The Brauer group of fields and schemes

David Harari

M2 2023-2024

Contents

1. Preliminaries

The aim of this section is to recall a few basic facts on Galois theory and profinite groups. Since they are quite standard, we will not give detailed proofs, but references will be included.

1.1. Infinite Galois theory

Let k be a field with separable closure $\bar{k}$ (which coincides with the algebraic closure if k is perfect, e.g. k finite or k of characteristic zero).

Definition 1.1 A separable and algebraic extension $K \subset \bar{k}$ of k is *Galois* over k if it is normal, that is: if $\alpha \in K$, then all roots (in $\bar{k}$) of the minimal polynomial of α still lie in K. When K/k is Galois, the group of k-automorphisms of K is denoted by $\mathrm{Gal}\,(K/k)$.

Remark 1.2 a) This coincides with the classical notion of Galois extension when K is a finite and separable extension of k.

b) The extension $\bar{k}$ itself is Galois over k. The group $\mathrm{Gal}\,(\bar{k}/k)$ is the *absolute Galois group* of the field k.

c) A Galois extension $K \subset \bar{k}$ of k is the union of finite Galois extensions of k. Indeed for every $\alpha \in K$, the splitting field of the minimal polynomial of α over k is a finite Galois extension of k contained in K. We will soon refine this remark.

Definition 1.3 A (filtered) inverse system of groups (G_i, f_{ij}) consists of:

- a partially ordered set $(\Lambda, \leq)$ such that for all $i, j \in \Lambda$, there is a $k \in \Lambda$ such that $i \leq k$ and $j \leq k$ ("directed poset").
- for each $i \in \Lambda$ a group G_i.
- For each $i \leq j$ a morphism $f_{ij} : G_j \to G_j$ ("transition map") such that $f_{ii} = \mathrm{Id}$ and $f_{ik} = f_{ij} \circ f_{jk}$ for all $i \leq j \leq k$.

The *inverse limit* $\varprojlim_{i\in\Lambda} G_i$ is the subgroup of $\prod_{i\in\Lambda} G_i$ consisting of families (g_i) such that $f_{ij}(g_j) = g_i$ for all $i \leq j$.

Proposition 1.4 *Let K/k be a Galois extension of fields. Then the groups* $\mathrm{Gal}\,(L/k)$ *of finite Galois subextensions L/k of K/k together with the canonical surjective morphisms* $\mathrm{Gal}\,(M/k) \to \mathrm{Gal}\,(L/k)$ *(defined when $L \subset M$) form an inverse system. The map*

$$\mathrm{Gal}\,(K/k) \to \prod_L \mathrm{Gal}\,(L/k)$$

(defined by restricting $\sigma \in \mathrm{Gal}\,(K/k)$ *to all finite Galois subextensions* L/k *of* K/k*) induces an isomorphism between* $\mathrm{Gal}\,(K/k)$ *and* $\varprojlim_L \mathrm{Gal}\,(L/k)$*. The corresponding projection* $\mathrm{Gal}\,(K/k) \to \mathrm{Gal}\,(L/k)$ *is surjective for all* L *as above.*

Proof : This follows easily from Galois theory of finite field extensions, cf. [2], Prop. 4.1.3. and Cor. 4.1.4.

□

Thus the Galois group $\mathrm{Gal}\,(K/k)$ appears as an inverse limit of finite groups. Such a group is called *profinite*. We will study the main properties of general profinite groups in the next paragraph.

Example 1.5 Assume that $\mathbf{F}$ is a finite field with algebraic closure $\overline{\mathbf{F}}$. Then $\mathrm{Gal}\,(\overline{\mathbf{F}}/\mathbf{F})$ is isomorphic to the inverse limit

$$\widehat{\mathbf{Z}} := \varprojlim_{n \in \mathbf{N}^*} \mathbf{Z}/n,$$

as for every $n \in \mathbf{N}^*$, there is a unique extension $L_n \subset \overline{\mathbf{F}}$ of $\mathbf{F}$ of degree n and we have $\mathrm{Gal}\,(L_n/\mathbf{F}) \simeq \mathbf{Z}/n$ with the transition maps corresponding to the canonical surjections $\mathbf{Z}/m \to \mathbf{Z}/n$ when $n|m$. The group $\widehat{\mathbf{Z}}$ is isomorphic to the direct product (over all prime numbers p) of the additive groups of the p-adic rings $\mathbf{Z}_p$ (each $\mathbf{Z}_p$ being the inverse limit of the $\mathbf{Z}/p^r\mathbf{Z}$, $r \in \mathbf{N}^*$).

Definition 1.6 Let K/k be a Galois extension. We equip

$$\mathrm{Gal}\,(K/k) \simeq \varprojlim_L \mathrm{Gal}\,(L/k) \subset \prod_L \mathrm{Gal}\,(L/k)$$

with the *Krull topology*, that is: the subspace topology associated to the product of discrete topologies on each finite group $\mathrm{Gal}\,(L/k)$.

The main theorem of infinite Galois theory can now be stated:

Theorem 1.7 (Krull) *Let* K/k *be a Galois extension. The map* $F \mapsto \mathrm{Gal}\,(K/F)$ *is a bijection between intermediate extensions* F *and closed subgroups of* $\mathrm{Gal}\,(K/k)$*. In this bijection, open subgroups correspond to finite extensions of* k *contained in* K *and normal subgroups correspond to extensions that are Galois over* k*. The converse bijection is given by* $H \mapsto K^H$*, where* K^H *is the subfield of* K *consisting of those elements* x *such that* $\sigma(x) = x$ *for all* $\sigma \in H$*.*

Proof : [2], Th. 4.1.12.

□

Remark 1.8 In general $\mathrm{Gal}\,(K/k)$ has many non closed subgroups. For instance subgroups generated by one element are not closed in $\widehat{\mathbf{Z}}$. It can even happen that some finite index subgroups of $\mathrm{Gal}\,(K/k)$ are not closed (see Remark 1.12 below).

1.2. Profinite groups

Recall that if (X_i) is a family of topological spaces, the set $\prod X_i$ is equipped with the *direct product topology*, meaning that a basis of open subsets consists of the $\prod U_i$, where U_i is open in X_i and $X_i = U_i$ for all but finitely many i.

Definition 1.9 A topological group G is *profinite* if it is an inverse limit $\varprojlim G_i$ of finite groups (each G_i endowed with the discrete topology), the topology on the inverse limit being defined as the subspace topology associated to the inclusion $\varprojlim G_i \subset \prod G_i$.

Recall that in any topological group, every open subgroup is closed and a finite index subgroup is open if and only if it is closed. A subgroup is open if and only if it is a neighborhood of the identity element 1.

Proposition 1.10 *a) Let G be a profinite group. Then* 1 *admits a basis* (G_i) *of neighborhoods which are open, normal, finite index subgroups. Moreover G identifies with $\varprojlim(G/G_i)$.*

b) A topological group is profinite if and only if it is compact and totally disconnected. Changing the projective system defining G does not change its structure as a topological group.

c) A closed subgroup H of a profinite group G is profinite, and the topological space G is isomorphic to the space $H \times (G/H)$. If H is closed and normal in G, then the quotient topological group G/H is profinite.

Proof : See [8], Prop 1.1.3, [10], Prop I.1.1., and [5], Prop. 4.2.

□

Example 1.11 a) A finite group is obviously profinite.

b) As seen in the previous paragraph, the Galois group $\mathrm{Gal}\,(K/k)$ of a Galois extension of fields is profinite

c) If M is a discrete torsion abelian group, then its *Pontryagin dual* $M^* = \mathrm{Hom}(M, \mathbf{Q}/\mathbf{Z})$ is a profinite group when endowed with the simple convergence topology (that is: the "compact open" topology). Actually $M \mapsto M^*$ induces an anti-equivalence of categories between discrete torsion groups and profinite groups. For instance the dual of $\mathbf{Q}/\mathbf{Z}$ is $\widehat{\mathbf{Z}}$.

d) The additive group of the ring of integers $\mathcal{O}_K$ of a local field (=field complete for a discrete version with finite residue field) is profinite. For instance $\mathbf{Z}_p$ is profinite. Same for the multiplicative group $\mathcal{O}_K^*$.

e) Let K be a p-adic field (that is: K is a finite field extension of $\mathbf{Q}_p$ for some prime number p). Let A be an *abelian variety* over K, namely a connected projective algebraic group over K. Then the group $A(K)$ of K-points of A is a profinite group.

Remark 1.12 In a profinite group, all open subgroups are of finite index but the converse is not true in general. For instance take the profinite group $\mathcal{O}_K = \mathbf{F}_q[[t]]$, which is the ring of integers of the local field $K = \mathbf{F}_q((t))$. Then the kernel of a non continuous $\mathbf{F}_q$-linear form on $\mathcal{O}_K$ is a non-closed finite index subgroup. Using class field theory, a similar example can be given with the profinite group $\mathrm{Gal}\,(K^{\mathrm{ab}}/K)$, where K^{ab} is the maximal abelian extension of K.

It turns out that it is possible (and useful) to extend the notion of index to any closed subgroup of a profinite group:

Definition 1.13 A *supernatural number* is a formal product $\prod_p p^{n_p}$, where p ranges through the set of prime numbers and $n_p \in \mathbf{N} \cup \{+\infty\}$. The product, the gcd, and the lcm of an arbitrary family of supernatural numbers are obviously defined.

Definition 1.14 Let G be a profinite group and H a closed subgroup of G. The *index* $[G : H]$ of H in G is the supernatural number defined as the lcm of the (finite) indexes $[G/U : H/(H \cap U)]$ when U ranges through the open normal subgroups of G. The *order* of G is the index of $\{1\}$ in G.

Proposition 1.15 *Let H be a closed subgroup of a profinite group G.*

a) The supernatural number $[G : H]$ is a natural number if and only if H is of finite index (in the usual sense), which is equivalent to saying that H is open in G. In this case $[G : H]$ is the usual index of H in G.

b) Let $P \subset H \subset G$ be profinite groups. Then

$$[G : P] = [G : H].[H : P].$$

Proof : [5], Lemma 4.7 and Prop 4.10.

□

Definition 1.16 Let p be a prime number. A *pro-p-group* is a profinite group G whose order is a power of p (equivalently, this means that G is a projective limit of finite p-groups). A *p-Sylow subgroup* (or simply a p-Sylow) of a profinite group G is a closed pro-p-group H of G such that the index $[G : H]$ is prime to p.

The next result follows easily from the similar statement for finite groups (plus the well-known lemma that a projective limit of non-empty finite sets is non empty).

Proposition 1.17 *Let G be a profinite group. Let p be a prime number.*

a) The group G has a p-Sylow, and p-Sylow are pairwise conjugated.

b) Every pro-p-subgroup of G is a subgroup of some p-Sylow of G.

c) If G is abelian, it is isomorphic to the direct product of its pro-p-Sylow. This extends to pro-nilpotent groups (inverse limit of finite nilpotent groups).

Proof : [5], Prop 4.10.

□

Example 1.18 a) The additive group $\mathbf{Z}_p$ is a pro-p-group, as the inverse limit of the $\mathbf{Z}/p^n$ for $n \in \mathbf{N}^*$. It is the p-Sylow subgroup of $\widehat{\mathbf{Z}}$.

b) Let G be a group. The *profinite completion* (resp. p-completion) $\widehat{G}$ (resp. $\widehat{G}_p$) of G is the inverse limit of the G/G_i, where G_i runs over the normal finite index subgroups (resp. normal subgroups of index p^n with $n \in \mathbf{N}^*$) of G. The group $\widehat{G}_p$ is the largest pro-p quotient of $\widehat{G}$.

c) Let K be a p-adic field with maximal unramified extension K^{nr} and maximal tamely ramified extension K^{tr}. The group $\mathrm{Gal}\,(K^{\mathrm{nr}}/K)$ is isomorphic to $\widehat{\mathbf{Z}}$. The theory of ramification groups yields that $I_p := \mathrm{Gal}\,(\overline{K}/K^{\mathrm{tr}})$ is the unique p-Sylow of the inertia group $I = \mathrm{Gal}\,(\overline{K}/K^{\mathrm{nr}})$, and the quotient I/I_p is isomorphic to $\prod_{\ell \neq p} \mathbf{Z}_l$.

2. Group cohomology

2.1. Cohomology of finite groups

In this paragraph, we recall the main properties of cohomology of finite groups. This will be extended to profinite groups by a limit process in the next paragraph. A comprehensive reference is the first chapter of [5]. Most results hold without the assumption G finite, but to avoid confusion with the cohomology of profinite groups (which will be defined in the next paragraph), we will always assume G finite when we speak of G-modules in this paragraph.

Definition 2.1 Let G be a finite group. A *G-module* A is an abelian group equipped with an action by automorphisms of groups. In other words, for every $g \in G$, the map $x \mapsto g.x$ is an automorphism of the group A. A *morphism of G-modules* is a morphism $f : A \to A'$ compatible with the action of G, namely $f(g.x) = g.f(x)$ for all $g \in G, x \in A$.

Equivalently, a G-module is a left-module on the (non commutative if G is not commutative) ring $\mathbf{Z}[G]$ (and likewise a morphism of G-modules corresponds to a morphism of $\mathbf{Z}[G]$-modules; similarly for a sub-G-module, an exact sequence of G-modules and so on).

Example 2.2 a) If A is an abelian group, it is a G-module for the trivial action $g.x := x,\ \forall x \in A, \forall g \in G$.

b) Let $G = \{\pm 1\}$, then $\mathbf{Z}$ is a G-module for the action $g.x = gx$.

c) Let L/K be a finite Galois field extension and $G := \mathrm{Gal}\,(L/K)$. Then both $(L, +)$ and $(L^*, \times)$ are G-modules for the natural action of G.

d) Let A and B be G-modules. Then the group $M := \mathrm{Hom}_{\mathbf{Z}}(A, B)$ of group homomorphisms from A to B is a G-module for the action

$$(g.f)(x) := g.f(g^{-1}.x),\ \forall f \in M, \forall g \in G, \forall x \in A.$$

e) Let H be a (not necessarily normal) subgroup of G. Then the abelian group $\mathbf{Z}[G/H] := \bigoplus_{\bar{g} \in G/H} \mathbf{Z}.\bar{g}$ is a G-module for the natural left-action of G, where G/H is the set of left-cosets.

f) Let A be an abelian group. Define $I_G(A)$ as the abelian group consisting of maps $f : G \to A$, equipped with the action of G given by $(g.f)(x) = f(xg)$ for all $f \in I_G(A)$, $g \in G$, $x \in G$. An *induced G-module* is a G-module isomorphic to $I_G(A)$ for some abelian group A. One can check that $I_G(A)$ is isomorphic to $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}[G], A)$, or (non canonically; this uses G finite) to $\mathbf{Z}[G] \otimes_{\mathbf{Z}} A$, the action of G being on the first factor. One also checks easily (cf. [5], Cor. 1.13) that

$$\mathrm{Hom}_{\mathbf{Z}}(B, A) = \mathrm{Hom}_G(B, I_G(A))$$

for every abelian group A and every G-module B, where Hom_G means the set of morphisms of G-modules.

The category of G-modules is abelian, we denote it by $\mathcal{M}od_G$. As in any abelian category, the covariant functor $\mathrm{Hom}_G(A, .)$ and the contravariant functor $\mathrm{Hom}_G(., A')$ (from $\mathcal{M}od_G$ to the category Ab of abelian groups) are left-exact, and we have the following definition:

Definition 2.3 A G-module A is *injective* if $\mathrm{Hom}_G(., A)$ is exact, *projective* if $\mathrm{Hom}_G(A, .)$ is exact.

For instance, a free $\mathbf{Z}[G]$-module is projective (and being projective is equivalent to being a direct factor of a free $\mathbf{Z}[G]$-module). A direct sum (resp. direct product) of projective G-modules (resp. injective G-modules) is projective (resp. injective). As every category of modules, the category of G-modules has *enough injectives*, that is: every G-module can be embedded into an injective module. Therefore, for any additive, covariant and left-exact functor $F : \mathcal{M}od_G \to \mathcal{B}$ (where $\mathcal{B}$ is an abelian category), the *right derived functors* R^iF are defined for $i \in \mathbf{N}$, with the following properties :

Proposition 2.4 *a) Let A be a G-module. Let*

$$0 \to A \to I_0 \to I_1 \to I_2 \to ...$$

be an injective resolution of A (that is: the sequence is exact and all I_j are injective, $j \in \mathbf{N}$). Then the objects $(R^iF)(A)$ are given as the cohomology groups of the complex :

$$0 \to F(I_0) \to F(I_1) \to F(I_2) \to ...$$

In particular $R^0F = F$ (recall that F is left-exact).

b) A short exact sequence

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

of G-modules induces a long exact sequence

$$R^iF(A') \to R^iF(A) \to R^iF(A'') \xrightarrow{\delta^i} R^{i+1}F(A') \to ...$$

and the maps δ^i are functorial with respect of morphisms of exact sequence.

c) In a), the $(R^iF)(A)$ can be computed using a resolution by any family of acyclic objects $(I_j)_{j\geq 0}$ (this means that $R^iF(I_j) = 0$ for every $i > 0$, which is a bit more general than all I_j being injective).

For every G-module A, define

$$A^G := \{x \in A, \forall g \in G, g.x = x\}.$$

Then:

Definition 2.5 The *cohomology groups* $H^i(G, A)$ of a G-module A are the right derived functors of the left-exact functor $A \mapsto A^G$ from $\mathcal{M}od_G$ to the category Ab of abelian groups.

The category of G-modules also has enough projectives (as every $\mathbf{Z}[G]$-module is a quotient of a free $\mathbf{Z}[G]$-module). It turns out that it is easier to compute the $H^i(G, A)$ using a projective resolution as follows :

Theorem 2.6 *Let*

$$... \to P_i \to P_{i-1} \to ... \to P_1 \to P_0 \to \mathbf{Z} \to 0 \tag{1}$$

be a projective resolution of the G-module $\mathbf{Z}$*. Let A be a G-module. Then the $H^i(G, A)$ are the cohomology groups of the complex*

$$0 \to \mathrm{Hom}_G(P^0, A) \to \mathrm{Hom}_G(P_1, A) \to \mathrm{Hom}_G(P_2, A) \to ...$$

Proof (sketch of): The functor $A \mapsto A^G$ identifies with the functor $A \mapsto \mathrm{Hom}_G(\mathbf{Z}, A)$, hence $H^i(G, A) = \mathrm{Ext}^i_G(\mathbf{Z}, A)$, where the Ext^i_G are by definition the derived functors of the functor $\mathrm{Hom}_G(\mathbf{Z}, .)$. A general property of the Ext ([12], Th. 2.7.6) shows that the $\mathrm{Ext}^i_G(\mathbf{Z}, A)$ are also obtained as derived functors (applied to $\mathbf{Z}$) of the contravariant functor $\mathrm{Hom}_G(., A)$, whence the result.

