsets to dense subsets due to its continuity, so O_x is dense in $\mathbf{GL}_N/G$; hence $\mathbf{GL}_N$ is versal. □

We can also construct a versal G-torsor out of the N-dimensional affine space V over k_0 on which $\mathbf{GL}_N$ acts. Fix an embedding $G \hookrightarrow \mathbf{GL}_N$ over k_0. If we remove all the closed subschemes that are fixed under some $1 \neq g \in G$ and end up with an open dense G-stable subscheme V' of V on which G acts freely, then Proposition 4.2.5 shows that $V' \to V'/G$ is a G-torsor. Indeed, it is a versal G-torsor.

Theorem 5.1.3. *Let G be a finite group embedded into $\mathbf{GL}_N$ for some N over k_0 and V the affine N-dimensional space over k_0 on which $\mathbf{GL}_N$ (and hence G) acts. Define*

$$V' = V \setminus \bigcup_{1 \neq g \in G} \ker(g - 1).$$

Then V' is an open dense G-stable subscheme of V. Furthermore, V' is a versal G-torsor over V'/G.

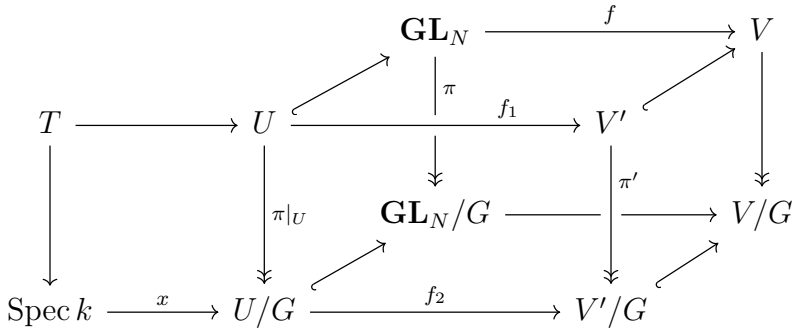
Proof. We verify that the G-action on $V' \subseteq V$ is free. By Proposition 3.1.9, it suffices to show that $G_{\bar{k}}$ acts on $V'_{\bar{k}}$ freely. Indeed, for any closed point $v \in V'_{\bar{k}}$, if there was a $1 \neq g \in G$ such that $gv = v$, then $v \in \ker(g - 1)$, which is contradictory.

It remains to show that $V' \to V'/G$ is versal. Because of the definition of versal torsors, we may assume k_0 is infinite. Pick a k_0-point $v = (Y_i - a_i \colon i =$

$1, \cdots, n) \in V'$, where $a_i \in k_0$. The natural $\mathbf{GL}_N$-action on V induces a G-equivariant dominant morphism of schemes $f\colon \mathbf{GL}_N \to V$ given by the homomorphism of coordinate rings (on the generators)

$$\mathcal{O}(V) = k_0[Y_1, \cdots, Y_N] \hookrightarrow k_0[X_{11}, \cdots, X_{NN}]_D = \mathcal{O}(\mathbf{GL}_N)$$
$$Y_i \mapsto \sum_j a_j X_{ij}.$$

Put $U = f^{-1}(V')$, then U is an open G-stable subset of $\mathbf{GL}_N$, and hence dense since $\mathbf{GL}_N$ is irreducible. Then f restricts to a G-equivariant dominant morphism $f_1\colon U \to V'$ which induces a dominant morphism $f_2\colon U/G \to V'/G$.



The quotient U/G is well-defined by Theorem 3.2.5 since $\pi^{-1}(\pi(U)) = U$, where $\pi\colon \mathbf{GL}_N \to \mathbf{GL}_N/G$ is the quotient map.

For any G-torsor T over a field extension k of k_0, we have shown in Theorem 5.1.2 that the k-points realizing T are dense in $\mathbf{GL}_N/G$. Since U/G is non-empty and open in $\mathbf{GL}_N/G$, there exists $x \in U/G(k)$ such that $\mathbf{GL}_N \times_{\mathbf{GL}_N/G} \operatorname{Spec} k \simeq T$ as G-torsors.

