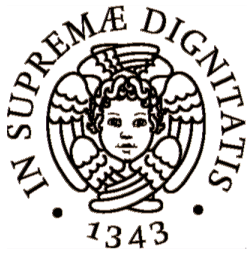


UNIVERSITÀ DI PISA

CORSO DI LAUREA MAGISTRALE IN MATEMATICA

THE ESSENTIAL DIMENSION OF FINITE GROUP SCHEMES

Relatore:
Prof. Angelo VISTOLI

Autore:
Denis NARDIN

Controrelatore:
Prof. Andrea MAFFEI

July 18, 2012

Mes poèmes ne méritent pas de survivre au papier sur lequel mon libraire les imprime à mes frais, quand par hasard j'ai les moyens de m'offrir comme un autre un frontispice et un faux titre.
Les lauriers d'Hippocrène ne sont pas pour moi ; je ne traverserai pas les siècles relié en veau. Mais quand je vois combien peu de gens lisent L'Iliade d'Homère, je prends plus gaiement mon parti d'être peu lu.
Marguerite Yourcenar - L'Oeuvre au Noir

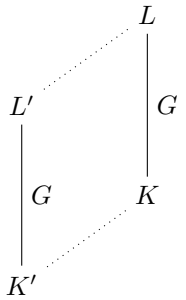
Contents

Introduction

This thesis treats the concept of essential dimension for an algebraic group, expecially for finite group schemes. Even though this concept addresses natural questions in Galois theory that go back at least from Klein it has been first introduced in [BR97] for finite groups and generalized later in [Rei00] to algebraic groups. Here we describe the basic problem behind the theory, in the hope that it will clarify the abstract development.

Let k be a fixed field from now on and fix a finite group G. We are interested in describing the Galois extensions of k with Galois group G.

Fix a Galois extension L/K with Galois group G. If K' is a subfield of K we will say that L/K is **defined over** K' if there is an extension L'/K' with Galois group G such that $L = L'K$.



A measure of the "complexity" of the extension L/K can be the minimum "size" of a subfield over which is defined. We will choose as "size" the trascendence degree over k and we will call such minimum **essential dimension** of the extension L/K:

$$\mathrm{ed}_k(L/K) = \min\{\mathrm{trdeg}_k K' \mid L/K \text{ is defined over } K'\}.$$

Moreover we can define the **essential dimension** of G as the supremum of the essential dimension for L/K varying among all Galois extensions of Galois group G.

This definition has as goal to answer a classical question: how many "parameters" are needed to describe a Galois extension of group G. For instance take $G = C_2$, the cyclic group of order 2. Then it is know from elementary Galois

theory that all extension of group C_2 are quadratic extensions. So $L = K(\sqrt{u})$ for some $u \in K$ and we can take $K' = k(u)$, $L' = k(\sqrt{u})$. Then L'/K' is still a Galois extension of order 2 and $L = KL'$. Moreover $\operatorname{trdeg}_k k(u) \leq 1$. Thus for every quadratic extensions L/K we have $\operatorname{ed}_k(L/K) \leq 1$. On the other hand it is easy to see that the extension $k(\sqrt{t})/k(t)$, where t is an indeterminate, cannot come from an algebraic extension. So we have

$$\operatorname{ed}_k(C_2) = 1\,.$$

This is essentially a way to formalize the fact that quadratic extensions "depend only on one parameter", namely the element of which we take the square root. With substantially the same reasoning one could show that if the base field k contains all the n-th roots of unity we have $\operatorname{ed}_k(C_n) = 1$ (and in fact every cyclic Galois extension can then be reduced to the prototipical $k(\sqrt[n]{t})/k(t)$ where t is a parameter).

Care should be given to the fact that, while the minimum trascendence degree is surely well defined, there may not exist in fact a minimal field of definition for L/K. In fact consider our previous example of $k(\sqrt{t})/k(t)$. Take as $K_n = k(t^{2n+1})$ and $L_n = k(t^{n+1/2})$. Then L/K is surely defined over K_n for each n but not on their intersection $\bigcap_n K_n = k$.

This thesis will not try to follow this direct approach, which proves itself inconvenient when trying to do computations of essential dimension that aren't trivial from the classical Galois theory. In fact a big part of it is devoted on the development of the main technical tools that we will need in order to study a more generalized notion of essential dimension, in which a Galois extension is replaced by a G-torsor, where G is an algebraic group over a field.

It is divided mainly in three chapters. In the first we develop the theory of Galois descent, a very special case of the faithfully flat descent, which allows to describe the relations between algebraic objects defined over a field and over its separable closure.

In the second chapter we will develop the elementary theory of algebraic groups (here meaning affine group schemes of finite type over a field) concentrating on the parts of interest for our aim: action of algebraic groups over varieties and representations.

In the third the definition of essential dimension for a functor is given. This is a strong generalization from the example above and it is due to A. Merkurjev, allowing to define essential dimension not only for Galois extensions but also for other kinds of objects like projective cubics and quadratic forms. In this chapter we will prove the main theorems relating essential dimension to a particular kind of torsors which arise often from faithful representations. In particular we will develop in detail the relations between essential dimension and versal torsors. We will also include an original result bounding the essential dimension of particular groups of multiplicative type, generalizing a result of Ledet in [Led02].

Notation and conventions

If F is a field we will denote its separable closure by F^s and its algebraic closure by F^a. With Γ_F we will usually indicate the absolute Galois group of F, that is the Galois group of F^s over F. The letter k will usually denote the ground field.

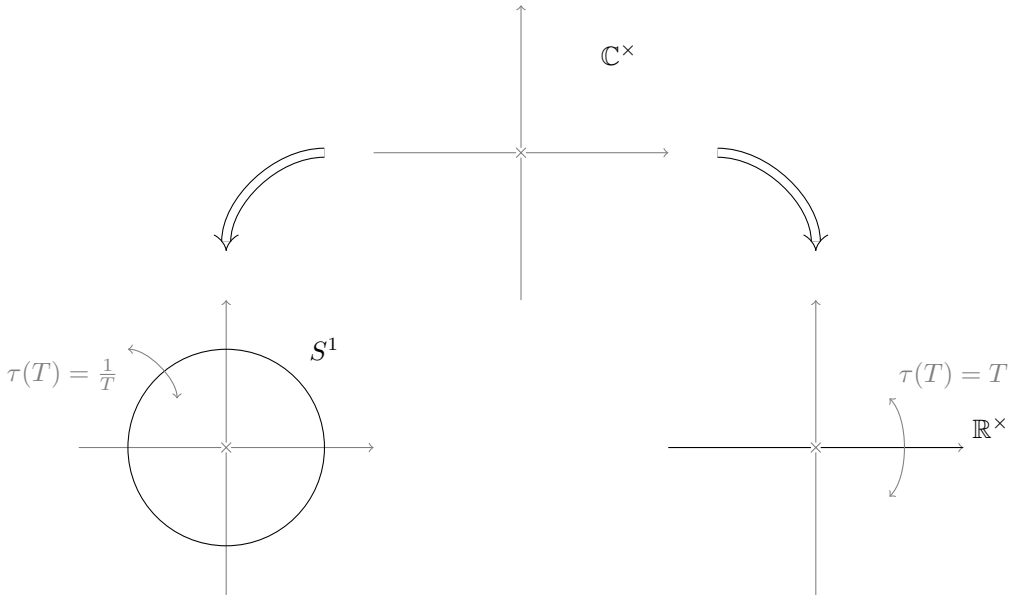
When talking of Galois extensions we will usually allow for infinite Galois extensions, when not explicitly excluded. The action of profinite groups is always intended as a continous action. In particular Galois cohomology for infinite extensions is, as usual, defined using continous cochains.

When G is some sort of group acting on an object X we will denote with X^G the fixed points of G.

With an algebraic group over a field k we will intend an affine group scheme of finite type over k.

Chapter 1

Descent and cohomology



The two twisted forms of $\mathbb{G}_{m,\mathbb{C}}$ with the action of the Galois group defining them.

Let $R \to S$ be an extension of rings. Descent theory is about the additional data required to push some kind of "structure" over S to a structure over R. Here we will be interested exclusively in descent along Galois extensions (finite or infinite). In this case the "descent data" will be an appropriate action of the Galois group on our structure.

For a general reference about Galois theory take [Lan02] chapter VI.

All the proofs here are semplification of a more general paradigm of fpqc descent. For more about fpqc descent see for instance [Vis07].

1.1 Descent of vector spaces

From now on let L/k be a fixed Galois extension with Galois group Γ. If V is a vector space over L a **semilinear** action of Γ is a continous action of Γ on V by group homomorphism such that

$$\gamma(\lambda v) = \gamma(\lambda)\gamma(v)$$

for each $\gamma \in \Gamma, \lambda \in L, v \in V$. Vector spaces over L with semilinear Γ-actions form a category with arrows Γ-equivariant linear maps.

If V is a vector space with a semilinear Galois action we will denote by $V^\Gamma := \{v \in V \mid \gamma v = v \ \forall \gamma \in \Gamma\}$ the set of fixed points of Γ. It is a k-subspace of V.

Now let W be a vector space over k. Then $W \otimes_k L$ is a vector space over L. Moreover it has a natural semilinear Γ-action given by

$$\gamma(w \otimes \lambda) = w \otimes \gamma(\lambda)\,.$$

Our task in this section is to prove that all semilinear actions arise in this way. In fact we will prove the following theorem

Theorem 1.1. *Let L/k be a Galois extension of Galois group Γ. There is an equivalence of categories between vector spaces over k and vector spaces over L with a semilinear action of Γ realized by the following functors:*

$$V \mapsto V^\Gamma,\ W \mapsto W \otimes_k L$$

The proof of the theorem passes through the following technical lemmas.

Lemma 1.2. *Let L/k be a finite Galois extension and let V be a vector space over L. Then the map $V \otimes_k L \to \bigoplus_{\gamma\in\Gamma} V \cdot e_\gamma$ (where the right hand side is simply the direct sum of a family of copies of V indexed by Γ and the e_γ are simply to remind the labeling of the addend) given by*

$$v \otimes \lambda \to \sum_{\gamma\in\Gamma} \gamma(\lambda) v \cdot e_\gamma$$

is an isomorphism of vector spaces over L. In particular we have $\sum_i v_i \otimes \lambda_i = \sum_j w_j \otimes \mu_j$ if and only if

$$\sum_i \gamma\lambda_i v_i = \sum_j \gamma\mu_j w_j$$

for each $\gamma \in \Gamma$.

Proof. First we note that if the thesis is true for a family $\{V_i\}_{i\in I}$ it is true for their direct sum. So it is sufficient to prove it in the case $V = L$. In that case by the primitive element theorem (see [Lan02], theorem V.4.6) we have that $L = k(u)$, that is $L = k[t]/(f(t))$. But, since the extension is Galois, we have that

$$f(t) = \prod_{\gamma\in\Gamma}(t - \gamma u)\,.$$

So, by Chinese remainder theorem,

$$L \otimes_k L = L \otimes_k k[t]/(f(t)) = L[t]/(f(t)) = L[t]/\prod_{\gamma\in\Gamma}(t-\gamma u) = \bigoplus_{\gamma\in\Gamma} L[t]/(t-\gamma u)\,.$$

And this is exactly the isomorphism described in the lemma. □

Lemma 1.3. *Let* $\sum_i v_i \otimes \lambda_i \in V \otimes_k L$. *Suppose that*

$$\sum_i \gamma(v_i) \otimes \lambda_i = \sum_i v_i \otimes \lambda_i$$

for each $\gamma \in \Gamma$. *Then* $\sum_i v_i \otimes \lambda_i \in V^\Gamma \otimes L$.

Proof. In fact V^Γ is the kernel of the map

$$V \to \bigoplus_{\gamma\in\Gamma} V \cdot e_\gamma \qquad\qquad v \mapsto \sum_{\gamma\in\Gamma}(v - \gamma v)\cdot e_\gamma\,.$$

So by the flatness of L over k we have that $V^\Gamma \otimes_k L$ is the kernel of the map

$$v \otimes \lambda \mapsto \sum_{\gamma\in\Gamma}(v - \gamma v)\otimes\lambda \cdot e_\gamma\,.$$

But this is exactly the thesis. □

The key step in the proof of the theorem is the following proposition.

Proposition 1.4 (Speiser)**.** *Let* L/k *a Galois extension of Galois group* Γ. *Let* V *a vector space over* L *with a semilinear action of* Γ. *Then the natural map*

$$V^\Gamma \otimes_k L \to V \qquad v \otimes \lambda \mapsto \lambda v$$

is an L*-linear isomorphism.*

Proof. First note that we may reduce to the case in which L/k is finite. In fact suppose that the thesis is true for every finite extension. Now take an element$\sum_i v_i \otimes \lambda_i$ in the kernel. But the λ_i are in a finite number, so they are contained in a finite Galois extension E/k. Let Γ' the Galois group of E/k and Γ'' the Galois group of L/E. But then $\sum_i v_i \otimes \lambda_i$ are in the kernel of the map

$$V^\Gamma \otimes_k E = (V^{\Gamma''})^{\Gamma'} \otimes_k E \to V^{\Gamma''}\,.$$

So by the result on the finite extension E/k we have that $\sum_i v_i \otimes \lambda_i = 0$. In a similar way if we take $v \in V$ its stabilizer is an open subgroup of Γ since the action is continous and so we can find a finite Galois extension E/k such that $v \in V^{\Gamma''}$ where Γ'' is the Galois group of L/E. But then v is in the image of the map $V^\Gamma \otimes_k E \to V^{\Gamma''}$.

Now we need to do the case of finite extensions. All we need to show is that the map is injective and surjective.

Injectivity
Suppose that $\sum_i v_i \otimes \lambda_i$ is an element in the kernel, that is such $\sum_i \lambda_i v_i = 0$. Then applying $\gamma \in \Gamma$ we have that

$$\sum_i \gamma(\lambda_i) v_i = 0$$

for each $\gamma \in \Gamma$. But then the image of $\sum_i v_i \otimes \lambda_i$ in $V \otimes_k L$ is 0 under the isomorphism of the lemma 1.2. So it is in the kernel of the map $V^\Gamma \otimes_k L \to V \otimes_k L$. But this map is injective since it is a change of basis of an injective map. That is

$$\sum_i v_i \otimes \lambda_i = 0$$

in $V^\Gamma \otimes_k L$.

Surjectivity
Take $v \in V$. Now because of the isomorphism of lemma 1.2 we may find $\sum_i v_i \otimes \lambda_i \in V \otimes_k L$ such that

$$\sum_i \gamma(\lambda_i) v_i = \gamma(v)$$

for each $\gamma \in \Gamma$. We want to show that $\sum_i v_i \otimes \lambda_i$ is in $V^\Gamma \otimes L$. In light of the criterion of lemma 1.3 we need to show that

$$\sum_i \gamma v_i \otimes \lambda_i = \sum_i v_i \otimes \lambda_i$$

for each $\gamma \in \Gamma$. But, using equality test in lemma 1.2 all we need to show is that

$$\sum_i (\delta\lambda_i)(\gamma v_i) = \sum_i (\delta\lambda_i) v_i$$

for each $\gamma, \delta \in \Gamma$. Now for the definition of v_i, λ_i the right end side is just δv, while collecting a γ on the left hand side we get that it is $\gamma\gamma^{-1}\delta v = \delta v$. So the thesis is proved. □

All we need to complete the proof of the theorem is to prove that the natural inclusion $W \to (W \otimes_k L)^\Gamma$ is an isomorphism. But now this is easy, in fact it is sufficient to check if it is an isomorphism after tensoring with L. But now this is

$$W \otimes_k L \to (W \otimes_k L)^\Gamma \otimes_k L = W \otimes_k L$$

thanks to the previous proposition.