□

Proposition 2.7 *Let I be an induced A-module. Then it is acyclic for the functor $A \mapsto A^G$.*

Proof : Take a projective resolution (exact sequence (1) as above) of $\mathbf{Z}$. As the P_i are projective $\mathbf{Z}[G]$-modules, they are free as $\mathbf{Z}$-modules (as direct factors of free $\mathbf{Z}$-modules), so the kernel and cokernels of the maps $P_i \to P_{i-1}$ are free $\mathbf{Z}$-modules. A short sequence

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

of free $\mathbf{Z}$-modules is split, hence induces an exact sequence

$$0 \to \mathrm{Hom}_{\mathbf{Z}}(M_1, X) \to \mathrm{Hom}_{\mathbf{Z}}(M_2, X) \to \mathrm{Hom}_{\mathbf{Z}}(M_3, X) \to 0.$$

for every abelian group X. Set $I = I_G(X)$ for some abelian group X, then $\mathrm{Hom}_G(P_i, I) = \mathrm{Hom}_{\mathbf{Z}}(P_i, X)$, hence the sequence

$$0 \to \mathrm{Hom}_G(P^0, I) \to \mathrm{Hom}_G(P_1, I) \to \mathrm{Hom}_G(P_2, I) \to ...$$

remains exact. Now apply Theorem 2.6.

□

Corollary 2.8 *Let $0 \to A \to I \to B \to 0$ be an exact sequence of G-modules with I injective. Then $H^i(G, B) \simeq H^{i+1}(G, A)$ for all $i > 0$.*

Proof : This follows from acyclicity of I combined with the long exact sequence of cohomology.

□

The previous corollary is especially useful, as every G-module A embeds into $I_G(A)$ as follows: send each $a \in A$ to the function $g \mapsto g.a$ from G to A (A is even a direct factor of $I_G(A)$ as a $\mathbf{Z}$-module via the retraction $f \mapsto f(1)$). Embedding A into an injective G-module will often be useful to obtain results by dimension shifting.

Observe also that $H^i(G, A \oplus B) = H^i(G, A) \oplus H^i(G, B)$ (as a finite direct sums of injectives is injectives), and multiplication by an integer n on A induces multiplication by n on the groups $H^i(G, A)$. In particular, if A is n-torsion, so is $H^i(G, A)$ for all $i \in \mathbf{N}$.

We will now compute the cohomology groups explicitely using cochains, thanks to Theorem 2.6, which will be convenient for small degrees. We define an explicit resolution of the G-module $\mathbf{Z}$ (equipped with the trivial action of G) as follows. For all $i \geq 0$, let $E_i = G^{i+1}$ be the set of $(i+1)$-tuples of elements of G. The action of G on E_i by left-translation

$$s.(g_0, ..., g_i) := (s.g_0, ..., s.g_i), \;\; s \in G, (g_0, ..., g_i) \in E_i$$

induces a structure of G-module on the free $\mathbf{Z}$-module L_i with basis E_i. Observe that L_i is then a free $\mathbf{Z}[G]$-module (a basis is obtained by choosing an element in each orbit for the action of G on E_i, as G acts withoud fixed point on E_i). We define a morphism of G-modules $d_i : L_i \to L_{i-1}$ by the formula:

$$d_i(g_0, ..., g_i) = \sum_{j=0}^{i} (-1)^j (g_0, ..., \hat{g}_j, ..., g_i)$$

for $i > 0$ and $d_0 : L_0 \to \mathbf{Z}$ sends every $g_0 \in G$ to 1.

Lemma 2.9 *The sequence*

$$... \to L_2 \stackrel{d_2}{\to} L_1 \stackrel{d_1}{\to} L_0 \stackrel{d_0}{\to} \mathbf{Z} \to 0$$

is exact, hence it is a resolution of $\mathbf{Z}$ *by free (hence projective)* $\mathbf{Z}[G]$*-modules.*

Proof (sketch of): (cf. [5], Lemma 1.26). The fact that the sequence is a complex is shown by an explicit computation; then one constructs morphisms of abelian groups $u_i : L_i \to L_{i+1}$ such that $u_{i-1} \circ d_i + d_{i+1} \circ u_i = \mathrm{Id}_{L_i}$ via the formula $u_i(g_0, ..., g_i) = (1, g_0, ..., g_i)$.

□

We now observe that if A is a G-module, an element of $K^i := \mathrm{Hom}_G(L_i, A)$ identifes itself with a function $f : G^{i+1} \to A$ satisfying

$$f(s.g_0, ..., s.g_i) = s.f(g_0, ..., g_i)$$

("homogeneous cochain"). Such a function is uniquely determined by the value it takes at the elements of G^{i+1} of the form $(1, g_1, g_1g_2, ..., g_1...g_i)$, hence we can also identifiy K^i with the set of "non homogeneous cochains", namely the set of functions from G^i to A (with the convention $G^0 = \{1\}$, hence $K^0 = A$). Applying Theorem 2.6, this yields:

Theorem 2.10 *The groups $H^i(G, A)$ for $i \geq 1$ are obtained as the cohomology groups of the complex of non homogeneous cochains*

$$0 \to K^0 \to K^1 \to K^2 \to ...,$$

the differential $d^i : K^i \to K^{i+1}$ being given by the formula

$$(d^i f)(g_1, ...g_{i+1}) := g_1.f(g_2, ..., g_{i+1}) + \sum_{j=1}^{i} (-1)^j f(g_1, ..., g_j g_{j+1}, ...g_{i+1})$$

$$+(-1)^{i+1} f(g_1, ..., g_i).$$

As G is assumed to be finite, this implies the following statement (which can also be proved by dimension shifting):

Corollary 2.11 *If A is finite, then the groups $H^i(G, A)$ are finite.*

The (non homogeneous) cochains of $\ker d^i$ are called *i-cocycles* and the i-coycles in the image of d^{i-1} are called *i-coboundaries.*

Example 2.12 a) The group $H^1(G, A)$ is the quotient of the group $Z^1(G, A)$ of functions $f : G \to A$ satisfying $f(g_1g_2) = f(g_1) + g_1.f(g_2)$ for all $g_1, g_2 \in G$ ("crossed homomorphisms") by the group of functions of the form $g \mapsto g.a - a$ for some $a \in a$. For instance if the action of G on A is trivial, then $H^1(G, A)$ identifies with the group homomorphisms from G to A.

b) A 2-cocycle is a *system of factors*, that is a map $f : G \times G \to A$ satisfying

$$g_1.f(g_2, g_3) - f(g_1g_2, g_3) + f(g_1, g_2g_3) - f(g_1, g_2) = 0$$

for all $g_1, g_2, g_3 \in G$. The theory of group extensions (cf. [12], §6.6) shows that $H^2(G, A)$ classifies group extensions E of G by A such that the action (by conjugation in E) of G on A corresponding to E is the action given by the G-module structure on A. The trivial action corresponds to central extensions.

We will sometimes need *Tate modified cohomology groups*, defined as follows.

Definition 2.13 Let A be a G-module. Let $N_G = N : A \to A$ be the *norm map*, defined as

$$N(x) = \sum_{g \in G} g.x.$$

Let I_G be the kernel of the *augmentation map* :

$$\mathbf{Z}[G] \to \mathbf{Z}, \ \sum a_g g \mapsto \sum a_g.$$

It is also the subgroup of $\mathbf{Z}[G]$ generated by the $(g-1), g \in G$. We set $\widehat{H}^0(G,A) = A^G/NA$. We also define $\widehat{H}^{-1}(G,A) = \ker N/I_G A$. For $q > 0$, we set $\widehat{H}^q(G,A) = H^q(G,A)$. It is also possible to define $\widehat{H}^q(G,A)$ for $q < -1$, using homology groups (see [5], §2.1), such that $(\widehat{H}^q(G,.))_{q \in \mathbf{Z}}$ is a cohomological functor.

The main theorem on these modified groups is the 2-periodicity of cohomology when G is cyclic:

Theorem 2.14 *Assume that G is cyclic, generated by some s. Let A be a G-module. Then the group $\widehat{H}^q(G,A)$ is isomorphic to $\widehat{H}^0(G,A)$ if q is even, and to $\widehat{H}^{-1}(G,A)$ (or $H^1(G,A)$) if q is odd.*

Proof (sketch of): Let n be the order of G. Let $D = (s-1) \in \mathbf{Z}[G]$. Observe that the norm map is the multiplication by $N = \sum_{i=0}^{n-1} s^i$, with $NA = \ker D$ and $I_G A = \operatorname{Im} D$. As $DN = ND = 0$, we define a complex $K(A)$ by $K^i(A) = A$ for all $i \in \mathbf{Z}$, the differentials d^i being defined as: d^i is multiplication by D (resp. by N) if i is even (resp. odd). Now $A \mapsto (H^q(K(A)))$ is a cohomological functor, which coincides (including the coboundary operator between $q = 0$ and $q = 1$) with $(\widehat{H}^q(G,.))$ in degrees -1 and 0. One concludes by dimension shifting that they coincide for all q, whence the result because cohomology of the complex $K(A)$ is obviously 2-periodic.

□

Example 2.15 a) Take $G = \mathbf{Z}/2\mathbf{Z}$. Let σ be the non trivial element of G. Then for i even, the group $H^i(G,A)$ is the quotient of A^σ by elements of the form $x + \sigma.x, x \in A$.

b) For an induced G-module $I = \mathbf{Z}[G] \otimes X$, it is not difficult to check directly that we have $\widehat{H}^0(G,I) = 0$. The same holds for H^{-1}.

We are now going to consider changing the group G acting on a G-module A. Let G' be a group endowed with a morphism $f : G' \to G$. There is now a structure of G'-module (denoted f^*A or simply A) on A via

$$g'.a := f(g').a, \; g' \in G', \; a \in A.$$

We obtain a morphism of functors from $H^0(G,.)$ to $H^0(G', f^*.)$ and the universal property of derived functors (cf. [12], Th. 2.4.7) show that there is a unique family of morphism of functors

$$f_i^* : H^i(G,.) \to H^i(G',.), i \in \mathbf{N}$$

compatible (in an evident way) with the map δ^i of the long exact cohomology sequences. Hence we just got a *morphism of cohomological functors.*

Let now A' be an arbitrary G'-module, and assume that we are given a morphism of abelian groups $u : A \to A'$ compatible with the morphism $f : G' \to G$, that is:

$$u(f(g').a) = g'.u(a), \forall g' \in G', \forall a \in A.$$

Then u is a G'-homomorphism from f^*A to A' and induces (for all i) a homomorphism $u_* : H^i(G', f^*A) \to H^i(G', A')$. Composing this homomorphism with the f_i^* yields a morphism of cohomological functor

$$H^i(G, A) \to H^i(G', A'), \; i \in \mathbf{N},$$

which has an obvious expression using the computation of $H^i(G, A)$ using the cochains (just use the pushout by $u : A \to A'$ and $f : G' \to G$ of the cocycles and coboundaries).

Example 2.16 a) Let H be a subgroup of G and A be a G-module. Taking for f the canonical injection $H \to G$, we obtain the *restriction homomorphisms* $\mathrm{Res} : H^i(G, A) \to H^i(H, A)$.

b) Let H be a normal subgroup of G. Let A be a G-module. Then A^H is equipped with a G/H-module structure, and the inclusion $A^H \to A$ is compatible with the canonical surjection $G \to G/H$. This yields the *inflation homomorphisms* $\mathrm{Inf} : H^i(G/H, A^H) \to H^i(G, A)$.

Observe that restriction and inflation also have obvious definitions in terms of cocycles.

c) If H is a subgroup of a cyclic group G, then the inflation map

$$H^2(G/H, A^H) \to H^2(G, A)$$

corresponds to the norm map $\widehat{H}^0(G/H, A^H) = A^G/N_{G/H}A^H \to \widehat{H}^0(G, A) = A^G/N_G(A)$, which is induced by the multiplication by $\#H$.

Definition 2.17 Let G be a finite group and H a subgroup of G. Let A be an H-module. Define the G-module $I_G^H(A)$ as the set of functions $f : G \to A$ satisfying $f(h.g) = h.f(g)$ for all $h \in H, g \in G$, the action of G on $I_G^H(A)$ being given by $(g.f)(g') = f(g'g)$ for all $g, g' \in G$. This extends the definition of the induced module $I_G(A)$ (which corresponds to the case $H = \{1\}$). In general $I_G^H(A)$ is isomorphic to $\mathbf{Z}[G] \otimes_{\mathbf{Z}[H]} A$ with the action of G on the first factor ([5], Remark 1.6. c).

Theorem 2.18 (Shapiro lemma) *There are isomorphisms*

$$H^i(G, I_G^H(A)) \to H^i(H, A), \ i \in \mathbf{N}$$

induced by the map $u \mapsto u(1)$ from $I_G^H(A)$ to A (which is compatible with the G-module structure of $I_G^H(A)$ and the H-module structure of A).

Proof (sketch of): One first checks ([5], Prop 1.12) that for any G-module B, the group $\mathrm{Hom}_H(B, A)$ identifies with $\mathrm{Hom}_G(B, I_G^H(A))$. This implies that the functor $F : A \mapsto I_G^H(A)$ preserves the injectives because its left-adjoint is the forgetful functor from $\mathcal{M}od_G$ to $\mathcal{M}od_H$. On the other hand it is easy to see that $(I_G^H(A))^G = A^H$. Taking an injective resolution of the H-module A and applying the functor F, it is sufficient to show that F is exact, which is straightforward (one can also use the fact that $I_G^H(A) \simeq \mathbf{Z}[G] \otimes_{\mathbf{Z}[H]} A$ and $\mathbf{Z}[G]$ is a free left $\mathbf{Z}[H]$-module).

□

Let A be a G-module. Let $t \in G$, denote by $f : g \mapsto t^{-1}gt$ the inner automorphism associated with t^{-1}. Then the map $a \mapsto t.a$ from A to A is compatible with f, whence (for all $i \geq 0$) homomorphisms $\sigma_t^i : H^i(G, A) \to H^i(G, A)$ (which yields a cohomological functor).

Proposition 2.19 *The map σ_t^i is the identity for all $i \geq 0$.*

Proof : The case $i = 0$ is trivial. We then argue by induction on i: embed A into an induced module I and set $B := I/A$, then the map $H^i(G, B) \to H^{i+1}(G, A)$ is surjective. Since the map σ_t^i is the identity on $H^i(G, B)$ by induction hypothesis, the map σ_t^{i+1} is the identity on $H^{i+1}(G, A)$.

□

Example 2.20 Let H be a normal subgroup of G. Let A be a G-module. The action of G on H by conjugation induces an action of G on $H^i(H, A)$, and Proposition 2.19 shows that the subgroup H acts trivially on $H^i(H, A)$, whence an action of G/H on $H^i(H,A)$. Another way to describe this action is to take an injective resolution

$$0 \to A \to I_0 \to I_1 \to ...$$

by induced G-modules, which are also induced (hence acyclic for $H^0(H,.)$) H-modules (because $\mathbf{Z}[G]$ is free as a $\mathbf{Z}[H]$-module). Then the $H^i(H,A)$ are computed as cohomology groups of the complex

$$0 \to I_0^H \to I_1^H \to ...,$$

thus they are naturally equipped with an action of G/H. The fact that both descriptions coincide is easily proved by dimension-shifting.

Theorem 2.21 (Hochschild-Serre) *Let A be a G-module. Let H be a normal subgroup of G. Then there is a spectral sequence*

$$E_2^{pq} = H^p(G/H, H^q(H,A)) \Rightarrow H^{p+q}(G,A).$$

Let us recall a few consequences:

Corollary 2.22 *a) Each group $H^r(G,A)$ is filtered by abelian groups such that each successive quotient is a subquotient of $H^p(G/H, H^q(H,A))$ for some (p,q) with $p+q=r$. In particular if all $H^p(G/H, H^q(H,A))$ with $p+q=r$ are finite (resp. zero), then $H^r(G,A)$ is finite (resp. zero).*

b) There is a low degree exact sequence

$$0 \to H^1(G/H, A^H) \stackrel{\text{Inf}}{\to} H^1(G,A) \stackrel{\text{Res}}{\to} H^1(H,A)^{G/H} \to H^2(G/H, A^H) \stackrel{\text{Inf}}{\to} ...$$

$$... \to \ker[H^2(G,A) \to H^2(H,A)^{G/H}] \to H^1(G/H, H^1(H,A)) \to ...$$

$$.... \to \ker[H^3(G/H, A^H) \stackrel{\text{Inf}}{\to} H^3(G,A)].$$

c) Let $n \in \mathbf{N}^*$. Assume that $H^q(H,A) = 0$ for $1 \le q \le n-1$. Then there is an exact sequence

$$0 \to H^n(G/H, A^H) \stackrel{\text{Inf}}{\to} H^n(G,A) \stackrel{\text{Res}}{\to} H^n(H,A)^{G/H}.$$

Proof of Theorem 2.21: This is a special case of Grothendieck's composed functors spectral sequence. The functor $A \mapsto A^G$ from $\mathcal{M}od_G$ to $\mathcal{A}b$ is the composed of $F_1 : A \mapsto A^H$ (from $\mathcal{M}od_G$ to $\mathcal{M}od_{G/H}$) and $F_2 : B \mapsto B^{G/H}$ (from $\mathcal{M}od_{G/H}$ to $\mathcal{A}b$). The derived functors of F_1 are the $H^i(H, .)$ (indeed a resolution of $\mathbf{Z}$ by projective G-modules is also a resolution by projective H-modules) and the derived functors of F_2 are by definition the $H^i(G/H, .)$. It remains to show that F_1 preserves the injectives, which follows from the obvious formula

$$\mathrm{Hom}_G(B, A) = \mathrm{Hom}_{G/H}(B, A^H),$$

which holds for every G-module A and every G/H-module (=G-module with trivial action of H) B.