Clearly U is the fiber product of $\mathbf{GL}_N$ and U/G over $\mathbf{GL}_N/G$. Furthermore, U is the fiber product of V' and U/G over V'/G by Corollary 4.1.8. Therefore, the fiber of $\pi'\colon V' \to V'/G$ over the k-point $f_2 \circ x$ is isomorphic to T as G-torsors by the transitivity of base change.

For any open subset $W \subset V'/G$, $f_2^{-1}(W)$ is non-empty since f_2 is dominant, so the existence of such x that realizes T in $f_2^{-1}(W)$ follows from the versal property of $\mathbf{GL}_N$ over $\mathbf{GL}_N/G$, which implies the versal property for V' over V'/G. □

Remark 5.1.4. Viewing V as a set of prime ideals, it would be too much if we remove all elements of V that are fixed by some $1 \neq g \in G$.

For example, let $G = \mathbb{Z}/2\mathbb{Z} = \langle g \rangle$ act on $X = \mathbb{A}^1_{\mathbb{R}}$ by $x \mapsto -x$ as in Remark 3.1.8. Take $k = k_0 = \mathbb{R}$. Prime ideals in $\mathbb{R}[x]$ are generated by a irreducible monic polynomial in $\mathbb{R}[x]$. We shall denote by c the ideals in the form $(x - c)$ for any $c \in \mathbb{R}$ and by $(b + ci, b - ci)$ the prime ideals in the form $((x - b)^2 + c^2)$ for any $b, c \in \mathbb{R}$ and $c > 0$ in Figure 5.1. Then the points in the form $(ci, -ci)$ are fixed by g as they correspond to ideals $(x^2 + c)$, and so is the generic point. However, if we remove all these points and pass to the quotient $X/G = \operatorname{Spec} \mathbb{R}[x^2]$, we end up with $\mathbb{R}$-points in the form $(c, -c)$ for $c > 0$ which realize only the trivial G-torsor. But we should have more because $H^1(k, G)$ is non-trivial (it contains two elements).

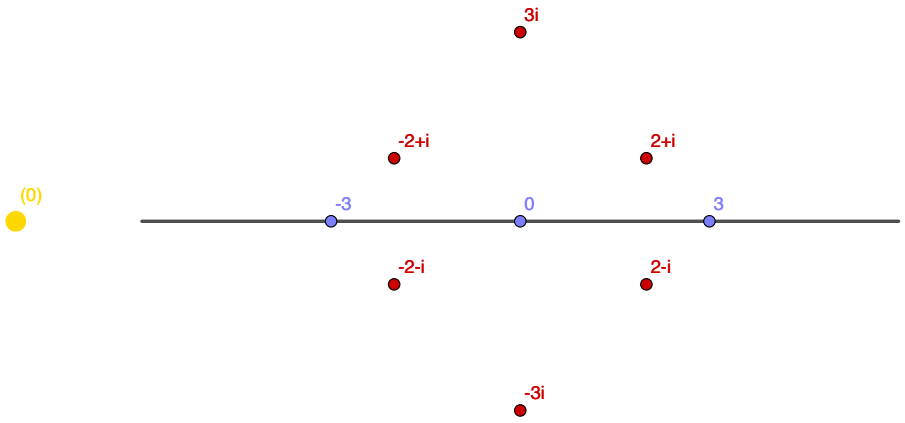


Figure 5.1: 1-dimensional affine space over $\mathbb{R}$.

Figure 5.2: $\mathbb{R}$-points in $\mathbb{A}^1_{\mathbb{R}}/G$.

5.2 An alternative proof of Theorem 5.1.3

In this section, we work in the context of Theorem 5.1.3; that is, let G be a finite group embedded into $\mathbf{GL}_N$ for some N over k_0 and V the N-dimensional affine space over k_0 on which $\mathbf{GL}_N$ (and hence G) acts. Let V' be the subscheme of V with the varieties $\ker(g-1)$ removed, for all $g \in G \setminus \{1\}$. Then V' is an open dense G-stable subscheme of V.