It is really important that descent preserves tensor products, i.e. that if V, W are vector spaces over L with a semilinear Γ-action

$$(V \otimes_L W)^\Gamma = V^\Gamma \otimes_k W^\Gamma$$

wher $V \otimes_L W$ has the natural action given by $\gamma(v \otimes w) = \gamma v \otimes \gamma w$. To see this observe that a standard reasoning with the universal property of tensor product guarantees that

$$(V^\Gamma \otimes_k L) \otimes_L (W^\Gamma \otimes_k L) = (V^\Gamma \otimes_k W^\Gamma) \otimes_k L\,.$$

Taking $(-)^\Gamma$ of both sides and recalling the descent theorem 1.1 allows us to conclude.

Remark 1.5. *This is particularly important since most algebraic stucture of interest are determined by maps between tensor products. This allows us to extend our descent theorem to other algebraic categories. For instance below we work out explicitely the case of algebras.*[1] *Note that all equational requirements (like associativity) are preserved by descent.*

Theorem 1.6. *Let L/k a Galois extension of Galois group Γ. The functors $B \to B \otimes_k L$ and $A \to A^\Gamma$ determine an equivalence of categories between algebras over k and algebras over L with a semilinear Γ-action by algebra automorphism.*

Proof. If B is an algebra over k it is clear that $B \otimes_k L$ is an algebra over L and the natural action $\gamma(x \otimes \lambda) = x \otimes \gamma(\lambda)$ is through algebra automorphisms. Then all we need to prove is that if A is an algebra over L with a semilinear action by algebra automorphisms then A^Γ inherits a structure of algebra over k. But a structure of algebra over L on a vector space A is given by two maps

$$\mu : A \otimes_L A \to A \qquad \eta : L \to A$$

that corresponds to $\mu(a \otimes b) = ab$, $\eta(1) = 1$. The condition that Γ acts by algebra automorphisms consists exactly in requiring that these maps are Γ-equivariant. So they descend to maps

$$\mu^\Gamma : (A \otimes_L A)^\Gamma = A^\Gamma \otimes_k A^\Gamma \to A^\Gamma \qquad \eta^\Gamma : L^\Gamma = k \to A^\Gamma\,.$$

These maps satisfy all commutative diagrams required by the algebra axioms since μ and η satisfy them and descent is an equivalence of categories. Then thet give a natural algebra structure on A^Γ. Then descent theory guarantees that these two functors give an equivalence of categories. □

The same theorem, with essentially the same proof, holds in many other situations. In particular we will use it freely in the case of Hopf algebras.

[1] For algebra over k we intend a commutative algebra with unity over k, that is a commutative ring with unity A together with a ring homomorphism $k \to A$.

1.2 Galois cohomology

Now we are interested to classify all the forms over k that may come out from a given form over L. In some sense we already did it: these corresponds to the semilinear Γ-actions. However it may be given a more explicit classification. To do so we will need Galois cohomology. In the following we will give a minimal introduction, for a more comprehensive treatment see [Mil08] chapter II.

Let G a finite group. A G-module is a module over the ring $\mathbb{Z}[G]$, that is an abelian group M with a left action of G by group automorphisms. Then we can define the i-th cohomology group of G with coefficients in M as

$$H^i(G, M) := \mathrm{Ext}^i_{\mathbb{Z}}(\mathbb{Z}[G], M)$$

where $\mathbb{Z}$ has the trivial G-action. That is it is the i-th derived functor of $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) = M^G$. From general abstract nonsense we have that if

$$0 \to M' \to M \to M'' \to 0$$

is an exact sequence of G-modules, we have a long exact sequence

$$0 \to M'^G \to M^G \to M''^G \to H^1(G, M') \to \cdots$$

$$\cdots \to H^i(G, M') \to H^i(G, M) \to H^i(G, M'') \to H^{i+1}(G, M') \to \cdots .$$

We can give a more explicit formula for the cohomology groups by using a particular projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module.

Consider

$$\cdots \xrightarrow{\delta_n} \mathbb{Z}[G^n] \xrightarrow{\delta_{n-1}} \cdots \xrightarrow{\delta_0} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

where δ_n is defined over the basis elements as

$$\begin{aligned}\delta_n(g_0, \ldots, g_n) =& g_0(g_1, \ldots, g_n) - \sum_{j=0}^{n-1} (-1)^j (g_0, \ldots, g_j g_{j+1}, \ldots, g_n) \\ &+ (-1)^n (g_0, \ldots, g_{n-1})\end{aligned}$$

and where $\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$ is the canonical augmentation map (i.e. $\varepsilon(g) = 1$ for each $g \in G$).

It is a routine check to see that this is an exact sequence and that in fact

$$\mathbb{Z}[G^n] = \mathbb{Z}[G]^{\oplus n}$$

as a $\mathbb{Z}[G]$-module. So it is a projective resolution and we can write

$$H^i(G, M) = H^i(\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^\bullet], M)) .$$

We are in fact interested in the $H^1(G, M)$. Observe that

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], M) = M$$

as a $\mathbb{Z}[G]$-module, with the map $f \mapsto f(1)$. In the same way

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^2], M) = \mathrm{Hom}_{(\mathrm{Set})}(G, M)$$

with the map $f \mapsto f(\cdot, 1)$. Under this identification it is trivial to observe that the 1-cocycles are

$$\{f : G \to M \mid f(gh) = f(g) + gf(h)\ \forall g, h \in G\}$$

and that the 1-coboundaries are the maps $g \mapsto gm - m$ for some $m \in M$.

Define a G-group as a group H with an action of G by group automorphism. In analogy with what we have seen we can define the first cohomology group[2] with coefficients in H as the set of cocycles

$$Z(G, H) = \{f : G \to H \mid f(gh) = f(g)gf(h)\ \forall g, h \in G\}$$

modulo the following equivalence relation:

$$f \sim f' \Leftrightarrow \exists x \in H\ f(g) = x^{-1} f'(g) gx\ \forall g \in G\,.$$

In general $H^1(G, H)$ has not the structure of a group but just the structure of a pointed set (pointed by the class of the constant map $f(g) = e$). However if

$$1 \to H' \to H \to H'' \to 1$$

is an exact sequence of G-groups there is always a short exact sequence of pointed sets

$$1 \to H'^G \to H^G \to H''^G \to H^1(G, H') \to H^1(G, H) \to H^1(G, H'')\,.$$

1.3 Twisted forms of algebraic structures

Let V be a vector space over a field k. An **algebraic structure** on V is a family of linear homomorphisms $\{\Phi_i : V^{\otimes k_i} \to V^{\otimes h_i}\}_{i \in I}$. The **type** of the algebraic structure is the triple $(I, \{k_i\}_{i \in I}, \{h_i\}_{i \in I})$. Fixed a type there is an obvious category of algebraic structure of the given type, where an arrow $(V, \{\Phi_i\}) \to (W, \{\Psi_i\})$ is a linear map $f : V \to W$ such that for each $i \in I$ $f^{\otimes h_i} \Phi_i = \Psi_i f^{\otimes k_i}$.

As in remark 1.5 if L/k is a Galois extension of Galois group Γ to give an algebraic structure over k is the same thing to give an algebraic structure over L with a semilinear Γ-action that commutes with all maps Φ_i. If $(V, \{\Phi_i\})$ is an algebraic structure we will denote with $(V_L, \{(\Phi_i)_L\})$ the structure obtained by tensoring with L.

Let V be an algebraic structure over k and fix a Galois extension L/k of Galois group Γ. Another algebraic structure W over k is said to be a **twisted form** of V split over L if $V_L \cong W_L$ as algebraic structures over L (that is discarding the Γ-action). The main result of this section is that twisted forms may be classified by an opportune cohomology group.

[2] In general it is not possible to define the higher cohomology group if the coefficient group is not abelian

Theorem 1.7. *Let $(V, \{\Phi_i\})$ be an algebraic structure. Fix a Galois and let $\underline{\mathrm{Aut}}(V_L)$ be the automorphism group of V_L. This has a natural Γ action by conjugation. Then the isomorphism classes of twisted forms of $(V, \{\Phi_i\}_{i\in I})$ split by L are in a natural bijection with*

$$H^1(\Gamma, \underline{\mathrm{Aut}}(V_L)) .$$

Proof. Let $(W, \{\Psi_i\}_{i\in I})$ be a twisted form of $(V, \{\Phi_i\}_{i\in I})$ split over L. This means that there is an isomorphism $f : V \otimes L \cong W \otimes L$ such that

$$f^{\otimes h_i}(\Phi_i)_L = (\Psi_i)_L f^{\otimes k_i}$$

for each $i \in I$. Then we can define $\hat{f} : \Gamma \to \underline{\mathrm{Aut}}(V_L)$ as

$$\hat{f}(\gamma) = f^{-1}\gamma f \gamma^{-1} .$$

With a trivial computation it can be verified that $\hat{f}$ is a cocycle and that the cohomology class of $\hat{f}$ does not depend on the choice of f. So we have a well defined map from the set of isomorphism classes of twisted forms of V and $H^1(\Gamma, \underline{\mathrm{Aut}}(V_L))$.

To prove injectivity take two twisted forms W_1, W_2 and choose isomorphisms f_1, f_2. Suppose that

$$[\hat{f}_1] = [\hat{f}_2]$$

Then we have that there exists $g \in \underline{\mathrm{Aut}}(V_L)$ such that

$$\hat{f}_1(\gamma) = g^{-1}\hat{f}_2(\gamma)\gamma g \gamma^{-1} \Rightarrow f_1^{-1}\gamma f_1 \gamma^{-1} = g^{-1} f_2^{-1}\gamma f_2 \gamma^{-1}\gamma g \gamma^{-1} .$$

Rearranging terms this means that

$$f_2 g f_1^{-1}\gamma = \gamma f_2 g f_1^{-1} .$$

So $f_2 g f_1^{-1}$ is a Γ-invariant isomorphism between $W_1 \otimes L$ and $W_2 \otimes L$. So it descends to an isomorphism between W_1 and W_2.

Now we will prove surjectivity. Let $\phi : \Gamma \to \underline{\mathrm{Aut}}(V_L)$ be a cocycle and define a twisted action of Γ on V_L by

$$\gamma * v = \phi(\gamma)\gamma(v)$$

Observe that this new action commutes with $(\Phi_i)_L$ for each i (since ϕ has values in $\underline{\mathrm{Aut}}(V_L)$). So if we take W as the fixed space of this new action Φ_L descends to an algebraic structure Ψ on W of the same type as Φ. It is clear that this is a twisted form of V. Moreover, by lemma 1.1 $V_L = W_L$, and if we take as isomorphism the identity we have that

$$\hat{1}(\gamma) = 1^{-1}\gamma * 1\gamma^{-1} = \phi(\gamma)\gamma\gamma^{-1} = \varphi(\gamma) .$$

So the map is surjective too and the proof is completed. □

Corollary 1.8 (Hilbert's theorem 90)**.** *Let L be a field. Then*

$$H^1(L, GL_n) = 0\,.$$

Proof. In fact we have seen that it classify the twisted forms of n-dimensional vector spaces. But there are only one isomorphism type of n-dimensional vector spaces over L, from which the thesis. □

1.4 An easy example

Consider the following algebraic structure over $\mathbb{R}$. As a vector space take $A = \mathbb{R}[x^{\pm 1}]$, equipped with the following maps:

$$\begin{aligned} \mu : A \otimes_{\mathbb{R}} A \to A \qquad & x^i \otimes x^j \mapsto x^{i+j} \\ \eta : \mathbb{R} \to A \qquad & \lambda \mapsto \lambda \\ \Delta : A \to A \otimes_{\mathbb{R}} A \qquad & x^i \mapsto x^i \otimes x^i \\ \varepsilon : A \to \mathbb{R} \qquad & x^i \mapsto 1 \\ S : A \to A \qquad & x^i \mapsto x^{-i} \end{aligned}$$

This is, as we will see, the Hopf algebra associated to the group scheme $\mathbb{G}_m$. Our goal is to classify all twisted forms split over $\mathbb{C}$. First we need to compute $\underline{\mathrm{Aut}}(A_{\mathbb{C}})$. It is clear that an automorphism $f : A_{\mathbb{C}} \to A_{\mathbb{C}}$ is determined by the image of x. Now we impose that $f^{\otimes 2}\Delta = \Delta f$, that is

$$f(x) \otimes f(x) = \Delta f(x)\,.$$

Now if we write $f(x) = \sum_{n\in\mathbb{Z}} f_n x^n$ with almost every $f_n = 0$ the previous equation becomes

$$\sum_{n,m\in\mathbb{Z}} f_n f_m x^n \otimes x^m = \sum_{k\in\mathbb{Z}} f_k x^k \otimes x^k\,.$$

It is clear that the only possibility is $f(x) = x^n$ for $n \in \mathbb{Z}$. Among these, the only invertible are the identity and the map determined by $\tau(x) = x^{-1}$. A simple check assures us that these are in fact both automorphism of the algebraic structure. On the other hand the Galois group Γ of $\mathbb{C}/\mathbb{R}$ is cyclic of order two, generated by the conjuge that we will indicate with σ. Now note that σ and τ commutes so the action of Γ on $\underline{\mathrm{Aut}}(A_L)$ is trivial. So the twisted forms split over $\mathbb{C}$ are classified by

$$H^1(\Gamma, \underline{(Aut)}(A_L)) = \mathrm{Hom}(\Gamma, \underline{\mathrm{Aut}}(A_L))\,.$$

This is a set of two elements. One is trivial and corresponds to A. The other is the one that sends σ in τ. So B is composed by the polyonmials $p = \sum_{n\in\mathbb{Z}} p_n x^n \in \mathbb{C}[x^{\pm 1}]$ such that

$$\sum_{n\in\mathbb{Z}} p_n x^n = \sum_{n\in\mathbb{Z}} \bar{p}_n x^{-n}\,.$$

It is a simple check that these polynomials are exactly polinomials in

$$u = \frac{1}{2}(x + x^{-1}), \qquad v = \frac{i}{2}(x - x^{-1})$$

And that the ring B is isomorphic to the ring

$$\mathbb{R}[u, v]/(u^2 + v^2 - 1)$$

the other maps are given by

$$\Delta(u) = u \otimes u - v \otimes v, \qquad \Delta(v) = u \otimes v + v \otimes u$$

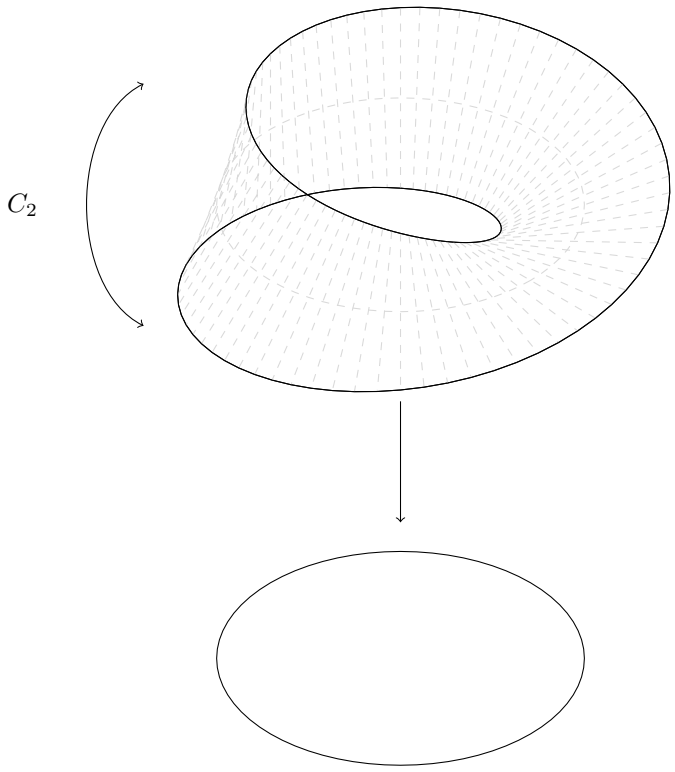
$$\varepsilon(u) = 1,\ \varepsilon(v) = 0$$

$$S(u) = u,\ S(v) = -v$$

We will see that this is the Hopf algebra corresponding to the algebraic group over $\mathbb{R}$ given by S^1.