□

Finally, we define for every subgroup H of G and every G-module A *corestriction* morphisms $H^i(H, A) \to H^i(G, A)$ as follows. For $i = 0$, it is the *norm map*:

$$N_{G/H} : a \mapsto \sum_{s \in G/H} s.a$$

from A^H to A^G. We then extend this to a unique morphism of cohomological functors from $H^i(H, f^*.)$ to $H^i(G, .)$, where f is the inclusion map $H \to G$. This is possible since the functor $H^i(H, f^*.)$ is effaceable in positive degree, hence universal ([12], ex. 2.4.5). Indeed every G-module A embeds into a induced G-module, which is also induced as an H-module. We obtain *corestriction morphisms*

$$\mathrm{Cores} : H^i(H, A) \to H^i(G, A),$$

which are compatible with morphisms of short exact sequences.

Theorem 2.23 *Let $m = [G : H]$. Then* Cores ∘ Res *is the multiplication by m in $H^i(G, A)$.*

Proof : This is clear for $i = 0$. The general case is then obtained by dimension shifting.

□

Corollary 2.24 *Let m the order of G. Let A be a G-module. Then $H^i(G, A)$ is m-torsion for all $i > 0$.*

Proof : Apply the previous theorem to $H = \{1\}$.

$\square$

Corollary 2.25 *Let A be a G-module. Then if A is of finite type (over $\mathbf{Z}$), the groups $H^i(G, A)$ are finite for $i > 0$.*

Proof : The cochain description shows that these groups are of finite type, and they are torsion by the previous corollary.

Corollary 2.26 *Let A be a G-module. Assume that it is uniquely divisible (as an abelian group). Then $H^i(G, A) = 0$ for all $i > 0$.*

Proof : Let m be the order of G. Then the groups $H^i(G, A)$ are m-torsion, but multiplication by m is a bijection on A, hence also on $H^i(G, A)$.

Example 2.27 The G-module $\mathbf{Q}$ (with trivial action is uniquely divisible. Therefore $H^i(G, \mathbf{Q}/\mathbf{Z}) \simeq H^{i+1}(G, \mathbf{Z})$ for all $i > 0$. In particular $H^2(G, \mathbf{Z})$ is isomorphic to the group of characters $H^1(G, \mathbf{Q}/\mathbf{Z}) = \mathrm{Hom}(G, \mathbf{Q}/\mathbf{Z})$ of the finite group G.

2.2. Extension to profinite groups

From now on, G denotes a profinite group.

Definition 2.28 A *discrete G-module* A is an abelian group endowed with an action of G by automorphism, such that for every $x \in A$ the map $g \mapsto g.x$ from G to A is continuous, where A is equipped with the discrete topology. The abelian category of discrete G-modules is denoted by C_G.

The continuity condition (which is of course obvious if G is finite) is equivalent to saying that the stabilizer of every element of A is an open subgroup of G. In this course, *we will consider only discrete G-modules*, hence we will often simply say "G-module" for "discrete G-module". If A is a discrete G-module, then we have $A = \bigcup_U A^U$, were U runs over all open subgroups of G. Observe also that A is of finite type as a $\mathbf{Z}[G]$-module if and only if it is of finite type as a $\mathbf{Z}$-module, thanks to the continuity condition. Therefore, "of finite type" is not ambiguous for a discrete G-module.

Example 2.29 We are mainly interested in the cas when $G = \mathrm{Gal}\,(\bar{k}/k)$ is the absolute Galois group of a field k.

a) The trivial action makes every abelian group A a discrete G-module, e.g. $A = \mathbf{Z}$ or $A = \mathbf{Z}/n$.

b) We can consider the additive group $\bar{k}$ or the multiplicative group $\bar{k}^*$ with the natural action of G, or the group μ_n of n-roots of unity in $\bar{k}$ (when n is a positive integer not divisible by the characteristic of k). More generally, if G is a commutative algebraic group (=group scheme of finite type) over k, the group $G(\bar{k})$ of $\bar{k}$-points is a discrete G-module. The modules $\bar{k}$ and $\bar{k}^*$ correspond respectively to the additive group $\mathbf{G}_a$ and the multiplicative group $\mathbf{G}_m$.

c) Let M be a finite G-module of order n, with n not divisible by the characteristic of k. The *Cartier dual* of M is the group $M' = \mathrm{Hom}(M, \mu_n) = \mathrm{Hom}(M, \bar{k}^*)$ equipped with the Galois action

$$(\gamma.f)(x) = \gamma.(f(\gamma^{-1}.x)), \ f \in M', \ \gamma \in G, x \in A.$$

This definition is made so that the tensor product $M \otimes M'$ is equipped with a natural G-equivariant perfect pairing to $\bar{k}^*$.

The category C_G of discrete G-modules has enough injectives ([5], Example A.35. c), so it is possible to define the cohomology groups $H^i(G, .)$ as derived functors of the functor $A \mapsto A^G$ from C_G to Ab. However, since the category C_G for G infinite does not have enough projectives (loc. cit., exercise 4.2; observe that for instance $\mathbf{Z}[G]$ is *not* a discrete G-module in this case), it is more convenient to adapt the cochain definition as follows.

Definition 2.30 Let $A \in C_G$. For $q \geq 0$, denote by $K^q(G, A)$ the set of *continuous* (i.e. locally constant) maps from G^q to A. Let $d : K^q(G, A) \to K^{q+1}(G, A)$ be the differential (defined with the usual formula, as in Theorem 2.10). The cohomology groups $H^q(G, A)$ are defined as the cohomology groups of the complex $(K^q(G, A))_{q \in \mathbf{N}}$.

Recall that an *inductive system* of abelian groups (or G-modules) consists of the data of: a directed poset Λ; for each $i \in \Lambda$, an abelian group A_i; for each pair $i, j \in \Lambda$ with $i \leq j$, a homomorphism $f_{ij} : A_i \to A_j$ such that $f_{ii} = \mathrm{Id}$ and $f_{jk} \circ f_{ij} = f_{ik}$ for all $i \leq j \leq k$. The *direct limit* (or inductive limit, or colimit) $\varinjlim_{i \in \Lambda} A_i$ is then defined as the quotient of the disjoint union of the A_i by the equivalence relation $a_i \sim a_j$ (with $a_i \in A_i$ and $a_j \in A_j$) if there exists $k \in \Lambda$ such that $k \geq i, k \geq j$, and $f_{ik}(a_i) = f_{jk}(a_j)$.

Theorem 2.31 *Let (G_i) be a projective system of profinite groups. Let (A_i) be an inductive system of discrete G_i-modules, the transition maps being compatible with those of the G_i. Let $G = \varprojlim G_i$ and $A = \varinjlim A_i$. Then for all $q \in \mathbf{N}$:*

$$H^q(G, A) \simeq \varinjlim H^q(G_i, A_i).$$

Proof (sketch of): As the direct limit functor is exact, it is sufficient to show that the canonical homomorphisms

$$\varinjlim K^q(G_i, A_i) \to K^q(G, A)$$

are isomorphisms, which is tedious but not difficult, see [5], Prop 4.18.

□

Corollary 2.32 *Let A be a discrete G-module. Then*

a) We have

$$H^q(G, A) = \varinjlim_U H^q(G/U, A^U),$$

where U runs over all normal open subgroups of G.

b) We also have

$$H^q(G, A) = \varinjlim_B H^q(G, B),$$

where B runs over all finite type sub-G-modules of A.

Proof : For a), we apply the previous theorem to $G = \varprojlim_U (G/U)$ and $A = \bigcup_U A^U = \varinjlim_U A^U$. For b), we use $A = \bigcup_B B = \varinjlim_B B$.

□

Corollary 2.33 *For $q \geq 1$, the groups $H^q(G, A)$ are torsion.*

Proof : This follows from Corollary 2.32 a), and Corollary 2.24.

□

Remark 2.34 Our definition of the groups $H^q(G, A)$ coincides with the definition as derived functors of $A \mapsto A^G$ from C_G to $\mathcal{A}b$. This follows from Corollary 2.32, a) and the easy fact that if I is injective in C_G, then I^U is injective in $C_{G/U}$ for every open normal subgroup U of G.

Using Corollary 2.32 a), most properties of the cohomology of finite groups immediately extend to profinite groups, provided we work with *closed* subgroups and *continuous* cochains. We list them in the following theorem:

Theorem 2.35 *Let G be a profinite group. Let H be a closed subgroup of G.*

a) For an abelian group (resp. an H-module) A, the G-modules $I_G(A)$ and $I_G^H(A)$ are defined the same way (with the restriction that the functions have to be taken continuous), and $I_G(A)$ is acyclic for the functor $H^0(G, .)$.

b) The restriction and inflation (if H is normal) homomorphisms are still defined as in the previous paragraph, and Shapiro's lemma is still valid.

c) For H normal, Hochschild-Serre spectral sequence and its consequences still hold [1].

d) If H is open (hence of finite index) in G, the corestriction maps are defined and formula 2.23 holds.

Definition 2.36 Let G be a profinite group. Let p be a prime number. The *cohomological p-dimension* of G (denoted $\mathrm{cd}_p(G)$ is the lower bound (in $\mathbf{N} \cup \{+\infty\}$) for the set of integers $n \in \mathbf{N}$ satisfying:

For any discrete *torsion* G-module A and any $q > n$, the p-primary component (or the p-torsion subgroup) of $H^q(G, A)$ is zero. The *cohomological dimension* of G is $\mathrm{cd}(G) = \sup_p \mathrm{cd}_p(G)$.

Example 2.37 If p does not divide the order of G, then $\mathrm{cd}_p(G) = 0$ by Corollaries 2.24 and 2.32, a). The notion is actually not interesting when G is finite, because in this case $\mathrm{cd}_p(G) = +\infty$ as soon as p divides the order of G ([5], exercice 5.1). This follows rather easily from Proposition 2.42 below and the fact that for every odd positive integer q, we have (by Theorem 2.14)

$$H^q(\mathbf{Z}/p, \mathbf{Z}/p) \simeq H^1(\mathbf{Z}/p, \mathbf{Z}/p) \simeq \mathbf{Z}/p \neq 0.$$

Recall that a non-zero G-module is *simple* if it has no sub-G-module except $\{0\}$ and itself.

Theorem 2.38 *Let G be a profinite group. Let p be a prime number and $n \in \mathbf{N}$. The following conditions are equivalent:*

i) $\mathrm{cd}_p(G) \leq n$.

ii) For all $q > n$ and every discrete G-modules A which is a p-primary abelian group, we have $H^q(G, A) = 0$.

iii) We have $H^{n+1}(G, A) = 0$ for every discrete G-module A which is simple and p-torsion.

Proof : A torsion G-module A is the direct sum of its primary components $A\{p\}$ (where p runs over all prime numbers). The equivalence of i) and ii) comes from the fact that by Corollary 2.32 b), the p-primary abelian group $H^q(G, A\{p\})$ is the p-primary component of $H^q(G, A)$. Obviously ii) implies iii). Assume iii) and let's prove that ii) holds. Assume first that the p-primary

[1] It is a little bit more difficult to check that an injective object of C_G remains injective in C_H, see [5], Prop .4.25.

G-module A is finite. We show by induction on $\#A$ that $H^{n+1}(G, A) = 0$. If A is simple, then $A = A[p]$ (since $A[p]$ is a non-trivial sub-G-module of A), whence the result with iii). Otherwise, we have an exact sequence of G-modules

$$0 \to A_1 \to A_2 \to A_3 \to 0$$

with A_1 and A_2 of cardinality strictly smaller than $\#A$, and the result follows from the induction assumption and the cohomology long exact sequence. Now $H^{n+1}(G, A) = 0$ holds for every p-primary G-module A thanks to Corollary 2.32, b) (indeed a finite type submodule of A is torsion and of finite type over $\mathbf{Z}$, hence finite). Finally we prove ii) by induction on $q > n$, using an embedding of A into the induced module $I_G(A)$ (which is indeed p-primary thanks to the continuity condition on elements of $I_G(A)$) and applying the induction assumption to $A/I_G(A)$.

□

Theorem 2.39 *Let G be a pro-p-group and $n \in \mathbf{N}$. Then $\mathrm{cd}_p(G) \leq n$ if and only if $H^{n+1}(G, \mathbf{Z}/p) = 0$.*

Proof : Obviously if $\mathrm{cd}_p(G) \leq n$, then $H^{n+1}(G, \mathbf{Z}/p) = 0$. Conversely, assume the latter. Let A be a simple discrete p-torsion module. By Theorem 2.38, it is sufficient to show that such an A is isomorphic to $\mathbf{Z}/p$ as a G-module. We observe that A is finite (indeed the G-module generated by a non-zero element of A is torsion and of finite type, hence finite, and it coincides with A because A is simple). In particular A is a G/U-module for some normal open subgroup U of G. As A still is simple as a G/U-module, we can assume that G is a finite p-group. It is then well-known that $A^G \neq \{0\}$ (use the class formula for the action of G on A), hence $A^G = A$ by simplicity of A, namely the action of G on A is trivial. It is then clear that $A = \mathbf{Z}/p$ (otherwise A has a non-trivial subgroup).

□

Remark 2.40 There is also a notion of *strict cohomological p-dimension* $\mathrm{scd}_p(G)$ and strict cohomological dimension $\mathrm{scd}(G)$: they are defined as in Definition 2.36, except that the G-module A is not assumed to be torsion. Actually $\mathrm{scd}_p(G)$ is at most $\mathrm{cd}_p(G) + 1$ ([5], Prop 5.8).

Example 2.41 The group $\mathbf{Z}_p$ is of p-cohomological dimension 1. Indeed

$$H^1(\mathbf{Z}_p, \mathbf{Z}/p) = Hom_c(\mathbf{Z}_p, \mathbf{Z}/p) = \mathbf{Z}/p \neq 0,$$

hence $\mathrm{cd}_p(\mathbf{Z}_p) \geq 1$. On the other hand

$$H^2(\mathbf{Z}_p, \mathbf{Z}/p) = \varinjlim_n H^2(\mathbf{Z}/p^n, \mathbf{Z}/p) \simeq \varinjlim_n \widehat{H}^0(\mathbf{Z}/p^n, \mathbf{Z}/p) = \varinjlim_n \mathbf{Z}/p,$$

the transition map being multiplication by p (this follows from the easy fact that for a finite group G, a normal subgroup H, and a G-module A, the inflation map $\widehat{H}^0(G/H, A^H) = A^G/N_{G/H}A^H \to \widehat{H}^0(G, A) = A^G/N_G A$ is induced by multiplication by $\#H$). The latter is zero, so $\mathrm{cd}_p(\mathbf{Z}_p) = 1$ by Proposition 2.39.

Proposition 2.42 *Let G be a profinite group. Let H be a closed subgroup of G. Then $\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G)$. The equality holds if $[G : H]$ is prime to p, or if H is open in G and $\mathrm{cd}_p(G) < +\infty$. The same holds for $\mathrm{cd}(G)$, $\mathrm{scd}_p(G)$ etc.*

Proof : The inequality $\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G)$ follows from Shapiro's lemma $H^q(H, A) = H^q(G, I_G^H(A))$ and the fact that $I_G^H(A))$ is p-primary as soon as A is p-primary. If $[G : H]$ is prime to p, then the restriction map $H^q(G, A) \to H^q(H, A)$ is injective for every p-primary G-module A by Corollary 2.32 and Theorem 2.23, whence $\mathrm{cd}_p(H) = \mathrm{cd}_p(G)$.

Assume now that $n := \mathrm{cd}_p(G) < +\infty$ and H is open in G. Let A be a p-primary G-module. Let us show that the corestriction morphism $\mathrm{Cor} : H^n(H, A) \to H^n(G, A)$ is surjective, which will prove that $\mathrm{cd}_p(H) = n$ (since we already know that $\mathrm{cd}_p(H) \leq n$ and a p-primary G-module A such that $H^n(G, A) \neq 0$ will provide one with $H^n(H, A) \neq 0$). We observe that Cor identifies with the map $H^n(G, I_G^H(A)) \to H^n(G, A)$ induced by Shapiro's lemma and the surjective map

$$f \mapsto \pi(f) = \sum_{g \in G/H} g.f(g^{-1})$$

from $I_G^H(A)$ to A (as usual, it is sufficient to check this in degree 0 to compare the two corresponding natural transformations of cohomological functors). It remains to apply the long exact cohomological sequence associated to

$$0 \to \ker \pi \to I_G^H(A) \to A \to 0$$

an the definition of p-cohomological dimension, observing that $I_G^H(A)$ and $\ker \pi$ are still p-primary.

□

Remark 2.43 In general there is no control on the cohomological dimension of a quotient G/H if we know $\mathrm{cd}_p(G)$. For instance $\mathbf{Z}_p$ is of p-cohomological dimension 1, but the quotient $\mathbf{Z}/p$ has infinite p-cohomological dimension. Also the last statement of Propositionn 2.42 is false if $\mathrm{cd}_p(G)$ is not finite: take $G = \mathbf{Z}/2$, $p = 2$, and $H = \{0\}$.

Proposition 2.44 *Let G be a profinite group. Let H be a closed normal subgroup of G. Then*

$$\mathrm{cd}_p(G) \leq \mathrm{cd}_p(H) + \mathrm{cd}_p(G/H)$$

(and same for $\mathrm{cd}(G)$ *etc.).*

Proof : This follows easily from Hochschild-Serre spectral sequence (Theorem 2.35, c).

□

2.3. Abelian Galois cohomology

In this paragraph, k is a field with separable closure $\bar{k}$ and absolute Galois group $\Gamma_k = \mathrm{Gal}\,(\bar{k}/k)$. For every discrete Γ_k-module M, the cohomology groups $H^q(\Gamma_k, M)$ have been defined. Using Proposition 2.19, we see that two different separable closures define canonically isomorphic groups $H^q(\Gamma_k, M)$, that we can denote by $H^q(k, M)$. More generally, if A is a commutative algebraic group (or even group scheme) over k, we set $H^q(k, A) := H^q(\Gamma_k, A(\bar{k}))$; for every field extension k_1/k, this induces a canonical map $H^q(k, A) \to H^q(k_1, A)$. This applies for instance to the additive group $\mathbf{G}_a$ (defined by $\Gamma = \mathrm{Spec}\,(k[t])$, so $\mathbf{G}_a(k_1) = k_1$) and the multiplicative group $\mathbf{G}_m$ (defined by $\mathbf{G}_m = \mathrm{Spec}\,(k[t, t^{-1}])$, so $\mathbf{G}_m(k_1) = k_1^*$).