Given k that is infinite and a field extension of k_0, we have seen in Section 4.2 that G-torsors over k are given by Galois G-algebras over k. To realize them out of $V' \to V'/G$, we proceed in the following steps:

First, we argue that to find a k-point of V'/G that realizes a Galois G-algebra L, it suffices to find a surjective G-equivariant k-algebra homomorphism $\mathcal{O}(V_k) \to L$. Next, we give a proof for the existence of such a homomorphism based on the fact that any Galois G-algebra over k has finitely many G-stable subalgebras. Finally, we show that the k-points of V'/G that realize L are dense.

Lemma 5.2.1. *Let L be a Galois G-algebra over k. If x is a G-equivariant embedding from* $\operatorname{Spec} L$ *to V_k, then x factors through V_k'.*

Proof. By Theorem 2.3.15, $\operatorname{Spec} L_{\bar{k}}$ is a finite set on which G acts simply transitively. Since $\tilde{x}$ is G-equivariant, this implies that G acts freely on $\operatorname{Spec} L$ by Proposition 3.1.9; hence also acts freely on $\operatorname{im}(x)$. Therefore, x factors through V_k'. □

Lemma 5.2.2. *To find a k-point of V'/G that realizes a Galois G-algebra L, it suffices to find a surjective G-equivariant k-algebra homomorphism $\mathcal{O}(V_k) \to L$, where G acts on the second component of $\mathcal{O}(V_k) = k \otimes_{k_0} \mathcal{O}(V)$.*

Proof. Suppose $h\colon \mathcal{O}(V_k) \to L$ is a surjective G-equivariant k_0-algebra homomorphism. Then the restriction of h on the G-invariants is a homomorphism $h|_{\mathcal{O}(V_k)^G}\colon \mathcal{O}(V_k/G) \to k$. By Lemma 5.2.1, the comorphisms factor through V_k' and V_k'/G, respectively, such that the diagram

$$\begin{array}{ccccc} \operatorname{Spec} L & \longrightarrow & V_k' & \longrightarrow & V_k \\ \downarrow & & \downarrow & & \downarrow \\ \operatorname{Spec} k & \longrightarrow & V_k'/G & \longrightarrow & V_k/G \end{array}$$

commutes. Note that the left two columns are G-torsors and the top row is G-equivariant, so $\operatorname{Spec} L \to \operatorname{Spec} k$ is a pullback of $V'_k \to V'_k/G$ by Corollary 4.1.8; hence a pullback of $V \to V/G$ by the transitivity of fiber products. □

Next, we find such a surjective homomorphism based on the fact that any Galois G-algebra has only finitely many G-stable subalgebras.

Lemma 5.2.3. *Any Galois G-algebra L over k has only finitely many G-stable subalgebras over k.*

Proof. This is an immediate corollary of Proposition 2.2.16. □

Lemma 5.2.4. *If L is a Galois G-algebra over k, then there is a k-point in V'/G that realizes L.*

Proof. First, by Lemma 5.2.2, it suffices to show that there is a surjective G-equivariant k-algebra homomorphism

$$h\colon \mathcal{O}(V_k) \to L,$$

where G acts on the second component of $\mathcal{O}(V_k) = k \otimes_{k_0} \mathcal{O}(V)$.

Let V_k^* denote the dual space of V_k. Consider the canonical bijections

$$\operatorname{Hom}_{k\text{-alg}}(\mathcal{O}(V_k), L) \simeq \operatorname{Hom}_k(V_k^*, L) \simeq L \otimes_k V_k,$$

where the first bijection comes from the universal property of the symmetric algebra $\mathcal{O}(V_k) = \operatorname{Sym}(V_k^*)$, and the second bijection is indeed a k-vector space isomorphism.