Chapter 2

Algebraic groups



A C_2-torsor over S^1.

In this chapter we will develop a little bit of the theory of algebraic groups over a field. We will concentrate on the properties of actions of algebraic groups on varieties. Most of the material here presented come from the standard references [Wat79] and [DG70].

2.1 Group schemes

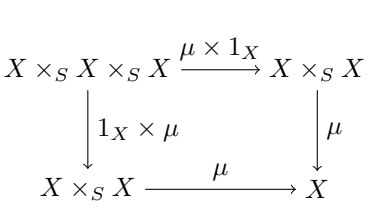
Fix a base scheme S. A group scheme over S is a group object in the category of schemes over S. That is a scheme X over S with a lifting of its functor of points to the category of groups. This is equivalent to the existence of three maps

$$\mu : X \times_S X \to X$$

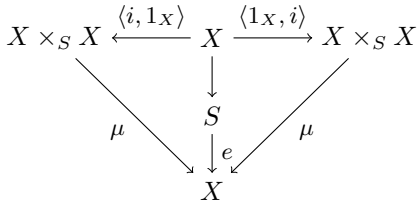
$$i : X \to X$$

$$e : S \to X$$

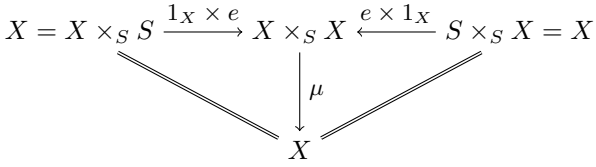
for which the following diagrams commute



Associativity



Inverses



Identity element

The group scheme is said to be **abelian** if the functor of points has values on the subcategory of abelian groups. This is equivalent to ask that $\mu\sigma = \mu$ where $\sigma : X \times_S X \to X \times_S X$ is the natural map that exchanges the two factors.

Note that the structure of group scheme is preserved by base change. That is if $T \to S$ is a scheme morphism and G is group scheme over S then $G \times_S T$ has a natural structure of group scheme over T. This is because for every T-scheme U we have

$$(G \times_S T)(U) = G(U)$$

when seen as a S-scheme. So if G has a natural lifting to the category of groups, so has $G \times_S T$.

Remark 2.1. *The structure of group scheme is completely determined by the multiplication map μ. In fact a map $\mu : X \times_S X \to X$ lifts the functor of points of X to a functor from S-schemes to magmas. But such a functor has at most one only lifting to the category of groups (essentially because if the magma structure on a set determines a group it does so uniquely). So by Yoneda's lemma the multiplication map determines the inverse and neutral element, provided they exist.*

Example 2.2. *For every abstract group G we can define the corresponding group scheme taking as a base scheme*

$$\coprod_{g \in G} S$$

and defininining the group operation as the map

$$\mu : \coprod_{g \in G} S \times_S \coprod_{h \in G} S = \coprod_{(g,h) \in G^2} S \times_S S \to \coprod_{k \in G} S$$

where μ sends to $S \times_S S$ corresponding to the pair (g, h) to S corresponding to gh with the obvious isomorphism.

Remark 2.3. *The functor that sends every abstract group G to the corresponding constant group scheme over S is the right adjoint of the "forgetful" functor that sends every group scheme over S to the group of its S-points. In fact a group homomorphism $G \to H$ with G constant is the same thing that choosing an S point $f(g)$ for every $g \in G$ such that the multiplication map sends $(f(g), f(h))$ in $f(gh)$.*

Example 2.4. *An elliptic curve over a field k (i.e. a complete curve of genus 1 over k with a distinguished point) is in a natural way a group scheme in which the distinguished point is the identity. More generally every abelian variety is a group scheme.*

Now let k be a field. An **algebraic group** over k is a affine of finite type group scheme over k. As usual for affine schemes we will use interchangeably their functor of points and the restriction to the category of affine schemes. To the study of algebraic groups it is very important to note that affine group schemes over a field have an interpretation as an Hopf algebra over k.

An **Hopf algebra** A over a field k is an algebra with three additional maps of algebras $\Delta : A \otimes_k A \to A$, $\varepsilon : A \to k$, $S : A \to A$ which satisfy the dual axioms respect to the those highlighted above:

$$(\Delta \otimes 1_A)\Delta = (1_A \otimes \Delta)\Delta$$

$$(1_A \otimes \varepsilon)\Delta = (\varepsilon \otimes 1_A)\Delta = 1_A$$

$$\langle S, 1_A \rangle \Delta = \varepsilon = \langle 1_A, S \rangle \Delta$$

It is clear from dualizing the definitions that a structure of Hopf algebra on a commutative algebra A is the same thing as a structure of group scheme on $\operatorname{Spec} A$.

Example 2.5. *If G is an abstract commutative group the group algebra $k[G]$ has a natural structure of Hopf algebra with comultiplication given by $\Delta g = g \otimes g$ for each $g \in G$.*

Example 2.6. *The affine line $\mathbb{A}^1$ has a natural structure of group scheme, with multiplication $k[T] \to k[T] \otimes_k k[T]$ given by $T \mapsto T \otimes 1 + 1 \otimes T$. This corresponds to the additive group in the sense that the functor of points evaluated at every k-algebra S is exactly the additive group of S. It will be denoted by $\mathbb{G}_a$.*

Example 2.7. *Let V be a finite dimensional vector space. Then the functor*

$$GL_V(S) = GL_S(V \otimes_k S)$$

that associates to every k-algebra S the group of S-linear automorphisms of $V \otimes_k S$ is representable by a scheme, and so is a group scheme. In fact suppose that $e_1, \ldots, e_n$ is a basis of V. Then every $f \in GL(V \otimes_k S)$ is determined by

$$f(e_i) = \sum_{i=1}^{n} \lambda_{ij} e_j \, .$$

So giving a S-linear automorphism is the same thing to give a matrix $(\lambda_{ij})_{i,j}$ with determinant in $S^\times$. So GL_V is represented by the localization of $k[a_{ij}]$ at $\det(a_{ij})$. We will denote GL_{k^n} with GL_n.

In particular $\mathbb{G}_m = GL_1$ is a group scheme.

Example 2.8. *If G is a finite commutative group, its associated constant group scheme (which we will denote with G as well) is affine and may be checked easily from the definition that its Hopf algebra is $k^{\oplus G}$ with comultiplication*

$$\Delta : k^{\oplus G} \to k^{\oplus G} \otimes_k k^{\oplus G} = k^{\oplus G^2} \qquad (\lambda_g)_{g \in G} \mapsto (\lambda_{gh})_{(g,h) \in G^2} \, .$$

The category of finite étale group schemes over a field has a particularly simple description.

Theorem 2.9. *Let k be a field. Taking the group of k^s points gives an equivalence of categories between finite étale group schemes over k and finite abstract groups with a continous action of Γ_k (the absolute Galois group of k).*

Proof. We need to describe a functor from finite groups with an action of Γ_k to finite étale group schemes. Let G be a such group and consider the constant group scheme over k^s corresponding to G. This is the spectrum of an Hopf algebra A over k^s. But the action of Γ_k on G yields an action of Γ_k on A that preserves the Hopf algebra structure. Then taking the fixed points A^{Γ_k} gives an Hopf algebra over k. The corresponding group scheme is étale since constant group schemes are étale and étaleness may be checked on the algebraic closure. The descent theorem 1.1 ensures us that the two operation are inverse to each other. □

A homomorphism of group schemes is an homomorphism of schemes over S such that respect the group structure. This may be taken both as to satisfy the obvious commutative diagrams or, somewhat more simply, to come from a natural transformation between the functors of points that has group homomorphisms as components.

A closed subgroup of a group scheme G is a closed subscheme H of G such that $\mu|_{H\times_k H}$, $\iota|_H$, e factor through H. Alternatively it is a closed subscheme such that $H(R) \subseteq G(R)$ is a subgroup for every k-algebra R. If $f : G \to H$ is an homomorphism of group schemes it is well defined the **kernel** of f as the pullback $G \times_H \operatorname{Spec} k$ of the neutral element $e \in H(k)$. It is clearly a closed subgroup (it is a closed subscheme since it is the base change of the closed subscheme e and its functor of points is trivially a subgroup for each R).

2.2 Representations of group schemes

Let G be a group scheme over a field k. By a **representation** of G we mean a group scheme homomorphism from G to GL_V for some vector space V over k. This amounts to the same thing as giving for all k-algebras R a R-linear action of the group $G(R)$ to $V \otimes_k R$ satisfying the obvious compatibility relations.

In the case we are most interested, that of affine group schemes over k, there is an Hopf-algebraic interpretation. Let A be an Hopf algebra over k and V a k-vector space. Then a **A-comodule** structure on V is the datum of a morphism $\rho : V \to A \otimes_k V$ such that the following diagrams commute

$$\begin{array}{ccc} V & \xrightarrow{\rho} & A \otimes_k V \\ {\scriptstyle\rho}\downarrow & & \downarrow{\scriptstyle 1\otimes\rho} \\ A \otimes_k V & \xrightarrow{\Delta\otimes 1} & A \otimes_k A \otimes_k V \end{array} \qquad \begin{array}{ccc} V & \xrightarrow{\rho} & A \otimes_k V \\ \| & \swarrow_{\varepsilon\otimes 1} & \\ k \otimes_k V & & \end{array}$$

Example 2.10. *k^n has a natural structure of $\mathcal{O}(GL_n) = k[a_{ij}, (\det A)^{-1}]$-comodule. In fact when $e_1, \dots, e_n$ is the canonical basis we can describe the comultiplication as*

$$e_i \mapsto \sum_{j=1}^{n} a_{ij} \otimes e_j \,.$$

In the same way if V is a vector space over k we can give V a natural structure of $\mathcal{O}(GL_V)$-comodule.

If $A \to B$ is an Hopf algebra homomorphism we can give every A-comodule V the structure of B comodule, by composing $V \to A \otimes_k V \to B \otimes_k V$. So every representation of rank n of an affine group scheme G gives to k^n the structure of $\mathcal{O}(G)$-comodule.

Proposition 2.11. *The functor that sends every G-representation to the corresponding $\mathcal{O}(G)$-comodule is an equivalence of categories.*

Proof. It is clear that it is fully faithful (i.e. a linear map $f : V \to W$ is G-equivariant if and only if it respects the comodule structure. All we need to prove is that it is essentially surjective. Take a $\mathcal{O}(G)$-comodule V. We want to construct a map of functors $G \to GL_V$. In fact take S a k-algebra and $g \in G(S)$. This is the same thing of a ring homomorphism $\mathcal{O}(G) \to S$. Then we may construct $\rho_f \in GL_V(S) = GL(V \otimes_k S)$ as the map

$$V \otimes_k S \xrightarrow{\rho \otimes 1} \mathcal{O}(G) \otimes_k V \otimes_k S \xrightarrow{g \otimes 1 \otimes 1} S \otimes_k V \otimes_k S \to V \otimes_k S$$

where the last arrow is the map $\lambda \otimes v \otimes \mu \mapsto v \otimes (\lambda\mu)$. It is easy to check that $\rho_{f^{-1}} = \rho_f^{-1}$ and thus $f \in GL_V(S)$. □

If V is an A-comodule a **subcomodule** of V is a vector subspace $W \subseteq V$ such that the map $W \to A \otimes_k V$ factors through $A \otimes_k W$. Subcomodules for $\mathcal{O}(G)$ correspond to subrepresentations of G.

Theorem 2.12. *Let V be a representation of an affine group scheme G over k. Then for every finite subset $\{v_1, \ldots, v_n\} \subseteq V$ there is a finite-dimensional subrepresentation $W \subseteq V$ such that $v_i \in W$ for all i.*

Proof. Let $\{a_i\}_{i \in I}$ be a basis of $\mathcal{O}(G)$ and let $\rho : V \to \mathcal{O}(G) \otimes_k V$ be the comodule map. Then we may write

$$\rho(v_i) = \sum_j a_i \otimes v_{ij} \,.$$

With all but a finite number of v_{ij} equal to 0. If we put

$$\Delta(a_i) = \sum_{i,j,k} r_{ijk} a_j \otimes a_k$$

then by $(1 \otimes \rho)\rho = (\Delta \otimes 1)\rho$ we get

$$\sum_i a_i \otimes \rho(v_{ij}) = \sum_{i,l,k} r_{ilk} a_l \otimes a_k \otimes v_{ij} \,.$$

Then, comparing the coefficients of a_l we get that

$$\rho(v_{lj}) = \sum_{ik} r_{ilk} a_k \otimes v_{ij} \,.$$

So the subspace of V spanned by the v_i and the v_{ij} is a finite-dimensional subcomodule containing v. □

We can rephrase the previous theorem saying that every G-representation is the direct limit of its finite-dimensional subrepresentations.

2.3 Properties of algebraic groups over a field

In this section we will investigate some more geometric properties of algebraic groups. Our main result will be the theorem of Cartier, that algebraic groups over a field of characteristic 0 are reduced.

