UNIVERSITÀ DI PISA

DIPARTIMENTO DI MATEMATICA

TESI DI LAUREA MAGISTRALE

ON THE ESSENTIAL DIMENSION OF CENTRAL SIMPLE ALGEBRAS

Relatore:
Prof. Angelo VISTOLI

Candidato:
Justin LACINI

Controrelatore:
Prof. Marco FRANCIOSI

ANNO ACCADEMICO 2014/2015

Contents

Introduction

In this thesis we present the notion of essential dimension and give estimates for the essential dimension of the algebraic group PGL_n. Essential dimension was introduced for finite groups by J.Buhler and Z.Reichstein in [5] and was extended to the class of algebraic groups over algebraically closed fields by Z.Reichstein in [25]. Later A.Merkurjev generalized it to functors in his notes [19]; we will follow this approach.

The essential dimension of an algebraic object is a formalization of the familiar concept of minimal number of 'parameters' needed to describe it and thus gives an idea of the complexity of its structure. Let us consider for example the case of quadratic extensions of a field. Fix k a base field, K/k an extension and suppose that L/K is a quadratic extension of K. If $char(k) \neq 2$ the resolution formula of equations of degree 2 tells us that L is generated by a square root of an element in K, so that $F = K(\alpha)$, where $\alpha^2 = a \in K$. It follows then that the extension L/K is in fact defined on the smaller field $k(a)$, since $L \simeq k(\alpha) \otimes_{k(a)} K$. This means that it is suffices a single parameter to describe quadratic extensions of fields, namely that their essential dimension is at most 1. It should be noted, however, that for the extension $k(t^{1/2})/k(t)$, where t is algebraically independent over k, there is not a minimal field of definition; there is instead a minimal value of the transcendence degree of the fields over which it is defined, and we will take this as a measure of the complexity.

More formally, consider a functor F from the category of field extensions of a fixed base field k to the category of sets. Let L/k an extension and $a \in F(L)$ an element. We will say that a descends to a sub-field $k \subseteq K \subseteq L$ if there exists an element $b \in F(K)$ such that b is mapped to a by the map $F(K) \to F(L)$. The essential dimension of a is the least transcendence degree among the fields to which descends, and the essential dimension of the functor F is the supremum of the essential dimensions of elements $a \in F(K)$ for K any extension of k. This generality makes the notion of essential dimension very flexible since it is applicable to many cases of interest: for example, $F(K)$ could be the class of isomorphism of quadratic forms on K^n, or of n-dimensional K-algebras, or of elliptic curves defined over K, and so on. In general we think of F as specifying the type of algebraic object we want to work with.

Essential dimension, which is defined in elementary terms, has surprising connections to many problems in algebra and algebraic geometry. For instance, consider the functor F that associates to the field K the classes of isomorphism

of central simple algebras of degree n over K; for an extension L/K the maps $F(K) \to F(L)$ are given by base change. Let's see how the essential dimension of a central simple algebra gives important information on its structure. Recall that a central simple algebra A/K of degree n is a crossed product if it contains a commutative Galois sub-algebra L/K of degree n. Let us restrict to the case in which the degree is a prime power $n = p^r$. In 1972 Amitsur [1] showed that for $r \geqslant 3$ a generic division algebra of degree p^r is not a crossed product, solving a long-standing open problem. For $r = 1, 2$ it is not known whether or not every central simple algebra A of degree p^r is a crossed product. If the answer was positive for the case $r = 1$, that would imply that every central simple algebra of prime degree is cyclic. If the base field contains a primitive n-th root of unity ω, a cyclic algebra has a very simple presentation: there exist $a, b \in K^*$ such that it is isomorphic to the algebra generated by the symbols x and y with relations $x^n = a$, $y^n = b$ and $xy = \omega yx$. We see therefore that a cyclic algebra is defined over the field $k(a, b)$ for suitable $a, b \in K$ and consequently that its essential dimension is at most 2. It is clear then that if every central simple algebra of prime degree was a crossed product the essential dimension of F would be 2. This is indeed true for $p = 2, 3$: the case $p = 2$ is easy and the case $p = 3$ was solved by Wedderburn in 1921 [36]. The case of general p is however very much open and the lower bounds that we present for the essential dimension of F become trivial in this case.

This thesis is divided into four parts. In the first part we give a brief introduction of the theory of central simple algebras by sketching the main facts. Particular attention is given to crossed products and to the cohomological description of the Brauer group. We also discuss Azumaya algebras, which are a generalization of central simple algebras to commutative rings.

In the second part, we explain the very important relation between PGL_n-torsors, Azumaya algebras and Brauer-Severi schemes, using descent theory.

In the third part we focus on general theorems about essential dimension. We discuss versal pairs and show that in the case of a smooth algebraic groups G, there generic fibers of torsors rising from representations are versal. This is useful for computations and gives one of the main methods to estimate essential dimension. We will also discuss the notion of essential p-dimension, which is often easier to compute.

In the fourth part we give bounds of the essential dimension of PGL_n. Upper bounds are given by studying the structure of the universal division algebra, while lower bounds rely on an important result about the essential dimension of algebraic tori.

Notation

Here we fix the notation that will be used in the sequel.

We will usually denote by k the base field. Other fields will be denoted by capital letters K, F, E, L and L/K will denote an extension. The category of field extension of k with field maps fixing k is $\mathcal{C}_k$. The rings we consider are unitary, but not necessarily commutative. They will usually be denoted by letters A, B, and D in the case of division rings; the notation A^{op} will denote the opposite ring. Homomorphisms of rings are supposed to take the unit into the unit. Modules over a ring are also unitary, meaning that $1 \cdot m = m$ for every $m \in M$ and M a module. The group of $n \times n$ matrices over a ring R is $M_n(R)$.

Chapter 1

Noncommutative rings

In this chapter we introduce the theory of non-commutative algebras. This is a very well-known theory and here we will only give the basic definitions and state the results we need, mainly without proofs. We will be particularly interested in the case of central simple algebras, which are one of the main objects of study in this thesis. Unless explicitly stated, rings in this section are not assumed to be commutative. Our standard references are [13], [15] and [10].

1.1 General properties

When talking about modules we will implicitly mean right modules.

Definition 1.1.1. A module M over a ring A is *simple* if it is non-zero and has no non-trivial sub-modules.

Definition 1.1.2. A *division ring* is a non-zero ring such that every non-zero element has an inverse.

Modules over division rings have many of the familiar properties of vector spaces and in particular they always admit a basis.

The following is a simple and important result known as Schur's lemma.

Lemma 1.1.3. Let M be a simple module over a ring A. Then $End_A(M)$ is a division ring.

Proof. See [13, Theorem 1.1.1]. □

Proposition 1.1.4. Consider a module M over a ring A. The following are equivalent:
1) M is a sum of simple modules
2) M is a direct sum of simple modules
3) for any sub-module $N \subseteq M$ there exists a sub-module N' such that $M \cong N \oplus N'$.

Proof. See [15, Theorem 2.4]. □

Definition 1.1.5. A module M over a ring A is *semi-simple* if it has one of the equivalent properties of the previous proposition.

Definition 1.1.6. A ring is *semi-simple* if it is semi-simple as a right module.

Lemma 1.1.7. Quotients and sub-modules of semi-simple modules are semi-simple.

Proof. This is an easy application of characterization (3) of semi-simplicity. In fact, suppose that M is a semi-simple R-module, N a sub-module, and P a quotient.

If T is a sub-module of N, it is also a sub-module of M, so that there exists a sub-module U such that $M \cong T \oplus U$. It is easy then to see that $N \cong T \oplus (U \cap N)$, which shows that N is semi-simple.

If S is a sub-module of P, consider its lifting S' to M and take again W such that $M \cong S' \oplus W$. Then W maps into a sub-module of P and P is a direct sum of this module and S. □

It is easy to see from the previous lemma that A is semi-simple as a ring if and only if every right module is semi-simple.

Suppose now that A is semi-simple and write $A \cong \oplus_{j \in J} I_j$ where I_j are right ideals of A. The identity of A is expressed as a finite sum, so J is also finite. Furthermore if we write $A \cong A_1 \oplus A_2 \oplus \cdots \oplus A_s$ where we group together the isomorphic components, the A_i are uniquely determined up to isomorphism, they are two-sided ideals and have a ring structure such that $A \cong A_1 \times A_2 \times \cdots \times A_s$.

Definition 1.1.8. In the above notation, a ring A is *simple* if it is semi-simple and $s = 1$, that is there is only one simple right module up to isomorphism.

We want to give now a very important structure theorem for semi-simple rings, which is due to Wedderburn. One first needs the following lemma.

Lemma 1.1.9. Let D be a division ring, V a finite dimensional D-module and $A = End_D(V)$. The natural homomorphism $D \to End_A(V_A)$ is an isomorphism.

Proof. See [15, Theorem 3.3]. □

Theorem 1.1.10 (Wedderburn)**.** Let A be any semi-simple ring. Then $A \cong M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$ for suitable division rings $D_1, ..., D_r$ and positive integers $n_1, ..., n_r$. The number r is uniquely determined, as are the pairs $(n_1, D_1), ..., (n_r, D_r)$ up to permutation and isomorphism. There are exactly r mutually non-isomorphic right simple modules over A.

Proof. See [15, Theorem 3.5]. □

We now introduce an important tool in the characterization of semi-simple rings.

Definition 1.1.11. Let A be a ring. The Jacobson radical of A is the intersection of all maximal right ideals; it is denoted by $J(A)$.

The Jacobson radical is immediately seen to be a right ideal, but in fact is a two-sided ideal. It has many different characterizations, see for example [13], pages 9 - 10 - 11. We will use the following.

Proposition 1.1.12. Let A be a ring. The Jacobson radical of A is the set of elements of A such that annihilate every simple A-module.

Definition 1.1.13. A ring A is a *k-algebra* if there is a map of rings $k \to A$ with image contained in the center of A. We say that it is finite dimensional algebra if it is so as a vector space over k. We say that it is *central* if its center is k.

An immediate corollary of the Wedderburn theorem is the classification of central simple algebras over algebraically closed fields.

Corollary 1.1.14. Let k be an algebraically closed field. Then every central simple algebra is isomorphic to $M_n(k)$ for some n.

Proof. This follows from Wedderburn's theorem and the fact that there are no non-trivial finite dimensional division algebras over algebraically closed fields. See [10, Corollary 2.1.7] or [13, Lemma 2.1.5]. □

Theorem 1.1.15. A finite dimensional algebra A over k is semi-simple if and only if its Jacobson radical is zero.

Proof. Suppose that A is semi-simple and write $A \cong A_1 \oplus \cdots \oplus A_n$ with each A_i being simple. Let $x \in J(A)$. From Proposition 1.1.12 we have that $A_i x = 0$ for each $1 \leqslant i \leqslant n$, and so $Ax = 0$, which means $x = 0$.

Conversely, suppose that $J(A) = 0$. The algebra A is finite-dimensional and so there are only finitely many maximal right ideals: call them $I_1, ..., I_n$. But then we have that A is isomorphic to a sub-module of $A/I_1 \oplus \cdots \oplus A/I_n$, which is semi-simple. From Lemma 1.1.7 we have that A is semi-simple. □

Observe that we used the fact that A is finite dimensional only in the second part of the proof.

From the theorem it is easy to deduce the following.

Theorem 1.1.16. A finite dimensional algebra A over k is simple if and only if it is non-zero and has no non-trivial two-sided ideals.

Proof. Suppose that $A \neq 0$ and that it has no non-trivial two-sided ideals. Then the Jacobson radical, which is a two-sided ideal, is null and so from the previous theorem A is semi-simple. In fact A is simple, because we can write $A \cong A_1 \oplus \cdots \oplus A_n$ with A_i two-sided ideals which are simple rings; the hypotheses forces $n = 1$.

On the other hand, suppose that A is simple. Suppose also that $I \subseteq A$ is a two-sided ideal such that $I \neq 0, A$. The ring A is in particular semi-simple,

so there exists a right ideal J such that $A \cong I \oplus J$ as right A-modules. If V is a simple right A-module, we have that $I \cong V^s$ and $J = V^r$. Recall that the automorphisms of A as a right A-module are given by left multiplication of elements of A, so that they necessarily are automorphisms of I. But from the presentation we discussed, we can switch two copies of V in I and J with and A-module automorphism, which is absurd. We deduce then that no I with the supposed properties can exist. □

We end this brief treatment mentioning a particular case of algebras that arise from representations. Let G be a group and define the algebra $k[G]$ to be the vector space spanned by linearly independent elements e_g for $g \in G$ and with multiplication given by linear extension of the rule $e_g \cdot e_h = e_{gh}$. It is immediate that left $k[G]$ modules correspond to G-representations. We will need the following important classical result due to Maschke.

Theorem 1.1.17. Let G be a finite group and k a field of characteristic zero or coprime with the order of G. Then the ring $k[G]$ is semi-simple.

Proof. See [13, Theorem 1.4.1]. □

1.2 Central simple algebras

We restrict our attention now to the special case of finite dimensional algebras over a field k that are both simple and central. These are called *central simple algebras*. We will not specify the base field when it is clear from the context.

From the Wedderburn theorem we know that every central simple algebra is a matrix ring with coefficients in a division ring, but in fact much more can be said. Let's begin with a technical result, which is very important in the study of central simple algebras.

Theorem 1.2.1. Let A and B be two simple algebras over k; suppose also that A is central. Then the algebra $A \otimes_k B$ is simple and $Z(A \otimes_k B) = Z(B)$.

Proof. See [13, Lemma 4.1.1]. □

In particular if both A and B are central simple algebras, their tensor product is also central simple over the same field, meaning that the class of central simple algebras over a field is closed by tensor product. Moreover, if K/k is any extension, the algebra $A \otimes_k K$ is central simple over K, so we have a natural extension of scalars.

If A is a central simple algebra, it is clear that so is the opposite algebra A^{op}. Being this association intrinsic, it is natural from the above to investigate the nature of $A \otimes_k A^{op}$.

Proposition 1.2.2. If A is a central simple algebra, then $A \otimes_k A^{op} \cong End_k(A)$.

Proof. See [13, Theorem 4.1.3]. □

Definition 1.2.3. Let A be a central simple algebra over the field k. A field K/k is a *splitting field* for A if $A \otimes_k K$ is isomorphic to $M_n(K)$ for some n. We shall also say that K *splits* A or that A is split over K.

It follows from Corollary 1.1.14 and Theorem 1.2.1 that an algebraically closed field over k is always a splitting field. The dimension as a vector space is invariant for extension of scalars, so we see that the dimension over k of every central simple algebra is a square.

We give now two definitions that play an essential role in the theory of central simple algebras.

Definition 1.2.4. Let A be a central simple algebra, and D a division algebra such that A is isomorphic to $M_n(D)$ for some n. The number $\sqrt{dim_k(A)}$ is the *degree* of A and the number $\sqrt{dim_k(D)}$ is the *index* of A.

There is an important relation between splitting fields and fields contained in a division algebra. In fact maximal sub-fields are splitting fields, and splitting fields of minimal degree can be embedded in the division algebra. One can ask if there are maximal fields which have nice properties; while it is always possible to find a separable maximal field, there are division algebras that do not admit maximal fields that are Galois over their center. We begin with a technical lemma.

Lemma 1.2.5. Let A be a central simple algebra and K/k a splitting field of finite degree. Then $ind_k(A)$ divides the degree of the extension.

Proof. According to the Wedderburn theorem $A \cong M_n(D)$ for some division algebra D, determined up to isomorphism. Let $m = ind_k(A) = \sqrt{dim_k D}$. We have that $A \otimes_k K \cong M_n(D \otimes_k K)$, so K is a splitting field also for D, and $D \otimes_k K \cong M_m(K)$. It follows that K^m has a natural structure of left D-module and

$$m \cdot [K : k] = dim_k K^m = (dim_k D) \cdot (dim_D K^m) = m^2 \cdot dim_D K^m$$

The thesis follows by $[K : k] = m \cdot dim_D K^m$. □

Remark 1.2.6. Let D be a central simple division algebra over k and K/k be a finite extension of degree $n = deg_k(D)$ that is also a splitting field for D. Then $dim_D K^n = 1$ so that D and K^n are isomorphic as D-modules. From the fact that $D \otimes_k K \cong M_n(K)$ we have that $K \subseteq End_D(K^n) \cong End_D D = D$.

A converse of the remark is given by the following theorem.

Theorem 1.2.7. Let D be a finite division algebra over k. If K is a maximal field in D containing k then the degree of the extension K/k is equal to the degree of D and K is a splitting field for D.

Proof. See [13, Corollary and Theorem 4.2.2]. □

Theorem 1.2.8. If D is a finite division algebra over k, then it admits a separable maximal subfield over k.

Proof. See [13, Theorem 4.3.3]. □

Definition 1.2.9. Let A be a central simple algebra. If A contains a Galois extension of K of degree equal to the degree of A, then A is called a *crossed product*.

It has been for a long time an open question whether all algebras were crossed products, until Amitsur gave a counterexample in 1972, [1].

A particular case of crossed products are cyclic algebras.

Definition 1.2.10. A central simple algebra over k is *cyclic* if contains a cyclic extension of the center of degree equal to the degree of A.

Crossed products and in particular cyclic algebras, have a nice description of the algebra structure. In order to obtain it, we first need an important theorem, known as Skolem-Noether theorem.

Theorem 1.2.11 (Skolem-Noether)**.** Let A be a central simple algebra over k and $B \subseteq A$ a simple sub-algebra over k. If $f : B \to A$ is an algebra homomorphism, it exists an invertible element a of A such that $f(x) = axa^{-1}$ for all x in B.

Proof. See [13, Theorem 4.3.1]. □

Theorem 1.2.12. Let A be a cyclic central simple algebra over k of degree n and let K/k be a maximal sub-field cyclic of degree n over k. Then there exists an element $a \in A^*$ such that $A \cong K \oplus aK \oplus \cdots \oplus a^{n-1}K$ as a K-vector space.

Proof. The algebra A has a $K \otimes_k K$-module structure given by $(e \otimes f)(x) = exf$ for $e, f \in K$ and $x \in A$. There is an isomorphism $\varphi : K \otimes_k K \to K^n$ defined as $\varphi(e \otimes f) = (e\sigma(f), e\sigma^2(f), \cdots, e\sigma^{n-1}(f))$, where σ is a generator of the Galois group of K over k. Consider the projections $\pi_i : E^n \to E$ on the i-th component; the algebra A is then isomorphic as a $K \otimes_k K$-module to $\varphi^{-1}(Ker(\pi_1))A \oplus \cdots \oplus \varphi^{-1}(Ker(\pi_n))A$. A simple calculation shows that $Ker(\pi_i)$ is generated over k by elements of the form $\sigma^i(e) \otimes 1 - 1 \otimes e$, so that calling $A_i = \{x \in A | such\ that\ \sigma^i(e)x = xe\ for\ all\ e \in K\}$, we have $A = A_1 \oplus \cdots \oplus A_n$.

Using the Skolem-Noether theorem, there exists an element $a \in A^*$ such that $\sigma(e) = aea^{-1}$ for all $e \in K$, so that $A_i = \{x \in A |\ a^i ea^{-i}x = xe\ for\ all\ e \in K\}$. It is obvious that $a^i K \in A_i$, so we conclude for dimensional reasons. □

If the base field k has a primitive n-th root of unity ω then we get even nicer presentations. Choose $a, b \in k^*$ and define the algebra $(a, b)_\omega$ the algebra generated over k by the symbols x and y with relations $x^n = a$, $y^n = b$ and $xy = \omega yx$. By the previous theorem and by Kummer theory, in this case every cyclic algebra is isomorphic to the algebra $(a, b)_\omega$ for some $a, b \in k^*$.

We want to present now the important result that all division algebras of degree 3 are cyclic. We first need to define the norm and the trace for central simple algebras, which are tools that have independent interest.

Definition 1.2.13. Let A be a central simple algebra of degree n over k. The *norm* of an element $a \in A^*$ is the determinant of the linear map $x \mapsto ax$. Similarly one defines the *trace* of an element in A. The norm is a multiplicative function, whereas the trace is additive.

Let now A be a central simple algebra of degree n and K be a splitting field. If we choose an isomorphism $f : A \otimes_k K \to M_n(K)$, we can compute the determinant and the trace of $f(a \otimes 1)$. From Skolem-Noether these do not depend on the chosen isomorphism, and general theory assures that their values are in k: see for example [10] pages 37 and 38. We will call these functions *reduced norm* and *reduced trace* and denote them by Nrd_A and Trd_A respectively. They are linked to the usual norm and trace by the following result.

Proposition 1.2.14. Let A be a central simple algebra of degree n, then $N_{A/k} = Nrd_A^n$ and $Tr_{A/k} = n \cdot Trd_A$.

Proof. See [10, Proposition 2.6.3]. □

We follow the paper [12] of Haile.