Let G act on $L \otimes_k V_k$ diagonally and act on $\operatorname{Hom}_{k\text{-alg}}(\mathcal{O}(V_k), L)$ by $(g \cdot f)(p) = g(f(g^{-1}p))$ for any $g \in G$ and $f \in \operatorname{Hom}_{k\text{-alg}}(\mathcal{O}(V_k), L)$ so that the bijection $\operatorname{Hom}_{k\text{-alg}}(\mathcal{O}(V_k), L) \simeq L \otimes_k V_k$ is G-equivariant and $(\operatorname{Hom}_{k\text{-alg}}(\mathcal{O}(V_k), L))^G = \operatorname{Hom}_{G\text{-alg}}(\mathcal{O}(V_k), L)$.

Let H denote the k-vector space $(L \otimes_k V_k)^G$. Restricting to the G-invariants, we obtain bijections

$$j\colon H \overset{j_1}{\simeq} (\operatorname{Hom}_k(V_k^*, L))^G \overset{j_2}{\simeq} \operatorname{Hom}_{G\text{-alg}}(\mathcal{O}(V_k), L).$$

Note that j_1 is a k-vector space isomorphism and each $h \in H$ gives a G-algebra morphism $j(h)\colon \mathcal{O}(V_k) \to L$. We will have shown that there exists an $h \in H$ such that $j(h)$ is surjective, which would complete the proof.

Assume towards a contradiction that $j(h)$ is not surjective for all $h \in H$. Since G is finite, the number of G-stable sub-k-algebras of L is finite by Lemma 5.2.3. Denote by $L_1, \cdots, L_m$ the distinct proper G-stable subalgebras. Consider the subsets of H

$$H_i := \{h \in H\colon \operatorname{im}(j(h)) \subseteq L_i\}, \text{ for } i = 1, \cdots, m.$$

These subsets are indeed subspaces of H, for $H_i = \{h \in H\colon \operatorname{im}(j_1(h)) \subseteq L_i\}$. Because $H = \bigcup_{i=1}^{m} H_i$ by assumption and we cannot write a vector space as a finite union of proper subspaces over an infinite field k, there must be an i such that $H = H_i$. This implies the images of all $j(h)$ are contained in L_i and

$$(L \otimes_k V_k)^G = (L_i \otimes_k V_k)^G \tag{5.3}$$

Consider the canonical bijections

$$\begin{aligned} j_{k_s}\colon k_s \otimes_k H &= (k_s \otimes_k L \otimes_k V_k)^G \simeq ((L_{k_s}) \otimes_k V_k)^G \\ &\simeq \operatorname{Hom}_{G\text{-alg}\,/k}\left(\mathcal{O}(V_k), L_{k_s}\right) \simeq \operatorname{Hom}_{G\text{-alg}\,/k_s}\left(\mathcal{O}(V_{k_s}), L_{k_s}\right). \end{aligned}$$

But taking equation (5.3) into account, one obtains

$$j_{k_s}\colon k_s \otimes_k H \simeq \operatorname{Hom}_{G\text{-alg}\,/k_s}\left(\mathcal{O}(V_{k_s}), (L_i)_{k_s}\right)$$

via the same maps, so all G-algebra homomorphisms from $\mathcal{O}(V_{k_s})$ have images contained in $(L_i)_{k_s}$.

However, $L_i \otimes_k k_s \neq L \otimes_k k_s \simeq \prod_G k_s$ by dimension consideration, and there is indeed a G-algebra homomorphism from $\mathcal{O}(V_{k_s})$ to L_{k_s} that is surjective. For instance, if one picks an arbitrary k_s-point $x \in V_{k_s}$ with trivial G-stabilizer (such points are dense), then the closed immersion $Gx \to V_{k_s}$ induces such a surjection. This contradiction implies that there exists an $h \in H$ such that $j(h)$ is surjective G-algebra homomorphism from $\mathcal{O}(V_k)$ to L as we desire.