Proposition 2.45 *Let k be a field. Let L be a finite Galois extension of k with group G. Then $H^q(G, L) = 0$ for all $q > 0$ and $\widehat{H}^q(G, L) = 0$ for $q \in \{-1, 0\}$. Similarly $H^q(k, \mathbf{G}_a) = 0$ for all $q > 0$.*

Proof : The first statement comes from the fact that by the normal basis theorem, the G-module L is induced (isomorphic to $\mathbf{Z}[G] \otimes_{\mathbf{Z}} k$). Now the second statement follows, by Corollary 2.32.

□

More interesting is the celebrated following result:

Theorem 2.46 (Hilbert 90) *Let L/k be a finite Galois extension with Galois group G. Then $H^1(G, L^*) = 0$, and $H^1(k, \mathbf{G}_m) = 0$.*

Proof : Thanks to Corollary 2.32, it is sufficient to prove the first assertion. Let $(s \mapsto a_s) \in Z^1(G, L^*)$ be a 1-cocycle. By Dedekind's theorem on linear independence (as maps $L^* \to L$) of the morphisms $L^* \to L^*$, there exists $c \in L^*$ such that

$$b = \sum_{t \in G} a_t t(c)$$

is not zero. Now for every $s \in G$, we have:

$$s(b) = \sum_{t \in G} s(a_t).(st)(c) = \sum_{t \in G} a_s^{-1} a_{st}.(st)(c) = a_s^{-1} \sum_{t \in G} a_{st}(st)(c),$$

thanks to the cocycle condition. Thus $s(b) = a_s^{-1} b$, which implies that $a_s = s(b^{-1})/b^{-1}$ for every $s \in G$. Namely $s \mapsto a_s$ is a 1-coboundary.

□

The two previous results have important corollaries. Denote by μ_n the k-group scheme of n-roots of unity (thus $\mu_n(\bar{k}) = \{x \in \bar{k}, x^n = 1\}$). If k is of positive characteristic p, denote by Φ the map $x \mapsto x^p - x$ from $\bar{k}$ to $\bar{k}$.

Theorem 2.47 *Let k be a field with separable closure $\bar{k}$.*

a) (Kummer theory) Let n be a positive integer not divisible by the characteristic of k. Then $H^1(k, \mu_n) = k^*/k^{*^n}$,

b) (Artin-Schreier theory) Assume that k is of characteristic $p > 0$. Then $H^1(k, \mathbf{Z}/p) = k/\Phi(k)$ and $H^q(k, \mathbf{Z}/p) = 0$ if $q \leq 2$.

c) If k is of positive characteristic p, then $\mathrm{cd}_p(\Gamma_k) \leq 1$ (hence $\mathrm{scd}_p(\Gamma_k) \leq 2$).

Proof : a) The exact sequence of Γ_k-modules (the last map being surjective because n does not divide $\mathrm{Char}\, k$, hence all n-roots of an element of $\bar{k}$ are in the separable closure $\bar{k}$)

$$1 \to \mu_n(\bar{k}) \to \bar{k}^* \xrightarrow{.n} \bar{k}^* \to 1$$

induces an exact sequence

$$H^0(\Gamma_k, \bar{k}^*) = k^* \xrightarrow{.n} k^* \to H^1(k, \mu_n) \to 0,$$

thanks to Hilbert 90. The result follows.

b) There is an exact sequence of Γ_k-modules

$$0 \to \mathbf{F}_p = \mathbf{Z}/p \to \bar{k} \xrightarrow{\Phi} \bar{k} \to 0.$$

Indeed the map $\Phi : \bar{k} \to \bar{k}$ is onto (the polynomial $X^p - X$ being separable because its derivative is -1) and elements of $\ker \Phi$ are exactly the elements of the prime subfield $\mathbf{F}_p$ of $\bar{k}$. Thanks to Proposition 2.45, we obtain an exact sequence

$$H^0(\Gamma_k, \bar{k}) = k \xrightarrow{\Phi} k \to H^1(\Gamma_k, \mathbf{Z}/p) \to 0,$$

hence $H^1(k, \mathbf{Z}/p) = k/\Phi(k)$. By loc. cit., we also have $H^q(k, \mathbf{Z}/p) = 0$ for $q \geq 2$ via the long exact sequence of cohomology.

c) Let H be a p-Sylow of Γ_k. By infinite Galois theory, we have $H = \mathrm{Gal}\,(\bar{k}/K)$, where K is some algebraic separable extension of k. By Proposition 2.42, we have $\mathrm{cd}_p(\Gamma_k) = \mathrm{cd}_p(H)$ and by Theorem 2.39, it is sufficient to show that $H^2(H, \mathbf{Z}/p) = 0$. But $H^2(H, \mathbf{Z}/p) = H^2(K, \mathbf{Z}/p) = 0$ by b), whence the result.

□

2.4. The Brauer group of a field: first properties

Definition 2.48 Let k be a field with separable closure k. The *Brauer group* of k is the abelian group $\mathrm{Br}\, k := H^2(k, \mathbf{G}_m) = H^2(k, \bar{k}^*)$.

Observe that by Corollary 2.32, we can compute $\mathrm{Br}\, k$ as the direct limit of the $\mathrm{Br}\,(L/k) := H^2(\mathrm{Gal}\,(L/k), L^*)$, where $L \subset \bar{k}$ runs over all finite Galois extensions of k. Also a homomorphism $k \to k_1$ of fields induces a homomorphism $\mathrm{Br}\, k \to \mathrm{Br}\, k_1$, hence $k \mapsto \mathrm{Br}\, k$ is a functor from the category of fields to the category of abelian groups.

Proposition 2.49 *a) For any finite Galois extension L of k, we have*

$$\mathrm{Br}\,(L/k) = \ker[\mathrm{Br}\, k \to \mathrm{Br}\, L].$$

b) Let n be a positive integer not divisible by the characteristic of k. Then $H^2(k, \mu_n)$ is the n-torsion subgroup $(\mathrm{Br}\, k)[n]$ *of* $\mathrm{Br}\, k$.

Proof : a) Let $G = \mathrm{Gal}\,(L/k)$. By Hilbert 90, we have $H^1(G, L^*) = 0$. Applying the profinite version of Corollary 2.22 c) to the open subgroup $H := \mathrm{Gal}\,(\bar{k}/L) \subset \Gamma_k := \mathrm{Gal}\,(\bar{k}/k)$, we get an exact sequence

$$0 \to H^2(G, L^*) \to H^2(\Gamma_k, \bar{k}^*) = \mathrm{Br}\, k \to H^2(H, \bar{k}^*) = \mathrm{Br}\, L.$$

b) follows from the exact sequence

$$1 \to \mu_n(\bar{k}) \to \bar{k}^* \to \bar{k}^* \to 1$$

and Hilbert's 90, which yield an exact sequence

$$0 \to H^2(k, \mu_n) \to \operatorname{Br} k \xrightarrow{\cdot n} \operatorname{Br} k.$$

$\square$

Example 2.50 a) By definition, we have $\operatorname{Br} k = 0$ for every separably closed field k.

b) We have $\operatorname{Br} \mathbf{R} \simeq \mathbf{Z}/2$. Indeed, let $G = \operatorname{Gal}(\mathbf{C}/\mathbf{R}) \simeq \mathbf{Z}/2$. Then

$$H^2(G, \mathbf{C}^*) \simeq \widehat{H}^0(G, \mathbf{C}^*) = \mathbf{R}^*/N_{\mathbf{C}/\mathbf{R}}\mathbf{C}^* = \mathbf{R}^*/\mathbf{R}^*_+ \simeq \mathbf{Z}/2.$$

c) Local class field theory yields that the Brauer group of a p-adic field is isomorphic to $\mathbf{Q}/\mathbf{Z}$.

In the next chapter, we will see another description of the Brauer group of a field, using central simple algebras and non-abelian cohomology.

Definition 2.51 Let k be a field with absolute Galois group Γ_k. Let p be a prime number. Assume that k is either of characteristic $\neq p$, or perfect of characteristic p. The *cohomological p-dimension* $\operatorname{cd}_p(k)$ is by definition $\operatorname{cd}_p(\Gamma_k)$. If k is perfect (e.g. of characteristic zero), the cohomological dimension of k is $\operatorname{cd}(k) := \operatorname{cd}(\Gamma_k)$.

Remark 2.52 The previous definition is not "the right one" for imperfect fields of characteristic p because of Theorem 2.47, c). Typically $(\operatorname{Br} k)[p] \simeq \mathbf{Z}/p \neq 0$ if k is a local field of characteristic p, so we don't want k to be of p-dimension ≤ 1, although Γ_k is.

Theorem 2.53 *Let k be a field. Let p be a prime number different from the characteristic of k. The following are equivalent:*

i) We have $\operatorname{cd}_p(k) \leq 1$.

ii) For every separable algebraic extension K of k, the p-torsion $(\operatorname{Br} K)[p]$ *of* $\operatorname{Br} K$ *is trivial.*

iii) For every finite separable extension K of k, the p-torsion $(\operatorname{Br} K)[p]$ *of* $\operatorname{Br} K$ *is trivial.*

If k is perfect (e.g. of characteristic zero), the theorem holds for all prime p, and one can replace everywhere $\operatorname{cd}_p(k)$ *by* $\operatorname{cd}(k)$ *and* $(\operatorname{Br} K)[p]$ *by* $\operatorname{Br} K$.

Proof : Let us first assume that the prime p is not the characteristic of the field k. Suppose i), and let $K \subset \bar{k}$ be an algebraic separable extension of k. Then by Proposition 2.42, the cohomological p-dimension of $H := \mathrm{Gal}\,(\bar{k}/K)$ is at most 1, which implies

$$(\mathrm{Br}\,K)[p] = H^2(K, \mu_p) = H^2(H, \mu_p) = 0.$$

The implication ii) $\Rightarrow$ iii) is trivial. Suppose iii). Let G_p be a p-Sylow of $\Gamma_k = \mathrm{Gal}\,(\bar{k}/k)$ and $K_p \subset \bar{k}$ its corresponding fixed field. We observe that K_p contains the group μ_p of p-roots of unity in $\bar{k}$ (indeed $[K_p(\mu_p) : K_p]$ is a p-power and divides $p-1$). Therefore $H^2(K_p, \mathbf{Z}/p) = H^2(K_p, \mu_p)$. As $\mathrm{cd}_p(\Gamma_k) = \mathrm{cd}_p(G_p)$ by Proposition 2.42, it is now sufficient (in order to get i)) to prove that $H^2(K_p, \mu_p) = 0$ via Theorem 2.39. We observe that

$$H^2(K_p, \mu_p) = H^2(G_p, \mu_p) = \varinjlim_{L} H^2(L, \mu_p),$$

where $L \subset K_p$ runs over all finite subextensions of K_p/k. Indeed the group $G_p = \mathrm{Gal}\,(\bar{k}/K_p)$ is the intersection (hence the projective limit, the transitions maps being the inclusions) of all open subgroups $\mathrm{Gal}\,(\bar{k}/L) \subset \Gamma_k$ for such L, and Theorem 2.31 applies. Assumption iii) tells that $H^2(L, \mu_p) = (\mathrm{Br}\,L)[p] = 0$, so i) holds.

Assume further that k is perfect. As $\mathrm{cd}_p(k) = \mathrm{cd}_p(\Gamma_k) \leq 1$ by Theorem 2.47 c), it remains to prove that if k is of characteristic p, we still have $(\mathrm{Br}\,K)[p] = 0$ for any algebraic extension K of k. We observe that K and its separable closure $\overline{K}$ still are perfect fields, hence $x \mapsto x^p$ is a group isomorphism from $\overline{K}^*$ to $\overline{K}^*$, which implies that multiplication by p in $\mathrm{Br}\,K = H^2(K, \overline{K}^*)$ is a bijection, so $(\mathrm{Br}\,K)[p] = 0$.

□

Example 2.54 We already saw that $\widehat{\mathbf{Z}}$ and $\mathbf{Z}_p$ are of cohomological dimension 1, so $\mathrm{cd}_p(\mathbf{F}) = 1$ for any finite field $\mathbf{F}$ and any prime p. In particular the Brauer group of a finite field is trivial. To get more examples, we will show that a C_1 *field* is also of cohomological dimension at most 1, but this is more difficult and requires either consequences of the *Tate-Nakayama Theorem* (cf. [5], chapter 3) or a reinterpretation of the Brauer group via central simple algebras. We will discuss the latter in the next chapter.

3. Non-abelian cohomology, central simple algebras

Let k be a field. By convention, a *k-algebra* is a ring A equipped with a k-vector space structure such that the product in A is k-bilinear, namely

$$(\alpha.x)y = \alpha.(xy) = x(\alpha.y)$$

for all $\alpha \in k, x \in A, y \in A$. In particular, if $A \neq \{0\}$, the map $\alpha \mapsto \alpha.1$ is a bijection from k to a subalgebra of the center of A.

3.1. Central simple algebras

In this paragraph, we recall (without proofs) the main results on central simple algebras. A good reference is [2], chapter 2.

Definition 3.1 A *division algebra* (or *skew field*) is a non-zero ring D such that every $x \neq 0$ in D is invertible. Equivalently, a division algebra is a ring D such that the set of non-zero elements of D is a (not necessarily commutative) multiplicative group.

Obvisously the center of a division algebra D is a field k, and D is a k-algebra.

Definition 3.2 Let k be a field. A *central simple algebra* over k is a finite dimensional k-algebra A such that:

i) $\alpha \mapsto \alpha.1$ is a bijection from k to the center of A.

ii) The only two-sided ideals of A are $\{0\}$ and A.

Example 3.3 a) A division algebra is a central simple algebra over its center k provided it is finite-dimensional over k.

b) Let D be a division algebra (assumed to be finite-dimensional over its center k). Then it is a classical exercise that for $n \in \mathbf{N}^*$, the ring $M_n(D)$ of (n,n) matrices with entries in D is a central simple algebra over k. In particular $M_n(k)$ is a central simple k-algebra.

c) Let k be a field with $\mathrm{Char}\, k \neq 2$. Let $a, b \in k^*$. The *quaternion algebra* $A = (a, b)$ is the 4-dimensional k-algebra with basis $(1, i, j, k = ij)$ with the multiplication rules:

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

One easily checks that an element $q = x + yi + zj + wk$ (with $x, y, z, w \in k$) is invertible if and only if its *norm* $N(q) = x^2 - ay^2 - bz^2 + abw^2$ is not zero.

Observe that $N(q) = q\bar{q}$, where $\bar{q} = x - yi - zj - wk$. The classical example of Hamilton's quaternions $\mathbf{H}$ corresponds to $k = \mathbf{R}, a = b = -1$, in which case $\mathbf{H}$ is a division algebra because the norm has no non trivial zero. In general (a, b) is either a division algebra or is isomorphic to $M_2(k)$ (depending on whether the quadratic form $f(x, y, z, w) := x^2 - ay^2 - bz^2 + abw^2$ is anisotropic or not on k^4), hence it is always a central simple algebra. Observe that f isotropic is equivalent to the assumption that b is a norm of the field extension $k(\sqrt{a})/k$, which in turn is equivalent to saying that the three-variable form $x^2 - ay^2 - bz^2$ is isotropic.

The main theorem on central simple algebras is the following, essentially due to Wedderburn:

Theorem 3.4 *Let A be a finite-dimensional algebra over a field k. The following are equivalent:*

i) A is a central simple k-algebra.

ii) The $\bar{k}$-algebra $A \otimes_k \bar{k}$ is isomorphic to $M_n(\bar{k})$ for some n (variant: replace $\bar{k}$ by the algebraic closure of k instead of the separable closure $\bar{k}$).

iii) There exists a finite Galois field extension L of k such that $A \otimes_k L$ is isomorphic to $M_n(L)$ for some n.

iv) There exists a division algebra D with center k such that the k-algebras A and $M_n(D)$ are isomorphic for some n.

A finite field extension L/k such that $A \otimes_k L$ is isomorphic to $M_n(L)$ for some n is called a *splitting field* of A.

Corollary 3.5 *a) If A is a central simple algebra over k, then $A \otimes_k L$ is a central simple algebra over L for every field extension L/k.*

b) If A and B are two central simple algebras over k, then $A \otimes_k B$ is again a central simple algebra over k.

c) The dimension as a k-vector space of a central simple algebra A is necessarily the square of a positive integer n. We say that $n := \sqrt{\dim_k A}$ is the degree (it is sometimes called the reduced degree) of A.

Definition 3.6 Two central simple algebras A and A' are *Morita-equivalent* (or simply *equivalent*) if they are respectively isomorphic to $M_m(D)$ and $M_n(D')$ for some integers m, n with the division algebra D k-isomorphic to D'.

Observe that two equivalent algebras are isomorphic if and only if they have the same degree.

Theorem 3.7 *The set of equivalence classes of central simple k-algebras, equipped with the tensor product $\otimes_k$, is an abelian group, denoted B_k. The neutral element is the class of $M_n(k)$ (for an arbitrary positive n). If A is a central simple k-algebra, the opposite of its class $[A] \in B_k$ is the class of the opposite algebra A° (which has the same underlying abelian group as A, but a multiplication defined by $x.y = yx$, where yx is a product in A).*

Our goal in this chapter is to show that B_k is the same as the Brauer group $\operatorname{Br} k$ defined via Galois cohomology. To do this, we need to extend the definition of H^0 and H^1 to a (possibly non commutative) group A equipped with a continuous action of a profinite group G. We will also use the notion of *twisted form* via Galois descent.

3.2. Non-abelian cohomology

In this paragraph, G denotes a profinite group.

Definition 3.8 A *G-set* is a discrete topological space A with an action of G such that for all $x \in E$, the map $g \mapsto g.x$ is continuous. A *G-group* is a G-set equipped with a (multiplicative) group structure such that

$$s.(xy) = (s.x)(s.y)$$

for all $s \in G, x \in A, y \in A$.