Theorem 2.13 (Cartier)**.** *Every Hopf algebra of finite type over a field k of characteristic 0 is reduced.*

Proof. Since A is noetherian the space I/I^2 is a finite vector space over k. Let $x_1, \dots, x_n$ be one basis over k. Consider the k-linear map $p_i : A \to k$ sending 1 and I^2 to 0 and x_j to δ_{ij} and define the maps $d_i : A \to A$ as

$$d_i = (1 \otimes p_i)\Delta$$

that is $d_i(a) = \sum_j p_i(b_j)a_j$ if $\Delta a = \sum_j a_j \otimes b_j$. Then these are derivations such that $\varepsilon d_i(x_j) = \delta_{ij}$. In fact if $x_j = \sum_l a_l \otimes b_l$

$$\varepsilon d_i(x_j) = \sum_l p_i(b_l)\varepsilon(a_l) = p_i\left(\sum_l \varepsilon(a_l)b_l\right) = p_i(x_j) = \delta_{ij}\,.$$

We claim that monomials of degree n in the x_i are a basis for I^n/I^{n+1}. In fact they clearly generate and all we need is to show that they are linearly indipendent. But if $(r_1, \dots, r_l)$ is a multiindex of total degree n we have that

$$\varepsilon d_1^{r_1} \cdots d_n^{r_n}$$

sends $x_1^{r_1} \cdots x_n^{r_n}$ to $r_1! \cdots r_n! \neq 0$ and the other monomials of degree n to 0. So by a standard reasoning they are linearly indipendent.

Now suppose that $y \in A$ is nilpotent. We want to show that $y \in \bigcap_{n\geq 0} I^n$. If this is true then $y = 0$ by Krull intersection theorem. So suppose that $y \in I^m$ but $y \notin I^{m+1}$. Then we may write $y = y_0 + y_1$ where y_0 is a nonzero homogeneous polynomial of degree m in the x_i and $y_1 \in I^{m+1}$. But then if $y^e = 0$ we have that $y_1^e \in I^{(m+1)e}$. But this is absurd because y_1^e is a nonzero homogeneous polynomial in the x_i of degree me. □

Remark 2.14. *If the field k is of characteristic $p > 0$ there are in fact nonreduced algebraic groups. For instance $\mu_p = \operatorname{Spec} k[x]/(x^p - 1)$, the group scheme of p-th roots of unit is not reduced, as $(x-1)^p = x^p - 1 = 0$.*

Theorem 2.15. *Let G be a group scheme of finite type over a field k and let $e \in G(k)$ be its neutral element. Suppose that $\mathcal{O}_{G,e} \otimes_k \bar{k}$ is reduced. Then G is smooth over k.*

Proof. Since smoothness is invariant by base extension we may suppose that k be algebraically closed. Since reducedness may be checked on closed points to check if G is reduced all we need is to check if $\mathcal{O}_{G,g}$ is reduced for all $g \in G(k)$. But $\mu_g = \mu(g, -)$ is a scheme automorphism of G which brings e to g, so $\mathcal{O}_{G,g}$ is reduced if and only if $\mathcal{O}_{G,e}$ is. Thus G is reduced. By the generic smoothness theorem then it is smooth on a dense open set U. But then the set $\{\mu_g(U)\}_{g\in G(k)}$ is a covering of G by smooth opens. Thus G is smooth. □

2.4 Action of group schemes and quotients

Let G a group scheme over S and X an S-scheme. Then a **right action** of G on X is a scheme morphism $X \times_S G \to X$ such that, for every S-scheme T, the map

$$X(T) \times G(T) \to X(T)$$

is a right action. We can define similarly left actions. When we will talk about an action, without specifying whether left or right, we will always mean a right action. If G is an affine algebraic group over a field k and X is an affine scheme over a field the action axioms amounts to asking that the map

$$\mathcal{O}(X) \to \mathcal{O}(X) \otimes_k \mathcal{O}(G)$$

is a ring homomorphism giving a comodule structure to $\mathcal{O}(X)$.

If G is a group scheme over S acting on X with the map $\rho : X \times_S G \to X$ we will call the **isotropy group** the group scheme G_X over X that makes the following square cartesian

$$\begin{array}{ccc} G_X & \longrightarrow & X \times_S G \\ \downarrow & & \downarrow{\scriptstyle pr_1 \times \rho} \\ X & \xrightarrow{\Delta_{X/S}} & X \times_S X \end{array}$$

The important property is that for every point $x \in X(T)$ the fiber x^*G_X is exactly the group scheme stabilizer of x, that is

$$(x^*G_X)(T') = \{g \in G(T') \mid xg = x\}$$

for every T-scheme T'. We will denote the stabilizer x^*G as G_x. It is a group scheme over T. An action is said to be **free** if the isotropy group scheme is trivial, i.e. for every S-scheme T the action of $G(T)$ on $X(T)$ is free. The following is an useful criterion for freeness.

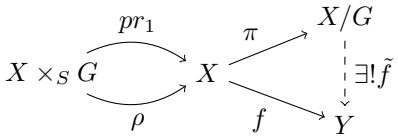
Proposition 2.16. *Let G an algebraic group over a field k and X a scheme of finite type over k with a G-action.*

- *If the characteristic of k is 0 the action is free if and only if the action of $G(k^a)$ on $X(k^a)$ is free.*
- *If the characteristic of k is positive the action is free if and only if the action of $G(k^a)$ on $X(k^a)$ is free and for every closed point $x \in X$ the Lie algebra of G_x is trivial.*

Proof. See [DG70], corollaries III.2.5 and III.2.8. □

If G is a group scheme over S acting on X we want to define the **quotient** X/G. This is an S-scheme with a map $\pi : X \to X/G$ which is the coequalizer of

the two maps $X \times_S G \to X$ given by the first projection and the action. That is for every S-scheme Y with a map $f : X \to Y$ such that $fpr_1 = f\rho$ there is exactly one map $\tilde{f} : X/G \to Y$ such that $f = \tilde{f}\pi$.



The problem of the existence of quotients in general is difficult. It is often necessary to enlarge the category of geometric objects[1] used in order to get a meaningful quotient. Moreover the categorical quotient in general is not at all well-behaved (for instance to be a quotient map is not a property local on the base). For our applications it will be enough to use the existence of a **generic quotient**, that is a quotient map $U \to U/G$ where U is a dense G-stable open subscheme of X such that it is also a G-torsor (see section 2.6). From the fact that this notion is indeed local on the base it is clear that there exists a maximal G-stable open subscheme U for which such a quotient map exists. The problem is in fact to find conditions for which that open is dense.

Theorem 2.17. *Let G and algebraic group over k and X be a scheme of finite type over k. Suppose that G acts freely on the right on X and that the projection map*

$$X \times_k G \to X$$

is flat and of finite type. Then there exists a maximal dense open G-invariant subscheme $U \subseteq X$ and a quotient map $\pi : U \to U/G$ such that π is a G-torsor (and in particular is onto, open and of finite type).

Proof. See [SGA3], Exposé V théorème 8.1. □

In a particular case we will be able to show that the generic quotient is in fact a quotient

Theorem 2.18. *Let G be an affine algebraic group over k and let H be a closed subgroup acting by right multiplication. Then there exists a scheme G/H and a quotient map $G \to G/H$.*

Proof. All we need to prove is that the maximal open U of the previous theorem is all G. But the left multiplication by elements of G are transitive H-equivariant morphism and so the maximal open set must be stable by it. But the only nonempty open subset of G invariant by left multiplication is G. □

Remark 2.19. *If H is a normal subgroup G/H has a natural structure of group scheme. It is true that it is an algebraic group over k but to prove this we would need to use a completely different construction of the quotient. For a reference, see [Wat79], chapter 16.*

[1] E.g. to algebraic spaces or stacks

2.5 Groups of multiplicative type

Let G be an affine group scheme over k. An element b of its Hopf algebra $\mathcal{O}(G)$ is said to be **group-like** if $\Delta b = b \otimes b$. This terminology is justified by the fact that if Γ is a commutative group the elements of Γ are group-like for the natural Hopf algebra structure on $k[\Gamma]$. Note that if g_1, g_2 are group-like elements so is $g_1 g_2$ and $S(g_1) = g_1^{-1}$. In fact

$$g_1 = (\varepsilon \otimes 1)\Delta g_1 = \varepsilon(g_1) g_1$$

that is $\varepsilon(g_1) = 1$. Moreover

$$1 = \mu(1 \otimes S)\Delta g = g S(g)\,.$$

So the group-like elements of A are a subgroup of the group of units $A^\times$. This is called the **character group** of G. It corresponds to the group of group schemes homomorphism $G \to \mathbb{G}_m$.

An abelian group scheme G is said to be **diagonalizable** if the group-like elements spans the group algebra over k. We will see that this is equivalent to being a subgroup of some $\mathbb{G}_m^r$.

Lemma 2.20. *Every subgroup of a diagonalizable algebraic group over k is diagonalizable.*

Proof. In fact if $A \to A/I$ is the corresponding Hopf algebra surjection, if A is spanned by group-like elements then so is A/I. □

Proposition 2.21. *Let A be an Hopf algebra. Then the nonzero group-like elements are linearly indipendent.*

Proof. Take $g_1, \dots, g_n$ be a maximal set of linearly indipendent group-like elements and take g to be a nonzero group like element. Then there is a linear dependence relation

$$g = \sum_i \lambda_i g_i\,.$$

But then applying Δ we got

$$g \otimes g = \sum_i \lambda_i g_i \otimes g_i\,.$$

But

$$g \otimes g = \left(\sum_i \lambda_i g_i\right) \otimes \left(\sum_j \lambda_j g_j\right) = \sum_{i,j} \lambda_i \lambda_j g_i \otimes g_j\,.$$

Since $\{g_i \otimes g_j\}_{i,j}$ are linearly indipendent we got that $\lambda_i \lambda_j = 0$ for all $i \neq 0$. Since g is nonzero there exists i such that $\lambda_i \neq 0$. But then $\lambda_j = 0$ for all $j \neq i$. Then we have $g = \lambda_i g_i$. Finally $\lambda_i^2 = \lambda_i$, that is $\lambda_i = 1$. So $g_1, \dots, g_n$ are the only group like elements of A. □

So if G is a diagonalizable group scheme its Hopf algebra $\mathcal{O}(G)$ has a basis made by group-like elements. Then

$$\mathcal{O}(G) = k[\Lambda]$$

where Λ is the commutative group of its group-like elements.

In fact from this we can give a fairly explicit description of all diagonalizable algebraic groups over k.

Theorem 2.22. *Let G be a diagonalizable group scheme of finite type over k. Then G is isomorphic to a product of copies of $\mathbb{G}_m$ and μ_n for $n \in \mathbb{N}$.*

Proof. In fact if G is of finite type over k, we have that $\mathcal{O}(G) = k[\Lambda]$ is finitely generated as a k-algebra, that is that Γ is a finitely generated abelian group. But then from the structure theorem for finitely generated abelian groups we have

$$\Lambda = \mathbb{Z}^r \oplus \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_n \,.$$

and so

$$k[\Lambda] = k[\mathbb{Z}]^{\otimes r} \otimes k[\mathbb{Z}/d_1] \otimes \cdots \otimes k[\mathbb{Z}/d_n] \,.$$

That is

$$G = \mathbb{G}_m^r \times \mu_{d_1} \cdots \times \mu_{d_n} \,.$$

□

The following important proposition explains a little the name "diagonalizable": the diagonalizable groups are exactly those for which the representations are simultaneously diagonalizable.

Proposition 2.23. *An abelian algebraic group G is diagonalizable if and only if every representation splits as a direct sum of one-dimensional representations.*

Proof. Suppose first that every representation splits. Then consider the regular representation $\mathcal{O}(G)$ that has the comodule structure given by the comultiplication map

$$\Delta : \mathcal{O}(G) \to \mathcal{O}(G) \otimes_k \mathcal{O}(G) \,.$$

Then, thanks to the hypotesis, there is a basis $g_1, \ldots, g_n$ such that $\Delta(g_i) = x_i \otimes g_i$. We see from the coassociativity that x_i are group-like elements. All we need to prove is that they span $\mathcal{O}(G)$. But in fact, since $(1 \otimes \varepsilon)\Delta = 1$ we get

$$\varepsilon(g_i)x_i = g_i \,.$$

And so the g_i are contained in the span of the x_i. But the g_i are a basis for $\mathcal{O}(G)$ and so we have concluded.

Conversely suppose now G is diagonalizable and let $g_1, \ldots, g_n$ be a basis of $\mathcal{O}(G)$ consisting of group-like elements. Take now V an $\mathcal{O}(G)$-comodule and let $\{v_i\}_i$ be a basis. Then

$$\rho(v_i) = \sum_{j=1}^{n} g_j \otimes w_{ij} \,.$$

But, using the comodule identities $(\Delta \otimes 1)\rho = (1 \otimes \rho)\rho)$ we get that $\rho(w_{ij}) = g_j \otimes w_{ij}$. Moreover, since $(\varepsilon \otimes 1)\rho = 1$ we get that

$$v_i = \sum_{j=1}^{n} \varepsilon(g_j) w_{ij} = \sum_{j=1}^{n} w_{ij} \,.$$

So the w_{ij} span all V. But then we can extract a basis $\{w_j\}_j$ from the w_{ij} and in this basis the group act in fact diagonally. □

More generally we will consider twisted forms of diagonalizable group schemes. That is we will consider algebraic groups G such that G_{k^s} is diagonalizable. This are called **groups of multiplicative type**. The Galois group Γ_k acts naturally on the character group of G_{k^s}, thus giving it the structure of a Galois module, called **character module** of G. We will denote it by Λ_G

It is clear that every group homomorphism $G \to H$ among groups of multiplicative type gives rise to a Galois module homomorphism $\Lambda_H \to \Lambda_G$ (it is nothing more that the restriction to group-like elements of the map induced on Hopf algebras $\mathcal{O}(H_{k^s}) \to \mathcal{O}(G_{k^s})$) and that this correspondence is functorial. A very important fact is that this is in fact an antiequivalence of categories.

Theorem 2.24. *The functor that sends each group of multiplicative type G to its character module Λ_G is an antiequivalence of categories.*

Proof. In fact we can describe the weak inverse for this functor. Take a Γ_k-module Λ. Its group algebra $\bar{k}[\Lambda]$ is an Hopf algebra over $\bar{k}$ and the natural action of Γ_k respects this structure, so $\bar{k}[\Lambda]^{\Gamma_k}$ is an Hopf algebra over k. Then our functor is the one which sends

$$\Lambda \mapsto G_\Lambda = \operatorname{Spec} \bar{k}[\Lambda]^{\Gamma_k} \,.$$

It is readily verified that this is a quasi-inverse for the functor $G \mapsto \Lambda_G$. □

A group of multiplicative type is called an **algebraic torus** if its character module is free as a $\mathbb{Z}$-module or, that is the same thing, if it is a twisted form of some $\mathbb{G}_m^r$. The **rank** of a torus is the rank of its character group. A torus is called **split** if it is in fact of the form $\mathbb{G}_m^r$ and **semisplit** if its character module is a permutation module (that is there is a basis of its character module which is permuted by the Galois group).

2.6 Torsors

This section is somewhat more advanced than the rest of the chapter. It will relay a lot on the notion of fppf cover and fppf cohomology. A good reference for them is [Mil80], expecially section III.4 which contains most of the material we will need.

Let G be a group scheme over S. A G-**torsor** is a sort of principal bundle. One good way to think about is like a collection of sets with a freely transitive action of G parametrized by some sort of space.