□

Lemma 5.2.5. *Let L be a Galois G-algebra over k. The k-points that realize L are dense in V'/G.*

Proof. Assuming without loss of generality that k_0 is infinite, we have demonstrated the existence of a k-point $y = \pi(x)$ in V'/G that realizes L. We assert that any $A \in \mathbf{GL}_N(k_0)$ also results in $\pi(Ax)$ realizing L. This is because the fiber of $\pi(Ax)$ is determined by the residue fields of Ax and $\pi(Ax)$, which are independent of the choice of A. As a result, the k-points that realize L are dense due to the density of the $\mathbf{GL}_N(k_0)$-orbit of x. □

Proof of Theorem 5.1.3. This follows immediately from the preceding lemmas. □

Example 5.2.6. Let $G = S_n$ act on the affine n-space $V = \operatorname{Spec} k[x_1, \cdots, x_n]$ by permuting the variables. Then V' contains closed points with distinct coordinates. By Lemma 3.2.4, V/G is given by the ring of symmetric polynomial in n variable. Then Vieta's formulas show that V'/G can be identified with polynomials of degree $\leq n$ with distinct roots. Theorem 5.1.3 shows that $V' \to V'/G$ is a versal torsor under S_n.

Bibliography

[1] M. F. Atiyah and I. G. MacDonald. *Introduction to commutative algebra*. Addison-Wesley, 1969.

[2] The Stacks Project Authors. Stacks project.

[3] Grégory Berhuy. *An Introduction to Galois Cohomology and its Applications*. London Mathematical Society Lecture Note Series. Cambridge University Press, 2010.

[4] Nicolas Bourbaki. *Algebra II*. Springer Berlin Heidelberg, 2003.

[5] Skip Garibaldi. *Cohomological Invariants in Galois Cohomology (University Lecture Series)*. American Mathematical Society, 2003.

[6] Alexander Grothendieck. Éléments de géométrie algébrique : IV. Étude locale des schémas et des morphismes de schémas, Seconde partie. *Publications Mathématiques de l'IHÉS*, 24:5–231, 1965.

[7] Alexander Grothendieck. Éléments de géométrie algébrique : IV. Étude locale des schémas et des morphismes de schémas, Quatrième partie. *Publications Mathématiques de l'IHÉS*, 32:5–361, 1967.

[8] Robin Hartshorne. *Algebraic geometry*. Graduate texts in mathematics: 52. Springer Science+Business Media, Inc., 2010.

[9] M.A. Knus, A. Merkurjev, M. Rost, and J.P. Tignol. *The Book of Involutions*. Number v. 44 in American Mathematical Society colloquium publications. American Mathematical Soc., 1998.

[10] Michiel Kosters. Algebras with only finitely many subalgebras. *Journal of Algebra and Its Applications*, 14(06):1550086, apr 2015.

[11] Tsit-Yuen Lam. *First Course in Noncommutative Rings*. Springer London, Limited, 2013.

[12] James S. Milne. *Étale Cohomology*. Princeton University Press, 1980.

[13] James S. Milne. *Algebraic Groups: The Theory of Group Schemes of Finite Type over a Field*. Cambridge University Press, sep 2017.

[14] Patrick Morandi. *Field and Galois Theory*. Springer eBook Collection. Springer New York, New York, NY, 1996.

[15] David Mumford. *Abelian Varieties*. Tata Institute of Fundamental Research. Studies in mathematics, 5. Published for the Tata Institute of Fundamental Research, Bombay by Oxford University Press, 1970.

[16] David Mumford, John Fogarty, and Frances Kirwan. *Geometric Invariant Theory (Ergebnisse der Mathematik und ihrer Grenzgebiete. 2. Folge)*. Springer, 2003.

[17] Jean-Pierre Serre. *Galois Cohomology*. Springer Berlin Heidelberg, 1997.

[18] Alexei Skorobogatov. *Torsors and Rational Points*. Cambridge University Press, 2010.

[19] Angelo Vistoli. Notes on Grothendieck topologies, fibered categories and descent theory, 2007.