Proposition 1.2.15. Let D be a central simple division algebra of degree n over k. Let K be a maximal sub-field. Then
(1) There is an element $d \in D^*$ such that $Trd(kd) = 0$ for all $k \in K$.
(2) Let d be as in (1). There is a k sub-space V of K such that $dim_k V = n-1$ and $Trd(k^{-1}d) = Trd(d^{-1}k) = 0$ for all $k \in V - \{0\}$.

In particular there is an $(n-1)$ dimensional sub-space W of D such that $Trd(w) = Trd(w^{-1}) = 0$ for all $w \in W - \{0\}$.

Proof. (1) There is a k-linear transformation U from D to $K^\vee$ given by $U(d)(k) = Trd(kd)$ for all $d \in D$, $k \in K^\vee$. The result follows comparing dimensions over k.

(2) Given d as in (1), there is a k linear map S on K given by $S(k) = Trd(d^{-1}k)$. Since $dim_k Ker(S) \geqslant n-1$ and by the choice of d, it suffices to take any $(n-1)$ dimensional subspace of $Ker(S)$.

Finally it suffices to take $W = d^{-1}V$. □

We remark that since the kernel of the map U in (1) has dimension at least $n^2 - n$, if $n \geqslant 3$ we can take $d \in Ker(U)$ and not lying in K^*.

Corollary 1.2.16. If D is a central simple division algebra of degree three over k, then there is an element $d \in D - k$ such that $d^3 \in k$.

Proof. From the proposition there is an element $d \in D^*$ such that $Trd(d) = Trd(d^{-1}) = 0$. It follows that the minimal polynomial of d over k is of the form $x^3 - a$ for some $a \in k^*$, that is $d^3 \in k$. □

Theorem 1.2.17 (Wedderburn)**.** Let D be a division algebra of degree 3. Then there is an element $d \in D - k$ such that $d^3 \in k$. Moreover if x is any element of $D - k$ such that $x^3 \in k$, then D contains a cyclic maximal subfield K such that $x \in L$ and $xLx^{-1} = L$.

Proof. By the corollary there is an element $x \in D - k$ such that $x^3 \in k$. Let $x^3 = a$ and $K = k(x)$.

Let us first note that if U and V are two-dimensional k-subspaces of K, then there is an element $c \in K$ such that $cU = V$. In fact, there exist k-linear functionals f and g in $K^\vee$ such that $U = Ker(f)$ and $V = Ker(g)$. Now $K^\vee$ is a one-dimensional K-space, so there exists an element $c \in K^*$ such that $cg = f$, and so $cU = V$.

To motivate the proof of the theorem, we first observe that if there is a cyclic maximal subfield $L = k(\theta)$ with $xLx^{-1} = L$, then $(\theta x)^3 = N_{L/k}(\theta)a \in k$ since the conjugation by x gives a generator of the Galois group of L/k. Similarly $(\theta x^2)^3 \in k$. Conversely if there is an element $\theta \in D - K$ such that $(\theta x)^3, (\theta x^2)^3 \in k$, then $L = k(\theta)$ satisfies $xLx^{-1} = L$ and hence is our desired extension being a cubic Galois extension. We have only to check that θ and $x\theta x^{-1}$ commute, because $\theta \notin K$. Let $Nrd : D^* \to k^*$ denote the reduced norm. Because $x^3, (\theta x)^3, (\theta x^2)^3 \in k$, it follows that $Nrd(x) = a$, $Nrd(\theta x) = (\theta x)^3$ and $Nrd(\theta x^2) = (\theta x^2)^3$. Moreover $Nrd(\theta x^2) = Nrd(\theta x)Nrd(x)$ and hence $(\theta x^2)^3 = a(\theta x)^3$. It follows that $x\theta x^2\theta x = a\theta x\theta$, and so $x\theta x^{-1}\theta = \theta x\theta x^{-1}$.

So it suffices to find $\theta \in D - K$ such that $(\theta x)^3, (\theta x^2)^3 \in k$. Now for any $y \in D$, we define $K_y = \{c \in K | Tr(y^{-1}c) = 0\}$. It is easy then to see that if $c \in K$, then $K_{cy} = cK_y$.

By the remark following the proposition there is an element $d \in D - K$ such that $Trd(cd) = 0$ for all $c \in K$. We claim there is an element $c \in K^*$ such that $K_{cd} \supseteq kx + kx^2$. To see this note that either $K_d = K$ (in which case the claim is proved) or $[K_d : k] = 2$. In this second case because K_d and $kx + kx^2$ are two-dimensional subspaces of K, there is an element $c \in K$ such that $cK_d = kx + kx^2$. Since $cK_d = K_{cd}$, we have proved the claim. Letting $\theta = cd$, we have $Trd(\theta x) = Tdr((\theta x)^{-1}) = Trd(\theta x^2) = Trd((\theta x^2)^{-1}) = 0$. Hence $(\theta x)^3, (\theta x^2)^3 \in k$ and we are done. □

Corollary 1.2.18. Every central division algebra of degree three is cyclic.

1.3 The Brauer Group

We have seen that the class of central simple algebras over k is closed under tensor product, which is an associative and commutative operation. It is then natural to look for a group structure in which the operation is given by the tensor product. It is indeed the case that a proper quotient of the class of central simple algebras is a group under tensor product. This group, which is called *Brauer group*, is a very important invariant of the base field k and has been studied extensively. One of the main properties of the Brauer group is that it has a cohomological description, which is quite useful.

Definition 1.3.1. Let A and B be two central simple algebras. We say that A and B are *Brauer equivalent* if $A \otimes_k M_n(k) \cong B \otimes_k M_m(k)$ for some $n, m \in \mathbb{N}$. The set of central simple algebras modulo Brauer equivalence is called *Brauer group*. We use the notation $Br(k)$.

As mentioned above, the group operation on $Br(k)$ is the tensor product: it is well-defined, associative, commutative and the inverse of an algebra is the opposite algebra by Proposition 1.2.2. For every extension of fields K/k there is a natural base-change map $Br(k) \to Br(K)$, which is an homomorphism. We denote the kernel of this map by $Br(K/k)$, and call it the *relative Brauer group*. It is clear from the definition that if A is a central simple algebra over k, then its class in $Br(k)$ is in the subgroup $Br(K/k)$ if and only if A is split by K.

We want now to present the cohomological description of the Brauer group. In order to achieve this, we have to develop a little more the theory of crossed products. Our treatment will follow that of Herstein in [13].

Proposition 1.3.2. If A is a central simple algebra over k that is split by K, then it is Brauer equivalent to a central simple algebra for which K is a maximal sub-field.

Proof. We can suppose that A is a division algebra. By Lemma 1.2.5 we have that $ind_k(A)$ divides $[K : k]$. Taking $n = [K : k]/ind_k(A)$, define $A' = A \otimes_k M_n(k)$. Now recall that Remark 1.2.6 tells us that $K \subseteq A'$. Since K is a splitting field for A', we have the thesis. □

Corollary 1.3.3. If A is a central simple algebra over k, then it is Brauer equivalent to a crossed product.

Proof. It is always possible to find a Galois splitting field. □

Now let A be a crossed product, with K maximal Galois subfield of degree n over k. Let G be the Galois group. By Skolem-Noether, for every $\sigma \in G$, there is an element $x_\sigma \in A$ such that $\sigma(c) = x_\sigma^{-1} c x_\sigma$ for all $c \in K$. The x_σ are linearly independent over K, so that their linear span over K is all of A for dimensional reasons.

If $\sigma, \tau \in G$ and $c \in K$, then the computation $x_\tau^{-1} x_\sigma^{-1} c x_\sigma x_\tau = (\sigma\tau)(c) = x_{\sigma\tau}^{-1} c x_{\sigma\tau}$ shows that $x_{\sigma\tau}(x_\sigma x_\tau)^{-1} \in K$. So $x_\sigma x_\tau = x_{\sigma\tau} f(\sigma, \tau)$ where $f(\sigma, \tau) \in K^*$ and we obtain a function $f : G \times G \to K^*$. If $\sigma, \tau, \nu \in G$, a simple computation yields the property $f(\sigma, \tau\nu) f(\tau, \nu) = f(\sigma\tau, \nu)\nu(f(\sigma, \nu))$; furthermore $x_e f(e, e)^{-1} = 1$. We isolate these properties in the following definition.

Definition 1.3.4. Let K be a normal extension of F with Galois group G. A function $f : G \times G \to K^*$ is called a *factor set* on G in K if, for all $\sigma, \tau, \nu \in G$ we have $f(\sigma, \tau\nu) f(\tau, \nu) = f(\sigma\tau, \nu)\nu(f(\sigma, \nu))$.

We have seen that when we have a crossed product we can obtain a factor set; conversely if we are give a base field k, a Galois extension K with Galois groups G, and a factor set f on G in K, we can construct a crossed product of which f is a factor set. In fact consider the algebra (K, G, f) which is the direct

sum of a copy of K for each element of G (with generator x_σ for $\sigma \in G$), with product defined by the rules $cx_\sigma = x_\sigma \sigma(c)$ and $x_\sigma x_\tau = x_{\sigma\tau} f(\sigma, \tau)$ for all $c \in K$, $\sigma, \tau \in G$. It is easy to see that (K, G, f) is indeed a central simple algebra over k and that it is a crossed product (see [13], pag 109, for more detail). Moreover it follows from what we have seen that any central simple algebra A is Brauer-equivalent to an algebra (K, G, f) for some choices of K and f. We have also proved in Proposition 1.3.2 that if K/k is a Galois extension, every class in $Br(K/k)$ is represented by an algebra (K, G, f).

It is important now to address the problem of when two algebras (K, G, f) and (K, G, g) are isomorphic. Let us begin by noticing that if we choose $\lambda_\sigma \in K^*$, the elements $y_\sigma = x_\sigma \lambda_\sigma$ span A over K and multiply by the rule $y_\sigma y_\tau = y_{\sigma\tau} \lambda_{\sigma\tau}^{-1} \tau(\lambda_\sigma) \lambda_\tau f(\sigma, \tau)$. This shows that $\lambda_{\sigma\tau}^{-1} \tau(\lambda_\sigma) \lambda_\tau f(\sigma, \tau)$ is a factor set and gives rise to an algebra isomorphic to A.

The converse is also true. Let ψ be an isomorphism of the k algebras (K, G, g) and (K, G, f), which we suppose to be generated by z_σ and x_σ respectively. Then the $y_\sigma = \psi(z_\sigma)$ induce the automorphism σ on K in A, so that $y_\sigma = x_\sigma \lambda_\sigma$ for $\lambda_\sigma \in K^*$. This shows that $g(\sigma, \tau) = \lambda_{\sigma\tau}^{-1} \tau(\lambda_\sigma) \lambda_\tau f(\sigma, \tau)$.

Definition 1.3.5. Two factor sets f, g are *equivalent* if there exists a function $\lambda : G \to K^*$ such that $g(\sigma, \tau) = \lambda_{\sigma\tau}^{-1} \tau(\lambda_\sigma) \lambda_\tau f(\sigma, \tau)$ for all $\sigma, \tau \in G$.

What we have proved is that two algebras (K, G, f) and (K, G, g) are isomorphic if and only if f and g are equivalent. Thanks to this fact, when studying crossed products, we can choose a factor set f such that $f(\sigma, e) = f(e, \sigma) = 1$ for all $\sigma \in G$. In fact, it suffices to take $\lambda(\sigma) = \sigma(f(e, e)^{-1})$ to obtain an equivalent factor set with the desired property. If f is a factor set such that $f(\sigma, e) = f(e, \sigma) = 1$ for all $\sigma \in G$ we call it *normalized*.

If f, g are two factor sets, we can define their multiplication in the obvious way and a calculation shows that we obtain again a factor set. Factor sets form a group under multiplication, with unit element the factor set which is identically 1. The factor sets that are equivalent to the unity form a subgroup and we see that the quotient group is precisely $H^2(G, K^*)$. We have seen that this group is in one-to-one correspondence with the isomorphism classes of the algebras (K, G, f). Remark 1.3.2 and ours previous considerations tell us that this induces a one-to-one correspondence between $H^2(G, K^*)$ and $Br(K/k)$. Next we prove that we have actually an isomorphism of abelian groups.

As a first step we have the following lemma.

Lemma 1.3.6. If K/k is a Galois extension with Galois group G, then $(K, G, e) \cong M_n(k)$.

Proof. See [13, Lemma 4.4.2]. □

We conclude by the following theorem.

Theorem 1.3.7. If K/k is a Galois extesion with Galois group G and if f, g are factor sets then $[(K, G, f)] \cdot [(K, G, g)] = [(K, G, fg)]$ in $Br(k)$.

Proof. See [13, Theorem 4.4.3]. □

Finally we have obtained the cohomological description of the Brauer group.

Theorem 1.3.8. Let k be a field and K/k a Galois extension with group G. Then $Br(k) \cong H^2(k)$ and $Br(K/k) \cong H^2(G, K^*)$.

We conclude this section on the Brauer group by stating some important results that are obtained thanks to the theorem.

Theorem 1.3.9. The Brauer group is a torsion group.

Proof. See [13, Theorem 4.4.4] and [10, Theorem 4.4.8]. □

Definition 1.3.10. The *period* of a central simple algebra is the order of its associated element in the Brauer group.

There is an important relationship between index and period.

Theorem 1.3.11. Let A be a central simple algebra over k. Then its period divides its index, and they have the same prime factors.

Proof. See [10, Proposition 4.5.13] or [13, Corollary], page 121. □

Theorem 1.3.12 (Brauer)**.** Let D be a central division algebra over k. Consider the primary decomposition $ind_k(D) = p_1^{m_1} \cdot p_r^{m_r}$. Then we may find central division algebras D_i for $1 \leqslant i \leqslant r$ such that

$$D \cong D_1 \otimes_k D_2 \otimes_k \cdots \otimes_k D_r$$

and $ind_k(D_i) = p_i^{m_i}$. Moreover, the D_i are uniquely determined up to isomorphism.

Proof. See [10, Theorem 4.5.16] or [13, Theorem 4.4.6]. □

1.4 Azumaya algebras

In this section we will give a very brief introduction to the theory of Azumaya algebras, which are a generalization of central simple algebras to rings. They were first studied over local rings by Azumaya [3] and then over arbitrary rings by Auslander and Goldman [2]. Our main references are [23] and [14].

Let us begin with the local case. Fix R a local ring with maximal ideal m and A a not necessarily commutative algebra over R.

Definition 1.4.1. We say that A is an *Azumaya algebra* over R if it is free of finite rank as an R-module and if the map $A \otimes_R A^{op} \to End_R(A)$ sending $a \otimes b$ to the endomorphism $x \mapsto axb$ is an isomorphism.

Proposition 1.4.2. Let A be an Azumaya algebra over R. Then A has center R; moreover, for any ideal I of A, $I \longmapsto I \cap R$ gives a bijection between the ideals of A and those of R.

Proof. See [23, IV, Proposition 1.1]. □

It follows from the previous Proposition that an Azumaya algebra over a field is a central simple algebra, and from Proposition 1.2.2 we see that in fact the converse is also true.

Proposition 1.4.3. If A is an Azumaya algebra over R and R' is a commutative local R algebra, then $A \otimes_R R'$ is an Azumaya algebra over R'. Furthermore, if B is free of finite rank as an R-module and $B \otimes_R R/m$ is an Azumaya algebra over R/m, then B is an Azumaya algebra over R.

Proof. See [23, IV, Proposition 1.2]. □

Corollary 1.4.4. If A and A' are Azumaya algebras over R, then $A \otimes_R A'$ is an Azumaya algebra over R. Furthermore, the matrix ring $M_n(R)$ is an Azumaya algebra over R.

Proof. Both statements follow from the previous Proposition and the corresponding statement for central simple algebras. □

We have a generalized Skolem-Noether theorem for Azumaya algebras in the local case.

Theorem 1.4.5 (Skolem-Noether)**.** Let A be an Azumaya algebra over R, then every automorphism of A as an R-algebra is inner.

Proof. See [23, IV, Proposition 1.4]. □

Corollary 1.4.6. The automorphism group of $M_n(R)$ as an R algebra is $PGL_n(R) = GL_n(R)/R^*$.

Proof. The algebra $M_n(R)$ is Azumaya over R and its units are $GL_n(R)$. □

We now are ready to approach the global case. From now on, R is a commutative ring and A is a R-algebra.

Definition 1.4.7. We say that A is an *Azumaya algebra* over R if it is finitely presented and for every localization at a maximal ideal m of R, we have that A_m is an Azumaya algebra over R_m in the previous sense.

Proposition 1.4.8. The following are equivalent:
1) A is an Azumaya algebra over R
2) A is finitely presented and for every localization at a prime ideal p of R, we have that A_p is an Azumaya algebra over the local ring R_p
3) A is a faithfully projective R-module such that the canonical map $A \otimes_R A^{op} \to End_R(A)$ is an isomorphism.

Proof. It follows from Proposition 1.4.3, [14, Théorème 5.1] and [14, Lemme 5.2]. □

Definition 1.4.9. We say that an R-algebra R' splits an Azumaya algebra A if $A \otimes_R R' \cong M_n(R')$.

We have seen that central simple algebras are split by a finite extension of their center. In fact a maximal subfield is always a splitting field. These results generalize to Azumaya algebras.

Proposition 1.4.10. For every maximal commutative sub-algebra S of an Azumaya algebra A over R, the product of A induces an isomorphism $A \otimes_R S \cong End_S(A)$, where A is considered as an S-module by right multiplication.

Proof. See [14, Proposition 6.1]. □

Proposition 1.4.11. Let R be a local ring and A an Azumaya algebra over R. Then A has a maximal commutative sub-algebra S such that A is a free S-module.

Proof. See [14, Théorème 6.4]. □

From the previous results, we can finally deduce the following important theorem.

Theorem 1.4.12. Let A be an R-algebra. The following are equivalent:
1) A is an Azumaya algebra over R
2) for every $p \in Spec(R)$ there is a finitely generated free R_p algebra that splits A_p
3) for every $p \in Spec(R)$ there exist $f \in R - p$ and a finitely generated free R_f algebra that splits A_f
4) There exists an etale and faithfully flat R-algebra that splits A

Proof. See [14, Théorème 6.6]. □

Proposition 1.4.13. Every endomorphism of an Azumaya algebra is an automorphism.

Proof. Being an isomorphism is a local property, and in the local case the thesis follows from Skolem-Noether. For a different point of view see [14, Corollaire 5.4]. □

Proposition 1.4.14. Let A be an Azumaya algebra over R. The group

$$Aut_R(A)/Int(A)$$

is torsion.

Proof. See [14, Corollaire 3.2]. □

Let us conclude this section with a remark on the Brauer group of a ring, which we can define in analogy with the field case. Two Azumaya algebras A_1 and A_2 are called *Brauer equivalent* if there exist two faithfully projective R-modules P_1 and P_2 such that $A_1 \otimes_R End_R(P_1) \cong A_2 \otimes_R End_R(P_2)$. The class of Azumaya algebras over R modulo Brauer equivalence has an abelian group structure, called *Brauer group*. If S is an R-algebra we have a base-change map $Br(R) \to Br(S)$.

Chapter 2

Descent theory

In this chapter we assume that the reader is familiar with descent theory and Groethendick topologies. Our references are [34] and [23]. We shall also use some basic concepts for group schemes, as in [35].

The aim here is to use descent theory to relate central simple algebras to $PGL_n(k)$-torsors and Brauer-Severi varieties.

2.1 Projective linear group scheme

Definition 2.1.1. The *fppf topology* on the category Sch/S of S-schemes is the topology in which the coverings $\{U_i \to U\}$ of an object U consist of jointly surjective collections of flat maps locally of finite presentation.

We call the category of affine schemes and scheme morphisms Aff. This is a subcanonical site with the fppf topology by [34, Theorem 2.55]. Let GL_n be the functor $Aff \to Grp$ such that $GL_n(S) = GL_n(\Gamma(S, O_S))$ for all affine schemes S. Then GL_n is represented by the group scheme

$$GL_{n,\mathbb{Z}} = Spec(\frac{\mathbb{Z}[T_{11}, ..., T_{nn}, T]}{Tdet(T_{ij} - 1)})$$

and so defines a sheaf on Aff. The group scheme $GL_{1,\mathbb{Z}}$ is just $\mathbb{G}_m$.

Consider now the functor $F : Aff \to Grp$ defined by

$$F(S) = GL_n(\Gamma(S, O_S))/\Gamma(S, O_S)^*$$

and its Zariski sheafification $\tilde{F}$. We want to show that $\tilde{F}$ is representable by an affine group scheme, which we call *projective linear group*.

Let PGL_n be the functor $Aff \to Grp$ such that $PGL_n(S) = Aut_S(M_n(S))$. It is easy to see that PGL_n is representable: indeed any automorphism of $M_n(S)$ as an S-algebra may be regarded as an endomorphism of $M_n(S)$ as an S module and thus PGL_n is a subfunctor of M_{n^2}. Futhermore, the condition that an endomorphism be an automorphism of algebras is described by polynomials,

and hence PGL_n is represented by a closed subscheme of M_{n^2}, which we call $PGL_{n,\mathbb{Z}}$. Thus PGL_n is also a sheaf for the fppf topology.