We will say that a G-torsor over S is a fppf sheaf P over S with a right action of G (that is a morphism of sheaves $P \times_S G \to P$ that pointwise determines a group action) that is locally trivial. That is there exists a fppf cover $U \to S$ such that $P|_U \cong G|_U$ in a such way that the action becomes the right multiplication one.

If G is a group scheme over S and X is a S-scheme a G-torsor over X is the same thing that a $(G \times_S X)$-torsor

Example 2.25. *If G is a finite costant group over a field k then every G-torsor is an étale k-algebra A such that its Galois group is G. In fact every étale cover of k is a (direct sum of) finite separable extension of k and so for every G-torsor P is trivial over k^s. Then a straightforward application of descent theory gives us the required result.*

Theorem 2.26. *Let G be an affine group scheme over a ring R. Then for every R-scheme S every G-torsor over S is representable (i.e. is the functor of points of a S-scheme.*

Proof. See [Mil80] theorem III.4.3. □

Theorem 2.27. *Let G be an affine group scheme over a field k. For every field extension K/k the isomorphism classes of G-torsors over K are classified by $H^1_{fppf}(K, G)$. In particular if G is reduced (and thus smooth) such torsors are classified by the Galois cohomology $H^1(K, G)$.*

Proof. See [Mil80] corollary III.4.7. □

Corollary 2.28. *Every GL_n-torsor over k is trivial.*

Proof. It follows easily from the previous theorem and Hilbert's theorem 90. □

Let G be an algebraic group. If we take a fppf sheaf F over S with a G-action and a G-torsor T over S we may define the **twist** of F by T as the sheaf quotient

$$T \times^G F = (T \times F)/G$$

where the G action is given by $(t, f)g = (tg, g^{-1}f)$ for $g \in G(U),\ t \in T(U),\ f \in F(U)$. This is still a fppf sheaf over S, but unfortunately it is not true that if F is representable then $T \times^G F$ is representable too.

We note that if T is the trivial torsor every section $s \in T(S)$ yields a natural isomorphism of $T \times^G F$ with F, given by

$$F(U) \to (T \times^G F)(U) \qquad f \mapsto [s|_U, f]\,.$$

So if T is a general torsor there is a fppf cover $U \to S$ such that $(T \times^G F)|_U \cong F|_U$.

If $G \to H$ is an algebraic group extension, then G acts on H by left multiplication. If $T \to k$ is a G-torsor then $T_H = T \times^G H$ has a natural structure of H-torsor. In fact the right action of H on H by multiplication gives an action on T_H and this is locally trivial since T is.

If $G \to H$ is an algebraic group extension and F is a fppf sheaf on S with an H action then for every G-torsor T on S we have

$$T \times^G F = (T \times^G H) \times^H F$$

as can be easily checked since they are the sheavifications of isomorphic presheaves. This produces the following very useful lemma.

Lemma 2.29. *Let K/k be a field extension and G is an algebraic group over k acting linearly on $\mathbb{A}^n_k$. If $T \to K$ is a G-torsor then the twist of $\mathbb{A}^n_K$ by T is isomorphic to $\mathbb{A}^n_K$.*

Proof. Note that the fact that G acts linearly can be seen as the fact that the G-action factors through the defining action of GL_n on $\mathbb{A}^n_K$. So if T is a G-torsor over K

$$T \times^G \mathbb{A}^n_K = (T \times^G GL_n) \times^{GL_n} \mathbb{A}^n_K = GL_n \times^{GL_n} \mathbb{A}^n_K = \mathbb{A}^n_K \,.$$

□

With a similar (but simpler) reasoning we see that if the action of G on F is trivial $T \times^G F = F$.

2.7 Examples

In this section we will show that torsors over a field k for some particular group schemes corresponds to genuinely interesting objects. Thus we will show that the study of the number of parameters necessary to describe a torsor is a generalization of several natural questions.

Let G be a finite group. A finite étale k-algebra A with an action of G is said to be **Galois** if $\dim A = \#G$ and $A^G = k$. For instance every Galois extension of Galois group G is a Galois algebra. We claim that G-torsors over k are exactly Galois k-algebras of Galois group G.

Proposition 2.30. *Let A a finite k-algebra with an action of G. Then A is Galois if and only if $A \otimes_k k^a$ is isomorphic to $\mathcal{O}(G_{k^a}) = \bigoplus_{g \in G} k^a \cdot e_g$ with the action given by $g(e_h) = e_{gh}$*

Proof. First suppose that $A \otimes_k k^a \cong \mathcal{O}(G_{k^s})$. Then A is étale, since it is certainly geometrically reduced, and $\dim A = \#G$. Now if we take a basis of A^G over k, they remains linearly indipendent over k^a since it is just a matter of determinants. Thus

$$\dim_k A^G \leq \dim_{k^a} (A \otimes_k k^a)^G = \dim_{k^a} k^a = 1 \,.$$

But $k \cdot 1 \subseteq A^G$ and so $A^G = k$ and A is Galois.

Now suppose that A is Galois over k. Then a trivial check shows that $A \otimes_k k^a$ is Galois over k^a. So it is enough to show the thesis if k is algebraically closed.

Since A is étale, then it is a direct product of $\#G$ copies of k.[2] So G acts by permutations on the factors. But $A^G = k$, so no factor is left fixed. Then the action of G on the factors is free and so is transitive for cardinality reasons. But then the factors are isomorphic to G as a G-set. Thus

$$A = \bigoplus_{g \in G} k \cdot e_g \,.$$

□

Corollary 2.31. *Let G be a finite constant group over k. A scheme with a $T \to \operatorname{Spec} k$ with a right G-action is a G-torsor if and only if it is the spectrum of a Galois algebra of Galois group G.*

For example spectra of Galois extensions are G-torsors.

Proof. It is merely a restatement of proposition 2.30. □

Let μ_n be the group scheme of n-th roots of unit. We want to describe the μ_n torsors over a field k.

Let $T \to \operatorname{Spec} k$ be a μ_n-torsor. Then it is affine, let $A = \mathcal{O}(T)$. Now, since μ_n is smooth, the torsor is étale-locally trivial, which means that $A \otimes_k k^s$ is isomorphic to $\mathcal{O}(\mu_n) = k^s[T]/(T^n - 1)$ as a μ_n-module. That is the map

$$k^s[S]/(S^n - 1) \to k^s[S]/(S^n - 1) \otimes_k k^s[T]/(T^n - 1) \qquad S \mapsto S \otimes T$$

is Γ_k-equivariant. Remember that the action of Γ_k on $\mathcal{O}(\mu_n)$ leaves T fixed. For each $\sigma \in \Gamma_k$ let $\sigma S = p_\sigma(S)$. Then the Γ_k-equivariance translate into the equality

$$p_\sigma(S) \otimes T = p_\sigma(S \otimes T) \,.$$

Substituting $p_\sigma(S) = \sum_{i=0}^{p-1} a_{i,\sigma} S^i$ into the equality is easy to see that the previous equality implies

$$p_\sigma(S) = a_\sigma S$$

for some $a_\sigma \in k^s$. Moreover $p_\sigma p_\tau = p_{\sigma\tau}$ and $p_1(S) = S$ imply that $\sigma \mapsto a_\sigma$ is a cocyle for the first cohomology group of $k^{s\times}$. But Hilbert's theorem 90 says that we may find $\xi \in k^{s\times}$ such that $a_\sigma = \xi/(\sigma\xi)$. This translate into

$$\sigma(\xi S) = \xi S \,.$$

Moreover $S^n = 1$, so $\xi^n \in k^\times$. Then it is easy to see that

$$(k^s[S]/(S^n - 1))^\Gamma_k = k[\xi S]/((\xi S)^n - \xi^n) \,.$$

We have proved

[2] In fact a finite algebra is an artinian ring, so it is a product of artinian local ring. But a reduced artinian local ring is a field, since the only prime is 0.

Theorem 2.32. *Let k be a field. A μ_n-torsor is of the form*

$$k \to k[S]/(S^n - a)$$

for some $a \in k^\times$, with the action $S \mapsto S \otimes T$.

Corollary 2.33. *Let k be a field of characteristic p. Then the reduced μ_{p^n}-torsors are exactly the principal completely inseparable field extensions of k of rank p^n.*

Proof. It is sufficient to note that the torsor $k \to k[S]/(S^{p^n} - a)$ is reduced if and only if a is not a p-th power. □

2.8 Weil restriction

Let R be a ring and R' be an R-algebra. Then for each R' scheme X we can form a functor from the category of R-algebras to sets called **Weil restriction** of X defined by

$$R_{R'/R}X(S) = X(S \otimes_R R')$$

for each R-algebra S. We want to investigate conditions on which this functor is representable by an R-scheme.

Remark 2.34. *It is clear that if X is a group scheme the structure of group scheme gives a lifting of $R_{R'/R}X$ to the category of groups. Thus if the Weil restriction is representable then it is in a natural way a group scheme.*

Theorem 2.35. *Let R be a ring and R' an R-algebra which is free and finite as a R-module. For each affine scheme $X = \operatorname{Spec} A'$ over R' the Weil restriction $R_{R'/R}(X)$ is represented by an affine R-scheme.*

Proof. At first suppose that A' is of the form $A' = R'[\mathscr{T}]$ where $\mathscr{T}$ is a set (of arbitrary cardinality) of indeterminates. Fix a basis $\mathscr{B} = \{b_1, \dots, b_n\}$ of R' over R. Then we claim that $A = R[\mathscr{T} \times \mathscr{B}]$ is such that $\operatorname{Spec} A$ is the Weil restriction of X. In fact for each R-algebra S we have

$$Hom_{R'}(A', S \otimes_R R') = Hom_{R'}(R'[\mathscr{T}], S^{\mathscr{B}}) = (S^{\mathscr{B}})^{\mathscr{T}} = S^{\mathscr{B}\times\mathscr{T}}$$

$$Hom_R(A, S) = Hom_R(R[\mathscr{T} \times \mathscr{B}], S) = S^{\mathscr{T}\times\mathscr{B}}.$$

To treat the general case we can write A' as $R'[\mathscr{T}]/I$ where $\mathscr{T}$ is a set of indeterminates and I an ideal. Consider the natural map of R-algebras

$$\psi : R'[\mathscr{T}] \to R[\mathscr{T} \times \mathscr{B}]$$

which sends each element of the basis of R' in the corresponding indeterminate. Then take J the ideal generated by the image of I. Then an easy control shows that

$$A = R[\mathscr{T} \times \mathscr{B}]/J$$

describes the Weil restriction of A'. □

Remark 2.36. *For a more comprehensive treatment of Weil restriction and a more general form of the previous theorem we advise the reader to look at [BLR90], paragraph 7.6.*

Proposition 2.37. *If L is a Galois algebra over k with Galois group Γ then $R_{L/k}(\mathbb{G}_m)$ is exactly the torus having for character module $\Lambda = \mathbb{Z}[\Gamma]$. In particular every semisplit torus can be written in this form.*

Proof. In fact for every k-algebra S

$$R_{L/k}(\mathbb{G}_m)(S) = \mathbb{G}_m(S \otimes_k L) = (S \otimes_k L)^\times$$

$$Hom_k((L[\Lambda])^\Gamma, S) = Hom_\Gamma(L[\Lambda], S \otimes_k L) = (S \otimes_k L)^\times$$

In fact $L[\Lambda] = L[x_\gamma^{\pm 1} \mid \gamma \in \Gamma]$ and so the Γ-equivariant homomorphism from $L[\Lambda]$ are determined by the image of x_e, where $e \in \Gamma$ is the neutral element. Moreover the image of x_e is forced to be an invertible element of $S \otimes_k L$ and can be anyone of them. □

This characterization is important because it allows us to prove that every semiplit torus has trivial Galois cohomology, a fact that will be important later.

Lemma 2.38. *Let G be a semisplit torus over k. Then for each field extension K/k we have*

$$H^1(K, G) = 0\,.$$

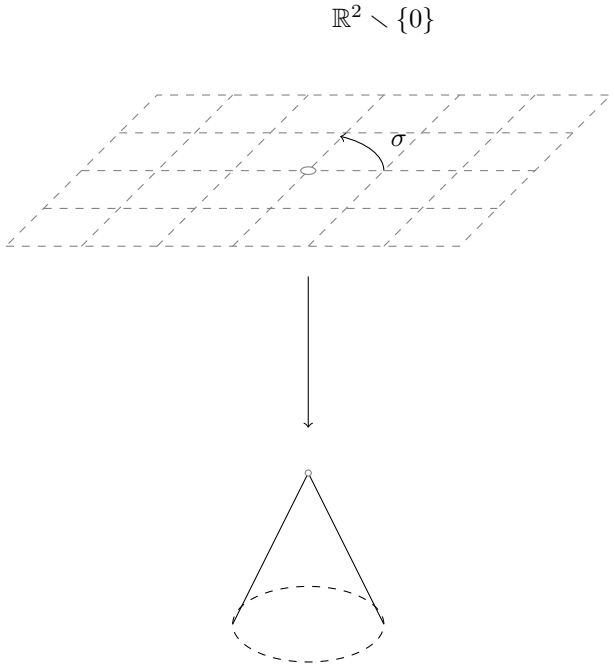
Proof. Since the base change of a semisplit torus is still a semisplit torus we may suppose $k = K$. Then note that, if $G = R_{L/k}(\mathbb{G}_m)$ with L étale algebra of dimension n

$$H^1(k, R_{L/k}(\mathbb{G}_m)) = H^1(\Gamma_k, (L \otimes \bar{k})^\times) = H^1(\Gamma_k, (\bar{k}^\times)^{\oplus n}) = H^1(\Gamma_k, \bar{k}^\times)^{\otimes n}\,.$$

But by Hilbert's Theorem 90 we have $H^1(\Gamma_k, \bar{k}^\times) = 0$, which is the thesis. □

Chapter 3

Essential dimension of algebraic groups



A minimal versal torsor for $C_4 = \langle \sigma \rangle$ over $\mathbb{R}$.

In this chapter finally we will describe essential dimension and prove theorems about it. We will show that the essential dimension of a group is correlated with the action of the group on varieties and in particular with representations. Most of the content of the chapter come from [BF03], even if part are original work.

The idea of essential dimension has been introduced first by Buhler and Reichstein in [BR97] for finite groups and has been generalized to algebraic groups in [Rei00]. The next generalization is due to Merkurijev in an unpublished paper referenced in [BF03] and it is that definition we are going to use. In this generality essential dimension is an invariant associated to set valued functors from the field extensions of a base field k. Examples of applications of this generality can be seen in [BF04] and [RV11].

3.1 Essential dimension of functors

Fix a base field k. We will consider functors from the category of field extensions of k to sets. Let F be such an object. For convenience if $a \in F(K)$ where K is an extension if $K \to L$ is a morphism of field we will denote with a_L the image of a in $F(L)$.