The continuity condition again means that all stabilizers are open, or that $A = \bigcup_U A^U$, where U runs over the normal open subgroups of G. A (discrete) G-module is nothing but a commutative G-group. We will sometimes write ${}^s a$ for $s(a)$ when $s \in G$ and $a \in A$. A *morphism of G-sets* (resp. of G-groups) $f : A \to A'$ is a map (resp. a homomorphism of groups) compatible with the action of G.

Definition 3.9 Let A be a G-group. Set $H^0(G, A) = A^G$. A 1-*cocycle* (or cocycle) from G to A is a continuous map $s \mapsto a_s$ satisfying

$$a_{st} = a_s . {}^s a_t$$

for all $s, t \in G$. The set of cocycles is denoted $Z^1(G, A)$.

Definition 3.10 Two cocycles $a, a' \in Z^1(G, A)$ are *cohomologous* if there exists $b \in A$ such that $a'_s = b^{-1} a_s \, {}^s b$ for all $s \in G$. The quotient of $Z^1(G, A)$ by this equivalence relation is the *cohomology set* $H^1(G, A)$.

Obviously, this definition coincides with the previous one when the group A is abelian. In general, $H^1(G, A)$ has no natural group structure, it is only a *pointed set*, the distinguished element 1 being the class of the trivial cocycle $s \mapsto 1$. The sets $H^0(G, A)$ and $H^1(G, A)$ are covariantly functorial in A. It is easy to see that the analog of Corollary 2.32 a) still holds for the non-abelian H^0 and H^1.

Theorem 3.11 *Let B be a G-group. Let A be a sub-G-group of B. Denote by B/A the set of left cosets (which is a G-set).*

a) There is an exact sequence of pointed sets

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, B/A) \xrightarrow{\delta} H^1(G, A) \to H^1(G, B).$$

b) Assume further that A is normal in B and set $C = B/A$ (it is now a G-group). Then the previous exact sequence can be extended with an exact sequence

$$H^1(G, A) \to H^1(G, B) \to H^1(G, C).$$

c) Assume further that the extension

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

is central. Then the previous exact sequence can be extended with an exact sequence

$$H^1(G, B) \to H^1(G, C) \xrightarrow{\Delta} H^2(G, A).$$

Proof : a) Let $c \in H^0(G, B/A)$. Lift c to some $b \in B$ and set $a_s = b^{-1}.{}^s b$ for all $s \in G$. We have $a_s \in A$ (as s^b and b have same image in B/A because c is fixed by G) and the map $s \mapsto a_s$ is clearly a cocycle. One immediately checks that the class of this cocycle does not depend on the choice of b (replacing b by ba with $a \in A$ replaces a_s by $a^{-1}a_s a$), so we get a map $c \mapsto \delta(c)$ from $H^0(G, B/A)$ to $H^1(G, A)$.

By definition the class of the cocycle $s \mapsto a_s$ is cohomologous to zero in B, hence $\delta(c) \in \ker[H^1(G, A) \to H^1(G, B)]$; conversely every cocycle of $Z^1(G, A)$ which becomes cohomologous to zero in $Z^1(G, B)$ can be written $s \mapsto b^{-1}.{}^s b$ for some $b \in B$, and the fact that this cocycle takes value in A means that the image of b in B/A belongs to $H^0(G, B/A)$. Whence the exactness of

$$H^0(G, B/A) \xrightarrow{\delta} H^1(G, A) \to H^1(G, B).$$

On the other hand, the element $c \in H^0(G, B/A)$ is in $\ker \delta$ if and only if we can choose b such that $b^{-1}.{}^s b = 1$ for all $s \in G$, that is: if and only if c can be lifted to a $b \in H^0(G,B)$. This shows that $\ker \delta$ is exactly the image of $H^0(G,B)$ in $H^0(G,B/A)$. Finally the exactness of

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

is straightforward.

b) Let $s \mapsto b_s$ be a cocycle in $Z^1(G,B)$. Then it becomes cohomologous to zero in $Z^1(G,C)$ if and only if there exists $c \in C$ such that $\bar{b}_s = c^{-1}.{}^s c$ for all $s \in G$, where $\bar{b}_s$ is the class of b_s in $C = B/A$. As A is normal in B, this is equivalent to the existence of a lifting $b' \in B$ of c and a map $s \mapsto a_s$ from G to A such that $b_s = (b')^{-1}.a_s.{}^s b'$ for all $s \in G$, that is to the fact that $s \mapsto b_s$ is cohomologous (in $Z^1(G,B)$) to some cocycle of $Z^1(G,A)$. Whence the result.

c) Let $s \mapsto c_s$ be a cocycle in $Z^1(G,C)$. Lift c_s to some $b_s \in B$. Since $b_{st} = b_s.s(b_t)$ modulo A for all $s,t \in G$, one defines $a_{s,t} \in A$ by the formula

$$a_{s,t} = b_s.s(b_t).b_{st}^{-1}.$$

One tediously checks that $(s,t)) \mapsto a_{s,t}$ is a 2-cocycle whose class in $H^2(G,A)$ does not depend on the choices of c_s in its class of 1-cocycle and of the lifting b_s. This yields a map $\Delta : H^1(G,C) \to H^2(G,A)$. It is immediate that the image of an element of $H^1(G,C)$ coming from a cocycle of $Z^1(G,B)$ is trivial. Conversely, assume that the class of $c \mapsto c_s$ is in $\ker \Delta$. Then the lifting b_s of c_s yields a 2-cocycle $(s,t) \mapsto b_s.s(b_t).b_{st}^{-1}$ cohomologous to zero, which means that it can be written $a_s s(a_t) a_{st}^{-1}$ for some map $s \mapsto a_s$ from G to A. Replacing b_s by $a_s^{-1} b_s$, we reduce the case when $a_{s,t} = 1$, which means that $s \mapsto b_s$ is a cocycle of $Z^1(G,B)$ whose class is mapped to the class of $s \mapsto c_s$. This is what we wanted to prove.

□

Remark 3.12 One should be careful about the fact that even if A is central in B and C is abelian, the map Δ is not in general a group homomorphism if B is not assumed to be abelian (it is even possible that the image of Δ is not a subgroup of $H^2(G,A)$). Also, an exact sequence of pointed sets does not give information about the fibers of the maps, unlike an exact sequence of abelian groups. For instance a map with trivial kernel is not always injective.

Theorem 3.13 (Hilbert 90, non-abelian version) *Let L/k be a Galois field extension, set $G = \mathrm{Gal}\,(L/k)$. Then $H^1(G, GL_n(L)) = 0$. In particular $H^1(k, GL_n) = H^1(\mathrm{Gal}\,(\bar{k}/k), GL_n(\bar{k}))$ is trivial.*

Proof (sketch of): This is very similar to the case $n = 1$. Let $s \mapsto a_s$ be a cocycle with values in $GL_n(L)$. For any matrix $c \in M_n(L)$, set

$$b = \sum_{s \in G} a_s.s(c).$$

As $s(b) = a_s^{-1}.b$, it is sufficient to show that c can be chosen such that the matrix b is invertible. This is a (slightly more complicated than in the case $n = 1$) application of Dirichlet's Theorem on independence of morphisms, see [9], Chapter X, Proposition 3.

□

Corollary 3.14 *Let L/K be a Galois field extension, let $G = \mathrm{Gal}\,(L/K)$. There is a functorial map with trivial kernel $H^1(G, PGL_n(L)) \to \mathrm{Br}\,(L/k)$. In particular there is a canonical map $H^1(k, PGL_n) \to \mathrm{Br}\,k$ with trivial kernel.*

Proof : It is sufficient to deal with the case of a finite extension L/k. Using the central exact sequence of G-groups

$$1 \to L^* \to GL_n(L) \to PGL_n(L) \to 1$$

and Theorem 3.11 c), we get an exact sequence of pointed sets

$$H^1(G, GL_n(L)) \to H^1(G, PGL_n(L)) \to H^2(G, L^*) = \mathrm{Br}\,(L/k).$$

Now apply Theorem 3.13.

□

This corollary will be refined later (Theorem 3.24).

3.3. Galois descent

In this paragraph, we will give examples of the following general (vague) principle: let X be an "object" defined over a field k. Let K/k be a Galois extension with group G. Then (under certain conditions) objects defined over k that become isomorphic to X over K are classified by the cohomology set $H^1(G, \mathtt{Aut}\,(X_K))$, where $X_K = X \otimes_k K$ and the action of G on the group of automorphisms $\mathtt{Aut}\,(X_K)$ of X_K is given by

$$(g.f)(x) = g.f(g^{-1}.x),\ \ g \in G, f \in \mathtt{Aut}\,(X_K), x \in X_K.$$

A *k-form* (or *twisted form over k*) of X is an object that becomes isomorphic to X over some Galois extension K (or over $\bar{k}$).

More precisely, let (V, x) be a pair consisting of a finite-dimensional k-vector space V and a (p, q)-*tensor* $x \in \bigotimes^p V \otimes \bigotimes^q V^*$. Here $V^* := \mathrm{Hom}_k(V, k)$ is the dual of V and tensor products are over k. For instance, a bilinear map $V \times V \to V$ (resp. a bilinear form on V) is nothing but an element of $\mathrm{Hom}_k(V, \mathrm{Hom}_k(V, V)) \simeq V \otimes V^* \otimes V^*$ (resp. of $\mathrm{Hom}_k(V, V^*) = V^* \otimes V^*$; recall that if W is a k-vector space, then $\mathrm{Hom}_k(V, W) \simeq W \otimes V^*$), hence it is a $(1, 2)$-tensor (resp. a $(0, 2)$-tensor). A k-isomorphism between (V, x) and (V', x') is a k-linear isomorphism $f : V \to V'$ such that the induced isomorphism

$$\bigotimes^p V \otimes \bigotimes^q V^* \to \bigotimes^p V' \otimes \bigotimes^q V'^*$$

sends x to x'.

For every finite field extension K of k, set $V_K = V \otimes_k K$, this induces a tensor $x := x_K = x \otimes 1$. We say that two pairs (V, x) and (V', x') are K-isomorphic if there exists a K-isomorphism between (V_K, x_K) and (V'_K, x'_K). Denote by $E(K/k) := E_{V,x}(K/k)$ the set of isomorphism classes of pairs (V', x') that become K-isomorphic to (V, x) and by A_K the group of K-automorphisms of (V_K, x_K). Then $G = \mathrm{Gal}\,(K/k)$ acts on V_K via its action on K, then on A_K by the formula

$$(s.f)(y) = s.f(s^{-1}.y), \;\; s \in G, f \in A_K, y \in V_K.$$

Theorem 3.15 *There is a natural bijective map of pointed sets*

$$\theta : E(K/k) \to H^1(G, A_K).$$

Proof : Let $(V', x') \in E(K/k)$. Let f be a K-isomorphism between (V_K, x_K) and (V'_K, x'_K). We define a map $G \to A_K$ by

$$s \mapsto a_s = f^{-1} \circ {}^s f = f^{-1} \circ s \circ f \circ s^{-1}.$$

One immediately checks that this defines a cocycle of $Z^1(G, A_K)$ whose class in $H^1(G, A_K)$ does not depend on the choice of f. This yields the required map θ. Two pairs (V'_1, x'_1) and (V'_2, x'_2) with same image by θ correspond to K-isomorphisms f_1, f_2 such that $f_2 f_1^{-1}$ is G-invariant, hence is a k-isomorphism. Hence θ is injective.

Now let $s \mapsto a_s$ be an element of $Z^1(G, A_K)$. By Hilbert's 90 (Theorem 3.13), it becomes trivial as an element of $H^1(G, GL(V_K))$, whence a K-automorphism f of V_K such that $a_s = f^{-1} \circ^s f$ for all $s \in G$. We can extend f to $\bigotimes^p V_K \otimes \bigotimes^q V_K^*$ and set $x' = f(x)$. Let $s \in G$. As x is defined over k, we have $s(x) = x$ and since a_s is an automorphism of A_K (and not not only of V_K), we have $a_s(x) = x$). Thus

$$s(x') = ({}^s f)(s(x)) = ({}^s f)(x) = f \circ a_s(x) = f(x) = x'$$

for all $s \in G$. Hence x' is also defined over k and the image of (V', x') by θ is clearly the class of $s \mapsto a_s$.

□

Remark 3.16 The formula for θ shows that (V'_K, x'_K) can also be seen as the same K-pair as (V_K, x_K) (via a K-isomorphism f), but with a *twisted* Galois action: namely the "new" Galois action is given by $s(y) := a_s({}^s y)$, where $(s, y) \mapsto {}^s y$ is the "former' Galois action and $s \mapsto a_s$ is a cocycle corresponding to the image of (V'_K, x'_K) by θ.

Going over to the limit over all finite Galois extensions $K \subset \bar{k}$ of k, this yields:

Corollary 3.17 *There is a natural bijective map of pointed sets between the set of isomorphism classes of pairs (V', x') that become $\bar{k}$-isomorphic to (V, x) and $H^1(k, A_{\bar{k}})$.*

Example 3.18 Assume $\operatorname{Char} k \neq 2$. Let q be a non-degenerate quadratic form of rank n on a finite dimensional k-vector space V. Then isomorphisms classes of quadratic forms of rank n over k are classified by the set $H^1(k, O(q))$, where $O(q)$ is the group of automorphisms of q over $\bar{k}$. Indeed, two quadratic forms of rank n automatically become isomorphic over $\bar{k}$.

Proposition 3.19 *Let K/k be a (finite) Galois extension with group G. Let $A(n, K/k)$ be the set of isomorphisms classes of k-algebras such that $A \otimes_k K$ is K-isomorphic to $M_n(K)$. Then there is a canonical bijection*

$$A(n, K/k) \to H^1(G, PGL_n(K)).$$

Central simple algebras of degree n are classified (up to isomorphism) by the cohomology set $H^1(k, PGL_n)$.

Proof : An element of $A(n, K/k)$ can be considered as a pair (V, x), where V is a k-vector space of dimension n and x is a $(1, 2)$-tensor. Applying Theorem 3.15, this yields a canonical bijection between $A(n, K/k)$ and $H^1(G, C_K)$, where C_K is the automorphism group of the K-algebra $M_n(K)$. The group C_K is known to be isomorphic to $PGL_n(K)$ (quotient of $GL_n(K)$ by its center) because every automorphism of $M_n(K)$ is inner. The second statement comes from Corollary 3.17 and Theorem 3.4.

□

Remark 3.20 The tensor product of central simple algebras induces a product operation

$$H^1(G, PGL_n(K)) \times H^1(G, PGL_m(K)) \to H^1(G, PGL_{nm}(K)),$$

which can also be described via the product of cocycles associated to the product

$$PGL_n(K) \times PGL_m(K) \to PGL_{nm}(K)$$

induced by the natural map $(f, g) \mapsto f \otimes g$,

$$\mathrm{End}_K(K^n) \times \mathrm{End}_K(K^m) \to \mathrm{End}_K(K^n \otimes_K K^m).$$

Definition 3.21 Let A be a central simple algebra of degree n over k. By Theorem 3.4 and Proposition 3.19, there is a finite Galois extension K of k such that A is the twisted form of $M_n(K)$ by a cocycle $s \mapsto a_s \in PGL_n(K)$, where $s \in G := \mathrm{Gal}\,(K/k)$. Namely (see Remark 3.16) there is a twisted action of the group G on $A \otimes_k K \simeq_K M_n(K)$ given by $s.M = a_s s(M) a_s^{-1}$. This means that the map $\det : A \otimes_k K \to K$ induced by the K-isomorphism $A \otimes_k K \simeq M_n(K)$ is compatible with the action of G. Taking G-invariants, we obtain a map $\mathrm{Nrd}_A : A \to k$, called the *reduced norm map*, which induces a group homomorphism $\mathrm{Nrd}_A : A^* \to k^*$. The construction does neither depend on the choice of the cocycle (indeed replacing it by a cohomologous cocycle does not affect the expression of $\det(s.M)$) nor on the choice of K because two splitting fields K, K' can be embedded into the same Galois extension L of k.

For a central simple algebra A over k, the classical norm map $N_{A/k} \to k$ is defined by: $N_{A/k}(x)$ is the determinant of the multiplication by x in the k-vector space A. The link to the reduced norm is the following:

Proposition 3.22 *Let n be the degree of A. Then $(N_{A/k}) = (\mathrm{Nrd}_A)^n$. In particular, the reduced norm can be viewed as a polynomial function of degree n in n^2 variables on k, and an element $a \in A$ is invertible if and only if* $\mathrm{Nrd}(a) \neq 0$.

Proof : Passing to a splitting field of A, we can assume that $A = M_n(k)$. For every $M \in M_n(k)$, the matrix of the multiplication by M (with respect to the standard basis of $M_n(k)$) is the block diagonal matrix $\mathrm{Diag}(M, ..., M)$, whence the formula. Now $a \in A$ is invertible if and only if multiplication by a in A is bijective, which is equivalent to saying that $N_{A/k}(a) \neq 0$, or $\mathrm{Nrd}_A(a) \neq 0$ thanks to the formula.

□

Example 3.23 For a quaternion algebra $A = (a,b)$, the reduced norm (sometimes called simply "norm") of $q = x + yi + zj + wk$ is $\mathrm{Nrd}_A(q) = x^2 - ay^2 - bz^2 + abw^2$.

3.4. The Brauer group via central simple algebras

Let K/k be a finite Galois extension of fields, set $G = \mathrm{Gal}\,(K/k)$. Combining Proposition 3.19 and Corollary 3.14, we obtain a map

$$\delta_n : A(n, K/k) \to \mathrm{Br}\,(K/k) \subset \mathrm{Br}\,k,$$

whose kernel is trivial (consisting of the class of $M_n(k)$). Denote by $B(K/k)$ the kernel of the map $B_k \to B_K$ given by extension of scalars: thus $B(K/k)$ consists of the equivalence classes of central simple algebras A over k such that $A \otimes_k K$ becomes isomorphic to a matrix algebra over K. An easy computation (using Remark 3.20 and the definition of the map Δ in Theorem 3.11, c) shows that for $A \in A(n, K/k)$ and $A' \in A(n', K/k)$, we have

$$\delta_{nn'}(A \otimes_k A') = \delta_n(A) + \delta_n(A').$$

Therefore all maps δ_n are compatible and induce an injective (as the kernel of δ_n is trivial) group homomorphism $\delta : B(K/k) \to H^2(G, K^*) \subset \mathrm{Br}\,k$.