Proposition 2.1.2. The functors $\tilde{F}$ and PGL_n are isomorphic.

Proof. We have a natural transformation $F \to PGL_n$, such that if $U \in F(S)$ then $U \mapsto \varphi_U$, where $\varphi_U(X) = UXU^{-1}$. Since PGL_n is a sheaf, this natural transformation factors through $\tilde{F}$, and we want to show that this is an isomorphism.

Let S be an affine scheme. Then every automorphism of $M_n(S)$ as an S-algebra is locally in the Zariski topology inner by the Skolem-Noether theorem in the local case. It follows that there is a Zariski cover U_i of S such that the restrictions of the automorphism to the U_i is in the image of $F(U_i) \to PGL_n(U_i)$, hence the surjectivity is proved.

The proof of the injectivity is analogous. Let $a \in \tilde{F}(S)$ an element that goes to the identity. By the definition of sheafification, there exists a fppf cover U_i of S such that the restrictions of a to U_i are in the image of $F(U_i) \to \tilde{F}(U_i)$. But then these restrictions are in fact in $\Gamma(U_i, O_{U_i})^*$ since $M_n(\Gamma(U_i, O_{U_i})$ has center $\Gamma(U_i, O_{U_i})$. Then they are trivial in $F(U_i)$, and by the properties of the sheafification, a is trivial. □

In fact we have also proved the following.

Corollary 2.1.3. The sequence

$$1 \to \mathbb{G}_m \to GL_n \to PGL_n \to 1$$

is exact as a sequence of sheaves for the Zariski topology.

2.2 Equivalence

Consider the site of affine schemes Aff with the fppf topology. Consider now the category whose objects are pairs (A, R), where R is a ring and A is an Azumaya algebra over R of rank n. The morphisms from a pair (A, R) to (B, S) are maps of rings $A \to B$ and $R \to S$ such that the diagram

$$\begin{array}{ccc} R & \longrightarrow & S \\ \downarrow & & \downarrow \\ A & \longrightarrow & B \end{array}$$

is commutative. Let us call this category $Azm(n)$. It is immediate that $Azm(n)^{op}$ is fibered over Aff with respect to the functor that associates $Spec(R)$ to (A, R), the fibered product of $Spec(S) \to Spec(R)$ with A being $A \otimes_R S$. In fact this category is fibered in grupoids, since we have seen that every endomorphism of and Azumaya algebra is an automorphism.

Next, let us consider the category of PGL_n-torsors over affine schemes. An object in this category is a $PGL_{n,R}$-torsor $T \to Spec(R)$ for the fppf topology.

By descent theory every such T is affine: see for example [23, I, Theorem 2.23]. The morphisms of this category are again commutative diagrams

$$\begin{array}{ccc} U & \longrightarrow & T \\ \downarrow & & \downarrow \\ Spec(S) & \longrightarrow & Spec(R) \end{array}$$

such that the map $U \to T$ is $PGL_{n,R}$ invariant. We call this category $\mathcal{B}PGL_n$, and it is easy to see that it is fibered in grupoids over Aff.

We shall introduce one more category, but first we need the following definition.

Definition 2.2.1. A *Brauer-Severi* scheme of rank n over the affine scheme S is a scheme P over S such that there exists a flat surjective locally of finite presentation map $S' \to S$ for which $P \times_S S'$ is isomorphic to the projective space of dimension $n-1$ over S'.

Consider the category whose objects are pairs (P, X) where X is an affine scheme, and P is a Brauer-Severi scheme of rank n over S. As usual morphisms are maps

$$\begin{array}{ccc} Q & \longrightarrow & P \\ \downarrow & & \downarrow \\ Spec(S) & \longrightarrow & Spec(R) \end{array}$$

such that the diagram is commutative. This is a fibered category over Aff. We restrict our attention to the subcategory whose morphisms are cartesian diagrams, which is fibered in grupoids. We call this subcategory $BS(n)$.

Finally we can state the main result, of which we only sketch the proof.

Theorem 2.2.2. The fibered categories $Azm(n)^{op}$, $\mathcal{B}PGL_n$ and $BS(n)$ are equivalent.

Let us begin by constructing a morphism of fibered categories $F : Azm(n) \to \mathcal{B}PGL_n$. Consider an Azumaya algebra A over the ring R. We associate to A the functor $I_A : Aff/Spec(R) \to Sets$, which is defined by putting $I_A(Spec(S)) = Iso_S(M_n(S), A \otimes_r S)$, that is the set of S-isomorphisms between the matrix algebra $M_n(S)$ and $A \otimes_r S$. The functor I_A has a natural $PGL_{n,R}$ right action, given by matrix multiplication. Locally in the Zariski topology an Azumaya algebra is split by an algebra that is a free module over its center, so locally in the fppf topology Azumaya algebras are matrix algebras. From this it follows that the functor I_A is a $PGL_{n,R}$-torsor in the fppf topology. Then an application of descent theory shows that I_A is representable in $Aff/Spec(R)$ by an affine scheme T_A: see [23, III, Theorem 4.3] or [34, Theorem 4.33]. We define $F(A) = T_A$. If $f : A \to B$ and $g : R \to S$ is a morphism in $Azm(n)$ between (A, R) and (B, S), we can restrict I_A to the category $Aff/Spec(S)$, where is is represented by $T_A \times_{Spec(R)} Spec(S)$. The map f extends to a map $f_S : A \otimes_R S \to B$

which is necessarily an isomorphism. Then there is an isomorphism $T_B \to T_A \times_{Spec(R)} Spec(S)$, which gives a morphism in $\mathcal{B}PGL_n$. Thus we have defined F on objects and morphisms; it is immediate that F is a morphism of fibered categories.

Conversely, we want to show that from a PGL_n-torsor we can get an Azumaya algebra. Let $Spec(A) \to Spec(R)$ be a $PGL_{n,R}$-torsor. On $Spec(A)$ we can consider the quasi-coherent sheaf of algebras defined by the A-algebra $M_n(A)$. Of course, $M_n(A)$ is an Azumaya algebra over A. We want to give $M_n(A)$ the structure of a $PGL_{n,A}$ invariant object, and to do so we must first give an action. This is the same as giving $M_n(A)$ the structure of a $PGL_{n,A}$ comodule. Let $PGL_{n,R} = Spec(C)$. Since $Spec(A)$ is a $PGL_{n,R}$-torsor, we have a map of R-algebras $\rho : A \to A \otimes_R C$ that corresponds to the action. We have another map $p : A \to A \otimes_R C$ that corresponds to the second projection $PGL_{n,R} \times_{Spec(R)} Spec(A) \to Spec(A)$, and is defined by $p(a) = a \otimes 1$. The map $\tilde{\rho} : M_n(A) \to M_n(A) \otimes_R C$ given by ρ defines a $PGL_{n,A}$-comodule. In fact this defines the required structure of invariant object by [34, Proposition 3.49]. The fibered category $Azm(n)$ is a stack in the fppf topology due to [34, Theorem 4.23] and an easy generalization of [34, Theorem 4.29]. Then descent theory along torsors gives us an Azumaya algebra M_A over R; it is obvious that this association is functorial. The algebra M_A is characterized as being the sub-algebra of $M_n(A)$ where $\tilde{\rho}$ and $\tilde{p}$ coincide. This can also be described as the algebra of invariants of the action of $PGL_{n,A}$ on $M_n(A)$. We leave to the reader to verify that the two functors we defined are one the inverse of the other, so that $Azm(n)^{op}$ and $\mathcal{B}PGL_n$ are indeed equivalent categories.

Let us show now that $\mathcal{B}PGL_n$ and $BS(n)$ are also equivalent. We start with the functor $BS(n) \to \mathcal{B}PGL_n$, which is analogous to the functor $Azm(n)^{op} \to \mathcal{B}PGL_n$. If $P \to Spec(R)$ is a Brauer-Severi scheme, consider the functor $I_P : Aff/Spec(R) \to Grp$ such that $I_P(Spec(S)) = Iso_{Spec(S)}(\mathbb{P}^{n-1}_S, P \times_{Spec(R)} Spec(S))$. This functor is a fppf sheaf and has a right $PGL_{n,R}$ action. Locally in the fppf topology, this action is trivial, since the automorphisms of the projective space are the projectivisation of the linear group. Then I_P is a PGL_n torsor, hence representable by an affine scheme.

Conversely, now we construct a functor $\mathcal{B}PGL_n \to BS(n)^{op}$. Consider a $PGL_{n,R}$-torsor $Spec(A) \to Spec(R)$. We have a right action of $PGL_{n,R}$ on $\mathbb{P}^{n-1}_R \times_{Spec(R)} Spec(A) = \mathbb{P}^{n-1}_A$. The class of maps from Brauer-Severi schemes to their bases is made of flat proper morphisms of finite presentation since they are so in a fppf cover; see Vistoli 2.36 and [11, IV.17.16.3]. They are also clearly local in the fppf topology. Then [34, Theorem 4.38] and [34, Proposition 4.20] tell us that the category $BS(n)$ is a stack for the fppf topology and by descent theory we obtain a Brauer-Severi scheme $P_A \to Spec(R)$.

This completes the sketch of proof of the theorem. We will be particularly interested in the study of central simple algebras, and so we will restrict our attention to the full subcategory of Aff given by fields. Brauer-Severi schemes over a field are called *Brauer-Severi varieties*, and they are split by a finite field extension.

Remark 2.2.3. Recall that if $f : Y \to X$ is smooth and surjective and X is quasi-compact, then there exists an affine scheme X', a surjective étale morphism $h : X' \to X$ and an X-morphism $g : X' \to Y$: see [11, IV.17.16.3] It follows that if G is a smooth group scheme, then G-torsors for the fppf and étale topology are the same. From the preceding discussion we deduce then that in fact Brauer-Severi schemes are split by an étale surjective map.

Remark 2.2.4. Brauer-Severi schemes have one more characterization, which we only state. Let $P \to S$ be a proper flat locally of finite presentation map, and suppose also that the geometric fibers are projective spaces of rank $n-1$. Then P is a Brauer-Severi scheme.

2.3 Cohomology

We are going to show that from the preceding discussions one can recover the cohomological description of the Brauer group.

Consider a site $\mathcal{C}$, an object X in $\mathcal{C}$ and a covering $\mathcal{U} = (U_i \xrightarrow{\phi_i} X)_{i\in I}$. For any $(p+1)$-tuple $(i_0, ..., i_p)$ with the i_j in I we write $U_{i_0} \times_X \cdots \times_X U_{i_p} = U_{i_0 \cdots i_p}$. Let P be a presheaf on $\mathcal{C}$. The canonical projection

$$U_{i_0 \cdots i_p} \to U_{i_0 \cdots \hat{i}_j \cdots i_p} = U_{i_0} \times \cdots \times U_{i_{j-1}} \times U_{i_{j+1}} \times \cdots \times U_{i_p}$$

induces a restriction morphism

$$P(U_{i_0 \cdots \hat{i}_j \cdots i_p}) \to P(U_{i_0 \cdots i_p})$$

which we write as res_j. Define a complex

$$C^\bullet(\mathcal{U}, P) = (C^p(\mathcal{U}, P), d^p)_p$$

as follows:

$$C^p(\mathcal{U}, P) = \prod_{I^{p+1}} P(U_{i_0 \cdots i_p})$$

and $d^p : C^p(\mathcal{U}, P) \to C^{p+1}(\mathcal{U}, P)$ is the homomorphism such that if $s = (s_{i_0 \cdots i_p}) \in C^p(\mathcal{U}, P)$, then

$$(d^p s)_{i_0 \cdots i_{p+1}} = \sum_{j=0}^{p+1} (-1)^j res_j(s_{i_0 \cdots \hat{i}_j \cdots i_{p+1}})$$

It is easy to see that this is indeed a complex. The cohomology groups of $(C^p(\mathcal{U}, P), d^p)$ are called *Cech cohomology groups* of P with respect to the covering $\mathcal{U}$ of X, and are denoted as $\check{H}^p(\mathcal{U}, P)$.

A second covering $\mathcal{V} = (V_j \xrightarrow{\psi_j} X)_{j\in J}$ is called a *refinement* of $\mathcal{U}$ if there is a map $\tau : J \to I$ such that for each j, ψ_j factors through $\phi_{\tau j}$, that is, $\psi_j = \phi_{\tau j}\eta_j$

for some $\eta_j : V_j \to U_{\tau j}$. The map τ, together with the family (η_j), induces maps $\tau^p : C^p(\mathcal{U}, P) \to C^p(\mathcal{V}, P)$ as follows: if $s = (s_{i_0 \cdots i_p}) \in C^p(\mathcal{U}, P)$, then

$$(\tau^p s)_{j_0 \cdots j_p} = res_{\eta_{j_0} \times \cdots \times \eta_{j_p}}(s_{\tau j_0 \cdots \tau j_p})$$

These maps τ^p commute with d and hence induce maps on the cohomology

$$\rho(\mathcal{V},\mathcal{U},\tau) : \check{H}^p(\mathcal{U}, P) \to \check{H}^p(\mathcal{V}, P)$$

Lemma 2.3.1. The map $\rho(\mathcal{V},\mathcal{U},\tau)$ does not depend on τ of the η_j.

Proof. See [23, III, Lemma 2.1]. □

Hence, if $\mathcal{V}$ is a refinement of $\mathcal{U}$, we get a homomorphism $\rho(\mathcal{V},\mathcal{U}) : \check{H}^p(\mathcal{U}, P) \to \check{H}^p(\mathcal{V}, P)$ depending only on $\mathcal{V}$ and $\mathcal{U}$. It follows that if $\mathcal{U}$, $\mathcal{V}$,$\mathcal{W}$ are three coverings of X such that $\mathcal{W}$ is a refinement of $\mathcal{V}$ and $\mathcal{V}$ is a refinement of $\mathcal{U}$, then $\rho(\mathcal{W},\mathcal{U}) = \rho(\mathcal{W}, \mathcal{V})\rho(\mathcal{V},\mathcal{U})$. Thus we may define the *Cech cohomology groups* of P over X to be $\check{H}^p(X, P) = \varinjlim \check{H}^p(\mathcal{U}, P)$, where the limit is taken over all coverings $\mathcal{U}$ of X.

Consider a category with a terminal object X.

Proposition 2.3.2. To any exact sequence of sheaves of groups

$$1 \to G' \to G \to G'' \to 1$$

there is associated an exact sequence of pointed sets

$$1 \to G'(X) \to G(X) \to G''(X) \xrightarrow{d} \check{H}^1(X, G') \to \check{H}^1(X, G) \to \check{H}^1(X, G'')$$

Proof. The map d is defined as follows: let $g \in G''(X)$, and let $(U_i \to X)$ be a covering of X such that there exist $g_i \in G(U_i)$ that map to $g|_{U_i}$ under $G(U_i) \to G''(U_i)$; then

$$d(g)_{ij} = (g_i|_{U_{ij}})^{-1}(g_j|_{U_{ij}})$$

The other maps are obvious and the checks that have to be done are routine. □

Let G be a group sheaf and S a torsor for G. Let $(U_i \to X)$ be a cover that trivializes S and choose $s_i \in S(U_i)$ for every U_i. Then there is a unique $g_{ij} \in G(U_{ij})$ such that $(s_i|_{U_{ij}})g_{ij} = (s_j|_{U_{ij}})$. Note that (g_{ij}) is a 1-cocycle, and that if the choice of the s_i is changed, then $g = (g_{ij})$ is replaced by a cohomologous cocycle. Also the cohomology class in unaltered if S is replaced by an isomorphic torsor or another covering. Thus S defines an element $c(S) \in \check{H}^1(X, G)$.

Proposition 2.3.3. The map $S \mapsto c(S)$ defines a one-to-one correspondence between isomorphism classes of sheaf torsors for G and elements of $\check{H}^1(X, G)$ under which the trivial class corresponds to the distinguished element.

Proof. We construct the inverse mapping. Let $\mathcal{U} = (U_i \to X)$ be a covering of X, and let $\underline{C}^0(\mathcal{U}, G)$ and $\underline{C}^1(\mathcal{U}, G)$ be the sheaves $V \mapsto \prod_i G(U_i \times V)$, $V \mapsto \prod_{i,j} G(U_{ij} \times V)$. These are sheaves because, for example, $\underline{C}^0(\mathcal{U}, G) = \prod \pi_*(G|_{U_i})$, where π_i are the maps $U_i \to X$. Let $d : \underline{C}^0 \to \underline{C}^1$ be the mapping $(h_i) \to (h_i^{-1} h_j)$. Now fix a 1-cocycle g for G relative to $\mathcal{U}$. For any V, g restricts to an element $g|_V$ of $\Gamma(V, \underline{C}^1(\mathcal{U}, G))$, and we define S to be the subsheaf of $\underline{C}^0(\mathcal{U}, G)$ such that $\Gamma(V, S)$ is in the inverse image of $g|_V$ for any V. There is an obvious right action of G on S, namely $((s_i), g) \mapsto (g^{-1} s_i)$. Suppose now that g is the trivial cocycle, that is $g_{ij} = (g_i|_{U_{ij}})^{-1}(g_j|_{U_{ij}})$ for some $(g_i) \in \prod_i G(U_i)$. Then the map $G \to S$ that sends a section h of G over V to $(h^{-1}|_{V \times U_i})(g_i|_{V \times U_i})$ is an isomorphism that commutes with the action of G. Since g becomes trivial on each U_i, and the definition of S commutes with restriction, this shows that $S|_{U_i} \cong G|_{U_i}$, that is, S is a G-torsor. Finally one checks that the 1-cocycle corresponding to S is the original cocycle g and conversely that the torsor defined by the cocycle obtained by a given torsor, is isomorphic to the given torsor. This shows there is a one-to-one correspondence between isomorphism classes of torsors that become trivial on a given covering $\mathcal{U}$ and elements $\check{H}^1(\mathcal{U}, G)$. Passing to the limit we obtain the thesis. □

Corollary 2.3.4. Let G be an affine group scheme. There is a canonical bijection between the set of fppf G-torsors over a base scheme X modulo isomorphism and $\check{H}^1_{fppf}(X, G)$. If G is a smooth they are also in bijective correspondence with $\check{H}^1_{et}(X, G)$.

Proof. The firs part is a consequence of the Proposition and the fact that fppf G-torsors are representable. For the second part, we already remarked that if the groups is smooth, then fppf torsors are the same as étale torsors. □

Recall now the exact sequance of étale sheaves

$$1 \to \mathbb{G}_m \to GL_{n,R} \to PGL_{n,R} \to 1$$

in the category $Aff/Spec(R)$.

Theorem 2.3.5. There is a canonical injective homomorphism

$$Br(R) \to H^2_{et}(Spec(R), \mathbb{G}_m)$$

Proof. We have shown in Theorem 2.2.2 that Azumaya algebras over R are in correspondence with $PGL_{n,R}$ torsors in the fppf topology. Then it follows from Corollary 2.3.4 that they are also in correspondence with $\check{H}^1_{et}(Spec(R), PGL_{n,R})$.

Furthermore, by descent theory for quasi-coherent sheaves, the set $\check{H}^1_{et}(Spec(R), GL_{n,R})$ is in correspondence with the set of isomorphism classes of locally free modules of rank n over R. Let us show that the map $\check{H}^1_{et}(Spec(R), GL_{n,R}) \to \check{H}^1_{et}(Spec(R), PGL_{n,R})$ sends an R module to the module of its endomorphisms. Let E be an R-module and $\mathcal{U} = (U_i)$ a Zariski covering of $Spec(R)$ that trivializes E through maps ϕ_i. Then E correponds to the 1-cocycle $(\phi_i^{-1}\phi_j)$. Consider $A = End_R(E)$ and the isomorphisms $\psi_i M_n(R_i) \to End_{R_i}(E_i)$, where

$\psi_i(a) = \phi_i a \phi_i^{-1}$. Thus A corresponds to the 1-cocycle $(\psi_i^{-1}\psi_j) = (\alpha_{ij})$, where $\alpha_{ij}(a) = \phi_i^{-1}\phi_j a \phi_j^{-1}\phi_i$. This is in the image of $(\phi_i^{-1}\phi_j)$ because the map $GL_{n,R_i} \to PGL_{n,R_i}$ maps u to the automorphism of $M_n(R_i)$ given by conjugation by u.

There is a an exact sequence of pointed sets

$$\check{H}^1_{et}(Spec(R), \mathbb{G}_m) \to \check{H}^1_{et}(Spec(R), GL_{n,R}) \to \check{H}^1_{et}(Spec(R), PGL_{n,R}) \xrightarrow{d} \\ \xrightarrow{d} \check{H}^2_{et}(Spec(R), \mathbb{G}_m)$$

The first part is just the exact sequence of Proposition 2.3.2. We can continue that exact sequence because $\mathbb{G}_m$ is in the center of $GL_{n,R}$. The map d is defined as follows: let $\gamma \in \check{H}^1_{et}(Spec(R), PGL_{n,R})$ be represented by a cocycle (c_{ij}) for the covering (U_i). After refining (U_i), we may assume that each c_{ij} is in the image of an element $c'_{ij} \in \Gamma(U_{ij}, GL_{n,R})$; the $d(\gamma)$ is the class of the 2-cocycle (a_{ijk}) where

$$a_{ijk} = c'_{jk}(c'_{ik})^{-1}c'_{ij} \in \Gamma(U_{ijk}, \mathbb{G}_m)$$

Moreover, $d(c(A \otimes_R A')) = dc(A)dc(A')$, where $c(A)$ denotes the class in $\check{H}^1_{et}(Spec(R), PGL_{n,R})$ of an Azumaya algebra A. The verification of the exactness and the other statements are routine.