Example 3.1. *Let Et_n be the functor such that $Et_n(K)$ are the isomorphism classes of étale K-algebras of dimension n and such that on arrows $K \to L$ sends an étale K-algebra A to its tensor product with L.*

Example 3.2. *Let $Quad_n$ be the functor such that $Quad_n(K)$ are isomorphism classes of (V, q) where V is a K-vector space of dimension n And q is a non-degenerate quadratic form on V. As before an arrow $K \to L$ send (V, q) to $(V \otimes_K L, q \otimes 1)$.*

Now take $a \in F(K)$ where K/k is a field extension. For a subextension $k \subseteq L \subseteq K$ we say that a is **defined** over L if there exists a $b \in F(L)$ such that $b_K = a$. Then the **essential dimension** of a is the minimum of $\operatorname{trdeg}_k L$ where L is a subextension of K/k where a is defined. In a similar way we define the **essential dimension** of F as the supremum of all essential dimension of its elements

$$\operatorname{ed}_k F = \sup\{\operatorname{ed}_k a \mid a \in F(K),\ K/k \text{ extension } \}.$$

As the example in the introduction shows, we must pay attention to the fact that if certainly the minimum trascendence degree of a field of definition certainly exists thanks to the well-ordering of the natural numbers, there may not be a minimal field of definition. In fact for instance the quadratic form $q(x, y) = tx^2 + y^2$ defined over $k(t)$ is isomorphic to the forms

$$q_n(x, y) = t^{3^n} x^2 + y^2$$

that are defined on the descreasing sequence of fields $k(t^{3^n})$ but not on their intersection (which is k).

Example 3.3. *Fix a positive integer n and let S be the functor such that*

$$S(K) = \begin{cases} \varnothing & \text{if } \operatorname{trdeg}_k K < n \\ \{0\} & \text{if } \operatorname{trdeg}_k K \geq n \end{cases}$$

with the obvious arrows. Then $\operatorname{ed}_k S = n$. So there are functor with essential dimension arbitrarily large and even infinite (letting n be ∞).

Proposition 3.4. *Let K/k be a field extension and let F be a functor from k-field extensions to sets. If we denote by $F|_K$ its restriction to the full subcategory of extensions of K*

$$\operatorname{ed}_k F \geq \operatorname{ed}_K F|_K .$$

So in order to provide lower bounds for essential dimension we may safely enlarge the base field.

Proof. Trivial since enlarging the base field means taking the supremum on a smaller set. □

Proposition 3.5. *Let k be a field and F, G be functors from the extension of k to sets. Then*

$$\operatorname{ed}_k(F \amalg G) = \max(\operatorname{ed}_k F, \operatorname{ed}_k G)$$

$$\operatorname{ed}_k(F \times G) \leq \operatorname{ed}_k F + \operatorname{ed}_k G .$$

Proof. The first equality is a restatement of the definitions, since

$$\operatorname{ed}_k(F \amalg G) = \sup\{\operatorname{ed}_k a \mid a \in F(L) \text{ or } a \in G(L)\} = \max(\operatorname{ed}_k F, \operatorname{ed}_k G) .$$

For the second equality take $(a, b) \in (F \times G)(L) = F(L) \times G(L)$. Then we have that a is defined on a subextension L' of trascendence degree at most $\operatorname{ed}_k F$ and b is defined on a subextension L'' of trascendence degree at most $\operatorname{ed}_k G$. Then (a, b) is defined on $L'L''$, that has trascendence degree at most $\operatorname{ed}_k F + \operatorname{ed}_k G$. □

The following theorem will be our main way to give bounds on the essential dimension.

Proposition 3.6. *Let $\phi : F \to G$ be a map of functors such that for every extension K/k the map $\phi_K : F(K) \to G(K)$ is surjective. Then $\operatorname{ed}_k G \leq \operatorname{ed}_k F$.*

Proof. We need to prove that for each $a \in G(K)$ $\operatorname{ed}_k a \leq \operatorname{ed}_k F$. Take $b \in F(K)$ such that $\phi_K(b) = a$. Then since $\operatorname{ed}_k b \leq \operatorname{ed}_k F$ we have that there exists a subextension L and a $b' \in F(L)$ such that $b'_K = b$. Then $\phi(b')$ is an element of $G(L)$ such that

$$\phi(b')_K = \phi(b'_K) = \phi(b) = a .$$

Then $\operatorname{ed}_k a \leq \operatorname{trdeg}_k L \leq \operatorname{ed}_k F$. □

For representable functors the computation of essential dimension is particularly easy

Proposition 3.7. *Let X be a scheme of finite type over k. Then* $\operatorname{ed}_k X = \dim X$*, where X is identified with its functor of points.*

Proof. Every point $p \in X(K)$ has a least field of definition $k(p)$. Then $\operatorname{ed}_k p = \operatorname{trdeg}_k k(p)$ and so

$$\operatorname{ed}_k X = \sup_{p \in X} \operatorname{trdeg}_k k(p) = \dim X \,.$$

□

3.2 Essential dimension of algebraic groups

Let G be an algebraic group. We are interested in the functor $G - Tors$, that associated to K/k the isomorphism classes of G-torsors over K, that is the functor $H^1(-, G)$. Many functors of interest are of this form, thanks to the result of theorem 1.7. Its essential dimension will be called **essential dimension** of G and simply denoted $\operatorname{ed}_k(G)$.

Example 3.8. *Since an étale algebra of dimension n is simply a twisted form of $(k^s)^{\oplus n}$ there is an isomorphism of functors $Et_n = H^1(-, S_n)$. So the essential dimension of the functor of étale algebras of dimension n is* $\operatorname{ed}_k S_n$*.*

Example 3.9. *Since all nondegenerate quadratic form are isomorphic over an algebraically closed field the previously cited result allow us to state that the functor $Quad_n$ of nondegenerate quadratic forms is isomorphic to $H^1(-, O_n)$ where O_n is the group scheme of matrices A such that ${}^tAA = 1_n$.*

The group μ_n

Consider μ_n, the group scheme of n-th roots of unity. Then we have a short exact sequence of algebraic groups

$$1 \to \mu_n \to \mathbb{G}_m \to \mathbb{G}_m \to 1$$

where the map $\mathbb{G}_m \to \mathbb{G}_m$ amounts to raising to the n-th power. Taking K-rational points it yields the Kummer long exact sequence

$$1 \to \mu_n(K) \to K^\times \to K^\times \to H^1(K, \mu_n) \to H^1(K, \mathbb{G}_m) = 1$$

where the last equality comes from Hilbert's theorem 90. Then this shows that

$$H^1(K, \mu_n) = K^\times / (K^\times)^n \,.$$

From this we can prove that $\operatorname{ed}_k(\mu_n) = 1$. In fact a class $[a] \in H^1(K, \mu_n) = K^\times/(K^\times)^n$ is surely defined on $k(a)$ which has at most trascendence degree 1 over k. So $\operatorname{ed}_k(\mu_n) \leq 1$. Now take t and indeterminate and consider $K = k(t)$, $[t] \in H^1(K, \mu_n)$. Suppose that $\operatorname{ed}_k[t] = 0$, then $[t]$ is defined over an algebraic subextension. But the only algebraic subextension of k in $k(t)$ is k itself, so

there exists $a \in k^\times$ such that $[t] = [a]$, that is $t/a \in (K^\times)^n$. But then there exists coprime polynomials $p, q \in k[t],\ q \neq 0$ such that

$$\frac{t}{a} = \left(\frac{p}{q}\right)^n \Rightarrow tq^n = ap^n\,.$$

But this is clearly absurd since the left hand side has degree congruent to 1 mod n and the right hand side has degree divisible by n. Then $\mathrm{ed}_k[t] = 1$ and so $\mathrm{ed}_k\,\mu_n = 1$.

Note that, thanks to our previous description of the μ_n-torsors, we have proved for example that, if the base field has characteristic p, the functor F such that $F(K)$ are the purely inseparable extensions of K of degree p^r have essential dimension 1. This could obiouvsly proved in a more direct fashion but it is interesting how it can be inserted in this more general framework.

The group $\mathbb{Z}/p$

Now suppose that the base field k is of characteristic p consider the constant group $\mathbb{Z}/p$. Then we may reason as in the previous case, applying Artin-Schreier exact sequence

$$0 \to \mathbb{Z}/p \to \mathbb{G}_a \xrightarrow{\mathscr{P}} \mathbb{G}_a \to 0$$

where the last map is given by $= x^p - x$. Then we have the long exact sequence in cohomology

$$0 \to \mathbb{Z}/p \to K \to K \to H^1(K, \mathbb{Z}/p) \to H^1(K, \mathbb{G}_a) = 0$$

where the last equality comes from the normal basis theorem (that essentially asserts that the additive group $(K, +)$ is a Γ_K permutation module and so has trivial cohomology). Then

$$H^1(K, \mathbb{Z}/p) = K/\mathscr{P}(K)\,.$$

Reasoning exactly like the previous case we get that $\mathrm{ed}_k(\mathbb{Z}/p) = 1$. The analogue Artin-Schreier exact sequence for truncated Witt vectors allows us to assert

$$\mathrm{ed}_k(\mathbb{Z}/p^n) \leq n\,.$$

Unfortunately not much more is known, although it is conjectured that the equality always holds.

The circle group

Now focus on the case of the circle group S^1. This is the group scheme of Hopf algebra

$$k[X, Y]/(X^2 + Y^2 - 1)$$

and comultiplication

$$\Delta X = X \otimes X - Y \otimes Y \qquad \Delta Y = X \otimes Y + Y \otimes X\,.$$

As we have already seen this is a twisted form of $\mathbb{G}_m$. In order to present a clearer treatment we will generalize to a wider class of groups.

Let L be an étale k-algebra. Then we may define $\mathbb{G}^1_{m,L}$ as a group scheme over k such that

$$1 \to \mathbb{G}^1_{m,L} \to R_{L/k}(\mathbb{G}_{m,L}) \xrightarrow{Nm_L} \mathbb{G}_m \to 1$$

where the last map is the norm map that sends each element of $R_{L/k}(\mathbb{G}_{m,L})(A) = (A \otimes_k L)^\times$ in the determinant over k of the multiplication map. The case of S^1 is exactly the case with $L = k[t]/(t^2+1)$. We are aiming to the following result

Proposition 3.10. *Let L/k be an étale algebra of dimension $n \geq 1$. Then $\operatorname{ed}_k \mathbb{G}^1_{m,L}$ is equal to 0 if L is product of separable extension of k of pairwise coprime degree.*

Remembering that the semisplit torus $R_{L/k}(\mathbb{G}_m)$ is acyclic then we have a long exact sequence

$$1 \to \mathbb{G}^1_{m,L}(K) \to (L \otimes_k K)^\times \to K^\times \to H^1(K, \mathbb{G}^1_{m,L}) \to 1\,.$$

So as usual

$$H^1(K, \mathbb{G}^1_{m,L} = K^\times / Nm_L((L \otimes_k K)^\times)\,.$$

and $\operatorname{ed}_k \mathbb{G}^1_{m,L}) \leq 1$. In fact with some more careful reasoning we may prove that $\operatorname{ed}_k \mathbb{G}^1_{m,L} = 0$ if and only if L is a product of finite separable field extensions of k of pairwise coprime degree. In particular $\operatorname{ed}_k(S^1) = 1$ if and only if the characteristic of k is not 2 and -1 is not a square in k.

3.3 Versal torsors

In order to do more refined calculations we need a different characterization of essential dimension, as the dimension of a minimal "space of parameters" which describes the G-torsors. This will not be a moduli space (although the notions are surely correlated) because instead of asking for an universal property we will not insist on the unicity requirement. So, following [AD07], these object are called "versal" (like *uni*versal but without the uniqueness).

Let G be an algebraic group over a field. A **weakly versal torsor** for G is a G-torsor $P \to X$ such that for every field extension K/k and every G-torsor $Q \to \operatorname{Spec} K$ there is a cartesian diagram

$$\begin{array}{ccc} Q & \longrightarrow & P \\ {\scriptstyle G}\downarrow & & \downarrow{\scriptstyle G} \\ \operatorname{Spec} K & \longrightarrow & X \end{array}$$

That is the natural map of functors $X \to H^1(-, G)$ that sends ever $p \in X(K)$ to the class $[p^*P]$ is surjective. But then using proposition 3.6 we get that

$$\operatorname{ed}_k G \leq \dim X\,.$$

A G-torsor $P \to X$ is said to be **versal** if for every open subscheme $U \subseteq X$ the restriction $P|_U$ is weakly versal.

If $T \to S$ is a G-torsor a **compression** of $T \to S$ is another G-torsor $T' \to S'$ with rational dominant G-equivariant maps $T \dashrightarrow T'$, $S \dashrightarrow S'$ such that the following diagram commutes

$$\begin{array}{ccc} T & \cdots\cdots\to & T' \\ \big\downarrow G & & \big\downarrow G \\ S & \cdots\cdots\to & S' \end{array}$$

Note that such a diagram, if it exists, is necessarily cartesian since the category of torsors over a base scheme is a groupoid.

The compression of a torsor is in some sense a simplification. The first thing we see is that the operation of compression doesn't alter the versality of a torsor.

Proposition 3.11. *Every compression of a versal torsor is versal.*

Proof. Let $T \to S$ be a versal torsor and $T' \to S'$ be a compression. Fix a G-torsor $P \to \operatorname{Spec} K$ and an open subset $U' \subseteq S'$. Then we must find a point $p \in U'(K)$ such that $p^*(T'|_{U'}) = P$. Now be U the preimage of U via the map $S \to S'$. This is not empty because the preimage of a nonempty open via a rational dominant map is nonempty Since the torsor $T \to S$ is versal we may find a point $q \in U(K)$ such that $q^*T = P$. But then choosing p as the image of q in S' we have the thesis. □

Theorem 3.12. *Let G be an algebraic group over k and let $P \to X$ be a versal torsor with X integral. Then the essential dimension of G is equal to the least dimension of X' where $P' \to X'$ is a compression of $P \to X$.*

Proof. Since the compression of a versal torsor is versal we have that $\operatorname{ed}_k G \leq \dim X'$ for each compression $P' \to X'$. So we need to prove the other inequality, i.e. to find a compression $P' \to X'$ such that $\dim X' = \operatorname{ed}_k X$. Let $K = K(X)$ be the function field of X and let $P_K \to \operatorname{Spec} K$ be the generic fibre. This is a G-torsor over K so we may find a subfield $L \subseteq K$ of trascendence degree $\operatorname{ed}_k G$ over which P_K is defined. Let $P'_L \to \operatorname{Spec} L$ be a torsor such that $P'_L \times_L K = P_K$. We claim that there exists a torsor $P' \to X'$ for which $P'_L \to \operatorname{Spec} L$ is the generic fibre. First note that we may suppose P and X to be affine (take an open dense affine subscheme $U \subseteq X$ and take the restriction of P to U).

Now let $A = \mathcal{O}(X)$, $B = \mathcal{O}(T)$, $\tilde{B} = \mathcal{O}(\tilde{T})$ and $\tilde{B}' = \mathcal{O}(\tilde{T}')$. The G-action on T and T' amounts to two map of rings

$$B \to B \otimes_k \mathcal{O}(G), \qquad \tilde{B}' \to \tilde{B}' \otimes_k \mathcal{O}(G)$$

that give to B and $\tilde{B}'$ the structure of $\mathcal{O}(G)$-comodule. Moreover the fact that they are G-torsor requires that the two induced maps

$$B \otimes_A B \to B \otimes_k \mathcal{O}(G), \qquad \tilde{B}' \otimes_L \tilde{B}' \to \tilde{B}' \otimes_k \mathcal{O}(G)$$

are isomorphism. Now, let $L = k(\alpha_1, \dots, \alpha_n)$. Without loss of generality we may suppose that $\alpha_i \in A$. Then we put $A' = k[\alpha_1, \dots, \alpha_n]$.