Theorem 3.24 *The homomorphism δ is an isomorphism. The group B_k (defined via equivalence classes of central simple k-algebras) is isomorphic to* $\mathrm{Br}\,k$.

Proof : Let $n = [K : k]$. It is sufficient to prove that δ_n is surjective, or that the coboundary map

$$\Delta_n : H^1(G, PGL_n(K)) \to H^2(G, K^*) = \mathrm{Br}\,(K/k)$$

is surjective. Indeed, the second assertion of the theorem is then proven by passing to the limit over all finite Galois extensions K of k. Let $(s,t) \mapsto a_{s,t}$ be a cocycle with values in K^*. Take a K-vector space V with basis $(e_s)_{s \in G}$ and denote by p_s the K-automorphism of V that sends e_t to $a_{s,t}e_{st}$. We compute

$$(p_s s(p_t))(e_u) = a_{s,tu} s(a_{t,u}) e_{stu};\;\; a_{s,t} p_{st}(e_u) = a_{s,t} a_{st,u} e_{stu}.$$

By the cocycle condition, we have $p_s s(p_t) = a_{s,t} p_{st}$, or $a_{s,t} = p_s s(p_t) p_{st}^{-1}$, which shows that a is indeed a coboundary via the formula that defines Δ_n (cf. Theorem 3.11, c).

□

Example 3.25 a) We saw that a finite field $\mathbf{F}$ is of cohomological dimension 1, hence its Brauer group is trivial. Therefore every finite division algebra D (which is finite-dimensional over its center $\mathbf{F}$) is isomorphic to $\mathbf{F}$, that is: D is a field (Wedderburn).

b) The Brauer group of $\mathbf{R}$ is $\mathbf{Z}/2$. This corresponds to the fact that the only division algebras of center $\mathbf{R}$ and finite-dimensional over $\mathbf{R}$ are $\mathbf{R}$ itself and the Hamiltonian quaternions $\mathbf{H}$.

c) Let k be a field complete (or, more generally, henselian) for a discrete valuation with perfect residue field κ. The first step to compute $\operatorname{Br} k$ consists of showing that a central, finite-dimensional division algebra over k is split by a finite unramified extension of k, see [9], chapter XII, §2. This implies that $\operatorname{Br} k^{\mathrm{nr}} = 0$, hence $\operatorname{Br} k$ identifies (by Proposition 2.49, which immediately extends to an infinite Galois extension) to $H^2(\operatorname{Gal}(k^{\mathrm{nr}}/k), k^{\mathrm{nr}^*})$. One then shows (loc. cit., Theorem 2) that the latter is a split extension of $H^1(\kappa, \mathbf{Q}/\mathbf{Z})$ by $\operatorname{Br} \kappa$, hence $\operatorname{Br} k \simeq \mathbf{Q}/\mathbf{Z}$ if the residue field κ is finite because the absolute Galois group of κ is then isomorphic to $\widehat{\mathbf{Z}}$ and $\operatorname{Br} \kappa = 0$.

Remark 3.26 A central simple k-algebra A of degree n can be split by a separable extension K of degree n ([2], Theorem 2.2.7). More precisely, if $A \simeq M_r(D)$ (where D is a division algebra), the smallest (for the usual order of $\mathbf{N}^*$ or the divisibility relation) positive integer d such that A is split by a separable extension of degree d is the degree of D over k (loc. cit., Prop 4.5.1.). This integer is called the *index* of A.

The image of $\delta_n : H^1(k, PGL_n) \to \operatorname{Br} k$ is therefore a subset of $(\operatorname{Br} k)[n]$, as it is in $\ker[\operatorname{Br} k \to \operatorname{Br} K]$ for some finite separable extension K/k of degree n. However, the order e of a central simple k-algebra A in $\operatorname{Br} k$ (called the *period* of A) can be smaller then the index, in other words A cannot always be split by an extension of degree e. See [2], §2.8 and 4.5. This difficulty disappears over local fields (loc. cit., Proposition 6.3.8), and also for function fields of surfaces over $\mathbf{C}$ (De Jong, 2004).

Here is a nice consequence of the definition of the Brauer group via the central simple algebras. Recall that a field k is C_1 if every homogeneous polynomial of degree d in $n > d$ variables has a non-trivial zero. For instance (see [2], Prop. 6.2.6. and 6.2.8), a finite field is C_1 (Chevalley), as well as a finite extension of $\mathbf{C}(t)$ (Tsen).

Theorem 3.27 *Let k be a (perfect) C_1 field. Then* $\operatorname{Br} K = 0$ *for every finite extension K of k. In particular* $\operatorname{cd}(k) \leq 1$.

Proof : Let D be a division algebra of finite dimension r^2 over its center K. It is sufficient to show that $r = 1$. Let $s = [K : k]$. Define

$$f : D \to k,\ x \mapsto N_{K/k}(\mathrm{Nrd}(x)).$$

Taking a basis of the k-vector space D, we see that f can be seen (via Proposition 3.22) as a homogeneous polynomial function of degree sr in sr^2 variables on k. Since D is a division algebra and K is a field, the only zero of f is 0. The C_1 property of k then implies that $sr^2 \leq sr$, hence $r = 1$. The fact that $\mathrm{cd}(k) \leq 1$ now follows from Theorem 2.53.

□

4. The Brauer group of a scheme

4.1. Étale sheaves

We recall a few basic facts on étale topology. A comprehensive reference (as well as for the next paragraph) is [7], chapters II and III. For the properties of flat and étale morphisms, see for instance loc. cit., chapter I. See also [6].

We recall that a locally finitely presented (=locally of finite type if X is noetherian) morphism $f : Y \to X$ is *étale* if it is flat and unramified; *unramified* means that for all $x \in X$, the fiber Y_x is isomorphic to $\coprod \operatorname{Spec} k_i$, where each k_i is a finite and separable extension of the residue field $k(x)$ (and the disjoint union is finite if f is assumed to be finitely presented). In particular an unramified morphism is quasi-finite as soon as it is finitely presented. "Étale" is equivalent to smooth of relative dimension zero.

Let X be a scheme. Denote by Sch/X the category of X-schemes. Consider a full subcategory C_X of Sch/X (so the morphism between two objects of C_X are the morphisms of X-schemes).

Definition 4.1 A *Grothendieck topology* on C_X consists of the datum of a subclass E of morphisms in C_X (called the *open sets*) satisfying:

i) Every isomorphism is in E.

ii) A composition of morphism in E is in E.

iii) If $V \to U$ is in E and $W \to U$ is an *arbitrary* morphism in C_X, then the pull-back $V \times_U W \to W$ is in E.

A *covering* (for this Grothendieck topology) of an object $U \in C_X$ is a family of morphisms $f_i : U_i \to U$, where every f_i is in E and $\bigcup_i f_i(U_i) = U$. The pair consisting of C_X and the family of all coverings is called a *site*, and is denoted by X_E.

Example 4.2 a) The (small) *Zariski site* X_{zar}: C_X is the category of open subschemes of X and E is the class of open immersions.

b) The (small) *étale site* $X_{\text{ét}}$: C_X is the category of all étale X-schemes and E is the class of étale maps (actually in this example, every morphism in C_X is in E).

c) The (big) *flat site* X_{fppf}: C_X is the category of all X-schemes and E is the class of flat and locally finitely presented morphisms.

Definition 4.3 Let X be a scheme. Let X_E be a site with underlying category C_X. A *presheaf* (of abelian groups) [2] on X_E is a contravariant functor $\mathcal{P}$ from C_X to the category of abelian groups. The *group of sections* of $\mathcal{P}$ over $Y \in C_X$ is $\Gamma(Y, \mathcal{P}) := \mathcal{P}(Y)$. To every morphism $u : Y' \to Y$ in C_X is associated a *restriction map* $\mathcal{F}(Y) \to \mathcal{F}(Y')$, which we usually denotes by $s \mapsto s_{|Y'}$ when the morphism u is understood.

Definition 4.4 A presheaf $\mathcal{F}$ on a site X_E is a *sheaf* if for every scheme $Y \in C_X$ and every covering $(U_i \to Y)_{i \in I}$, the following properties hold:

i) Every section $s \in \mathcal{F}(Y)$ whose restriction to each U_i is zero satisfies $s = 0$.

ii) For every family $(s_i)_{i \in I}$ (where $s_i \in \mathcal{F}(U_i)$) such that the restriction of s_i and s_j to $U_i \times_Y U_j$ coincide for all pairs $i, j \in I$, there exists an $s \in \mathcal{F}(Y)$ whose restriction to each U_i is s_i.

The category of sheaves is denoted by $S(X_E)$ (or sometimes $S(X)$ if E is understood). It is a full subcategory of the abelian category of presheaves $P(X_E)$.

Example 4.5 a) A commutative group scheme G over X defines a sheaf for the étale or the flat topology via $Y \mapsto G(Y)$. Examples are: the *additive group* $\mathbf{G}_{a,X} = X \times_{\mathbf{Z}} \mathbf{Z}[T]$, the multiplicative group $\mathbf{G}_{m,X} = X \times_{\mathbf{Z}} \mathbf{Z}[T^{\pm 1}]$, or the group of n-roots of unity $\mu_{n,X} = X \times_{\mathbf{Z}} (\mathbf{Z}[T]/(T^n - 1))$. If A is an abelian group, the *constant sheaf* A is the sheaf associated to the constant group scheme A_X (as a scheme $A_X = \coprod_{a \in A} X$; in particular $A_X(Y) = A$ for every connected X-scheme Y).

b) A sheaf on the Zariski site of X is just a sheaf on the topological space X, equipped with Zariski topology.

c) In all our examples, there is an exact sheafification functor

$$a : P(X_E) \to S(X_E),$$

[2]Similar definitions can be given for sets, rings etc.

which is a left-adjoint functor for the inclusion functor $i : S(X_E) \to P(X_E)$ (i is only left-exact). An exact sequence

$$0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}"$$

of sheaves is exact if and only if the associated sequence of presheaves is exact.

From now on, all schemes (unless it is clearly specified) are equipped with the étale topology.

Definition 4.6 A *geometric point* of a scheme X is a morphism $u_x : \bar{x} \to X$, where $\bar{x}$ is the spectrum of some separably closed field. Let $\mathcal{F}$ be a sheaf (or even a presheaf) on X. The *stalk* of $\mathcal{F}$ at $\bar{x}$ is

$$\mathcal{F}_{\bar{x}} = \varinjlim \mathcal{F}(U),$$

where the limit runs over all étale neighborhoods U of $\bar{x}$ in X, that is over all commutative diagram

$$\begin{tikzcd} \bar{x} \arrow[r] \arrow[dr] & U \arrow[d] \\ & X \end{tikzcd}$$

with $U \to X$ étale (one can restrict to connected U).

Recall that a local ring $(A, \mathcal{M})$ is *henselian* if it satisfies the analogue of Hensel's lemma, namely: every non-singular zero modulo $\mathcal{M}$ of a polynomial of $A[X]$ can be lifted to a zero in A. It is *strictly henselian* (or *stricly local*) if its residue field $A/\mathcal{M}$ is further assumed to be separably closed. Every local ring A has a henselization A^h and a strict henselization A^{sh}, the latter being obtained by a limit process from the A-algebras B with $\operatorname{Spec} B \to \operatorname{Spec} A$ étale.

Example 4.7 Take $\mathcal{F} = \mathbf{G}_a$. Let $\mathcal{O}_{X,\bar{x}} := \mathcal{O}_{X,x}^{\mathrm{sh}}$, where $x \in X$ is the image of $\bar{x}$ in X. Then $\mathcal{O}_{X,\bar{x}}$ is the stalk of $\mathcal{F}$ at $\bar{x}$. It plays the same role for the étale topology as the ring $\mathcal{O}_{X,x}$ for the Zariski topology. More generally, if $\mathcal{F}$ is defined by a locally finitely presented group scheme G, then $\mathcal{F}_{\bar{x}} = G(\mathcal{O}_{X,\bar{x}})$.

A map of sheaves $\phi : \mathcal{F} \to \mathcal{F}'$ is surjective if and only if the map $\mathcal{F}_{\bar{x}} \to \mathcal{F}'_{\bar{x}}$ induce on the stalks is surjective for every geometric point $\bar{x}$ of X (this is in general weaker than demanding that the corresponding map of presheaves is surjective). The category $S(X)$ is abelian, but it is not an abelian subcategory of $P(X)$, as the cokernels are not the same.

Example 4.8 a) The sequence

$$0 \to \mu_n \to \mathbf{G}_m \stackrel{.n}{\to} \mathbf{G}_m$$

is clearly exact in $P(X)$, hence also in $S(X)$. For every strictly local ring A with $n \in A^*$, the map $x \mapsto x^n$ is surjective from A^* to A^* by Hensel's lemma which proves that the *Kummer sequence*

$$0 \to \mu_n \to \mathbf{G}_m \stackrel{.n}{\to} \mathbf{G}_m \to 0$$

is exact on $S(X)$ as soon as the integer n is invertible on X (it is exact on X_{fppf} without any assumption on the residue characteristics of X).

b) Similarly, there is an analog of Artin-Schreier exact sequence

$$0 \to \mathbf{Z}/p\mathbf{Z} \to \mathbf{G}_a \stackrel{\Phi}{\to} \mathbf{G}_a \to 0$$

on any scheme of characteristic p (=$\mathbf{F}_p$-scheme). Here Φ is the map $x \mapsto x^p - x$ on every $\mathbf{F}_p$-algebra.

The following result make the link between étale sheaves on $\operatorname{Spec} k$ and Galois modules:

Theorem 4.9 *For every sheaf $\mathcal{F}$ on $X = \operatorname{Spec} k$, define*

$$M_{\mathcal{F}} := \varinjlim_{K} \mathcal{F}(K),$$

where the limit is taken over all finite (Galois) field extensions $K \subset \bar{k}$. Equip $M_{\mathcal{F}}$ with the action of $\Gamma := \operatorname{Gal}(\bar{k}/k)$ induced by its action on each K. Then $M_{\mathcal{F}}$ is a discrete Γ-module and the functor $\mathcal{F} \mapsto M_{\mathcal{F}}$ induces an equivalence of categories between $S(X_{\text{ét}})$ and the category C_Γ of discrete Γ-modules.

Definition 4.10 Let $\pi : X' \to X$ be a morphism of schemes. Let $\mathcal{F}'$ be a sheaf on X'. Its *direct image* by π is the sheaf defined on X by

$$(\pi_* \mathcal{F}')(U) = \mathcal{F}'(U \times_X X')$$

for every $U \in C_X$, where the fibred product is relative to π. The functor $\pi_* : S(X') \to S(X)$ is left-exact, and it has an exact left-adjoint functor $\pi^* : S(X) \to S(X')$, the *inverse image* functor.

Example 4.11 a) Let G be a commutative group scheme on X. The inverse image π^*G of the sheaf defined by G is not always represented by the group scheme $G_{X'} := G \times_X X'$; indeed there is only a canonical map (in general neither injective nor surjective) $\Phi_G : \pi^*G \to G_{X'}$, which is an isomorphism in two important case: when π is étale, or when G itself is étale over X.

b) Let $K \subset K'$ be an extension of field, which induces a morphism of absolute Galois groups $\psi : \Gamma_{K'} \to \Gamma_K$ and a morphism $\pi : \operatorname{Spec} K' \to \operatorname{Spec} K$. Let N be a Γ_K-module, then the $\Gamma_{K'}$-module π^*N corresponds to the group N with the action of $\Gamma_{K'}$ given by $s(x) = \phi(s).x$ for all $s \in \Gamma_{K'}, x \in N$. For a $\Gamma_{K'}$-module M, its direct image π_*M is the Γ_K-module $I_{\Gamma_K}^{\psi(\Gamma_{K'})}(M^{\ker \psi})$, which is nothing but $I_{\Gamma_K}^{\Gamma_{K'}}$ if K'/K is algebraic (then ψ is injective).

The direct image functor π_* is exact if π is finite, but not in general.

4.2. Étale cohomology

Let X be a scheme. Then the category $S(X)$ of étale sheaves on X has enough injectives. Therefore right derived functors $R^i f(\mathcal{F})$ of a left-exact functor f on $S(X)$ are defined: they are computed via an injective resolution

$$0 \to \mathcal{F} \to I^0 \to I^1 \to ...$$

of $\mathcal{F}$, then by taking the cohomology of the complex

$$f(I^0) \to f(I^1) \to ...$$

The functor $S(X) \to \mathbf{Ab}$ defined by $\mathcal{F} \mapsto \Gamma(X, \mathcal{F})$ is left-exact, whence:

Definition 4.12 We denote by $H^r(X, .)$ ($r \in \mathbf{N}$) the right derived functors of the functor $\Gamma(X, .) = H^0(X, .)$. For a sheaf $\mathcal{F}$ on X, the group $H^r(X, \mathcal{F})$ is called the *r-th étale cohomology group of X with values in $\mathcal{F}$*. Similar definitions can be made for flat topology (and of course also for Zariski topology).

As a general property of derived functors, for every short exact sequence of étale sheaves

$$0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$$

on X, there is a long exact sequence of the related cohomology groups

$$0 \to H^0(X, \mathcal{F}') \to H^0(X, \mathcal{F}) \to H^0(X, \mathcal{F}'') \to H^1(X, \mathcal{F}') \to ...$$
$$... \to H^{r-1}(X, \mathcal{F}'') \to H^r(X, \mathcal{F}') \to H^r(X, \mathcal{F}) \to H^r(X, \mathcal{F}'') \to ...$$

The special case $X = \operatorname{Spec} k$ corresponds to Galois cohomology.