Thus we have obtained an injective homomorphism

$$Br(Spec(R)) \to \check{H}^2_{et}(Spec(R), \mathbb{G}_m)$$

By Milne Theorem 2.17 there is a canonical isomorphism $\check{H}^2_{et}(Spec(R), \mathbb{G}_m) \to H^2_{et}(Spec(R), \mathbb{G}_m)$, and so we have concluded. □

Corollary 2.3.6. If k is a field, $Br(k) \to H^2(k, k^*)$ is an isomorphism.

Proof. This follows from [23, IV, Corollary 2.12] and the fact that for fields étale cohomology is the same as Galois cohomology. □

Chapter 3

Essential dimension

In this chapter we are finally going to talk about essential dimension. We will study its basic properties, following [4]. For a more complete point of view on the subject, see the introductory papers [26] and [21].

3.1 General properties

Fix a base field k. We denote by $\mathcal{C}_k$ the category of field extensions of k, with morphism field maps that fix k. Let $F : \mathcal{C}_k \to Sets$ be a functor.

Definition 3.1.1. Let $a \in F(K)$, with K/k a field extension. We say that a is *defined* over an intermediate field $k \subseteq E \subseteq K$ if there is an element $b \in F(E)$ such that $F(E \to K)(b) = a$.

Definition 3.1.2. If $a \in F(K)$ with K/k a field extension, we define the *essential dimension* of a as $ed(a) = min\ trdeg(E : k)$, where E runs over the extensions of k over which a is defined.

Definition 3.1.3. The essential dimension of F is the supremum of $ed(a)$ for all $a \in F(K)$ and all the extensions K/k.

Let us show some examples. First consider the trivial functor F such that $F(K) = S$ for every K, where S is a fixed non-empty set. It is clear that the essential dimension of F is zero, since every element of $F(K)$ is defined over k. Next, consider the forgetful functor F such that assigns to each field its underlying set. If a is an element in $F(K)$, then the essential dimension of a is zero if it is algebraic, one otherwise. It is clear then that $ed_k(F) = 1$. Finally, fix an integer n and a set $S = \{a, b\}$ with $a \neq b$. Define the functor F on an extension K/k to be $\{a\}$ if $trdeg(K : k) < n$, and S otherwise. The essential dimension of F is n, and this shows that the essential dimension of a functor can be arbitrary large.

Now we study the behavior of essential dimension with respect to elementary operations on functors.

Definition 3.1.4. Let k'/k be a field extension and consider the natural functor $G : \mathcal{C}_{k'} \to \mathcal{C}_k$. For a functor $F : \mathcal{C}_k \to Sets$, we define $F_{k'}$ to be the functor $F \circ G$.

Proposition 3.1.5. If k'/k is a field extension, then $ed_{k'}(F_{k'}) \leqslant ed_k(F)$.

Proof. If $ed_k(F) = \infty$, the results is obvious. Let $ed_k(F) = n$. Take K/k' a field extension and $a \in F(K)$. There is a subextension $k \subseteq E \subseteq K$ with $trdeg(E : k) \leqslant n$ such that a is in the image of the map $F(E) \to F(K)$. The composite extension $E' = Ek'$ then satisfies $trdeg(E' : k') \leqslant n$ and a is in the image of the map $F(E') \to F(K)$. Thus $ed(a) \leqslant n$ and $ed_{k'}(F_{k'}) \leqslant n$. □

Proposition 3.1.6. Let $f : F \to G$ be a surjection of functors. Then $ed(G) \leqslant ed(F)$.

Proof. Let K/k be an extension and $b \in G(K)$. By surjectivity, there is an element $a \in F(K)$ such that $f_K(a) = b$. Suppose that $ed(F) = n$ and take a subextension $k \subseteq E \subseteq K$ such that $trdeg(E : k) \leqslant n$ and such that $a \in im(F(E) \to F(K))$. The thesis now follows from the naturality of f. □

Proposition 3.1.7. Let F and G be two functors. Then, if we still denote by X the functor it represents, $ed(F \times G) \leqslant ed(F) + ed(G)$.

Proof. Consider K/k a field extension and $(a, a') \in F(K) \times G(K)$. Take two extensions $k \subseteq E \subseteq K$ and $k \subseteq E' \subseteq K$ with $trdeg(E : k) \leqslant ed(F)$ and $trdeg(E' : k) \leqslant ed(G)$, such that a and a' come from $F(E)$ and $G(E')$. This means that exist $b \in F(E)$ and $b' \in G(E')$ such that $b_K = a$ and $b'_K = a'$. Now take $L = EE'$ and notice that (b_L, b'_L) maps to (a, a'). The thesis follows from $trdeg(EE' : k) \leqslant trdeg(E : k) + trdeg(E' : k)$. □

Proposition 3.1.8. Let X be a scheme locally of finite type over k. Then $ed(X) = dim(X)$.

Proof. Every point $p \in X(K)$ has least field of definition $k(p)$, so $ed(X) = sup_p\ trdeg(k(p)) = dim(X)$. □

Definition 3.1.9. Let F be a functor. A *classifying scheme* of F is a locally of finite type k-scheme X such that there is a surjection $X \to F$.

Corollary 3.1.10. If X is a classifying scheme of F then $ed(F) \leqslant dim(X)$.

3.2 Essential p-dimension

Let $F : \mathcal{C}_k \to Sets$ be a functor, K/k a field extension, $x \in F(K)$ and K_0 a field extension of k. We say that x is *p-defined* over K_0 if there are morphisms $K_0 \to K'$ and $K \to K'$ in $\mathcal{C}_k$ for some field K'/k and an element $x_0 \in F(K_0)$ such that K'/K is a finite extension of degree prime to p and $(x_0)_{K'} = x_{K'}$ in $F(K')$. We define the *essential p-dimension* of x as $ed_p(x) = min\ trdeg_k(K_0)$, where the minimum is taken over all fields of p-definition K_0 of x. The *essential*

p-dimension of the functor F is $ed_p(F) = sup\ ed_p(x)$, where the supremum runs over all field extensions K/k and all $x \in F(K)$.

Remark 3.2.1. It follows from the definition that $ed_p(x) = min\ ed(x_L)$, where L runs over all finite and prime to p extensions of K. In particular, for every p, we have that $ed_p(F) \leqslant ed(F)$.

Remark 3.2.2. The general properties proved above hold also in the case of the essential p-dimension.

Essential p-dimension is in some sense the 'local' version of essential dimension. Most of the existing methods for proving lower bounds on the essential dimension are in fact well suited for problems that are not sensitive to prime-to-p extensions, and thus for computations the essential p-dimension. On the other hand most of the difficult and important problems are sensitive to prime-to-p extensions. For instance, it is not known if every division algebra of prime degree is a crossed product, however every such algebra becomes a crossed product after a prime-to-p extension of its center: see Rowen and Saltman [31].

3.3 Essential dimension of algebraic groups

In this section we are going to define the essential dimension of algebraic groups, that are group schemes of finite type over a base field k. This definition is due to Reichstein, who first introduced it in [25]. The definition is given using Galois cohomology, for which the standard reference is Serre's book [33]. See also [10] for a more elementary introduction.

Definition 3.3.1. Let G be an algebraic group. The *essential dimension* of G is defined as $ed_k(G) = ed_k(H^1(-, G))$.

The functor $H^1(-, G) : \mathcal{C}_k \to Sets$ is the first Cech cohomology group of $Gal(K^s, K)$ with values in $G(K^s)$. This group is the same as the first Cech cohomology group for G in the étale topology on $\mathcal{C}_k$, which we have seen to describe the isomorphism classes of G-torsors on $Spec(k)$. In the case $G = PGL_{n,k}$ we have seen that the functor of torsors is isomorphic to the functor of central simple algebras and that of Brauer-Severi varieties. Thus the essential dimension of $PGL_{n,k}$ is precisely the object of study of this thesis.

Remark 3.3.2. Since the object of interest of the thesis is the projective linear group, in the sequel we shall always assume that the algebraic group G is smooth.

Now we give some simple examples.

Example 3.3.3. Consider the affine group $GL_{n,k}$. Using descent theory the same way we did for $PGL_{n,k}$ we see that the groups $H^1(K, GL_{n,k})$ classify vector spaces that become isomorphic in a finite extension of K. Clearly two such vector spaces are already isomorphic over K since dimension is a complete invariant, so $H^1(K, GL_{n,k}) = 0$ for every K/k. This fact is known as Hilbert Theorem 90. Of course, this shows that $ed_k(GL_{n,k}) = 0$. In particular, $ed_k(\mathbb{G}_m) = 0$.

Example 3.3.4. Consider the affine group $SL_{n,k}$. We have an exact sequence in the étale topology

$$1 \to SL_{n,k} \to GL_{n,k} \to \mathbb{G}_m \to 1$$

Taking the exact sequence in cohomology we see that $H^1(K, SL_{n,K}) = 0$ for every K, so that $ed_k(SL_{n,k}) = 0$.

Example 3.3.5. Consider now the finite constant group scheme S_n over k. This is the functor group of automorphisms of the k-algebra k^n. We remark here that if K/k is a Galois extension with group G, then $Spec(K) \to Spec(k)$ is a G torsor for the étale topology. Thus by descent along torsors, $H^1(k, S_n)$ classifies the set of isomorphism classes of commutative k-algebras A such that there exists a finite Galois extension K/k with $A \otimes_k K \cong K^n$. These are precisely the étale algebras. The essential dimension of S_n is unknown, but it has been proved by Buhler and Reichstein in [5] that $\lfloor n/2 \rfloor \leqslant ed_k(S_n) \leqslant n-3$ for $n \geqslant 5$.

Definition 3.3.6. Let $\mathcal{C}$ be a category, G a functor $\mathcal{C} \to Grp$ and F a functor $\mathcal{C} \to Sets$. We say that G acts *freely* on F if the action of $G(X)$ on $F(X)$ is free for every object X. If $\mathcal{C} = Sch/S$, G is a group object in Sch/S and X is an S-scheme, we say that G acts freely on X if $G(T)$ acts freely on $X(T)$ for every S-scheme T.

There is a geometric interpretation of the definition of free action. Consider G a group scheme over S and X a scheme over S. Let $x \in X$ be a point. The *scheme-theoretic stabilizer* of x is the pull-back of the diagram

$$\begin{array}{ccc} & & G \times_S x \\ & & \downarrow \\ Spec(k(x)) & \longrightarrow & X \end{array}$$

where the vertical map is the composite $G \times_S x \to G \times_S X \to X$. We denote it by G_x; it is a group scheme over $Spec(k(x))$ and is a closed group subscheme of $G \times_S \{x\}$.

Proposition 3.3.7. Let G be an algebraic group over k and X an algebraic variety over k. Then G acts freely on X if and only if G_x is trivial for all points $x \in X$.

Proof. See [6, III, Chapter 2, Corollary 2.3]. □

Free actions give rise to torsors in a natural way.

Theorem 3.3.8. Let G act freely on a S-scheme of finite type X such that the second projection $G \times_S X \to X$ is flat and of finite type. Then there exists a non-empty G-invariant dense open subscheme U of X satisfying the following properties:
1) There exists a quotient map $\pi : U \longmapsto U/G$ in the category of schemes.
2) π is onto, open and U/G is of finite type over S.
3) $\pi : U \longmapsto U/G$ is a flat G-torsor.

Proof. See [7, V, Théorème 8.1]. □

Definition 3.3.9. Let G act on X. An open subscheme U which satisfies the conclusion of the above theorem will be called a *friendly* open subscheme of X.

Definition 3.3.10. Let $\pi : X \to Y$ be a G-torsor. For any field extension K/k we define a map $\partial : Y(K) \to H^1(K, G)$ as follows: for any $y \in Y(K)$, the fiber X_y is a torsor over $Spec(K)$, and we set $\partial(y)$ to be the isomorphism class of X_y over $Spec(K)$.

Let us proceed by studying certain torsors that arise from group representations, which will be useful later.

Definition 3.3.11. We say that G acts *generically freely* on X if there exists a non-empty G-stable open subscheme U of X on which G acts freely.

Proposition 3.3.12. Let G be an algebraic group over k acting linearly and generically freely on an affine space $\mathbb{A}(V)$, where V is a finite dimensional k-vector space. Let U be a non-empty friendly open subscheme of $\mathbb{A}(V)$ on which G acts freely. Then U/G is a classifying scheme of $H^1(-, G)$. In particular we have $ed(G) \leqslant dim(V) - dim(G)$.

Proof. We have to show that, for any field extension K/k, the map $\partial : U/G(K) \to H^1(K, G)$ is surjective. Let $g \in Z^1(K, G)$, that is a Galois 1-cocycle. We twist the action of $Gal(K^s/K)$ over $V(K^s)$ by setting $\gamma * v = \gamma \cdot v \cdot g(v)^{-1}$ for all $\gamma \in Gal(K^s/K)$ and $v \in V(K^s)$. A quick check shows that this action is $Gal(K^s/K)$ semilinear, that is $\gamma * (\lambda v) = \gamma(\lambda)(\gamma * v)$ for all $\lambda \in K^s$. By Galois descent the invariant set $V(K^s)^{Gal(K^s/K),*}$ is a K-linear subspace such that is isomorphic to $V(K^s)$ when base-changed to K^s. It is then in particular Zariski dense, so that it intersects the dense open subset U. Let $v_0 \in U(K)$ be an invariant point for the new action $*$. If π is the projection map $U \to U/G$, we want to show that $\partial(\pi(v_0)) = g$. First of all the fact that v_0 is invariant implies that $v_0 \cdot g(\gamma) = \gamma \cdot v_0$ for every $\gamma \in Gal(K^s/K)$. Then for every $\gamma \in Gal(K^s/K)$, $\gamma \cdot \pi(v_0) = \pi(\gamma \cdot v_0) = \pi(v_0 \cdot g(\gamma)) = \pi(v_0)$, where the last equality holds since U is a G-torsor. From this we have that $\pi(v_0) \in U/G(K)$. Recalling the explicit description of the relation between torsors and cocycles, and using once again that $v_0 \cdot g(\gamma) = \gamma \cdot v_0$ we see that in fact $\partial(\pi(v_0)) = g$. □

We remark here that any algebraic group has a generically free action over some vector space. Indeed, G is isomorphic to a closed subgroup of some GL_n, and in suffices to take $V = M_n(k)$.

In particular we see that the essential dimension of an algebraic group is finite.

3.4 Versal pairs

In this section we introduce the notion of versal pairs and show how it can be used to compute the essential dimension of algebraic groups.

Let k be a field and $\mathcal{U}_k$ be the category of all commutative k-algebras with homomorphism of k-algebras as morphisms. Every functor $F : \mathcal{U}_k \to Sets$ defines by restriction a functor $\mathcal{C}_k \to Sets$. We shall relate the essential dimension of this restriction with versal pairs.

Definition 3.4.1. Let $F : \mathcal{U}_k \to Sets$ be a functor and (a, K) be a pair such that K is an extension of k and $a \in F(K)$. We say that the pair (a, K) is a *versal pair* if for every extension L/k and every element $b \in F(L)$, there exist a local k-subalgebra $\mathcal{O}$ of K and an element $c \in F(\mathcal{O})$ such that $F(\mathcal{O} \to K)(c) = a$, there is a morphism $\mathcal{O} \to L$ in $\mathcal{U}_k$ such that $F(\mathcal{O} \to L)(c) = b$.

Definition 3.4.2. Let $F : \mathcal{U}_k \to Sets$ be a functor which has a versal pair. We say that a versal pair (a, K) is *nice* if for any $k \subseteq L \subseteq K$ and $a' \in F(L)$ such that $a = a'_K$, the pair (a', L) is versal. We say that F is *nice* if it has a nice versal pair.

Proposition 3.4.3. Let $F : \mathcal{U}_k \to Sets$ be a functor which has a versal pair. Then the essential dimension of the restriction of F to $\mathcal{C}_k$ is at most the minimum transcendence degree of the fields for which there is a versal pair. Moreover, if F is nice, then $ed_k(F) = ed_k(a)$, where (a, K) is any nice versal pair.

Proof. Let L/k be any field extension, and let $b \in F(L)$. Let (a, K) be a versal pair such that $trdeg(K : k)$ is minimal. Since (a, K) is versal, then b comes from an element of $F(\kappa(O))$, where $\kappa(O)$ is the residue field of some local k-algebra O. Then $ed(b) \leqslant trdeg(\kappa(O) : k) \leqslant trdeg(K : k)$. This proves the first assertion.

Let now (a, K) be a nice versal pair. Take a subextension $k \subseteq L \subseteq K$ with an element $a' \in F(L)$ such that $a = a'_L$ and $trdeg(L : k) = ed(a)$. By assumption, (a', L) is versal, so by the preceding point $ed_k(F) \leqslant trdeg(L : k) = ed(a)$. On the other hand, $ed(a) \leqslant ed_k(F)$ by definition of essential dimension. □

Definition 3.4.4. Let $f : X \to Y$ be a G-torsor with Y irreducible. We say that it is *classifying* for G if, for any field extension k'/k and for any torsor P' of G over k'/k, the set of points $y \in Y(k')$ such that P' is isomorphic to the fiber $f^{-1}(y)$ is dense in Y.

Remark 3.4.5. The proof of Proposition 3.3.12 actually tells us that we obtain a classifying torsor. Furthermore one can always find a reduced classifying torsor for G. Indeed, take $X \to Y$ a classifying torsor for G and let $\varphi : Y_{red} \to Y$ be the canonical reduced scheme associated to Y. Then pulling back the torsor $X \to Y$ along φ gives a torsor which is isomorphic to $X_{red} \to Y_{red}$ and which is also classifying.

Definition 3.4.6. Let G be an algebraic group over k, K a field extension of k and $P \to Spec(K)$ a G-torsor. We say that P is *k-generic* if
1) there exists an integral scheme Y with function field $k(Y) \cong K$ and a G-torsor $f : X \to Y$ whose generic fiber $f^{-1}(\eta) \to Spec(K)$ is isomorphic to $P \to Spec(K)$.

2) For every extension k'/k with k' infinite, for every non-empty open set U of Y and for every G-torsor $P' \longmapsto Spec(k')$, there exists a k'-rational point $x \in U$ such that $f^{-1}(x) \cong P'$.

Generic torsors are by definition generic fibers of classifying torsors.

Proposition 3.4.7. Let $P \to Spec(k(Y))$ be a generic torsor. Then $(P, k(Y)$ is a versal pair for the functor of G-torsors.

Proof. Take $T \to Spec(L)$ any torsor defined over L/k. Since $X \to Y$ is a classifying torsor, there exists a L-rational point $y : Spec(L) \to Y$ such that $T \to Spec(L)$ is the pullback along y. Take $O_{Y,y}$ the local ring at the point y and let $\phi : Spec(O_{Y,y}) \to Y$ be the canonical morphism. Consider $P' \to Spec(O_{Y,y})$ the torsor obtained by pulling back $X \to Y$ along ϕ. The local ring $O_{Y,y}$ in naturally a sub k-algebra of $k(Y)$, so $P \to Spec(k(Y))$ is a pullback of $P' \to Spec(O_{Y,y})$. Moreover, the morphism $y : Spec(L) \to Y$ factorizes through $Spec(k(y))$; if we denote by $P'' \to Spec(k(Y))$ the torsor obtained by pulling back $P' \to Spec(O_{Y,y})$ along the morphism $Spec(k(y)) \to Spec(O_{Y,y})$, it is clear that $T \to Spec(L)$ comes from $P'' \to Spec(k(y))$. This shows the thesis. □

Definition 3.4.8. Let $f : X \to Y$ and $f' : X' \to Y'$ be two G-torsors. We say that f' is a *compression* of f if there is a diagram

$$\begin{array}{ccc} X & \overset{g}{\dashrightarrow} & X' \\ \downarrow f & & \downarrow f' \\ X' & \overset{h}{\dashrightarrow} & Y' \end{array}$$

where g is a G-equivariant rational dominant morphism and h is a rational morphism.

Remark 3.4.9. Take as above a compression of $f : X \to Y$ and let $U \subseteq Y$ the open subscheme on which h is defined. Taking the pullback of $X' \to Y'$ along h, one obtains a G-torsor $f'' : P \to U$ which fits into a diagram

$$\begin{array}{ccccc} X & \dashrightarrow & P & \to & X' \\ \downarrow f & & \downarrow f'' & & \downarrow f' \\ Y & \dashrightarrow & U & \to & Y' \end{array}$$

and f'' is a compression too. So we can basically reduce a compression to a pullback.