Consider $\tilde{B}' = L[T_1, \dots, T_m]/(f_i)_i$. Then $\tilde{B}' \otimes_K L = K[T_1, \dots, T_m]/(f_i)_i$. But $\tilde{B}' \otimes_K L = B \otimes_A K = \mathcal{O}(T')$ and so, up to localizing at an opportune $d \in A'$, we may suppose that $f_i \in A'[T_1, \dots, T_m]$ and that $B = A[T_1, \dots, T_m]/(f_i)_i$. Now the comodule structure on $\tilde{B}'$ is determined by the images of the T_i, that is

$$T_i \to \sum_l h_{il} \otimes g_{il} \qquad h_{il} \in L[T_1, \dots, T_m]/(f_i)_i \; g_{il} \in \mathcal{O}(G)\,.$$

Then up to localize further we may suppose that even $h_{il} \in A'[T_1, \dots, T_m]$. Now we put

$$B' = A'[T_1, \dots, T_m]/(f_i)_i\,.$$

This has a natural structure of comodule inherited by $\tilde{B}'$ and so, up to an even further localization to assure the existence of the isomorphisms, we get that $A' \to B'$ determine a compression of T on $\operatorname{Spec} A'$, exept maybe for the flatness of the map $A' \to B'$. But the generic freeness lemma allows us to get it to the price of localizing again, which does not disrupt the previous properties. So we have found a compression of T with base dimension $\dim A' = \operatorname{trdeg}_k L = \operatorname{ed}_k G$. □

Lemma 3.13. *Let G be a finite étale group scheme over k such that $\operatorname{ed}_k G = 1$. Then G is isomorphic to a closed subgroup of PGL_2.*

Proof. Take a faithful representation V of G. Then $V \to V/G$ is a versal torsor. Since $\operatorname{ed}_k G = 1$ we can find a compression $T \to S$ with $\dim S = 1$. But then $\dim T = \dim S + \dim G = \dim S = 1$ and T is unirational since there is a rational dominant map $V \to T$. By Luroth's theorem every unirational variety is rational so T is birational to $\mathbb{P}^1$. So G is a closed subgroup of the group of birational automorphism of $\mathbb{P}^1$, which is exactly PGL_2. □

3.4 Essential dimension and representations

Let X be a scheme of finite type over a field k and suppose that G is an algebraic group acting generically freely on X. We will call an open G-invariant subscheme of X that satisfies the thesis of the theorem 2.17 a **friendly** open subscheme of X.

Proposition 3.14. *Let G an algebraic group over k that acts linearly and generically freely on $\mathbb{A}^n_k$. Suppose that $U \subseteq \mathbb{A}^n_k$ is a friendly open subscheme (whose existence is guaranteed by the theorem). Then $U \to U/G$ is a versal G-torsor. In particular*

$$\operatorname{ed}_k G + \dim G \leq n\,.$$

Proof. Let $T \to \operatorname{Spec} K$ be a G-torsor. Our goal is to find a point $p \in U/G(K)$ such that $p^*U = T$. Now consider $\mathbb{A}^n_K$ as a G-space and twist the action by T getting $Y = T \times^G \mathbb{A}^n_K$. But every twist of $\mathbb{A}^n_K$ by a linear action is isomorphic to $\mathbb{A}^n_K$ so the rational points are dense, so we can pick $y \in T \times^G U(K)$, which is an open subscheme of $T \times^G \mathbb{A}^n_K$. Now $T \times^G U/G = U/G$ since the action of G on U/G is trivial. So we may take as p the image of y in $U/G(K)$. Now it is easy to construct a simple Γ_K-equivariant isomorphism between p^*U and T over K^s, that descends to an isomorphism over K. □

Lemma 3.15. *Let G be a finite étale group scheme and let V be a faithful G-representation. Then the action of G on V is generically free.*

Proof. Consider the action of $G(k^s)$ on $V \otimes_k k^s$. For every $g \in G(k^s)$ its set $(V \otimes_k k^s)^g$ of the fixed points of g is a proper subvariety of $V \otimes_k k^s$ (precisely a proper vector subspace), and since $G(k^s)$ is a finite group the set

$$S = \bigcup_{g \in G(k^s)} (V \otimes_k k^s)^g$$

is a proper subvariety of $V \otimes_k k^s$. Moreover is clearly stable for the action of the Galois group Γ_k, so by descent theory it came out from a closed subscheme C of V. On $V \smallsetminus C$ the action of G is free, by the criterion of proposition 2.16. □

Recently Merkuriev and Karpenko have proved that this bound is sharp for p-groups if the ground field contains the p-th roots of unity.

Theorem 3.16 (Merkurjev-Karpenko)**.** *Let G be a p-group and k a field of characteristic different from p containing a primitive p-th root of unity. Then $\operatorname{ed}_k(G)$ coincides with the least dimension of a faithful representation of G over k.*

Proof. See [KM08]. □

Theorem 3.17. *Let G be a closed subgroup of GL_n such that the natural map $G \to PGL_n$ is still injective. Then*

$$\dim G + \operatorname{ed}_k G \leq n - 1$$

Proof. In fact we may find a friendly open of $\mathbb{P}^n$ U and a friendly open V in the preimage of U in $\mathbb{A}^n$. Then $U \to U/G$ is a compression of $V \to V/G$ and so it is still a versal torsor. Then $\operatorname{ed}_k G \leq \dim V/G$, which is the thesis. □

3.5 Essential dimension and subgroups

Now we begin to investigate the way essential dimension behave with respect to the operation of passing at subgroups.

Theorem 3.18. *Let G be an algebraic group over k and let H be a closed subgroup of G. Then*

$$\operatorname{ed}_k H + \dim H \leq \operatorname{ed}_k G + \dim G\,.$$

Proof. Take a generically free G representation V and pick a friendly open subscheme U for the action of G. Note that U is also H-stable, since H is a subgroup of G.

Then there exists $U \to U/G$ and pick a compression $X \to X/G$ with $\dim X/G = \operatorname{ed}_k G$. But then H acts on X freely (since G does so) and so we may pick a friendly open subscheme $W \subseteq X$ such that $W \to V/H$ exists. But then $W \to W/H$ is versal, since the action of $\mathbb{A}^n_k$ is, and so

$$\operatorname{ed}_k H \leq \dim W/H = \dim W - \dim H = \dim X - \dim H =$$

$$= \dim X/G + \dim G - \dim H = \operatorname{ed}_k G + \dim G - \dim H$$

which is exactly the thesis. □

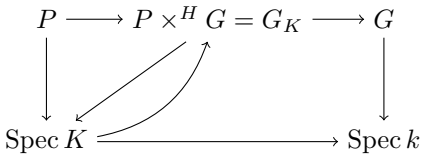
Proposition 3.19. *Let G an algebraic group over a field k and let H a closed subgroup such that for each field extension K/k the map*

$$H^1(K, H) \to H^1(K, G)$$

is trivial. Then $G \to G/H$ is a weakly versal H-torsor and in particular

$$\operatorname{ed}_k H + \dim H \leq \dim G\,.$$

Proof. Since $G \to G/H$ is clearly an H-torsor all we have to show is that for each H-torsor $P \to \operatorname{Spec} K$ there is $x \in G/H(K)$ such that $x^*G = P$. But since the map $H^1(K, H) \to H^1(K, G)$ is trivial we have that $P \times^H G$ is the trivial G-torsor. So it has a section $\operatorname{Spec} K \to P \times^H G$ and a projection $P \times^H G \to G$ in such way that the following diagram commutes.



So if we call $x : \operatorname{Spec} K \to G/H$ the composition we have that $x^*G \cong P$ and the theorem is proved.

□

3.6 More essential dimension computations

In this section we will give more refined computations of essential dimension.

The symmetric group S_n

Lemma 3.20. *If $G = C_2 \times \cdots \times C_2$ is the product of n copies of the cyclic group of order two we have*

$$\mathrm{ed}_k(G) = n\,.$$

Proof. It is trivial from

$$H^1(K, C_2 \times \cdots \times C_2) = K^\times/(K^\times)^2 \times \cdots \times K^\times/(K^\times)^2\,.$$

□

Theorem 3.21. *Let S_n be the symmetric group on n elements. Then, if $n \geq 5$*

$$\left\lfloor \frac{n}{2} \right\rfloor \leq \mathrm{ed}_k\, S_n \leq n-3\,.$$

Proof. Consider the subgroup H of S_n generated by the transpositions $(12), (34), (56), \ldots$. This is a subgroup of S_n isomorphic to $(C_2)^{\lfloor \frac{n}{2}-1 \rfloor}$. Then $\mathrm{ed}_k\, S_n$ is greater or equal to that of H. This proves the lower bound.

For the upper bound consider the permutation representation of S_n on $V = \mathbb{A}^n_k$. This is clearly faithful, so it is generically free. So

$$\mathrm{ed}_k(S_n) = \mathrm{ed}_k(k(x_1, \ldots, x_n)/k(x_1, \ldots, x_n)^{S_n})\,.$$

We need to find a subfield of $k(x_1, \ldots, x_n)$ that is S_n stable and on which the action of S_n is faithful. We may take the subfield generated by the biratios

$$[x_i, x_j, x_l, x_m] = \frac{(x_i - x_l)(x_j - x_m)}{(x_j - x_l)(x_i - x_m)}\,.$$

This is clearly S_n-stable. Moreover if $n \geq 5$ for every nontrivial $\sigma \in S_n$ there is i such that $\sigma(i) \neq i$. So we may find a biratios containing i and non containing $\sigma(i)$. Then that biratio cannot be fixed by σ and the action is faithful.

All we need to prove is that the trascendence degree of the biratios is less or equal to $n-3$. But this is easy, since the field is generated by the $n-3$ elements $\{[x_1, x_2, x_3, x_i] \mid 4 \leq i \leq n\}$ thanks to the well known symmetry property of the biratios and the identity

$$[x_i x_j x_l x_m][x_i x_s x_m x_l] = [x_i x_j x_l x_s]\,.$$

So the thesis is proved. □

If $n = 3, 4$ all we can hope to prove is $\mathrm{ed}_k\, S_n \leq n-2$, and this is done by considering the representation of the subspace of V given by $x_1 + \cdots + x_n = 0$. So $k(x_1, \ldots, x_{n-1})$ is still versal. Then we may take $k(x_1/x_{n-1}, \ldots, x_{n-2}/x_{n-1})$ and this gives the bound required.

So we have the following values

$$\begin{aligned} \operatorname{ed}_k S_2 &= 1 \\ \operatorname{ed}_k S_3 &= 1 \\ \operatorname{ed}_k S_4 &= 2 \\ \operatorname{ed}_k S_5 &= 2 \\ \operatorname{ed}_k S_6 &= 3 \\ 3 \leq \operatorname{ed}_k S_7 &\leq 4 \end{aligned}$$

Recently Duncan has proved that if k has characteristic 0 we have $\operatorname{ed}_k S_7 = 4$ (see [Dun09]).

Cyclic and dihedral groups

Lemma 3.22. *Let n be an integer and k a field such that n is coprime with the characteristic of k. Let $\zeta \in k^s$ be a primitive n-th root of unity and set $\alpha = \zeta + \zeta^{-1}$. Suppose $\alpha \in k$. Then the subgroup of $GL_2(k)$ generated by the matrices*

$$S = \begin{pmatrix} \alpha & 1 \\ -1 & 0 \end{pmatrix}, \; T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

is isomorphic to the dihedral group $D_n = \langle r, s \mid r^n = s^2 = rsrs = 1 \rangle$. Moreover if n is odd the map $D_n \to PGL_2(k)$ is injective.

Proof. It is clear that $T^2 = 1$ and a direct computation shows that that $STST = 1$. Computing the characteristic polynomial of S we see that it is

$$p_S(\lambda) = \lambda(\lambda - \alpha) + 1 = (\lambda - \zeta)(\lambda - \zeta^{-1}) \, .$$

Since all eigenvalues are distinct and of exact order n the matrix S is diagonalizable of exact order n.

Now suppose that n is odd. Since $T \neq 1$ in $PGL_2(k)$ it still has order 2. All we need to show is that S has exact order n (since the only quotient of D_n which is injective on the copy of $\mathbb{Z}/n$ and on a reflection is the identity). But suppose that $S^d = \lambda$ for some $d < n$. Then $\zeta^d = \lambda$ and $\zeta^{-d} = \lambda$, since they are the eigenvalues of S. But then $\zeta^{2d} = 1$ and so $n \mid 2d$. But n is odd so $n \mid d$ and the thesis is proved. □

Theorem 3.23. *Let n be an integer and k a field of characteristic not diving n which contains $\zeta + \zeta^{-1}$ for ζ a primitive n-th root of unity. Then*

$$1 \leq \operatorname{ed}_k \mathbb{Z}/n \leq \operatorname{ed}_k D_n \leq 2 \, .$$

Moreover if n is odd

$$\operatorname{ed}_k \mathbb{Z}/n = \operatorname{ed}_k D_n = 1 \, .$$

Proof. The previous lemma easily implies the upper bounds, together with the fact that $\mathbb{Z}/n < D_n$. We need to show that $\operatorname{ed}_k \mathbb{Z}/n \geq 1$. But then $\mathbb{Z}/n$ becomes isomorphic to μ_n on $k(\zeta)$ and so

$$\operatorname{ed}_k \mathbb{Z}/n \geq \operatorname{ed}_{k(\zeta)} \mathbb{Z}/n = \operatorname{ed}_{k(\zeta)} \mu_n = 1 \, .$$

□

Corollary 3.24. *For every field k we have* $\mathrm{ed}_k(\mathbb{Z}/3) = \mathrm{ed}_k(D_3) = 1$.

Proof. If k is of characteristic 3 we already knew the result from the Artin-Schreier exact sequence. Suppose now that k has characteristic coprime with 3. Then if ζ is a primitive root of unity we have $\zeta + \zeta^{-1} = 1 \in k$ and so we may apply the previous theorem. □

3.7 Groups of multiplicative type

In this section I want to present an original result about the essential dimension of groups of multiplicative type. As we have seen if the base field has not enough roots of unity the computation of essential dimension of finite constant group is significantly harder. In [Led02] Ledet has proved that the essential dimension of a twisted form of μ_{p^r} for a prime p is less or equal to $\varphi(p-1)p^{r-1}$. So, in particular, if k has not characteristic p

$$\mathrm{ed}_k \mathbb{Z}/p^r \leq \varphi(p-1)p^{r-1}\,.$$

Here we generalize his methods to get a bound on the essential dimension of twisted forms of $\mu_{p^r}^n$.

Our bound will be a direct consequence of lemma 3.19 and lemma 2.38.