Example 4.13 a) The groups $H^i(X, \mathbf{G}_a)$ are the classical coherent cohomology groups $H^i(X, \mathcal{O}_X)$.

b) The *Picard group* $\operatorname{Pic} X$ of X is $H^1(X, \mathbf{G}_m)$; it coincides with the group $H^1_{\mathrm{Zar}}(X, \mathcal{O}_X^*)$ defined via Zariski topology (extension of Hilbert's 90). This coincidence does not extend to higher degrees: we will define the Brauer group of X as $H^2(X, \mathbf{G}_m)$, which can be non trivial even when $X = \operatorname{Spec} k$ is the spectrum of a field; of course $H^2_{\mathrm{Zar}}(\operatorname{Spec} k, \mathcal{O}_X^*) = 0$, as the topological space $\operatorname{Spec} k$ consists of one single point.

c) We have $H^1(X, \mathbf{Z}) = 0$ if X is integral, normal and noetherian (slight extension of $H^1(k, \mathbf{Z}) = 0$ for a field k).

d) Étale cohomology over a noetherian scheme commutes with direct limit of sheaves (e.g. with direct sums). Also, if S is a noetherian scheme, (X_i) is a projective system of noetherian S-schemes with affine transition morphisms, and G is a locally finitely presented S-group scheme, then

$$H^q(X, G_X) \simeq \varinjlim H^q(X_i, G_{X_i})$$

for all $q \in \mathbf{N}$, where $X := \varprojlim X_i$. this applies in particular when $X = \operatorname{Spec} K$ is the generic point of an integral an noetherian scheme Y and the family (X_i) consists of all non empty affine open subsets of Y.

Remark 4.14 The functor $H^r(X, \mathcal{F})$ is contravariant on X. More precisely, if $\pi : X' \to X$ is a morphism, then the universal property of derived functors (as δ-functors) yields maps $H^r(X, \mathcal{F}) \to H^r(X', \pi^*\mathcal{F})$ induced by the obvious map $H^0(X, \mathcal{F}) \to H^0(X', \pi^*\mathcal{F})$. There is also a canonical map $H^r(X, \pi_*\mathcal{F}) \to H^r(X', \mathcal{F})$ (induced by the corresponding map for $r = 0$), which is an isomorphism if π_* is exact. In general, there is only the *Leray spectral sequence*

$$E_2^{rs} := H^r(X, R^s\pi_*\mathcal{F}) \Rightarrow H^{r+s}(X', \mathcal{F}),$$

where the $R^s\pi_*$ are the *higher direct images*, i.e. the right derived functors of the direct image functor π_*.

Assume that $\pi : X' \to X$ is a *Galois covering with group G* (this means that π is finite étale, X' and X are connected, and the right action of the group $G := \mathtt{Aut}_X(Y)$ on $F(Y) := \operatorname{Hom}_X(\bar{x}, Y)$ is transitive, where $\bar{x}$ is some geometric point of X). then there is the *Hochschild-Serre spectral sequence*

$$H^r(G, H^s(X', \mathcal{F}_{X'})) \Rightarrow H^{r+s}(X, \mathcal{F}),$$

which extends to an infinite Galois covering (=projective limit of Galois coverings) when X is noetherian. Here $\mathcal{F}_{X'}$ is the restriction of the sheaf X to X' via π.

The sheaf $R^i\pi_*\mathcal{F}$ (for a morphism $\pi : Y \to X$ and a sheaf $\mathcal{F}$ on Y) is associated to the presheaf $U \mapsto H^i(U \times_X Y, \mathcal{F})$ ([6], Prop 3.7. a), but the stalks of the higher direct images are in general quite difficult to compute. Nevertheless, we have the following statement (see [7], Theorems III.1.15 and Corollary VI.2.5):

Theorem 4.15 *Let $\pi : Y \to X$ be a morphism. Let G be a locally finitely presented commutative group scheme over Y. Let $\bar{x}$ be a geometric point of X with image x, set $\widetilde{Y} = Y \times_X \operatorname{Spec}(\mathcal{O}_{X,\bar{x}})$.*

a) If X and Y are noetherian, then $(R^q\pi_*G)_{\bar{x}} \simeq H^q(\widetilde{Y}, G_{\widetilde{Y}})$.

b) (proper base change) If π is proper and G is torsion[3] *(e.g. finite over Y), then $(R^q\pi_*G)_{\bar{x}} \simeq H^q(Y_{\bar{x}}, G_{Y_{\bar{x}}})$, where $Y_{\bar{x}} = Y \times_X \bar{x}$.*

Remark 4.16 There is also a finiteness statement for étale cohomology (which uses the proper base change theorem as well as a purity theorem due to Gabber): for a smooth variety X over a separably closed field k and an étale and commutative finite type X-group scheme G whose torsion is prime to $\operatorname{Char} k$, the groups $H^i(X, G)$ are finite.

4.3. First properties of the Brauer group

Definition 4.17 Let X be a scheme. The *Brauer group* of X is the étale cohomology group $H^2(X, \mathbf{G}_m)$.

Remark 4.18 a) What we call the Brauer group is sometimes called the *cohomological Brauer group*, to make the difference with a possibly smaller subgroup $\operatorname{Br}_{\mathrm{Az}} X$ of $H^2(X, \mathbf{G}_m)$ defined in terms of *Azumaya algebras*. When $X = \operatorname{Spec} k$ is the spectrum of a field, both coincide because an Azumaya algebra is the analogue over X of a central simple algebra (it is defined as a sheaf of $\mathcal{O}_X$-algebras that become isomorphic to $M_n(\mathcal{O}_X)$ over an étale covering of X). Azumaya algebras are classified (for a given n) by a cohomology set $\check{H}^1(X, \mathrm{PGL}_n)$ (which is defined via Čech cocycles for the étale topology). The group $\operatorname{Br}_{\mathrm{Az}} X$ is always torsion, and it is known that $\operatorname{Br}_{\mathrm{Az}} X = (\operatorname{Br} X)_{\mathrm{tors}}$ if X is quasi-projective over an affine scheme, thanks to works by Gabber and Cesnavicius (see [1], Th. 4.2.1.). See also Theorem 4.22 below.

b) Let $f : Y \to X$ be a morphism of schemes. Using the canonical map $f^*(\mathbf{G}_{m,X}) \to \mathbf{G}_{m,Y}$, we get a morphism $\operatorname{Br} X \to \operatorname{Br} Y$ between Brauer groups, hence Br is a contravariant functor on the category of schemes. In particular, if A is a ring, every A-point $x \in X(A) = \operatorname{Hom}(\operatorname{Spec} A, X)$ gives rise to a map $x^* : \operatorname{Br} X \to \operatorname{Br} A := \operatorname{Br}(\operatorname{Spec} A)$.

[3] This means that $G(U)$ is a torsion group for all quasi-compact Y-schemes U.

Example 4.19 a) For $X = \operatorname{Spec} k$, we recover the Brauer group of the field k.

b) Let A be a henselian local ring with residue field κ. Then the canonical map $\operatorname{Br} A \to \operatorname{Br} \kappa$ (associated to $\operatorname{Spec} \kappa \to \operatorname{Spec} A$) is an isomorphism. Indeed, the map $H^i(\operatorname{Spec} A, G) \to H^i(\kappa, G_0)$ is more generally an isomorphism for every $i \geq 1$ and every smooth quasi-projective A-group scheme G, where G_0 is the special fiber of G (see [7], Remark III.3.11). This shows that $\operatorname{Br} A = 0$ if A is strictly local.

Proposition 4.20 *Let X be a scheme. Let n be a positive integer, assume that n is invertible on X. Then there are exact sequences*

$$0 \to \operatorname{Pic} X/n \to H^2(X, \mu_n) \to (\operatorname{Br} X)[n] \to 0.$$

$$0 \to \operatorname{Br} X/n \to H^3(X, \mu_n) \to H^3(X, \mathbf{G}_m)[n] \to 0.$$

Proof : Apply the long exact sequence in étale cohomology to Kummer exact sequence of sheaves

$$0 \to \mu_n \to \mathbf{G}_m \xrightarrow{.n} \mathbf{G}_m \to 0.$$

□

Without assumption on n, the previous proposition still holds provided $H^2(X, \mu_n)$ and $H^3(X, \mu_n)$ are replaced by their flat counterparts (as $\mathbf{G}_m$ is smooth, it turns out that $\operatorname{Br} X$ is also $H^2_{\mathrm{fppf}}(X, \mathbf{G}_m)$).

4.4. Brauer groups and function fields

In this paragraph, we link the Brauer group of an integral scheme to the Brauer group of its function field. For a normal and integral scheme X, the piece of notation $X^{(1)}$ denotes the set of integral divisors (or, equivalently, of points of codimension 1) on X.

Proposition 4.21 *Let X be an integral, normal and noetherian scheme with function field F. Denote by $j : \eta = \operatorname{Spec} F \to X$ its generic point. For every integral divisor D of X, denote by $k(D)$ its function field and by i_D : $\operatorname{Spec}(k(D)) \to X$ the embedding of the generic point of D into X. Let $\mathbf{Z}_{k(D)}$ be the constant sheaf $\mathbf{Z}$ on $\operatorname{Spec}(k(D))$.*

a) There is an exact sequence of étale sheaves on X:

$$0 \to \mathbf{G}_{m,X} \to j_* \mathbf{G}_{m,F} \xrightarrow{u} D_X := \bigoplus_{D \in X^{(1)}} (i_D)_* \mathbf{Z}_{k(D)}.$$

b) Assume further that X is regular. Then the map u is surjective.

Wa call D_X the *sheaf of divisors* on X.

Proof : a) Let $U \to X$ be étale, connected and of finite type with generic fibre U_η. It is sufficient (cf. [6], Example 3.39) to check that the corresponding sequence of sections over such a U is exact. The scheme U is then integral, as it is noetherian and normal; denote by $R(U)$ its function field. Then

$$\Gamma(U, j_*\mathbf{G}_{m,F}) = \Gamma(U_\eta, \mathbf{G}_m) = R(U)^*.$$

Define the morphism of sheaves u via the map

$$R(U)^* \to \bigoplus_{D \in X^{(1)}} ((i_D)_*\mathbf{Z}_{k(D)})(U) = \bigoplus_{E \in U^{(1)}} \mathbf{Z}$$

defined by the valuations associated to the integral divisors on U. Since $\mathbf{G}_{m,X}(U) = \mathcal{O}_U(U)^*$ is the group of invertible functions on U and the sequence

$$0 \to \mathcal{O}_U(U)^* \to R(U)^* \to \bigoplus_{E \in U^{(1)}} \mathbf{Z}$$

is exact (the scheme U being integral and normal), we are done.

b) It is sufficient to check the surjectivity at the level of geometric stalks. Let $x \in X$, $A := \mathcal{O}^{\mathrm{sh}}_{X,x}$ and $K = \operatorname{Frac} A$. Using Theorem 4.15, we have to check that the map $K^* \to \bigoplus_{\wp} \mathbf{Z}$, where the direct sum is over the prime ideals of height 1 and the map is given by the valuations, is surjective, or in other words that the ideal class group of A is trivial. Since A is local and regular (it is a direct limit of regular rings), it is a UFD, whence the result. □

Theorem 4.22 *Let X be a noetherian, integral and regular scheme with function field F. Then the canonical map $\operatorname{Br} X \to \operatorname{Br} F$ is injective. In particular $\operatorname{Br} X$ is a torsion group.*

Proof : Let $j : \operatorname{Spec} F \to X$ be the generic point of X. Consider Leray spectral sequence

$$H^r(X, R^s j_*\mathbf{G}_m) \Rightarrow H^{r+s}(F, \mathbf{G}_m). \tag{2}$$

We have that $R^1 j_*\mathbf{G}_m = 0$ by Hilbert's 90, as the sheaf $R^1 j_*\mathbf{G}_m$ is associated to the presheaf $U \mapsto H^1(U \times_X \operatorname{Spec} F, \mathbf{G}_m)$ and the fiber $U \times_X \operatorname{Spec} F$ is étale over a field, hence is isomorphic to a disjoint union of spectra of fields. The exact sequence of the first terms of the spectral sequence now yields an injection $H^2(X, j_*\mathbf{G}_m) \hookrightarrow \operatorname{Br} F$. On the other hand, we can apply cohomology to the exact sequence (cf. Proposition 4.21, b):

$$0 \to \mathbf{G}_{m,X} \to j_*\mathbf{G}_{m,F} \to \bigoplus_{D \in X^{(1)}} (i_D)_*\mathbf{Z}_{k(D)} \to 0,$$

which in turn gives an injective map $\operatorname{Br} X \to H^2(X, j_*\mathbf{G}_{m,F})$ because we have $H^1(X, \bigoplus_{D\in X^{(1)}}(i_D)_*\mathbf{Z}_{k(D)}) = 0$: indeed $H^1(X, (i_D)_*\mathbf{Z}_{k(D)})$ injects into $H^1(k(D), \mathbf{Z})$ via Leray spectral sequence for i_D, and $H^1(K, \mathbf{Z}) = 0$ for any field K. Whence the result.

□

Without the regularity assumption, it is not always true that $\operatorname{Br} X$ is a torsion group (unlike the Azumaya Brauer group $\operatorname{Br}_{\mathrm{Az}} X$); see [1], §8.1.

It is possible to say a lot more than Theorem 4.22 when X is of dimension 1 and some additional assumptions are made. For every profinite group G, denote by $G^D = H^1(G, \mathbf{Q}/\mathbf{Z})$ the group of continuous homomorphism from G (or its abelianized group G^{ab}) to the discrete group $\mathbf{Q}/\mathbf{Z}$.

Proposition 4.23 *Let X be a noetherian, integral and regular scheme of dimension 1 with function field K. Assume that all residue fields $k(x)$ for $x \in X^{(1)}$ are perfect and denote by G_x the absolute Galois group of $k(x)$. Then there is an exact sequence*

$$0 \to \operatorname{Br} X \to \operatorname{Br} K \to \bigoplus_{x \in X^{(1)}} G_x^D \to H^3(X, \mathbf{G}_m) \to H^3(K, \mathbf{G}_m).$$

Proof : Let $j : \operatorname{Spec} K \to X$ be the generic point of X. Let $x \in X^{(1)}$, it is a closed point of X because X is of dimension 1. By Theorem 4.15, the stalk of $R^2 j_*\mathbf{G}_m$ at a geometric point $\bar{x}$ with image x is $H^2(K_x^{\mathrm{sh}}, \mathbf{G}_m) = \operatorname{Br} K_x^{\mathrm{sh}}$, where $K_x^{\mathrm{sh}} = \operatorname{Frac}(\mathcal{O}_{X,x}^{\mathrm{sh}})$. This group is known (cf. Example 3.25, c) to be zero because the residue field of the henselian discrete valuation ring $\mathcal{O}_{X,x}^{\mathrm{sh}}$ is perfect and separably closed. For a geometric point $\bar{\eta}$ with image the generic point of X, we still have $(R^2 j_*\mathbf{G}_m)_{\bar{\eta}} = 0$ (it is the Brauer group of a separably closed field). Finally $R^2 j_*\mathbf{G}_m = 0$ and we already saw (proof of Theorem 4.22) that $R^1 j_*\mathbf{G}_m = 0$. Using Leray spectral sequence, this yields

$$H^2(X, j_*\mathbf{G}_m) = \operatorname{Br} K;\ \ H^3(X, j_*\mathbf{G}_m) \hookrightarrow H^3(K, \mathbf{G}_m).$$

On the other hand, we also have Leray spectral sequence for the closed immersion $i_x : x \mapsto X$ with $x \in X^{(1)}$. Since $(i_x)_*$ is then exact, we have

$R^q(i_x)_* = 0$ for all $q > 0$, which gives $H^r(X, (i_x)_*\mathbf{Z}) = H^r(k(x), \mathbf{Z})$ for all non negative integers r. Set $D_X = \bigoplus_{x\in X^{(1)}}(i_x)_*\mathbf{Z}$, we thus have $H^r(X, D_X) = \bigoplus_{x\in X^{(1)}} H^r(k(x), \mathbf{Z})$. We observe that this group is zero for $r = 1$, and is $\bigoplus_{x\in X^{(1)}} G_x^D$ for $r = 2$ (cf. Example 2.27, which immediately extends to a profinite group). Proposition 4.21 b) yields an exact sequence

$$0 \to \mathbf{G}_{m,X} \to j_*\mathbf{G}_{m,K} \to D_X \to 0. \tag{3}$$

Applying cohomology, we get an exact sequence

$$0 \to \operatorname{Br} X \to \operatorname{Br} K \to \bigoplus_{x\in X^{(1)}} G_x^D \to H^3(X, \mathbf{G}_m) \to H^3(X, j_*\mathbf{G}_m), \tag{4}$$

whence the results because $H^3(X, j_*\mathbf{G}_m) \hookrightarrow H^3(K, \mathbf{G}_m)$.

□

Remark 4.24 Assume further that K is of characteristic zero[4]. Then the fields K_x^{sh} are of cohomological dimension 1, (cf. Theorem 2.53 and Example 3.25, c). This implies that $H^q(K_x^{\mathrm{sh}}, \mathbf{G}_m) = 0$ for every $q > 0$. In this case, we have $R^q j_*\mathbf{G}_m = 0$ for all $q > 0$, hence $H^q(X, j_*\mathbf{G}_m)$ identifies with $H^q(K, \mathbf{G}_m)$ and sequence (4) extends to a long exact sequence

$$\ldots \to H^r(X, \mathbf{G}_m) \to H^r(K, \mathbf{G}_m) \to \bigoplus_{x\in X^{(1)}} H^{r-1}(k(x), \mathbf{Q}/\mathbf{Z}) \to H^{r+1}(X, \mathbf{G}_m) \to \ldots$$

Example 4.25 a) Assume that A is a discrete valuation ring with perfect residue field κ and function field K. Then exact sequence (4) becomes

$$0 \to \operatorname{Br} A \to \operatorname{Br} K \to H^1(\kappa, \mathbf{Q}/\mathbf{Z}).$$

The map $\partial_A : \operatorname{Br} K \to H^1(\kappa, \mathbf{Q}/\mathbf{Z})$ is called the *residue map*. There are other definitions for this map (Serre residue, Witt residue), which coincide up to a sign (see [1], §1.4).

b) If we assume further A henselian, then $\operatorname{Br} A \simeq \operatorname{Br} \kappa$, and the previous sequence has a section given by the composition of the inflation map $H^1(\kappa, \mathbf{Q}/\mathbf{Z}) \simeq H^2(\kappa, \mathbf{Z}) \to H^2(K, \mathbf{Z})$ with the map $H^2(K, \mathbf{Z}) \to H^2(K, \mathbf{G}_m)$ induced by $m \mapsto \pi^m, m \in \mathbf{Z}$, where π is a uniformizing parameter of A. In particular the residue map is surjective if A is henselian. Using Remark 4.24, one actually has short split exact sequences

$$0 \to H^r(A, \mathbf{G}_m) \to H^r(K, \mathbf{G}_m) \to H^{r-1}(\kappa, \mathbf{Q}/\mathbf{Z}) \to 0.$$

[4] This assumption is actually superfluous, see [1], Prop 1.4.5.

for all $r \geq 2$. We recover in particular that the Brauer group of a p-adic field or a finite extension of $\mathbf{F}_q((t))$ is isomorphic to $\mathbf{Q}/\mathbf{Z}$.

c) If X is a smooth curve over an algebraically closed field k, then its function field K is C_1 by Tsen's Theorem, so $H^r(K, \mathbf{G}_m) = 0$ for $r > 0$, and we also have $H^r(k(x), \mathbf{Q}/\mathbf{Z}) = 0$ for all closed points x of X, the field $k(x)$ being algebraically closed. Thus $H^q(X, \mathbf{G}_m) = 0$ for all $q \geq 2$.