Lemma 3.4.10. Let $g : X \dashrightarrow X'$ be a rational dominant G-equivariant morphism between generically free schemes. Then exists X_0 and X'_0 friendly open subschemes of X and X' such that g induces a compression of torsors

$$\begin{array}{ccc} X_0 & \overset{g}{\dashrightarrow} & X'_0 \\ \downarrow & & \downarrow \\ X_0/G & \overset{h}{\dashrightarrow} & X'_0/G \end{array}$$

Proof. Take U some friendly open subscheme of X. Since g is dominant, we can find an open subscheme U' of X', which lies in the image of g. Intersecting U' with some friendly open set of X' gives a friendly open set X'_0 in the image of U. Then $X_0 = g^{-1}(X'_0)$ is the desired open set. □

Proposition 3.4.11. Let $f : X \to Y$ be a G-torsor with Y integral. Let $T \to Spec(k(Y))$ be its generic fiber; then its essential dimension is equal to the smallest dimension of the base scheme of a compression of f.

Proof. Let f and T be as above. Let $f' : X' \to Y'$ be a compression of f and $T' \to Spec(k(Y'))$ its generic fiber. By Remark 3.4.9 one can suppose that the compression is a pullback. But then it is clear that T' maps to T under $H^1(k(Y'), G) \longmapsto H^1(k(Y), G)$, so that the essential dimension of $T \to Spec(k(Y))$ is at most the dimension of the scheme Y'.

Conversely suppose there is a subextension $k \subseteq K' \subseteq K = k(Y)$ together with a torsor T' over K' such that T' maps to T under $H^1(K', G) \to H^1(k(Y), G)$; we have to find a G-torsor $f' : X' \to Y'$ such that T' is isomorphic to its generic fiber and a compression from f to f'. We can suppose everything to be affine, since the problem is local. So let us write $Y = Spec(A)$, $X = Spec(B)$, $T = Spec(P)$, $T' = Spec(P')$ and let $k[G]$ denote the algebra of G. We have to find a subring A' of K' whose field of fractions is K', a G-torsor B'/A' such that $P' \cong B' \times_{A'} K'$ and a rational compression from B'/A' to B/A.

Since K is of finite type over k, we can write it as $K = k(\alpha_1, ..., \alpha_n)$; since P is of finite type over K we write it $P = K[\beta_1, ..., \beta_m]$. In the same way we write $K' = k(\alpha'_1, ..., \alpha'_s)$ and $P' = K'[\beta'_1, ..., \beta'_t]$.

Since both $P' \times_{K'} P'$ and $P' \times_k k[G]$ are finitely generated algebras over K' one can find a polynomial f in the α'_i such that $B' \times_{A'} B' \cong B' \times_k k[G]$ where $A' = k[\alpha']_f$ and $B' = A'[\beta']$. It is clear that $P' \cong B' \times_{A'} K'$, so we have to find a rational morphism from B'/A' to B/A. The image of A' under the map $A' \subseteq K' \subseteq K$ lies in a subring of the form $k[\alpha]_g$ for some polynomial g in the α'_i. Now $A = k[\alpha]_h$ for some h and we have a natural map $A' \to A_g$. In the same way one finds a rational map $B' \to B_p$ compatible with the previous one. Then the thesis follows. □

Lemma 3.4.12. Let $f' : X' \to Y'$ be a compression of a classifying torsor $f : X \to Y$. Then f' is also classifying.

Proof. Let

$$\begin{array}{ccc} X & \overset{g}{\dashrightarrow} & X' \\ \downarrow f & & \downarrow f' \\ X' & \overset{h}{\dashrightarrow} & Y' \end{array}$$

be such a compression. Let k'/k be a field extension with k' infinite and let $P' \in H^1(k', G)$. Since f is classifying one can find a k' rational point $y \in Y(k')$ which lies in U, the open set on which h is defined, such that $f^{-1}(y) \cong P'$. Then the fiber of f' at $h(y)$ clearly gives a torsor isomorphic to P'. □

Corollary 3.4.13. Let $T \to Spec(K)$ be a generic G-torsor, $K' \subseteq K$ and $T' \to Spec(K')$ such that $T'_K = T$. Then T' is also a generic torsor.

Proof. Take a classifying G-torsor $X \to Y$ which is a model for T. Then, by the proof of Lemma 3.4.10, defining T over a smaller field means compressing the torsor $X \to Y$. Since the compression of a classifying torsor is again classifying it follows that T comes from a generic torsor. □

The following Corollary is very important for some computations of essential dimension.

Corollary 3.4.14. The functor of G-torsors is nice. Furthermore, if $T \in H^1(K, G)$ is a generic torsor, then the essential dimension of G is equal to the essential dimension of T.

Using compressions we are able to describe the behavior of essential dimension with respect to closed subgroups.

Theorem 3.4.15. Let G be an algebraic group and H a closed algebraic subgroup of G. Then

$$ed(H) + dim(H) \leqslant ed(G) + dim(G)$$

In particular, if G is finite, we have $ed(H) \leqslant ed(G)$.

Proof. Let $\mathbb{A}(V)$ be an affine space on which G acts generically freely. Take U open in $\mathbb{A}(V)$ such that U/G and U/H both exist and are torsors. Now take a G-compression

$$\begin{array}{ccc} U & \overset{g}{\dashrightarrow} & X \\ \downarrow & & \downarrow \\ U/G & \overset{h}{\dashrightarrow} & Y \end{array}$$

such that $dim(Y) = ed(G)$. Since the stabilizer in H of a point is a subgroup of G_x, it follows that H acts generically freely on U and on X too. Now g is also H-equivariant and by Lemma 3.4.10 g gives rise to an H-compression $U \to U/H$. It follows that

$$\begin{aligned} ed(H) &\leqslant dim(X) - dim(H) \\ &= dim(Y) + dim(G) - dim(H) \\ &= ed(G) + dim(G) - dim(H) \end{aligned}$$

□

We conclude this section with an example. Consider the algebraic group PGL_n over $Spec(k)$. There is a natural representation of $PGL_n(k)$ on the k-vector space $M_n(k) \times M_n(k)$ given by conjugation, that is

$$g(m_1, m_2) = (gm_1g^{-1}, gm_2g^{-1})$$

This gives a generically free representation of PGL_n. Then we obtain a torsor, whose generic fiber given a versal pair for PGL_n. More precisely we have a commutative diagram

$$\begin{array}{ccc} P & \longrightarrow & Spec(k[x_{ij}, y_{ij}]) \\ \downarrow & & \downarrow \\ Spec(k(x_{ij}, y_{ij})^{PGL_n(k)} & \longrightarrow & Spec(k[x_{ij}, y_{ij}])^{PGL_n(k)} \end{array}$$

where $1 \leqslant i, j \leqslant n$ and P is the generic torsor.

From the description of the relation between PGL_n torsors and Azumaya algebras, we see that from P one obtains a central simple algebra $M_n(k(x_{ij}, y_{ij}))^{PGL_n(k)}$, which is called also *universal algebra* and denoted by $UD(n)$. Then Corollary 3.4.14 tells us that $ed_k(PGL_n) = ed_k(UD(n))$.

Chapter 4

Computations

In this chapter we will use the general theory developed so far to give estimates of the essential dimension of PGL_n.

Upper bounds in the case of algebraically closed fields were first given in [16] by Lorenz and Reichstein, and then in the general case in [17] by Lorenz, Reichstein, Rowen and Saltman. We will also present estimates for the essential p-dimension, following [22], which were sharpened by A. Ruozzi in [32].

Lower bounds are more difficult to produce. The first lower bounds are due to Reichstein and Youssin in [27]. These were sharpened in the work of A. Merkurjev in [20], which we will follow.

4.1 Upper bounds

Here we give upper bounds of the essential of PGL_n for n odd using central simple algebras. Almost all the discussion in taken from [17].

4.1.1 Essential dimension of crossed products

In this subsection we will denote by G a finite group and H a subgroup of G. Let us briefly recall the main definitions. We will assume that the characteristic of the base field is coprime with the order of G.

Definition 4.1.1. A G-module is a left module over the ring $\mathbb{Z}[G]$. A *G-lattice* is a G-module that is free of finite rank over $\mathbb{Z}$. A G-lattice M is called a *permutation lattice* if M has a $\mathbb{Z}$-basis that is permuted by G, and *permutation projective* if M is a direct summand of some permutation G-lattice.

A G-module M is called faithful if the only element of G acting trivially is the identity. The G/H augmentation ideal $\omega(G/H)$ is defined as the kernel of the natural augmentation map $\mathbb{Z}[G/H] = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} \mathbb{Z} \to \mathbb{Z}$. Thus there is a short exact sequence of G-lattices

$$0 \to \omega(G/H) \to \mathbb{Z}[G/H] \to \mathbb{Z} \to 0$$

Lemma 4.1.2. Let $d_G(\omega(G/H))$ denote the minimum number of generators of $\omega(G/H)$ as a $\mathbb{Z}[G]$- module. For any $r \geqslant d_G(\omega(G/H))$ take an exact sequence

$$0 \to M \to \mathbb{Z}[G]^r \xrightarrow{f} \omega(G/H) \to 0$$

where f maps the standard basis of $\mathbb{Z}[G]^r$ to a set of r generators. Then M is a faithful G-lattice if and only if $r \geqslant 2$ or $H \neq \{1\}$.

Proof. It is enough to show that $M \otimes_{\mathbb{Z}} \mathbb{Q}$ is G-faithful, thus we may work over the algebra $\mathbb{Q}[G]$, which is semi-simple due to Maschke's theorem. Since $f \otimes id$ splits, we have a $\mathbb{Q}[G]$- isomorphism $(\omega(G/H) \otimes_{\mathbb{Z}} \mathbb{Q}) \oplus (M \otimes_{\mathbb{Z}} \mathbb{Q}) \cong \mathbb{Q}[G]^r$. Similarly, the canonical exact sequence $\mathbb{Z}[G]\omega H \to \mathbb{Z}[G] \to \mathbb{Z}[G/H]$ gives $(\omega(G/H) \otimes_{\mathbb{Z}} \mathbb{Q}) \oplus \mathbb{Q} \oplus \mathbb{Q}\omega H \cong \mathbb{Q}[G]$. Therefore, $M \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}[G]^{r-1} \oplus \mathbb{Q} \oplus \mathbb{Q}[G]\omega H$.

If $r \geqslant 2$ then $\mathbb{Q}[G]^{r-1}$ is G-faithful, and if $H \neq \{1\}$ then $\omega H \otimes_{\mathbb{Z}} \mathbb{Q}$ is H-faithful and so $\mathbb{Q}[G]\omega H \cong (\omega H \otimes_{\mathbb{Z}} \mathbb{Q}) \uparrow_H^G$ is G-faithful. In either case, $M \otimes_{\mathbb{Z}} \mathbb{Q}$ is faithful, as desired. On the other hand, $r = 1$ and $H = \{1\}$ leads to $M \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$ which is not faithful. □

We shall call a central simple algebra A/F an $(E, G/H)$-*crossed product* if A has a maximal subfield L whose Galois closure E over F has the property that $Gal(E/F) = G$ and $Gal(E/L) = H$. We will say that A is a G/H-crossed product if it is an $(E, G/H)$ crossed product for some faithful G-field E.

Since the degree of a G/H crossed product is equal to $[G : H]$, we see that isomorphism classes of $(E, G/H)$ crossed products are in bijective correspondence with the relative Brauer group $B(L/F)$, which is in turn identified with the kernel of the restriction homomorphism $H^2(G, E^*) \to H^2(H, E^*)$.

A G-module M is called H^1-*trivial* if $H^1(H, M) = 0$ for every $H \leqslant G$. Equivalently, M is H^1 trivial if $Ext_G(P, M) = 0$ for all permutation projective G-lattices P.

Lemma 4.1.3. Given an exact sequence $0 \to M \to P \to \omega(G/H) \to 0$ of G-lattices, with P permutation, let N be an H^1-trivial G-module. Denote the kernel of the restriction homomorphism $H^2(G, N) \to H^2(H, N)$ by $K(G/H, N)$. Then there is a natural isomorphism $\phi_N : Hom_G(M, N)/Im(Hom_G(P, N)) \to K(G/H, N)$.

Here the word 'natural' means that for every homomorphism $N \to N'$ of H^1-trivial G-modules, the following diagram commutes

$$\begin{array}{ccc} Hom_G(M,N)/Im(Hom_G(P,N)) & \xrightarrow{\phi_{N'}} & K(G/H,N') \\ \uparrow & & \uparrow \\ Hom_G(M,N)/Im(Hom_G(P,N)) & \xrightarrow{\phi_N} & K(G/H,N) \end{array}$$

Proof. See [30, Theorem 1.4]. □

In subsequent applications we will always take $N = E^*$, where E is a faithful G-field. Note that E^* is H^1-trivial by Hilbert's Theorem 90. In the identification of $K(G/H, E^*)$ with $(E, G/H)$ crossed products, we shall denote the $(E, G/H)$ crossed product associated to a G-homomorphism $f : M \to E^*$ by $Alg(f)$.

Definition 4.1.4. Let A/F and B/K be central simple algebras. We call B/K a *rational specialization* of A/F if there exists a field F' containing both F and K such that F'/K is rational and $B \otimes_K F' \cong A \otimes_F F'$. This is equivalent to requiring that $degA = degB$ and A embeds in some $B(t_1, ..., t_n)$, where $t_1, ..., t_n$ are independent variables over F.

If S is a set of central simple algebras, we say that an algebra A in S has the *rational specialization property* in S if every element of S is a rational specialization of A.

We need one more technical lemma.

Lemma 4.1.5. Let A/F and B/K be central simple algebras. If $A' \cong A \otimes_F F'$ for some rational field extension F'/F then $ed(A) = ed(A')$. In particular, if A is a rational specialization of B, then $ed(A) \leqslant ed(B)$.

Proof. See [17, Lemma 2.7]. □

Consider now an exact sequence of G-modules

$$0 \to M \to P \to \omega(G/H) \to 0$$

with P permutation and M faithful.

Lemma 4.1.6. Let E be a G-field and $f : M \to E^*$ be a homomorphism of G-modules. If $k(f(M))$ is contained in a faithful G-subfield E_0 of E then $Alg(f)$ is defined over E_0^G.

Proof. Since f is the composition of $f_0 : M \to E_0^*$ with the inclusion $E_0^* \hookrightarrow E^*$, Lemma 4.1.3 tells us that $A = Alg(f_0) \otimes_{E_0^G} E^G$. □

Theorem 4.1.7. Let $\mu : M \hookrightarrow k(M)^*$ be the natural inclusion. Then $D = Alg(\mu)$ has the rational specialization property in the class of G/H crossed products containing a copy of k in their center. In particular, $ed(A) \leqslant rank(M)$ for any G/H crossed product A/F with $k \subseteq F$.

Proof. Write $A = Alg(f)$ for some G-homomorphism $f : M \to E^*$, where E is a faithful G-field with $E^G = F$. Let $E(P)$ denote the fraction field of the group algebra $E[P]$,with the G-action induced from the G-action on E and P. By [17, Proposition 2.4], there exists an E-isomorphism $j : E(P) \cong E(t)$ of G-fields, where $t = (t_1, ..., t_r)$ are indeterminates on which G acts trivially and $r = rank(P)$. Therefore, $E(P)^G \cong E^G(t) = F(t)$ is a rational extension of F. Let $f_t : M \to E(t)^*$ denote the composition of f with the natural inclusion $E^* \hookrightarrow E(t)^*$. Then $Alg(f_t) = Alg(f) \otimes_F F(t) = A \otimes_F F(t)$. By

the Lemma 4.1.3, $Alg(f_t) \cong Alg(f_t + g|_M)$ for any $g \in Hom_G(P, E(t)^*)$. Let g be the composite $g : P \hookrightarrow E(P)^* \to E(t)^*$ and let φ be the G-module map $\varphi : M \to E(t)^*$ defined by $\varphi(m) = f_t(m)g(m)$. Now we will show that φ lifts to an embedding of G-fields $k(M) \hookrightarrow E(t)$. Indeed, modulo E^*, $\varphi(m) \equiv g(m) \in P \subseteq E(t)^*$. Hence, $\{\varphi(m)\}_{m\in M}$ is an E-linearly independent subset of $E(t)$, and so the map $k[\varphi] : k[M] \to E(t)$, is a G-equivariant embedding of the group ring $k[M]$ into $E(t)$. This embedding lifts to an embedding of G-fields $\phi : k(M) = Q(k[M]) \hookrightarrow E(t)$, as claimed. So $\phi \circ \mu = \varphi$, and hence $D \otimes_{k(M)^G} F(t) = Alg(\phi \circ \mu = Alg(\varphi) \cong Alg(f_t) = A \otimes_F F(t)$. This proves that A is a rational specialization of D.

The previous lemmas imply that $ed(A) \leqslant ed(D) \leqslant trdeg_k k(M)^G = rank(M)$. □

Corollary 4.1.8. Let A be a G/H crossed product. Then

$$ed(A) \leqslant r|G| - [G : H] + 1$$

where $r = d_G(\omega(G/H))$ if $H \neq \{1\}$ and $r = max\{2, d_G(\omega(G/H))\}$ if $H = \{1\}$.

Proof. Applying Theorem 4.1.7 to an exact sequence

$$0 \to M \to \mathbb{Z}[G]^r \xrightarrow{f} \omega(G/H) \to 0$$

we obtain

$$ed(A) \leqslant rank(M) = rank(\mathbb{Z}[G]^r) - rank(\omega(G/H)) = r|G| - [G : H] + 1$$

□

4.1.2 Brauer factor sets

Here we briefly review some results of the theory of Brauer factor sets, following [29]. Let A be a central simple algebra over k of degree n. Suppose K is a maximal separable subfield of A over k and E is the normal closure of K, with $G = Gal(E/k)$. Then $K = k(u)$ for some u in K, implying that the minimal polynomial of u has degree n, and E is its splitting field over K. Let r_i be its roots in E, for $1 \leqslant i \leqslant n$. The group G permutes the r_i and thus can be viewed as a subgroup of the permutation group on n elements.

There exists an element v in A such that $A = KvK$, and one can view naturally $A \subseteq A \otimes_k K \cong M_n(K) \subseteq M_n(E)$. Write $v = (v_{ij}) \in M_n(E)$, where each v_{ij} is non-zero due to $A = KvK$. Let $c_{ijk} = v_{ij}v_{jk}v_{ik}^{-1}$. Then the set of the c_{ijk} satisfies the following conditions:
1) $\sigma c_{ijk} = c_{\sigma i,\sigma j,\sigma k}$ for all σ in G
2) $c_{ijk}c_{ikm} = c_{ijm}c_{jkm}$.

A set of n^3 elements in E that satisfies these conditions is called *Brauer factor set*. We show now that conversely, a Brauer factor set gives rise to a

central simple algebra. Let (c_{ijk}) be a Brauer factor set and consider the k-vector subspace $A = \{(a_{ij}) \in M_n(E) | \sigma a_{ij} = a_{\sigma i,\sigma j} \text{ for all } \sigma \text{ in } G\}$. On A we define an associative multiplication by the rule

$$(a_{ij})(b_{ij}) = \sum_{j=1}^{n} (a_{ij} c_{ijk} b_{jk}) e_{ik}$$

Then A is a simple k-algebra which can be injected into $M_n(E)$ via the map $(a_{ij}) \to \sum_j (c_{ij1} a_{ij}) e_{ij}$. If we take the trivial Brauer set that is identically 1, then we obtain the matrix algebra.

Suppose that (c_{ijk}) and (c'_{ijk}) are Brauer factor sets with respect to the same field K/k. The ensuing simple algebras are isomorphic if and only if there are some elements w_{ij} in E such that:
1) $\sigma w_{ij} = w_{\sigma i,\sigma j}$
2) $c'_{ijk} = w_{ij} w_{jk} w_{ik}^{-1} c_{ijk}$.

In these case the two sets are called *equivalent*. A Brauer set (c_{ijk}) is called *normalized* if $c_{iij} = c_{iji} = c_{jii} = 1$ and $c_{kji} = c_{ijk}^{-1}$ for all i, j, k.

Let us state now the results that we will need.

Theorem 4.1.9. For any Brauer factor set (c_{ijk}) there is a normalized Brauer factor set equivalent to $(c_{ijk})^2$. In particular, if n is odd then every Brauer factor set has an equivalent normalized Brauer factor set.

Proof. Let $c'_{ijk} = c_{ijk} c_{kji}^{-1}$. Then (c'_{ijk}) is a normalized Brauer set equivalent to (c_{ijk}). In n is odd, consider $c''_{ijk} = (c'_{ijk})^{(n+1)/2}$. This is normalized and equivalent to (c_{ijk}). See [29, Theorem 4] for more detail. □

We will need the following version of Lemma 4.1.6.

Proposition 4.1.10. Let A be an $(E, G/H)$ crossed product defined by a reduced Brauer factor set (c_{ijh}). Suppose that (c_{ijh}) is contained in a faithful G-subfield E_0 of E. Then A is defined over E_0^G.