Theorem 3.25. *Let G a group of multiplicative type over k with character module Λ. Consider the natural suriective map*

$$\varepsilon : \mathbb{Z}^\Lambda \to \Lambda$$

which sends e_λ to λ for each $\lambda \in \Lambda$. Then if $M \subseteq \mathbb{Z}^\Lambda$ is a Γ-submodule such that $\varepsilon(M) = \Lambda$ then

$$\mathrm{ed}_k G \leq \mathrm{rk}\, M$$

Proof. If we denote by T, T' the algebraic tori associated with the modules $M, \mathbb{Z}^X$ we have that there is a monomorphism of algebraic groups $G \to T$ which factors through T'. Then the map

$$H^1(K, G) \to H^1(K, T)$$

factors through $H^1(K, T') = 0$ and so is the null map. Then, by proposition 3.19

$$\mathrm{ed}_k(G) \leq \dim T = \mathrm{rk}\, M\,.$$

□

Thanks to the previous theorem we may reduce bounds on the essential dimension of groups of multiplicative type to the existence of certain subrepresentation of their character module.

Let Γ be a profinite group and M a Γ-module. Then a **pure subrepresentation** of M is a Γ-submodule which is pure as a $\mathbb{Z}$-submodule[1]. We will call

[1] Recall that a $\mathbb{Z}$-submodule N of a module M is pure if and only if the quotient M/N is torsion-free.

a representation **pure irreducible** if it has no nontrivial pure subrepresentations.[2]

The maps $R \mapsto R \otimes_{\mathbb{Z}} \mathbb{Q}$ and $S \mapsto S \cap M$ give a correspondence between pure subrepresentation of M and subrepresentation over $\mathbb{Q}$ of $M \otimes_{\mathbb{Z}} \mathbb{Q}$. It is easy to check that this is a bijective correspondence and that sends pure irreducible representations in irreducible representations.

Lemma 3.26. *Let $q = p^r$ be a prime power and consider the regular representation R of $\mathbb{Z}/q^\times$. Let $\varepsilon : R \to \mathbb{Z}/q$ be the canonical augmentation map (which sends e_l to l). Then there is an unique minimal pure subrepresentation $S \subseteq R$ with the property that $\varepsilon(S) = \mathbb{Z}/q$. Moreover S has $\mathbb{Z}$-rank $\varphi(p-1)p^{r-1}$.*

Proof. We will first treat the case in which p is an odd prime. Then $\mathbb{Z}/q^\times$ is a cyclic group of order $\varphi(q)$. If we make a choice of a generator l we can identify its group algebra with the commutative ring

$$\mathbb{Z}[T]/(T^{\varphi(q)} - 1)$$

Then the augmentation map ε is simply the map of rings that sends T to l. Now observe that the pure subrepresentations are in bijective correspondance with the ideals of the ring

$$\mathbb{Q}[T]/(T^{\varphi(q)} - 1)$$

which are principal and generated by $P(T)$ where $P(T) \mid T^{\varphi}(q)-1$. If we choose the P to be monic polynomials the Gauss lemma ensures that they generate also the corresponding pure subrepresentations over $\mathbb{Z}$. Now recall that in $\mathbb{Z}/p$ we have $\Phi_{p^h d}(T) = (\Phi_d(T))^{\varphi(p^h)}$ where the Φ are cyclotomic polynomial and $p \not| d$.

So we have that $\Phi_d(l) \in \mathbb{Z}/q^\times$ if and only if d is of the form $p^h(p-1)$. So it is easy to see that the minimal pure subrepresentation such that the augmentation map is surjective is that generated by the product of Φ_{dp^h} where $d \mid p-1$ but $d \neq p-1$ and $0 \leq h \leq p-1$. That subrepresentation is isomorphic to

$$\mathbb{Z}[T]/(\prod_{h=0}^{p-1} \Phi_{(p-1)p^h})$$

and so has rank

$$\sum_{h=0}^{r-1} \varphi((p-1)p^h) = \varphi(p-1)\left(1 + (p-1)\sum_{h=1}^{r-1} p^{h-1}\right) = \varphi(p-1)p^{r-1}\,.$$

To do the case $p = 2$ it is sufficient to note that there is no proper pure subrepresentation such that ε is surjective. In fact note that the ring algebra is

$$\mathbb{Z}[T, S]/(T^{2^{n-2}} - 1, S^2 - 1)$$

[2] We note here that in most texts in integral representation theory the adjective "pure" is dropped.

Then every subrepresentation of lesser rank is composed of zerodivisors of the ring algebra. From elementary commutative algebra we see that zerodivisors are all contained in ideals of the form

$$(\Phi_{2^h}(T), S \pm 1)\,.$$

By the prime avoidance principle then our subrepresentation is contained in one ideal of this form. But now it is a simple check that ε is not surjective when restricted to any of them (in particular it can't have odd values). □

Now we can prove the main theorem of this section.

Theorem 3.27. *Let G a twisted form of $\mu_{p^r}^n$ over a field k. Then*

$$\operatorname{ed}_k G \leq \varphi(p-1)p^{n(r-1)}\frac{p^n-1}{p-1}$$

Proof. The character module of G is $\Lambda = (\mathbb{Z}/p^r)^n$ with an action of Γ_k. We want to find a linear $GL_n(\mathbb{Z}/p^r)$-invariant submodule of $\mathbb{Z}^\Lambda$ which suriects on to Λ. First of all we note that the set $X = \Lambda \smallsetminus p\Lambda$ is the only orbit for the action of $GL_n(\mathbb{Z}/p^r)$ which generates Λ as a module. So surely we can restrict our attention to $\mathbb{Z}^X$. We observe that $\#X = p^{rn} - p^{n(r-1)}$

Consider now the action of $(\mathbb{Z}/p^r)^\times$ on Λ via scalar matrix multiplication. This decomposes X in orbits of cardinality $p-1$, corresponding to elements of $\mathbb{P}^{n-1}(\mathbb{Z}/p^r)$, since the action is free. So this gives a decomposition of $\mathbb{Z}^X$ as a $(\mathbb{Z}/p^r)^\times$-module:

$$\mathbb{Z}^\Lambda = \mathbb{Z} \oplus \bigoplus_{a \in \mathbb{P}^{n-1}(\mathbb{Z}/p^r)} \mathbb{Z}^a$$

Note that for each $a \in \mathbb{P}^{n-1}(\mathbb{Z}/p^r)$ the $(\mathbb{Z}/p^r)^\times$-representation $\mathbb{Z}^a$ is regular (since the actio on a is freely transitive).

Now for each $a \in \mathbb{P}^{n-1}(\mathbb{Z}/p^r)$ we can take R_a the only pure subrepresentation of $\mathbb{Z}^a$ whose existence is granted by the previous lemma and take

$$R = \bigoplus_{a \in \mathbb{P}^{n-1}(\mathbb{Z}/p^r)} R_a$$

I claim that R is a $GL_n(\mathbb{Z}/p^r)$ pure subrepresentation which surjects onto Λ. That surjects is trivial, since each R_a surjects onto $\mathbb{Z}/p \cdot a$. Moreover if $g \in GL_n(\mathbb{Z}/p^r)$ we have that g is an isomorphism between $\mathbb{Z}^a$ and $\mathbb{Z}^{ga}$, so it must be an isomorphism betweem R_a and R_{ga} (since they are the only pure irreducible subrepresentations which surjects onto the corresponding $\mathbb{Z}/p^r \cdot a$). So $gR = R$.

At last we note that $\operatorname{rk} R = \#\mathbb{P}^{n-1}(\mathbb{Z}/p^r) \cdot \operatorname{rk} R_a = \varphi(p-1)p^{n(r-1)}\frac{p^n-1}{p-1}$. Now since R is $GL_n(\mathbb{Z}/p^r)$-invariant is also clearly Γ_k-invariant and the thesis follows from theorem 3.25. □

Remark 3.28. *Note that our bound is very poor in the case of* $(\mathbb{Z}/p^r)^n$*. In fact, since the essential dimension of a product is less or equal the sum of essential dimensions*

$$\operatorname{ed}_k (\mathbb{Z}/p^r)^n \leq n \operatorname{ed}_k \mathbb{Z}/p^r \leq n\varphi(p-1)p^{r-1} < \varphi(p-1)p^{n(r-1)} \frac{p^n - 1}{p-1} .$$

Bibliography

[AD07] Zinovy Reichstein Alexander Duncan. Versality of algebraic group actions and rational points on twisted varieties, 2007.

[BF03] G. Berhuy and G. Favi. Essential dimension: a functorial point of view (after A. Merkurjev). *Doc. Math*, 8:279–330, 2003.

[BF04] Grégory Berhuy and Giordano Favi. Essential dimension of cubics, 2004.

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raunaud. *Néron Models*. Ergebnisse der Mathematik und Ihrer Grenzgebiete. Springer-Verlag, 1990.

[BR97] J. Buhler and Z. Reichstein. On the essential dimension of a finite group. *Compositio Mathematica*, 106(2):159–179, 1997.

[DG70] M. Demazure and P. Gabriel. *Groupes algébriques. Tome I: Géométrie algébrique. Généralités. Groupes commutatifs.* North-Holland, 1970.

[SGA3] M. Demazure and A. Grothendieck. *Schemas En Groupes (Sga 3): Proprietes Generales Des Schemas En Groupes.* Documents mathématiques. Société mathematique de France, 2011.

[Dun09] Alexander Duncan. Essential Dimensions of A_7 and S_7, August 2009.

[KM08] N.A. Karpenko and A.S. Merkurjev. Essential dimension of finite p-groups. *Inventiones Mathematicae*, 172(3):491–508, 2008.

[Lan02] S. Lang. *Algebra*. Graduate Texts in Mathematics. Springer-Verlag, 2002.

[Led02] A. Ledet. On the essential dimension of some semi-direct products. *Canadian Mathematical Bulletin*, 45(3):422–427, 2002.

[Mil80] J.S. Milne. *Étale Cohomology*. Princeton Mathematical Series. Princeton University Press, 1980.

[Mil08] J.S. Milne. Class field theory (v4.00), 2008. Available at www.jmilne.org/math/.

[Rei00] Z. Reichstein. On the notion of essential dimension for algebraic groups. *Transformation Groups*, 5(3):265–304, 2000.

[RV11] Zinovy Reichstein and Angelo Vistoli. A genericity theorem for algebraic stacks and essential dimension of hypersurfaces, April 2011.

[Vis07] A. Vistoli. Notes on grothendieck topologies, fibered categories and descent theory. *arXiv:math/0412512v4*, 2007.

[Wat79] W.C. Waterhouse. *Introduction to affine group schemes*, volume 66. Springer, 1979.

Acknowledgements

Thanks to my advisor, prof. Angelo Vistoli. In these years he believed in me and helped me to do what I did.

Thanks to Maria and Eleonora. Thanks for the long hours of study together, thanks for the evenings spent playing, cooking or simply watching a movie. Thanks for being something more than room neighbours or study mates.

Thanks to Bolzo and Enri, for providing cars when we wanted to do some trip. Thanks for the time spent playing, walking and doing jokes.

Thanks to all the class of 1988: Roberto, Mattia, Soba... . Expecially during the first years we have been strongly tied together. No other year will ever be the same.

Thanks to Fabrizio, Marco, Pietro, Giove, Alessandra and all the others with which I spend my time. Thanks for your presence these years. I will never forget it.

Thanks to Gennady. The discussions about math, life, the universe and everything are something I know I will miss dearly. It was something more than chatting, but with all the same leisure. The lectures of russian will come in handy too.

Thanks to all people who have been close with me, too many to name. I will remember you all.

Thanks to all my relatives, who have been always made me feel near them. Thanks for your support and your presence.

Thanks to my mother, who waited at home for any time I returned. Thanks for the wonderful lunches and dinners that you prepared me when I arrived late in the evening tired and hungry. Thanks for caring for all things that needed to be done, from burocreacy to the lawn. Thanks for being so strong in the difficult times that have been, always without complaining.

Thanks to Alessio, who always cheered me up. Thanks for your music and for your passion. Thanks for your will of trying always new things and for your energy.

Thanks to Sara, my love, for forgiving with my distance and my moments of forgetfulness. Thanks for being there when I needed you and for being patient when I couldn't be there if you needed me. Thanks for never letting me feel alone, and for always giving me a reason to continue when didn't see one. Thanks for giving me the best time I ever had, with you. You are part of my life, and you will always be.

Thanks to everyone I came across during these five wonderful years. If they have been the best years of my life it is also because of you.

Thanks to my father, for being the exceptional person you were. I will remember you forever.

Ringraziamenti

Grazie al mio relatore, prof. Angelo Vistoli. In questi anni ha creduto in me e mi ha aiutato a fare quello che ho fatto.

Grazie a Maria e Eleonora. Grazie per le lunghe ore di studio assieme, grazie per le sere spese a giocare o semplicemente a guardare un film. Grazie per essere state qualcosa di più che vicine di stanza o compagne di studi.

Grazie a Bolzo e Enri, per averci sempre fornito macchine quando volevamo andare a farci un giro. Grazie per il tempo speso a giocare, chiacchierare, passeggiare e a fare scherzi.

Grazie a tutta la classe del 1988: Roberto, Mattia, Soba... Specialmente durante i primi anni siamo stati molto legati. Nessun altro anno sarà mai lo stesso.

Grazie a Fabrizio, Marco, Pietro, Giove, Alessandra e tutti gli altri con cui passo il mio tempo. Grazie per la vostra presenza questi anni. Non lo dimenticherò mai.

Grazie a Gennady. Le discussioni sulla matematica, la vita, l'universo e tutto quanto sono qualcosa che mi mancherà molto. È qualcosa di più di chiacchierare, ma latrettanto piacevole. Anche le lezioni di russo saranno utili.

Grazie a tutte le persone che mi sono state vicine, troppe per nominarle. Vi ricorderò tutti.

Grazie a tutti i miei parenti, che mi hanno sempre fatto sentire vicino. Grazie per il supporto e la presenza.

Grazie a mia mamma, che mi ha aspettato a casa ogni volta che tornavo. Grazie per i meravigliosi pranzi e cene che mi hai preparato quando arrivavo tardi alla sera affamato e stanco. Grazie per aver avuto cura di tutte le cose che bisognava fare, dalla burocrazia al prato. Grazie per essere stata così forte nei momenti difficili che ci sono stati, sempre senza mai lamentarti.

Grazie ad Alessio che mi ha sempre tirato su. Grazie per la tua musica e la tua passione. Grazie per la tua volontà di provare cose sempre nuove e per la tua energia.

Grazie a Sara, il mio amore, per avermi perdonato i momenti di distanza e dimenticanza. Grazie per esserci stata quando avevo bisogno di te e per essere stata paziente quando non potevo esserci se avevi bisogno di me. Grazie per non avermi mai fatto sentire solo e per avermi dato una ragione per continuare quando non ne vedevo una. Grazie per avermi dato i migliori momenti che io abbia mai avuto, con te. Sei parte della mia via e lo sarai sempre.

Grazie a tutti quelli che ho incrociato in questi cinque meravigliosi anni. Se sono stati i migliori anni della mia vita è anche grazie a voi.

Grazie a mio papà, per essere stato la persona eccezionale che eri. Ti ricorderò per sempre.