Proof. There is an exact sequence

$$0 \to \omega(G/H)^{\otimes_{\mathbb{Z}}^2} \to P' \to \omega(G/H) \to 0$$

where P is the permutation sublattice $P = \bigoplus_{\bar{g_1} \neq \bar{g_2} \in G/H} \mathbb{Z}(\bar{g_1} \otimes_{\mathbb{Z}} \bar{g_2})$ of $\mathbb{Z}[G/H]^{\otimes_{\mathbb{Z}}^2}$.

In fact, tensoring the exact sequence $0 \to \omega(G/H) \to \mathbb{Z}[G/H] \to \mathbb{Z} \to 0$ with $\omega(G/H)$ on $\mathbb{Z}$ we obtain the previous one via the identification $\omega(G/H) \otimes_{\mathbb{Z}} \mathbb{Z}[G/H] \cong P$ given by sending the elements $(\bar{g_1} - \bar{g_2}) \otimes_{\mathbb{Z}} \bar{g_2}$ to $\bar{g_1} \otimes_{\mathbb{Z}} \bar{g_2}$.

The G-module $\omega(G/H)^{\otimes_{\mathbb{Z}}^2}$ has the convenient set of generators $y_{ijh} = (\bar{g_i} - \bar{g_j}) \otimes_{\mathbb{Z}} (\bar{g_j} - \bar{g_h})$, where i, j, h range from 1 to $[G : H]$. If $f : \omega(G/H)^{\otimes_{\mathbb{Z}}^2} \to E^*$ is a G-module homomorphism then the elements $c_{ijh} = f(y_{ijh})$ form a reduced Brauer factor set for $Alg(f)$. Conversely, for any reduced Brauer factor set (c_{ijh}) in E^*, there exists a homomorphism $f : \omega(G/H)^{\otimes_{\mathbb{Z}}^2} \to E^*$ such that $f(y_{ijh}) = c_{ijh}$: see [30, Corollary 1.3]. □

4.1.3 Universal algebras

In this subsection we shall assume that $G = S_n$ and $H = S_{n-1}$. We will use the notations $\mathbb{Z}[S_n/S_{n-1}] = U_n$ and $\omega(S_n/S_{n-1}) = A_{n-1}$. The natural generators of U_n will be denoted by $u_1, ..., u_n$ and the symmetric group S_n permutes them via $\sigma(u_i) = u_{\sigma(i)}$. Notice that A_{n-1} is the sublattice of U_n generated by $u_i - u_1$ as i ranges from 2 to n.

Recall that the universal division algebra $UD(n)$ is the localisation over the non-central elements of the algebra generated by two generic matrices X and Y. It is a division algebra of degree n by [28, Theorem 3.2.6]. We may assume without loss of generality that X is diagonal and we denote the diagonal entries of X by ζ'_{ii} and the entries of Y by ζ_{ij}, where ζ'_{ii} and ζ_{ij} are algebraically independent variables over k. The group S_n permutes these variables as follows : $\sigma(\zeta'_{ii}) = \zeta_{\sigma(i)\sigma(i)'}$ and $\sigma(\zeta_{ij}) = \zeta_{\sigma(i)\sigma(j)}$.

We identify the multiplicative group generated by ζ'_{ii} with the S_n lattice U_n via $\zeta'_{ii} \leftrightarrow u_i$, and the multiplicative group generated by ζ_{ij} with $U_n \otimes_{\mathbb{Z}} U_n$ via $\zeta_{ij} \leftrightarrow u_i \otimes_{\mathbb{Z}} u_j$. Consider the exact sequence

$$0 \to Ker(f) \to U_n \oplus U_n^{\otimes_{\mathbb{Z}} 2} \xrightarrow{f} A_{n-1} \to 0$$

of S_n-lattices, where $f(u_i, u_j \otimes u_h) = u_j - u_h$. This sequence is the sequence of Proposition 4.1.10 for $G = S_n$ and $H = S_{n-1}$, with two extra copies of U_n added: the second copy of U_n is the sublattice of $U_n^{\otimes_{\mathbb{Z}} 2}$ that is spanned by all elements $u_i \otimes u_i$. Both copies of U_n belong to $Ker(f)$, and in fact $Ker(f) = U_n \oplus U_n \oplus A_{n-1}^{\otimes_{\mathbb{Z}} 2}$, where $A_{n-1}^{\otimes_{\mathbb{Z}} 2}$ is identified with the sublattice of $U_n^{\otimes_{\mathbb{Z}} 2}$ that is spanned by all elements $(u_i - u_j) \otimes (u_l - u_m)$.

Let $E = k(Ker(f))$ and $F = E^{S_n}$. By [8, Theorem 3] Theorem 3, F is naturally isomorphic to the center $Z(n)$ of $UD(n)$. Note that $E = F(\zeta'_{11}, ..., \zeta'_{nn})$ is generated over F by the eigenvalues of the generic matrix X. Consequently, $UD(n)$ is an $(E, S_n/S_{n-1})$ product and $E^{S_{n-1}}$ is isomorphic to the maximal subfield $Z(n)(X)$ of $UD(n)$; see [24] Section II.1.

Theorem 4.1.11. Let $n \geqslant 5$ be an odd integer. Then $UD(n)$ is defined over $F_0 = k(\bigwedge^2 A_{n-1})^{S_n}$.

Proof. We need to construct a reduced Brauer factor set contained in $E_0 = k(\bigwedge^2 A_{n-1})$. Note that the S_n action on E_0 is faithful.

The computation in [29] Section 2 shows that the elements $c_{ijh} = \zeta_{ij}\zeta_{jh}\zeta_{ih}^{-1} \in E^*$ form a Brauer factor set of $UD(n)$. If n is odd, $UD(n)$ has a normalized Brauer factor set (c'_{ijh}) given by

$$c'_{ijh} = (c_{ijh}/c_{hji})^{\frac{n+1}{2}} = (\zeta_{ij}\zeta_{ji}^{-1}\zeta_{jh}\zeta_{hj}^{-1}\zeta_{hi}\zeta_{ih}^{-1})^{\frac{n+1}{2}}$$

Now observe that $\zeta_{ij}\zeta_{ji}^{-1}\zeta_{jh}\zeta_{hj}^{-1}\zeta_{hi}\zeta_{ih}^{-1}$ is precisely the element of $U_n^{\otimes_{\mathbb{Z}} 2}$ we identified with $(u_i - u_j) \wedge (u_j - u_h)$. □

We have seen in the previous chapter that the universal division algebra gives a versal pair for the algebraic group PGL_n, so we have obtained an upper bound for the essential dimension of PGL_n for n odd.

Theorem 4.1.12. The essential dimension of $PGL_{n,k}$ is at most $(n-1)(n-2)/2$ if $n \geqslant 5$ is odd.

4.1.4 Essential p-dimension

In this subsection we prove an upper bound for the essential p-dimension of PGL_n. This will be a consequence of an upper bound of the essential dimension of crossed products with certain properties. Here we follow the work of Meyer and Reichstein, [22]

In the sequel we will use once more the notation introduced at the beginning of the chapter.

Lemma 4.1.13. Let $G \neq \{1\}$ be a finite group, H be a subgroup of G and $H_1, ..., H_r$ be subgroups of H. Let

$$0 \to M \to \bigoplus_{i=1}^{r} \mathbb{Z}[G/H_i] \to \omega(G/H) \to 0$$

be an exact sequence of G-lattices. Assume that H does not contain any nontrivial normal subgroup of G. Then the G-action on M is not faithful if and only if $s = 1$ and $H_1 = H$.

Proof. To determine whether or not the G-action on M is faithful, we may replace M by $M_{\mathbb{Q}} = M \otimes_{\mathbb{Z}} \mathbb{Q}$. After tensoring with $\mathbb{Q}$, the sequence splits, and we have an isomorphism $\omega(G/H)_{\mathbb{Q}} \oplus M_{\mathbb{Q}} \cong \oplus_{i=1}^{r} \mathbb{Q}[G/H_i]$.

Assume that $r \geqslant 2$. Then H_r is a subgroup of H, we have a natural surjective map $\mathbb{Q}[G/H_r] \to \mathbb{Q}[G/H]$. Using complete irreducibility over $\mathbb{Q}$ once again, we see that $\mathbb{Q}[G/H]$ is a subrepresentation of $\mathbb{Q}[G/H_r]$. Thus the previous isomorphism tells us that $\mathbb{Q}[G/H_{r-1}]$ is a subrepresentation of $M_{\mathbb{Q}}$. The kernel of the G-representation on $\mathbb{Q}[G/H_{r-1}]$ is a normal subgroup of G contained in H_{r-1}; by our assumption on H, any such subgroup is trivial. This shows that H acts faithfully on $\mathbb{Q}[G/H_{r-1}]$ and hence on M.

Assume now that $r = 1$. Our exact sequence assumes the form

$$0 \to M_{\mathbb{Q}} \to \mathbb{Q}[G/H_1] \to \omega(G/H)_{\mathbb{Q}} \to 0$$

If $H = H_1$ then $M \cong \mathbb{Z}$, with trivial G-action.

We want to show that if $H_1 \subset H$ then the G-action on $M_{\mathbb{Q}}$ is faithful. Denote by $\mathbb{Q}[1]$ the trivial representation of some group. Observe that

$$\begin{aligned}
\mathbb{Q}[G/H_1] &\cong Ind_{H_1}^{G} \mathbb{Q}[1] \cong Ind_{H}^{G} Ind_{H_1}^{H} \mathbb{Q}[1] \cong Ind_{H}^{G} \mathbb{Q}[H/H_1] \\
&\cong Ind_{H}^{G} (\omega(H/H_1)_{\mathbb{Q}} \oplus \mathbb{Q}[1] \\
&\cong Ind_{H}^{G} \omega(H/H_1)_{\mathbb{Q}} \oplus \mathbb{Q}[G/H] \\
&\cong Ind_{H}^{G} \omega(H/H_1)_{\mathbb{Q}} \oplus \omega(G/H)_{\mathbb{Q}} \oplus \mathbb{Q}[1]
\end{aligned}$$

and we obtain $M_{\mathbb{Q}} \cong Ind_{H}^{G} \omega(H/H_1)_{\mathbb{Q}} \oplus \mathbb{Q}[1]$. If $H_1 \subset H$, then the kernel of the G-representation $Ind_{H}^{G} \omega(H/H_1)_{\mathbb{Q}}$ is a normal subgroup of G contained in H_1. By our assumption on H, this kernel is trivial. □

Lemma 4.1.14. Let V be a $\mathbb{Z}[G]$-submodule of $\omega(G/H)$. Then the set $G_V = \{g \in G | \bar{g} - \bar{1} \in V\}$ is a subgroup of G containing H.

Proof. The inclusion $H \subseteq G_V$ follows directly from the definition.

To see that G_V is closed under multiplication, suppose $g, g' \in G_V$, so that $\bar{g} - \bar{1}$ and $\bar{g'} - \bar{1}$ lie in V. Then

$$\overline{gg'} - \bar{1} = g \cdot (\bar{g'} - \bar{1}) + (\bar{g} - \bar{1})$$

also lies in V. □

Definition 4.1.15. We say that $g_1, ..., g_s \in G$ generate G over H if the subgroup generated by $g_1, ..., g_s$ and H is the entire G.

Theorem 4.1.16. Let A be a G/H crossed product. Suppose that
1) $g_1, ..., g_s \in G$ generate G over H
2) if G is cyclic then $H \neq \{1\}$.
Then $ed(A) \leqslant \sum_{i=1}^{s} [G : (H \cap H^{g_i})] - [G : H] + 1$.

Proof. We claim that the elements $\bar{g_1} - \bar{1}, ..., \bar{g_s} - \bar{1}$ generate $\omega(G/H)$ as a $\mathbb{Z}[G]$-module.

Indeed, let V be the $\mathbb{Z}[G]$-submodule of $\omega(G/H)$ generated by these elements. Lemma 4.1.14 and condition (1) tell us that V contains $\bar{g} - \bar{1}$ for every $g \in G$. Translating these elements by G, we see that V contains $\bar{a} - \bar{b}$ for every $a, b \in G$. Hence, $V = \omega(G/H)$, as claimed.

For $i = 1, ..., s$, let $S_i = \{g \in G | g \cdot (\bar{g_i} - \bar{1}) = \bar{g_i} - \bar{1}\}$ be the stabilizer of $\bar{g_i} - \bar{1}$ in G. We may assume here that g_i is not in H, otherwise it could be removed since it is not needed to generate G over H. Then clearly $g \in S_i$ if and only if $\overline{gg_i} = \bar{g_i}$ and $\bar{g} = \bar{1}$. From this it is easily seen that $S_i = H \cap H^{g_i}$. Thus we have an exact sequence

$$0 \to M \to \oplus_{i=1}^{s} \mathbb{Z}[G/S_i] \xrightarrow{\phi} \omega(G/H) \to 0$$

where ϕ sends a generator of $\mathbb{Z}[G/S_i]$ to $\bar{g_i} - \bar{1} \in \omega(G/H)$. By Theorem 4.1.7 it remains to show that G acts faithfully on M.

By Lemma 4.1.13 G fails to act faithfully on M if and only if $r = 1$ and $S_1 = H = H^{g_1}$. But this possibility is ruled out by (2). Indeed, assume that $s = 1$ and $S_1 = H = H^{g_1}$. Then $G = \langle g_1, H \rangle$ and $H = H^{g_1}$. Hence, H is normal in G. Condition (2) tells us that $H = \{1\}$. Moreover, in this case $G = \langle g_1, H \rangle = \langle g_1 \rangle$ is cyclic, contradicting (2). □

Theorem 4.1.17. Let A be a G/H-crossed product. Suppose that H is contained in a normal subgroup N of G and G/H is generated by r elements. Furthermore, assume that either $H \neq \{1\}$ or $r \geqslant 2$. Then

$$ed(A) \leqslant r[G : H] \cdot [N : H] - [G : H] + 1$$

Proof. Let $t_1, ..., t_r \in G/N$ be a set of generators for G/N. Choose $g_1, ..., g_r \in G$ representing $t_1, ..., t_r$ and let $H' = \langle H, H^{g_1}, ..., H^{g_r} \rangle$. Since $H \leqslant N$ and N is normal in G, H' is a subgroup of N. The group H' depends on the choice of $g_1, ..., g_r \in G$ such that $g_i N = t_i$. Fix $t_1, ..., t_r$ and choose $g_1, ..., g_r \in G$ representing them, so that H' has the largest possible order; this is equivalent to requiring that it has the smallest possible index in N, which we denote by m. In particular $m = [N : H'] \leqslant [N : (H^{g_i g} \cdot H)]$ for any $i = 1, ..., r$ and any $g \in N$.

Choose a set of representatives $n_1 = 1, n_2, ..., n_m \in N$ for the distinct left cosets of H' in N. We will show that the elements $\{g_i n_j | i = 1, ..., r; j = 1, ..., m\}$ generate G over H. Indeed, let G_0 be the subgroup of G generated by these elements and H. Since $n_1 = 1$, G_0 contains $g_1, ..., g_r$, hence G_0 contains H'. Moreover, G_0 contains $n_j = g_1^{-1}(g_1 n_j)$ for every j, hence G_0 contains all of N. Finally, since $t_1 = g_1 N, ..., t_r = g_r N$ generate G/N, we conclude that G_0 contains all of G.

We now apply Theorem 4.1.16 to the elements $\{g_i n_j\}$. Substituting

$$[G : H] \cdot [H : (H \cdot H^{g_i n_j})]$$

for $[G : (H \cap H^{g_i n_j})]$, we calculate

$$\begin{aligned} ed(a) &\leqslant \sum_{i=1}^{r} \sum_{j=1}^{m} [G : (H \cap H^{g_i n_j})] - [G : H] + 1 \\ &= [G : H] \cdot \sum_{i=1}^{r} \sum_{j=1}^{m} [H : (H \cdot H^{g_i n_j}) - [G : H] + 1 \\ &= [G : H] \cdot \sum_{i=1}^{r} \sum_{j=1}^{m} \frac{[N : H]}{[N : (H \cdot H^{g_i n_j})]} - [G : H] + 1 \\ &\leqslant [G : H] \cdot \sum_{i=1}^{r} \sum_{j=1}^{m} \frac{[N : H]}{m} - [G : H] + 1 \\ &= r[G : H] \cdot [N : H] - [G : H] + 1 \end{aligned}$$

□

Corollary 4.1.18. Let A/K be a central simple algebra of degree n. Suppose that A contains a field F, Galois over K and $Gal(F/K)$ can be generated by $r \geqslant 1$ elements. If $[F : K] = n$ then we further assume that $r \geqslant 2$. Then

$$ed(A) \leqslant r \frac{n^2}{[F : K]} - n + 1$$

Proof. By [22, Lemma 2.1] we may assume that F is contained is a subfield L of A such that L/K is a separable extension of degree $n = deg(A)$. Denote by E the Galois closure of L over K and by G the associated Galois group. Consider also $H = Gal(E/L)$ and $N = Gal(E/F)$. Then A/K is a G/H-crossed product, and it suffices to apply the previous theorem. □

Corollary 4.1.19. Let $n = p^s$ for some natural number $s \geqslant 2$. Then

$$ed(PGL_n; p) \leqslant 2\frac{n^2}{p^2} - n + 1$$

Proof. Call $A = UD(n)$ the universal algebra. In [31] Rowen and Saltman showed that $A' = A \otimes_K K'$ contains a field F, Galois over K' with $Gal(F/K) \cong \mathbb{Z}/p \times \mathbb{Z}/p$. Thus Corollary 4.1.18 tells us that

$$ed(PGL_n; p) = ed(A; p) \leqslant ed(A') \leqslant 2\frac{n^2}{p^2} - n + 1$$

This is the thesis. □

4.2 Lower bounds

As previously mentioned, here we follow the work of Merkurjev in [20]. We refer to the book of J.P. Serre [33] for Galois cohomology and profinite groups.

4.2.1 Preliminaries

Let k be a base field, k^s a separable closure and $\Gamma = Gal(k^s/k)$. The *character group* $Ch(k)$ of k is defined as

$$Hom_{cont}(\Gamma, \mathbb{Q}/\mathbb{Z}) = H^1(k, \mathbb{Q}/\mathbb{Z}) \cong H^2(k, \mathbb{Z})$$

where $Hom_{cont}(\Gamma, \mathbb{Q}/\mathbb{Z})$ are the continuous homomorphism from the profinite group Γ to the discrete group $\mathbb{Q}/\mathbb{Z}$. For a character $\chi \in Ch(k)$, set $k(\chi) = (k^s)^{Ker(\chi)}$. If $\phi \subseteq Ch(k)$ is a finite subgroup, set $k(\phi) = (k^s)^{\cap Ker(\chi)}$, where the intersection is taken over all $\chi \in \phi$. The Galois group $G = Gal(k(\phi)/k)$ is abelian and ϕ is canonically isomorphic to the character group $Ch(G) = Hom(G, \mathbb{Q}/\mathbb{Z})$ of G.

If $k' \subseteq k$ is a subfield and $\chi \in Ch(k')$, we write χ_k for the image of χ under the natural map $Ch(k') \to Ch(k)$ and $k(\chi)$ for $k(\chi_k)$.

Remark 4.2.1. If $\phi \subseteq Ch(k)$ is a finite subgroup, then the character $\chi_{k(\phi)}$ is trivial if and only if $\chi \in \phi$.

Lemma 4.2.2. Let $\phi, \phi' \subseteq Ch(k)$ be two finite subgroups. Suppose that for a field extension K/k, we have $\phi_K = \phi'_K$ in $Ch(K)$. Then there is a finite subextension K'/k in K/k such that $\phi_{K'} = \phi'_{K'}$ in $Ch(K')$.

Proof. Choose a set of characters $\{\chi_1, ..., \chi_m\}$ generating ϕ and a set of characters $\{\chi'_1, ..., \chi'_m\}$ generating ϕ' such that $(\chi_i)_K = (\chi'_i)_K$ for all i. Let $\eta_i = \chi_i - \chi'_i$. As all η_i vanish over K, the finite field extension $K' = k(\eta_1, ..., \eta_m)$ of k can be viewed as a subextension in K/k. As $(\chi_i)_{K'} = (\chi'_i)_{K'}$, we have $\phi_{K'} = \phi'_{K'}$. □

Consider now the cup-product

$$Ch(k) \otimes_{\mathbb{Z}} k^* = H^2(k, \mathbb{Z}) \otimes_{\mathbb{Z}} H^0(k, (k^s)^*) \to Br(k)$$

that takes $\chi \otimes a$ to the class $\chi \cup (a)$ in $Br(k)$ that is split by $k(\chi)$.

For a finite subgroup $\phi \subseteq Ch(k)$ write $Br_{dec}(k(\phi)/k)$ for the *subgroup of decomposable elements* in $Br(k(\phi)/k)$ generated by the elements $\chi \cup (a)$ for all $\chi \in \phi$ and $a \in k^*$. The *indecomposable relative Brauer group* $Br_{ind}(k(\phi)/k)$ is the factor group $Br(k(\phi)/k)/Br_{dec}(k(\phi)/k)$.

Let now E be a complete field with respect to a discrete valuation v and K its residue field. Let p be a prime integer different from $char(K)$. There is a natural injective homomorphism $Ch(K)\{p\} \to Ch(E)\{p\}$ of the p-primary components of the character groups that identifies $Ch(K)\{p\}$ with the character group of an unramified field extension of E. For a character $\chi \in Ch(K)\{p\}$, we write $\hat{\chi}$ for the corresponding character in $Ch(E)\{p\}$. By [9] Chapter 7.9. there is an exact sequence

$$0 \to Br(K)\{p\} \xrightarrow{i} Br(E)\{p\} \xrightarrow{\partial_v} Ch(K)\{p\} \to 0$$

If $a \in Br(K)\{p\}$, then we write $\hat{a}$ for the element $i(a)$ in $Br(E)\{p\}$. It holds, for example, that if $a = \chi \cup (\bar{u})$ for some $\chi \in Ch(K)\{p\}$ and a unit $u \in E$, then $\hat{a} = \hat{\chi} \cup (u)$.

Proposition 4.2.3. Let E be a complete field with respect to a discrete valuation v and K its residue field of characteristic different from p. Then
1) $ind(\hat{a}) = ind(a)$ for any $a \in Br(K)\{p\}$
2) Let $b = \hat{a} + (\chi \cup (x))$ for an element $a \in Br(K)\{p\}$, $\chi \in Ch(K)\{p\}$ and $x \in E^*$ such that $v(x)$ is not divisible by p. Then $ind(b) = ind(a_{K(\chi)}) \cdot ord(\chi)$
3) Let E'/E be a finite field extension and v' the discrete valuation on E' extending v with residue field K'. Then for any $b \in Br(E)\{p\}$, one has $\partial_{v'}(b_{E'}) = e \cdot \partial_v(b)_{K'}$, where e is the ramification index of E'/E.

Proof. See [9, Proposition 8.2]. □

The choice of a prime element π in E provides with a splitting of the sequence (1) by sending a character χ to the class $\hat{\chi} \cup (\pi)$ in $Br(E)\{p\}$. Thus, any $b \in Br(E)\{p\}$ can be written in the form $b = \hat{a} + (\hat{\chi} \cup (\pi))$ for $\chi = \partial_v(b)$ and a unique $a \in Br(K)\{p\}$.

The homomorphism

$$s_\pi : Br(E)\{p\} \to Br(K)\{p\}$$

defined by $s_\pi(b) = a$, where a is given by the above relation, is called a *specialization* map. We have $s_\pi(\hat{a}) = a$ for any $a \in Br(K)\{p\}$ and $s_\pi(\hat{\chi} \cup (x)) = \chi \cup (\bar{u})$, where $\chi \in Ch(K)\{p\}$, $x \in E^*$ and u is the unit in E such that $x = u\pi^{v(x)}$.

Moreover, if v is trivial on a subfield $k \subseteq E$ and $\phi \subseteq Ch(k)\{p\}$ a finite subgroup, then $s_\pi(Br_{dec}(E(\phi)/E)) \subseteq Br_{dec}(K(\phi)/K)$.

Remark 4.2.4. For an abelian group A we write ${}_pA$ for the subgroup of all elements in A of exponent p.

This technical lemma will be used later on.

Lemma 4.2.5. Let (E, v) be a complete discrete valued field with the residue field K of characteristic different from p containing a primitive p^2-th root of unity. Let $\eta \in Ch(E)$ be a character of order p^2 such that $p \cdot \eta$ is unramified, that is $p \cdot \eta = \hat{\nu}$ for some $\nu \in Ch(K)$ of order p. Let $\chi \in_p Ch(K)$ be a character linearly independent from ν. Let $a \in Br(K)$ and set $b = \hat{a} + (\hat{\chi} \cup (x)) \in Br(E)$, where $x \in E^*$ is an element such that $v(x)$ is not divisible by p. Then
1) If η is unramified, that is $\eta = \hat{\mu}$ for some $\mu \in Ch(K)$ of order p^2, then $ind(b_{E(\eta)}) = p \cdot ind(a_{K(\mu,\chi)})$
2) If η is ramified, then there exists a unit $u \in E^*$ such that $K(\nu) = K(\bar{u}^{1/p})$ and $ind(b_{E(\eta)}) = ind(a - (\chi \cup (\bar{u}^{1/p})))_{K(\nu)}$.

Proof. (1) If $\eta = \hat{\mu}$ for some $\mu \in Ch(K)$, then $K(\mu)$ is the residue field of $E(\eta)$ and we have

$$b_{E(\eta)} = \hat{a}_{K(\mu)} + (\hat{\chi}_{K(\mu)} \cup (x))$$

As χ and ν are linearly independent, the character $\chi_{K(\mu)}$ is nontrivial. The first statement follows from Proposition 4.2.3 (2).

(2) Since $p \cdot \eta$ is unramified, the ramification index of $E(\eta)/E$ is equal to p, hence $E(\eta) = E((ux^p)^{1/p^2})$ for some unit $u \in E$. Note that $K(\nu) = K(\bar{u}^{1/p})$ is the residue field of $E(\eta)$. As $u^{1/p}x$ is a p-th power in $E(\eta)$, the class

$$b_{E(\eta)} = \hat{a}_{K(\nu)} - (\hat{\chi}_{K(\nu)} \cup (u^{1/p}))$$

is unramified. It follows from Proposition 4.2.3 (1) that the elements $b_{E(\eta)}$ in $Br(E(\eta))$ and $a_{K(\nu)} - (\chi_{K(\nu)} \cup (\bar{u}^{1/p}))$ in $Br(K(\nu))$ have the same indices. □

4.2.2 Brauer group and algebraic tori

Remark 4.2.6. Let S be an algebraic torus over k. We embed S into the quasi-trivial torus $P = R_{L/k}(\mathbb{G}_{m,L})$, where L in an étale k-algebra and $R_{L/k}$ is the Weil restriction. Then S acts on the vector space L by multiplication, so that the action on P is regular. If T is the factor torus P/S, then the S-torsor $P \to T$ is versal.

Let F be a field, ϕ a subgroup of ${}_pCh(F)$ of rank r and $L = F(\phi)$. Let $G = Gal(L/F)$ and choose a basis $\chi_1, ..., \chi_r$ of ϕ. We can view each χ_i as a character of G, that is a homomorphism $\chi_i : G \to \mathbb{Q}/\mathbb{Z}$. Let $\sigma_1, ..., \sigma_r$ be the dual basis for G, that is $\chi_i(\sigma_j) = (\frac{1}{p} + \mathbb{Z})\delta_{ij}$.

We call R the group ring $\mathbb{Z}[G]$. Consider the surjective homomorphism of G-modules $k : R^r \to R$ taking the basis element e_i to $\sigma_i - 1$; the image of k is the augmentation ideal I of R. Define N_i the element $1 + \sigma_i + \sigma_i^2 + \cdots + \sigma_i^{p-1}$ of R, and call $N = ker(k)$.

Lemma 4.2.7. Consider the elements $e_{ij} = (\sigma_i - 1)e_j - (\sigma_j - 1)e_i$ and $f_i = N_i e_i$ for $i, j = 1, ..., r$. The G-module N is generated by e_{ij} and f_i.

Proof. See [20, Lemma 3.4]. □

Now let $\epsilon_i : R^r \to \mathbb{Z}$ be the i-th projection followed by the augmentation map ϵ. It follows from the lemma that $\epsilon_i(N) = p\mathbb{Z}$ for every i. Moreover, the G-homomorphism $l : N \to \mathbb{Z}^r$ defined by $m \to (\epsilon_1(m)/p, ..., \epsilon_r(m)/p)$ is surjective. Set $M = Ker(l)$ and $Q = R^r/M$.

Lemma 4.2.8. The G-module M is generated by the e_{ij}.

Proof. See [20, Lemma 3.5]. □

Let P^ϕ, S^ϕ, T^ϕ and V^ϕ be the algebraic tori over F with character G-modules R^r, Q, M, I and N, respectively.

Let K/F be a field extension and set $KL = K \otimes_F L$. The exact sequence of G-modules $0 \to I \to R \to \mathbb{Z}$ gives an exact sequence of the tori

$$1 \to \mathbb{G}_m \to R_{L/F}(\mathbb{G}_{m,L}) \to U \to 1$$

Taking cohomology we obtain the exact sequence

$$0 \to H^1(K, U^\phi) \to H^2(K, \mathbb{G}_m) \to H^2(KL, \mathbb{G}_m)$$

Hence $H^1(K, U^\phi) \cong Br(KL/K)$.

Lemma 4.2.9. The homomorphism $(K^*)^r \to H^1(K, U^\phi) \cong Br(KL/K)$ induced by

$$U^\phi \to S^\phi \to \mathbb{G}_m^r$$

takes $(x_1, ..., x_r)$ to $\sum_{i=1}^r ((\chi_i)_K \cup (x_i))$.

Proof. See [20, Lemma 3.6]. □

Corollary 4.2.10. The map $H^1(K, U^\phi) \to H^1(K, S^\phi)$ induces an isomorphism $H^1(K, S^\phi) \cong Br_{ind}(KL/K)$.

The previous Corollary and the triviality of the group $H^1(K, P^\phi)$ give us a commutative diagram

$$\begin{array}{ccccc} V(K) & \longrightarrow & H^1(K, U^\phi) & = & Br(KL/K) \\ \downarrow & & \downarrow & & \downarrow \\ T(K) & \longrightarrow & H^1(K, S^\phi) & = & Br_{ind}(KL/K) \end{array}$$

with surjective homomorphisms.

Consider $K = F(V)$ and choose an element

$$a \in Br(L(T)/F(T)) \tag{4.2.1}$$

corresponding to the generic point of T over $F(T)$ in the above diagram. Consider also the exact sequence of G-modules

$$0 \to L^* \oplus N \to L(V)^* \to Div(V_L) \to 0$$

Then $H^2(G, N) \cong \mathbb{Z}/p^r\mathbb{Z}$, see [20] 3.3.

Lemma 4.2.11. If $r \geqslant 2$, then the class $p^{r-1}a$ in $Br(F(T))$ does not belong to the image of $Br(F) \to Br(F(T))$.

Proof. See [20, Corollary 3.9]. □

4.2.3 Essential dimension of algebraic tori

Let S be an algebraic torus over F with splitting group G. We assume that G is a p-group of order p^r. Let X be the G-module of characters of S. A p-presentation of X is a G-homomorphism $f : P \to X$ with P a permutation G-module and finite cokernel of order prime to p. A p-presentation with the smallest rank is called *minimal*.

Theorem 4.2.12. Let S be an algebraic torus over F as above and $f : P \to X$ a minimal p-presentation of X. Then $ed_p(S) = rank(Ker(f))$.

Proof. See [18, Theorem 1.4]. □

Corollary 4.2.13. Suppose that X admits a surjective minimal p-presentation $f : P \to X$. Then $ed(S) = ed_p(S) = rank(Ker(f))$.

Proof. A surjective G-homomorphism f yields a generically free representation of S of dimension $rank(P)$. Then

$$ed_p(S) \leqslant ed(S) \leqslant rank(P) - dim(S) = rank(Ker(f))$$

□

In this subsection we derive from Theorem 4.2.12 an explicit formula for the essential p-dimension of algebraic tori. Define the group $\overline{X} = X/(pX + IX)$. For any subgroup $H \subseteq G$, consider the composition $X^H \hookrightarrow X \to \overline{X}$. For every k, let V_k denote the image of the homomorphism $\coprod_{H \subseteq G} X^H \to \overline{X}$, where the coproduct is taken over all subgroups H with $[G : H] \leqslant p^k$. We have the sequence of subgroups $0 = V_{-1} \subseteq V_0 \subseteq \cdots \subseteq V_r = \overline{X}$.

Theorem 4.2.14. It holds the following explicit formula for the essential p-dimension of S:

$$ed_p(S) = \sum_{k=0}^{r} (rankV_k - rankV_{k-1})p^k - dim(S)$$

Proof. Set $b_k = rank(V_k)$; by Theorem 4.2.12 it suffices to prove that the smallest rank of the G-module P in a p-presentation of X is equal to $\sum_{k=0}^{r}(b_k - b_{k-1})p^k$. Let $f : P \to X$ be a p-presentation of X and A a G-invariant basis of P. The set A is the disjoint union of the G-orbits A_j, so that P is the direct sum of the permutation G-modules $\mathbb{Z}[A_j]$. The composition $\bar{f} : P \to X \to \overline{X}$ is surjective. As G acts trivially on $\overline{X}$, the rank of the group $\bar{f}(\mathbb{Z}[A_j])$ is at most 1 for all j and $\bar{f}(\mathbb{Z}[A_j]) \subseteq V_k$ if $|A_j| \leqslant p^k$. It follows that the group $\overline{X}/V_k$ is generated by the images under the composition $P \xrightarrow{\bar{f}} \overline{X} \to \overline{X}/V_k$ of all $\mathbb{Z}[A_j]$ with $|A_j| > p^k$. Denote by c_k the number of such orbits A_j, so we have

$$c_k \geqslant rank(\bar{X}/V_k) = b_r - b_k$$

Set $c'_k = b_r - c_k$, so that $b_k \geqslant c'_k$ for all k and $b_r = c'_r$. Since the number of orbits A_j with $|A_j| = p^k$ is equal to $c_{k-1} - c_k$, we have

$$\begin{aligned} rank(P) &= \sum_{k=0}^{r}(c_{k-1} - c_k)p^k = \sum_{k=0}^{r}(c'_k - c'_{k-1})p^k \\ &= c'_r p^r + \sum_{k=0}^{r-1} c'_k(p^k - p^{k+1}) \geqslant b_r p^r + \sum_{k=0}^{r-1} b_k(p^k - p^{k+1}) \\ &= \sum_{k=0}^{r}(b_k - b_{k-1})p^k \end{aligned}$$

It remains to construct a p-presentation with P of rank $\sum_{k=0}^{r}(b_k - b_{k-1})p^k$. For every $k \geqslant 0$ choose a subset X_k in X of the pre-image of V_k under the canonical map $X \to \overline{X}$ with the property that for any $x \in V_k$ there is a subgroup $H_x \subseteq G$ with $x \in X^{H_x}$ and $[G : H_x] = p^k$ such that the composition

$$X_k \to V_k \to V_k/V_{k-1}$$

yields a bijection between X_k and a basis of V_k/V_{k-1}. In particular $|X_k| = b_k - b_{k-1}$. Call

$$P = \coprod_{k=0}^{r} \coprod_{x \in X_k} \mathbb{Z}[G/H_x]$$

and consider the G-homomorphism $f : P \to X$ taking 1 in $\mathbb{Z}[G/H_x]$ to x in X. By construction, the composition of f with the canonical map $X \to \overline{X}$ is surjective. As G is a p-group, the ideal $pR_{(p)} + I$ of $R_{(p)}$ is the Jacobson radical of the ring $R_{(p)} = R \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$. By Nakayama lemma $f_{(p)}$ is surjective. Hence the cokernel of f is finite of order prime to p. The rank of the permutation G-module P is equal to

$$\sum_{k=0}^{r} \sum_{b \in B_k} p^k = \sum_{k=0}^{r} |B_k|p^k = \sum_{k=0}^{r}(b_k - b_{k-1})p^k$$

□

The following computation will be used in the sequel.

Example 4.2.15. Let F be a field, ϕ a subgroup of ${}_pCh(F)$ of rank r, $L = F(\phi)$ and $G = Gal(L/F)$. We have an exact sequence $\overline{N} \to (\overline{R})^r \to \bar{I} \to 0$. It follows from Lemma 4.2.7 that $N \subseteq pR^r + I^r$, hence the first homomorphism in the sequence is trivial. The middle group is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^r$, hence $rank(\bar{I}) = r$.

For any subgroup $H \subseteq G$, the Tate cohomology group $\hat{H}^0(H, I) \simeq \hat{H}^{-1}(H, \mathbb{Z})$ is trivial; it follows that the group I^H is generated by $N_H x$ for all $x \in I$, where $X_H = \sum_{h \in H} h \in R$. Since $\bar{I}$ is of period p with the trivial G-action, the classes of the elements $N_H x$ in $\bar{I}$ are trivial if H is a nontrivial subgroup of G. It follows that the maps $I^H \to \bar{I}$ are trivial for all $H \neq 1$. With the previous notation we have $V_0 = \cdots = V_{r-1}$ and $V_r = \bar{I}$. By the Theorem 4.2.14

$$ed_p(U^\phi) = rp^r - dim(U^\phi) = rp^r - p^r + 1 = (r-1)p^r + 1$$

and the rank of the permutation module in a minimal p-presentation of I is equal to rp^r. Therefore, $k : R^r \to I$ is a minimal p-presentation of I that appears to be surjective. By Corollary 4.2.13,

$$ed(U^\phi) = ed_p(U^\phi) = (r-1)p^r - 1$$

Consider now the torus S^ϕ. The homomorphism k factors through a surjective map $R^r \to Q$, which is then necessarily a minimal p-presentation of Q. According to Theorem 4.2.14

$$ed(S^\phi) = ed_p(S^\phi) = rp^r - dim(S^\phi) = (r-1)p^r - r + 1$$

4.2.4 Degeneration

Let F be a field, p a prime integer different from $char(F)$ and $\phi \subseteq_p Ch(F)$ a finite subgroup. For an natural number k and a field extension K/F, denote $B_k^\phi = \{a \in Br(K)\{p\}\ such\ that\ ind(a_{K(\phi)}) \leqslant p^k\}$. On the set $B_k^\phi(K)$ consider the following equivalence relation: two elements a and a' are equivalent if and only if $a - a' \in Br_{dec}(K(\phi)/K)$. Denote by $F_k^\phi(K)$ the set of equivalence classes. We view B_k^ϕ and F_k^ϕ as functors from $Fields/F$ to $Sets$.

Remark 4.2.16. If ϕ is the zero subgroup, then $F_k^\phi = B_k^\phi \simeq Alg(p^r) \simeq PGL(p^r) - torsors$.

Remark 4.2.17. The set $B_0^\phi(K)$ is naturally bijective to $Br(K(\phi)/K)$ and $F_0^\phi(K) \simeq Br_{ind}(K(\phi)/K)$. By Corollary 4.2.10 the latter group is naturally isomorphic to $H^1(K, S^\phi)$.

Let $\phi' \subseteq \phi$ be a subgroup of index p and $\eta \in \phi \backslash \phi'$. Let E/F be a field extension such that $\eta_E \notin \phi'_E$ in $Ch(E)$. Choose an element $a \in B_k^\phi(E)$. Let E' be a field extension of F that is complete with respect to a discrete valuation v' over F with residue field E and set

$$a' = \hat{a} + (\hat{\eta_E} \cup (x)) \in Br(E')$$

for some $x \in E'^*$ such that $v'(x)$ is not divisible by p. By Proposition 4.2.3 (2) $ind(a_{E'(\phi')}) = p \cdot ind(a_{E(\phi)}) \leqslant p^{k+1}$, hence $a' \in B_{k+1}^{\phi'}(E')$.

Proposition 4.2.18. Suppose that for any finite field extension N/E of degree prime to p and any character $\rho \in Ch(N)$ of order p^2 such that $p \cdot \rho \in \phi_N \backslash \phi'_N$, we have $ind(a_{N(\phi',\rho)}) > p^{k-1}$. Then

$$ed_p^{F_{k+1}^{\phi'}}(a') \geqslant ed_p^{F_k^{\phi}}(a) + 1$$

Proof. Let M/E' be a finite field extension of degree prime to p, $M_0 \subseteq M$ a subfield over F and $a'_0 \in B_{k+1}^{\phi'}(M_0)$ such that $(a'_0)_M = a'_M$ in F_k^{ϕ} and $tr.deg_F(M_0) = ed_p^{F_{k+1}^{\phi'}}(a')$. We have

$$a'_M - (a'_0)_M \in Br_{dec}(M(\phi')/M) \tag{4.2.2}$$

We also have

$$a'_M = \hat{a_N} + (\hat{\eta_N} \cup (x)) \tag{4.2.3}$$

and $\partial_{v'}(a') = q \cdot \eta_E$, where $q = v'(x)$ is relatively prime to p. Extend the discrete valuation v' on E' to a unique discrete valuation v on M. The ramification index e' and inertia degree are both prime to p, thus the residue field N of v is a finite extension of E of degree prime to p. By Proposition 4.2.3 (3)

$$\partial_v(a'_M) = e' \cdot \partial_{v'}(a') = e'q \cdot \eta_N$$

Let v_0 be the restriction of v to M_0 and N_0 its residue field. It follows from 4.2.2 that

$$\partial_v(a'_M) - \partial_v((a'_0)_M) \in \phi'_N$$

Recall that $\eta_E \notin \phi'_E$; as $[N : E]$ is not divisible by p, it follows that $\eta_N \notin \phi'_N$. By the preceding, $\partial_v((a'_0)_M) \neq 0$, which means that $(a'_0)_M$ is ramified and therefore v_0 is nontrivial, so that v_0 is a discrete valuation on M_0.

Let $\eta_0 = \partial_{v_0}(a'_0) \in Ch(N_0)\{p\}$. By Proposition 4.2.3 we have

$$\partial_v((a'_0)_M) = e \cdot (\eta_0)_N$$

where e is the ramification index of M/M_0, hence $(\eta_0)_N \neq 0$. It follows from the preceding that

$$e'q \cdot \eta_N - e \cdot (\eta_0)_N \in \phi'_N$$

As $e'q$ is relatively prime to p, $\eta_N \in \langle \phi'_N, (\eta_0)_N \rangle$ in $Ch(N)$. Let p^t be the order of $(\eta_0)_N$. It holds that $v_p(e) = t - 1$ and

$$p^{t-1} \cdot (\eta_0)_N \in \phi_N \backslash \phi'_N$$

Choose a prime element π_0 in M_0 and write

$$(a'_0)_{\hat{M_0}} = \hat{a}_0 + (\hat{\eta}_0 \cup (\pi_0))$$

in $Br(\hat{M}_0)$, where $a_0 \in Br(N_0)p$.

Applying the specialization homomorphism $s_\pi : Br(M)p \to Br(N)p$ to 4.2.2, 4.2.3 and the previous relation, we get

$$a_N - (a_0)_N \in Br_{dec}(N(\phi', \eta_0)/N)$$

It follows that $a_{N(\phi',\eta_0)} = (a_0)_{N(\phi',\eta_0)}$ in $Br(N(\phi', \eta_0))$. We have

$$(a'_0)_{\hat{M}_0(\phi')} = (\hat{a_0})_{N_0(\phi')} + ((\hat{\eta_0})_{N_0(\phi')} \cup (\pi_0))$$

As no nontrivial multiple of $(\eta_0)_N$ belongs to ϕ'_N, the order of the character $(\eta_0)_{N_0(\phi')}$ is at least p^t. It follows from Proposition 4.2.3 (2) that

$$ind(a_0)_{N_0(\phi',\eta_0)} = ind(a'_0)_{\hat{M}_0(\phi')}/ord(\eta_0)_{N_0(\phi')} \leqslant p^{k+1}/p^t = p^{k-t+1}$$

By the previous relations, we have $ind(a_{N(\phi',\eta_0)}) \leqslant p^{k-t+1}$.

Suppose that $t \geqslant 2$ and consider the character $\rho = p^{t-2} \cdot (\eta_0)_N$ of order p^2 in $Ch(N)$. We have $p \cdot \rho = p^{t-1}(\eta_0)_N \in \phi_N \backslash \phi'_N$. Moreover, the degree of the field extension $N(\phi', \eta_0)/N(\phi', \rho)$ is equal to p^{t-2}. Hence

$$ind(a_{N(\phi',\rho)}) \leqslant ind(a_{N(\phi',\eta_0)}) \cdot p^{t-2} \leqslant p^{k-t+1} \cdot p^{t-2} = p^{k-1}$$

This contradicts the assumption, therefore $t = 1$, which means $ord(\eta_0)_N = p$. Then e and p are coprime and it follows that $(\eta_0)_N \in \langle \phi'_N, \eta_N \rangle$. Moreover, $\langle \phi', \eta_0 \rangle_N = \langle \phi', \eta \rangle_N = \phi_N$. By Lemma 4.2.2, there is a finite subextension N_1/N_0 of N/N_0 such that $\langle \phi', \eta_0 \rangle_{N_1} = \phi_{N_1}$. Replacing N_0 by N_1 and a_0 by $(a_0)_{N_1}$, we may assume that $\langle \phi', \eta_0 \rangle_{N_0} = \phi_{N_0}$. In particular, η_0 is of order p in $Ch(N_0)$. Now

$$ind(a_0)_{N_0(\phi)} = ind(a_0)_{N_0(\phi',\eta_0)} \leqslant p^k$$

so we have $a_0 \in B_k^\phi(N_0)$.

It follows that

$$a_N - (a_0)_N \in Br_{dec}(N(\phi)/N)$$

hence the classes of a_N and $(a_0)_N$ are equal in $F_k^\phi(N)$. The class of a_N in $F_k^\phi(N)$ is then defined over N_0, therefore

$$ed_p^{F_{k+1}^{\phi'}}(a') = tr.deg_F(M_0) \geqslant tr.deg_F(N_0) + 1 \geqslant ed_p^{F_k^\phi}(a) + 1$$

□

4.2.5 Multiple degeneration

In this subsection assume that the base field F contains a primitive p^2-th root of unity. Let ϕ be a subgroup in ${}_pCh(F)$ of rank r and choose a basis $\chi_1, ..., \chi_r$ of ϕ. Let E/F be a field extension such that $rank(\phi_E) = r$ and let $a \in Br(E)\{p\}$ be an element that is split by $E(\phi)$. Let $E_0 = E, E_1, ..., E_r$ be field extensions

of F such that for any $k = 1, 2, ..., r$, the field E_k is complete with respect to a discrete valuation v_k over G and E_{k-1} is its residue field. For any k choose elements $x_k \in E_k^*$ such that $v_k(x_k)$ is not divisible by p and define the elements $a_k \in Br(E_k)\{p\}$ inductively by $a_0 = a$ and $a_k = a_{k-1}\hat{} + ((\hat{\chi}_{k\,E_{k-1}} \cup (x_k))$. Let ϕ_k be the subgroup of ϕ generated by $\chi_{k+1}, ..., \chi_r$. Thus, $\phi_0 = \phi$, $\phi_r = 0$ and $rank(\phi_k) = r - k$. Note that the character $(\chi_k)_{E_{k-e}(\phi_k)}$ is not trivial. It follows from Proposition 4.2.3 that

$$ind(a_k)_{E_k(\phi_k)} = p \cdot ind(a_{k-1})_{E_{k-1}(\phi_{k-1})}$$

for any k. As $ind(a_{E(\phi)}) = 1$, we have $ind(a_k)_{E_k(\phi_k)} = p^k$ for all k; in particular $a_k \in B_k^{\phi_k}(E_k)$.

The following lemma gives conditions on the element a such that the hypothesis of Proposition 4.2.18 are satisfied.

Lemma 4.2.19. Suppose that $p^{r-1}a \notin Im(Br(F) \to Br(E))$. Then for every $k = 0, 1, ..., r$ and any finite field extension N/E_k if degree prime to p and any character $\rho \in Ch(N)$ of order p^2 such that $p \cdot \rho \in (\phi_k)_N \backslash (\phi_{k+1})_N$, we have

$$ind(a_k)_{N(\phi_{k+1,\rho})} > p^{k-1} \tag{4.2.4}$$

Proof. Let's proceed by inductions on r; the case $r = 1$ is trivial. Suppose that the inequality does not hold for some k, a finite extension N/E_k and a character $\rho \in Ch(N)$. Suppose first that $k < r - 1$, consider the fields $F' = F(\phi_{k+1})$, $E' = E(\phi_{k+1})$, $E'_i = E_i(\phi_{k+1})$, $N' = N(\phi_{k+1})$, the sequence of characters $(\chi_i)_{F'}$ and the sequence of elements $a'_i = (a_i)_{E'_i} \in Br(E_i)$ for $i = 0, 1, ..., k+1$. As $(a'_k)_{N'(\rho)} = (a_k)_{N(\phi_{k+1,\rho})}$, the inequality does not hold for the term a'_k of the new sequence, the field extension N'/E'_k and the character ρ'_N. Note that $p^k a_{E'} \notin Im(Br(F') \to Br(E'))$, because otherwise, taking the norm map for the extension F'/F of degree p^{r-k-1} we would get $p^{r-1}a \in Im(Br(F) \to Br(E))$. By induction, the inequality 4.2.4 holds for all the terms of the new sequence, in particular for a'_k, a contradiction.

Thus we can assume that $k = r - 1$. We construct a new sequence of fields $\tilde{E}_0, \tilde{E}_1, ..., \tilde{E}_r$ such that each $\tilde{E}_i$ is a finite extension of $\tilde{E}_i$ of degree prime to p as follows. We set $\tilde{E}_{r-1} = N$ and let $\tilde{E}_r$ be an unramified extension of E_r with the residue field $\tilde{E}_{r-1}$. The fields $\tilde{E}_j$ with $j < r - 1$ are constructed by descending induction on j. If we have constructed $\tilde{E}_j$ as a finite extension of E_j of degree prime to p, then we extend the valuation v_j to $\tilde{E}_j$ and let $\tilde{E}_{j-1}$ to be its residue field. Replacing E_i by $\tilde{E}_i$ and a_i by $(a_i)_{\tilde{E}_i}$, we may assume that $N = E_{r-1}$.

Suppose that the character ρ is unramified with respect to v_{r-1}, that is $\rho = \hat{\mu}$ for a character $\mu \in Ch(E_{r-2})$ of order p^2. By Lemma 4.2.5 (1)

$$ind(a_{r-2})_{E_{r-2}(\chi_{r-1},\mu)} = ind(a_{r-1})_{E_{r-1}(\rho)}/p = ind(a_{r-1})_{E_{r-1}(\phi_r,\rho)}/p \leqslant p^{r-3}$$

Consider the fields $F' = F(\chi_{r-1})$, $E' = E(\chi_{r-1})$, $E'_i = E_i(\chi_{r-1})$, $N' = N(\chi_{r-1})$, the sequence of characters $\chi_1, ..., \chi_{r-2}, \chi_r$ and the elements $a'_i \in$

$Br(E'_i)$ for $i = 0, 1, ..., r-1$ defined by $a'_i = (a_i)_{E'_i}$ for $i \leqslant r-2$ and $a'_{r-1} = \hat{a}_{r-2} + (\hat{\chi}_r \cup (x_{r-1}))$ over E'_{r-1}. As $(a'_{r-2})_{N'(\mu)} = (a_{r-2})_{N(\chi_{r-1},\rho)}$, the inequality above shows that the result does not hold for the term a'_{r-2} of the new sequence, the field extension N'/E'_{r-2} and the character μ'_N. Note that $p^{r-2}a_{E'} \notin Im(Br(F') \to Br(E'))$, as otherwise, taking the norm map for the extension F'/F of degree p, we get $p^{r-1}a \in Im(Br(F) \to Br(E))$. By induction, the result holds for all the terms of the new sequence, in particular for a'_{r-2}, a contradiction.

Suppose now that ρ is ramified. Note that $p \cdot \rho$ is a nonzero multiple of $(\chi_r)_{E_{r-1}}$. As the result fails for a_{r-1}, we have $ind(a_{r-1})_{E_{r-1}(\rho)} \leqslant p^{r-2}$. By Lemma 4.2.5 (2), there exists a unit $u \in E_{r-1}$ such that $E_{r-2}(\chi_r) = E_{r-2}(\bar{u}^{1/p})$ and

$$ind(a_{r-2} - (\chi_{r-1} \cup (\bar{u}^{1/p})))_{E_{r-2}(\chi_r)} = ind(a_{r-1})_{E_{r-1}(\rho)} \leqslant p^{r-2}$$

By descending induction on j we show that there exists a unit u_j in E_{j+1} and a subgroup $\theta_j \subseteq \phi$ of rank $r-j-1$ such that $\langle \chi_1, ..., \chi_j, \chi_{r-1} \rangle \cap \theta_j = 0$, $E_j(\chi_r) = E_j(\bar{u}_j^{1/p})$ and

$$ind(a_j - (\chi_{r-1} \cup (\bar{u}_j^{1/p})))_{E_j(\theta_j} \leqslant p^j \tag{4.2.5}$$

If $j = r-2$, we set $u_j = u$ and $\theta_j = \{\chi_r\}$. Let us prove the inductive step. The field $E_j(\bar{u}_j^{1/p}) = E_j(\chi_r)$ is unramified over E_j, hence $v_j(\bar{u}_j)$ is divisible by p. Modifying u_j by a p^2-th power, we may assume that $\bar{u}_j = u_{j-1}x_j^{m_p}$ for a unit $u_{j-1} \in E_j$ and an integer m. Then

$$(a_j - (\chi_{r-1} \cup (\bar{u}_j^{1/p})))_{E_j(\theta_j)} = \hat{b} + (\hat{\eta} \cup (x_j))_{E_j(\theta_j)}$$

where $\eta = \chi_j - m\chi_{r-1}$ and $b = (a_{j-1} - (\chi_{r-1} \cup (\bar{u}_{j-1}^{1/p})))_{E_{j-1}(\theta_j)}$. As η is not contained in θ_j, the character $\eta_{E_{j-1}(\theta_j)}$ is not trivial. Set $\theta_{j-1} = \langle \theta_j, \eta \rangle$; it follows from Proposition 4.2.3 (2) that $ind(b_{E_{j-1}(\theta_{j-1})} = (a_j - (\chi_{r-1} \cup (\bar{u}_j^{1/p})))_{E_j(\theta_j)}/p \leqslant p^{j-1}$. Applying the inequality 4.2.5 in the case $j = 0$, we get

$$a_{E(\theta_0)} = (\chi_{r-1} \cup (w^{1/p}))_{E(\theta_0)}$$

for an element $w \in E^*$ such that $E(w^{1/p}) = E(\chi_r)$. The degree of the extension $E(\theta_0)/E$ is equal to p^{r-1} and $E^(w^{1/p}) \subseteq E(\theta_0)$. Taking norm for the extension $E(\theta_0)/E$, we get that $p^{r-1}a$ is a multiple of $\chi_{r-1} \cup (w)$. As the character χ_r is defined over F, we may assume that $w \in F^*$, hence $p^{r-1}a \in Im(Br(F) \to Br(E))$, a contradiction. □

Corollary 4.2.20. Suppose that $p^{r-1}a \notin Im(Br(F) \to Br(E))$. Then

$$ed_p^{Alg(p^r)}(a_r) \geqslant ed_p^{S^\phi - torsors}(a) + r$$

Proof. By iterated application of Proposition 4.2.18 and by Example 4.2.15 we have

$$ed_p^{Alg(p^r)}(a_r) = ed_p^{F_r^{\phi_r}}(a_r) \geqslant ed_p^{F_{r-1}^{\phi_{r-1}}}(a_{r-1}) + 1 \geqslant \cdots$$
$$\geqslant ed_p^{F_1^{\phi_1}}(a_1) + (r-1) \geqslant ed_p^{F_0^{\phi_0}} + r = ed_p^{S_\phi - torsors}(a) + r$$

□

Theorem 4.2.21. Let F be a field and p an integer different from $char(F)$. Then

$$ed_p(Alg_F(p^r)) \geqslant (r-1)p^r + 1$$

Proof. As $ed_p(Alg_F(p^r)) \geqslant ed_p(Alg_{F'}(p^r))$ for any field extension F'/F, we can replace F by any field extension. In particular, we may assume that F contains a primitive p^2-th root of unity and there is a subgroup ϕ of ${}_pCh(F)$ of rank r. Let T^ϕ be the algebraic torus constructed in the section about algebraic tori. Set $E = F(T^\phi)$ and let $a \in Br(EL/E)$ be the element defined in 4.2.1. Let $a_r \in Br(E_r)$ be the element of index p^r constructed in the beginning of the subsetcion. By Lemma 4.2.11 the class $p^{r-1}a$ in $Br(E)$ does not belong to the image of the map $Br(F) \to Br(E)$. It follows from the previous Corollary that

$$ed_p^{Alg(p^r)}(a_r) \geqslant ed_p^{S^\phi - torsors}(a) + r$$

The S^ϕ-torsor a is the generic fiber of the versal S^ϕ-torsor $P^\phi \to S^\phi$, hence a is a generic torsor (see Remark 4.2.6). Then

$$ed_p^{S^\phi - torsors}(a) = ed_p(S^\phi)$$

The essential p-dimension of S^ϕ is given by $ed_p(S^\phi) = (r-1)p^r - r + 1$. Putting all the results together, we have the thesis. □

Corollary 4.2.22. Let k a field of characteristic different from p. Then

$$ed_p(PGL_{p^2}) = p^2 + 1$$

Proof. This follows directly by the previous Theorem and Corollary 4.1.19. □

Bibliography

[1] S. Amitsur. On central division algebras. *Israel journal of mathematics*, 12(4):408–420, 1972.

[2] M. Auslander and O. Goldman. The brauer group of a commutative ring. *Transactions of the American Mathematical Society*, pages 367–409, 1960.

[3] G. Azumaya et al. On maximally central algebras. *Nagoya Mathematical Journal*, 2:119–150, 1951.

[4] G. Berhuy and G. Favi. Essential dimension: a functorial point of view (after a. merkurjev). *Doc. Math*, 8(106):279–330, 2003.

[5] J. BUHLER and Z. REICHSTEIN. On the essential dimension of a finite group. *Compositio Mathematica*, 106:159–179, 4 1997.

[6] M. Demazure and P. Gabriel. *Groupes algébriques*, volume 1. Masson et Cie, 1970.

[7] M. Demazure and A. Grothendieck. *Schémas en groupes: Groupes de type multiplicatif et structure des schémas en groupes généraux*, volume 2. Springer, 1970.

[8] E. Formanek. The center of the ring of $3\times$ 3 generic matrices. *Linear and Multilinear Algebra*, 7(3):203–212, 1979.

[9] S. Garibaldi, A. Merkurjev, and J. P. Serre. *Cohomological invariants in Galois cohomology*. Number 28. American Mathematical Soc., 2003.

[10] P. Gille and T. Szamuely. *Central simple algebras and Galois cohomology*, volume 101. Cambridge University Press, 2006.

[11] A. Grothendieck. Éléments de géométrie algébrique. *New York*, 1967.

[12] D. Haile. A useful proposition for division algebras of small degree. *Proceedings of the American Mathematical Society*, 106(2):317–319, 1989.

[13] I. N. Herstein. *Noncommutative rings*. Number 15. Cambridge University Press, 2005.

[14] M.-A. Knus and M. Ojanguren. Théorie de la descente et algèbres d' azumaya. Technical report, Lecture Notes in Mathematics. 389. Berlin-Heidelberg-New York: Springer-Verlag. IV, 163 p. DM 20.00; 8.20, 1974.

[15] T.-Y. Lam. *A first course in noncommutative rings*. Springer Science & Business Media, 2013.

[16] M. Lorenz and Z. Reichstein. Lattices and parameter reduction in division algebras. *arXiv preprint math/0001026*, 2000.

[17] M. Lorenz, Z. Reichstein, L. H. Rowen, and D. J. Saltman. Fields of definition for division algebras. *Journal of the London Mathematical Society*, 68(03):651–670, 2003.

[18] R. Lötscher, M. MacDonald, A. Meyer, and Z. Reichstein. Essential p-dimension of algebraic tori. *arXiv preprint arXiv:0910.5574*, 2009.

[19] A. S. Merkurjev. Essential dimension. *Contemporary Mathematics*, 493:299, 2009.

[20] A. S. Merkurjev. Essential dimension of simple algebras. *Preprint. URL http://www. math. ucla. edu/ merkurev/publicat. htm*, 2009.

[21] A. S. Merkurjev. Essential dimension: a survey. *Transformation groups*, 18(2):415–481, 2013.

[22] A. Meyer and Z. Reichstein. An upper bound on the essential dimension of a central simple algebra. *Journal of Algebra*, 329(1):213–221, 2011.

[23] J. S. Milne. *Etale Cohomology (PMS-33)*. Number 33. Princeton university press, 1980.

[24] C. Procesi and A. nazionale dei Lincei. *Non-commutative affine rings*. Accademia Nazionale dei Lincei, 1967.

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

[26] Z. Reichstein. Essential dimension. In *Proceedings of the International Congress of Mathematicians*, volume 2, pages 162–188. World Scientific, 2010.

[27] Z. Reichstein, B. Youssin, J. Kollár, and E. Szabó. Essential dimensions of algebraic groups and a resolution theorem for g-varieties. *arXiv preprint math/9903162*, 1999.

[28] L. Rowen. *Polynomial identities in ring theory*. Elsevier, 1980.

[29] L. H. Rowen. Brauer factor sets and simple algebras. *Transactions of the American Mathematical Society*, 282(2):765–772, 1984.

[30] L. H. Rowen and D. Saltman. Normalized brauer factor sets. *Journal of Algebra*, 198(2):446–468, 1997.

[31] L. H. Rowen and D. J. Saltman. Prime to p extensions of division algebra. *Israel Journal of Mathematics*, 78(2):197–207, 1992.

[32] A. Ruozzi. Essential p-dimension of pgln. *Journal of Algebra*, 328(1):488–494, 2011.

[33] J.-P. Serre. *Galois cohomology*. Springer Science & Business Media, 2013.

[34] A. Vistoli. Notes on grothendieck topologies, fibered categories and descent theory. *arXiv preprint math/0412512*, 2004.

[35] W. C. Waterhouse. *Introduction to affine group schemes*, volume 66. Springer Science & Business Media, 2012.

[36] J. H. Wedderburn. On division algebras. *Transactions of the American Mathematical Society*, 22(2):129–135, 1921.