4.5. Purity and residues

The next theorem identifies more precisely the Brauer group of a regular integral scheme (of arbitrary dimension) inside the Brauer group of its field of functions. It is much more difficult than Proposition 4.23, and uses *Gabber's purity Theorem*; see [6], Theorem 6.9. and 6.10.

Theorem 4.26 *Let X be an integral, regular, noetherian, excellent scheme (e.g. a scheme of finite type over a field or over $\mathbf{Z}$). Let U be a non empty open subset of X, set $Z = X - U$ (with its reduced structure) and denote by c the codimension of Z. Let ℓ be a prime invertible on X.*

a) If $c \geq 2$, then the restriction map $(\operatorname{Br} X)\{\ell\} \to (\operatorname{Br} U)\{\ell\}$ is an isomorphism.

b) Assume $c = 1$; denote by $D_1, ..., D_m$ the irreducible components of Z of codimension 1 in X and by $K_1, ..., K_m$ their respective function fields. Then there is an exact sequence

$$0 \to (\operatorname{Br} X)\{\ell\} \to (\operatorname{Br} U)\{\ell\} \to \bigoplus_{i=1}^{m} H^1(K_i, \mathbf{Q}_\ell/\mathbf{Z}_\ell).$$

If Z is further assumed to be regular, then the groups $H^1(K_i, \mathbf{Q}_\ell/\mathbf{Z}_\ell)$ can be replaced by their subgroups[5] *$H^1(D_i, \mathbf{Q}_\ell/\mathbf{Z}_\ell)$.*

Corollary 4.27 *Let X be an integral, regular, noetherian, excellent scheme with function field K. Let ℓ be a prime invertible on X. Then there is an exact sequence*

$$0 \to (\operatorname{Br} X)\{\ell\} \to (\operatorname{Br} K)\{\ell\} \to \bigoplus_{D \in X^{(1)}} H^1(K_D, \mathbf{Q}_\ell/\mathbf{Z}_\ell),$$

where $X^{(1)}$ is the set of integral divisors (or points of codimension 1) of X and K_D is the function field (=residue field of the corresponding point of codimension 1) of D.

[5] See [6], Remark 4.23, for the fact that the restriction map $H^1(D_i, \mathbf{Q}_\ell/\mathbf{Z}_\ell) \to H^1(K_i, \mathbf{Q}_\ell/\mathbf{Z}_\ell)$ is indeed injective.

Proof : Take the direct limit over all non empty affine open subsets U of X in Theorem 4.26 and apply Example 4.13, d).

□

If all residual characteristics of X are zero, we can of course remove $\{\ell\}$ everywhere and replace $\mathbf{Q}_\ell/\mathbf{Z}_\ell$ by $\mathbf{Q}/\mathbf{Z} = \bigoplus_\ell \mathbf{Q}_\ell/\mathbf{Z}_\ell$.

Remark 4.28 Let x be a point of codimension 1 of X with residue field $k(x)$ (thus $k(x)$ is the function field K_D of the divisor D defined as the Zariski closure of $\{x\}$). The residue map $(\mathrm{Br}\,K)\{\ell\} \to H^1(k(x), \mathbf{Q}_\ell/\mathbf{Z}_\ell)$ appearing in the previous theorem coincides (up to a sign) with the map defined [6] in Example 4.25, a) with $A = \mathcal{O}_{X,x}$ (which can also be defined by going to the henselization A^h of A). See [1], Theorem 3.7.3.

Corollary 4.29 *Let X be a regular, noetherian, integral, excellent scheme with function field K. Let ℓ be a prime number invertible on X. Then:*

a) The subgroup $(\mathrm{Br}\,X)\{\ell\}$ *of* $\mathrm{Br}\,K$ *is given by*

$$(\mathrm{Br}\,X)\{\ell\} = \bigcap_{x \in X^{(1)}} \mathrm{Br}\,(\mathcal{O}_{X,x})\{\ell\}.$$

b) Let $(A_i)_{i\in I}$ be the family of discrete valuation rings with quotient field K which lie over X (that is: such that the map $\mathrm{Spec}\,K \to X$ *factors through* $\mathrm{Spec}\,A_i$*). Then*

$$(\mathrm{Br}\,X)\{\ell\} = \bigcap_{i\in I} (\mathrm{Br}\,A_i)\{\ell\} \subset (\mathrm{Br}\,K)\{\ell\}.$$

c) Assume further that X is proper over a scheme S. Let $(B_i)_{i\in I}$ be the family of discrete valuation rings with quotient field K which lie over S. Then

$$(\mathrm{Br}\,X)\{\ell\} = \bigcap_{i\in I} (\mathrm{Br}\,B_i)\{\ell\} \subset (\mathrm{Br}\,K)\{\ell\}.$$

The main example of application of c) is a proper and regular variety X over a field k; then (B_i) is the family of d.v.r. containing k and with function field K.

[6] It is not necessary to assume $k(x)$ perfect here, because ℓ is invertible on X.

Proof : a) follows from Corollary 4.27 and Remark 4.28. b) is an immediate consequence of a). c) is deduced from b) using the valuative criterion of properness.

$\square$

Remark 4.30 K. Cesnavicius has proved recently that for every regular, noetherian and integral scheme X and every open subset U of X such that $\operatorname{codim}(X - U, X) \geq 2$, the restriction map $\operatorname{Br} X \to \operatorname{Br} U$ is an isomorphism (without restriction to $(\operatorname{Br} X)\{\ell\}$ with ℓ invertible on X). A consequence is that it is possible to remove the $\{\ell\}$ everywhere in Corollary 4.29, see [1], Theorem 3.7.8. and Proposition 3.7.10.

4.6. Birational invariance of the Brauer group

We start with a definition due to D. Saltman.

Definition 4.31 Let $k \subset K$ be an extension of fields. The *unramified Brauer group of K over k* is the subgroup $\operatorname{Br}_{\mathrm{nr}}(K/k)$ of $\operatorname{Br} K$ consisting of those elements α such that for every discrete valuation ring A with quotient field K and such that $k \subset A$, the element α is in the image of the map $\operatorname{Br} A \hookrightarrow \operatorname{Br} K$

Observe that if we assume further that k is of characteristic zero, then the condition $\alpha \in \operatorname{Br}_{\mathrm{nr}}(K/k)$ can be rephrased as: for every discrete valuation ring A with quotient field K and such that $k \subset A$, the residue $\partial_A(\alpha)$ is zero (since the residue field of A is then automatically perfect).

Remark 4.32 Let $k \subset K \subset L$ be field extensions. Then it isnot difficult to see from the definition that the image of $\operatorname{Br}_{\mathrm{nr}}(K/k)$ by the restriction map $\operatorname{Br} K \to \operatorname{Br} L$ is a subgroup of $\operatorname{Br}_{\mathrm{nr}}(L/k)$.

Theorem 4.33 *Let X be a proper, integral, regular variety over a field k with function field $K = k(X)$. Then $\operatorname{Br}_{\mathrm{nr}}(K/k)$ is the subgroup $\operatorname{Br} X$ of $\operatorname{Br} K$.*

Proof : If k is of characteristic zero, this follows immediately of Corollary 4.29, c). In the general case, one has to use Cesnavicius's purity Theorem (see Remark 4.30).

$\square$

Corollary 4.34 (Birational invariance) *Let X and Y be two k-birational proper, integral, regular varieties over a field k. Then $\operatorname{Br} X \simeq \operatorname{Br} Y$.*

Proof : The condition that X and Y are k-birational means that there are Zariski-dense open subsets $U \subset X$ and $V \subset Y$ such that U is k-isomorphic to V, which in turn is equivalent to saying that the function fields $k(X)$ and $k(Y)$ are k-isomorphic. Now apply Theorem 4.33.

□

Theorem 4.33 is especially useful to compute explicitely $\operatorname{Br} X$ (in particular when X is given as a smooth and projective model of a possibly singular variety, it is not necessary to explicitely write down equations for X to compute the unramified Brauer group of its function fields).

5. Applications of the Brauer group

5.1. Birationality and stable birationality of varieties

In this paragraph, we denote by k a field with separable closure $\bar{k}$ and absolute Galois group $\Gamma = \operatorname{Gal}(\bar{k}/k)$. For a k-variety X, we set $\overline{X} := X \times_k \bar{k}$ and $\bar{k}[X]^* = H^0(\overline{X}, \mathbf{G}_m)$. We let $\operatorname{Br}_1 X := \ker[\operatorname{Br} X \to \operatorname{Br} \overline{X}]$ be the *algebraic Brauer group* of X (elements of $\operatorname{Br} X$ that are not in $\operatorname{Br}_1 X$ are called *transcendental*).

Theorem 5.1 *Assume that $\bar{k}[X]^* = \bar{k}^*$ (e.g. X is proper and geometrically integral, or $X = \mathbf{A}^n_k$). Then there is an exact sequence*

$$0 \to \operatorname{Pic} X \to (\operatorname{Pic} \overline{X})^\Gamma \to \operatorname{Br} k \to \operatorname{Br}_1 X \to H^1(k, \operatorname{Pic} \overline{X}) \to N \to 0,$$

where $N := \ker[H^3(k, \mathbf{G}_m) \to H^3(X, \mathbf{G}_m)]$. If $X(k) \neq \emptyset$, then the map $\operatorname{Br} k \to \operatorname{Br}_1 X$ is injective and $\operatorname{Br}_1 X/\operatorname{Br} k \simeq H^1(k, \operatorname{Pic} \overline{X})$.

Proof : By Hilbert's Theorem 90, we have $H^1(k, \bar{k}[X]^*) = H^1(k, \bar{k}^*) = 0$. Now the sequence just consists of the exact sequence of the first terms in Hochschild-Serre spectral sequence, given that $H^0(\overline{X}, \mathbf{G}_m) = \bar{k}^*$ by assumption. If we assume further that $X(k) \neq \emptyset$, then the structural morphism $X \to \operatorname{Spec} k$ has a section, hence the morphism $\operatorname{Br} k \to \operatorname{Br} X$ (as well as the morphism $H^3(k, \mathbf{G}_m) \to H^3(X, \mathbf{G}_m)$) has a retraction, hence is injective, which gives the second statement.

□

Theorem 5.2 *Let S be an integral, regular, noetherian scheme with function field K (assumed of characteristic zero). Then the canonical map $\operatorname{Br} S \to \operatorname{Br}(\mathbf{A}^n_S)$ is an isomorphism.*

Proof : By induction on n, it is sufficient to deal with the case $n = 1$. The map $\mathrm{Br}\, K \to \mathrm{Br}_1\, \mathbf{A}^1_K$ is an isomorphism thanks to Theorem 5.1, because the Picard group of the affine space is zero. Besides, we have $\mathrm{Br}\, \mathbf{A}^1_{\overline{K}} = 0$ by Tsen's Theorem (the separable closure $\overline{K}$ of K being algebraically closed), whence the result for $S = \mathrm{Spec}\, K$.

In the general case, we observe that there is a commutative diagram

$$\begin{array}{ccc} \mathrm{Br}\,(\mathbf{A}^1_S) & \longrightarrow & \mathrm{Br}\,(\mathbf{A}^1_K) \\ \uparrow & & \uparrow \\ \mathrm{Br}\, S & \longrightarrow & \mathrm{Br}\, K \end{array}$$

The horizontal maps are injective by Theorem 4.22 (both groups on the first line are subgroups of $\mathrm{Br}\,(K(T))$). Choose a section (which clearly exists, for example via the choice of a $\mathbf{Z}$-point of $\mathbf{A}^1_{\mathbf{Z}}$) of the structural morphism $\mathbf{A}^1_S \to S$, it induces a retraction s of the left vertical map and a retraction s_K of the right vertical map. By the case $S = \mathrm{Spec}\, K$, we already know that s_K is an isomorphism, hence so is s by diagram chasing.

□

Corollary 5.3 *Let k be a field of characteristic zero. Then the canonical map $\mathrm{Br}\, k \to \mathrm{Br}\, \mathbf{P}^n_k$ is an isomorphism for $n \geq 1$. More generally $\mathrm{Br}\, S \simeq \mathrm{Br}\, \mathbf{P}^n_S$ for every S as in Theorem 5.2.*

Proof : Let $K \simeq k(T_1, ..., T_n)$ be the function field of $\mathbf{P}^n_k$ and $\mathbf{A}^n_k$. By Theorem 4.22, we have injective maps

$$\mathrm{Br}\, k \to \mathrm{Br}\, \mathbf{P}^n_k \to \mathrm{Br}\, \mathbf{A}^n_k \to \mathrm{Br}\, K,$$

and the corresponding map $\mathrm{Br}\, k \to \mathrm{Br}\, \mathbf{A}^n_k$ is surjective, whence the result. The argument for an arbitrary noetherian, integral, regular S (with function field of characteristic zero) is similar.

□

Remark 5.4 Theorem 5.2 still holds in characteristic p provided one restricts to the ℓ-primary torsion of the Brauer group with $\ell \neq p$. Over an arbitrary perfect field k of characteristic p, we still have $(\mathrm{Br}\, k)\{p\} \simeq \mathrm{Br}\,(\mathbf{A}^1_k)\{p\}$, the separable closure of k being algebraically closed. This is no longer true over a non perfect field or for $\mathrm{Br}\,(\mathbf{A}^n_k)$ $(n \geq 2)$ over an algebraically closed field of characteristic p, see [1], Remark 6.1.2. Corollary 5.3 still holds in positive characteristic, but the proof is more complicated, see [1], Theorem 6.1.3.

We now go back to the unramified Brauer group.

Definition 5.5 Two k-varieties X and Y are *stably k-birationally equivalent* if there exists non negative integers m and n such that $X \times_k \mathbf{P}^k_m$ is k-birational to $Y \times_k \mathbf{P}^k_n$. A k-variety X is *stably k-rational* if $X \times \mathbf{P}^k_n$ is k-rational for some n.

Theorem 5.6 *Let k be a field of characteristic zero. Let X and Y be integral k-varieties with respective function fields $k(X)$ and $k(Y)$. Then, if X and Y are stably k-birationally equivalent, we have* $\mathrm{Br}_{\mathrm{nr}}\,(k(X)/k) \simeq \mathrm{Br}_{\mathrm{nr}}\,(k(Y)/k)$. *In particular, if X is stably k-rational, then* $\mathrm{Br}_{\mathrm{nr}}\,(k(X)/k)$*, is trivial, that is isomorphic to* $\mathrm{Br}\,k$.

Proof : Let X' (resp. Y') be a smooth and proper k-variety which is k-birational to X (resp. to Y). The existence of X' is ensured by Hironaka's Theorem on resolution of singularities. The assumption that X and Y are stably k-birational yields integers m, n such that the proper and smooth varieties $X' \times_k \mathbf{P}^k_m$ and $Y' \times_k \mathbf{P}^k_n$ are k-birational. By corollary 4.34:

$$\mathrm{Br}\,(X' \times_k \mathbf{P}^k_m) \simeq \mathrm{Br}\,(Y' \times_k \mathbf{P}^k_n).$$

By Corollary 5.3, we now have $\mathrm{Br}\,X' \simeq \mathrm{Br}\,Y'$, hence $\mathrm{Br}_{\mathrm{nr}}\,(k(X)/k) \simeq \mathrm{Br}_{\mathrm{nr}}\,(k(Y)/k)$ by Theorem 4.33.[7]

□

This theorem is very important, because it can be used to prove that two varieties are *not* stably k-birationally equivalent, e.g. that a k-unirational variety is not stably k-rational.

5.2. An example of computation of the Brauer group

Let k be a field with separable closure $\bar{k}$ and absolute Galois group $\Gamma = \mathrm{Gal}\,(\bar{k}/k)$. Let A, B be Γ-modules. Then there are bilinear maps, called *cup-product*

$$H^r(k, A) \times H^s(k, B) \to H^{r+s}(k, A \otimes_{\mathbf{Z}} B).$$

See for instance [5], §2.5., for the main properties of the cup-product.

Example 5.7 a) An interesting case is the following: let n be a positive integer which is not divisible by $\mathrm{Char}\,k$. Consider the cup-product pairing

$$H^1(k, \mathbf{Z}/n) \times H^1(k, \mu_n) \to H^2(k, \mu_n) = (\mathrm{Br}\,k)[n], \ (\chi, b) \mapsto \chi \cup b.$$

[7] It is also possible to avoid the use of Hironaka's Theorem by proving directly (via the definition with residues) that $\mathrm{Br}_{\mathrm{nr}}\,(K/k) \simeq \mathrm{Br}_{\mathrm{nr}}\,(K(T)/k)$ for every field extension K/k, see [6], Prop 7.7.

The image of a pair (χ, b) (consisting of an n-torsion character χ of the Galois group Γ and the class b modulo k^{*^n} of an element of k^*) is the class in the Brauer group of what is called the *cyclic algebra* associated to (χ, b), which is an example of central simple k-algebra (cf. [2], Prop 2.5.2).

b) The special case $n = 2$ corresponds to the quaternion algebra (a, b) associated to $a, b \in H^1(k, \mathbf{Z}/2) = k^*/k^{*^2}$. Recall that (a, b) is zero in $\operatorname{Br} k$ if and only if the equation $x^2 - ay^2 - bz^2 = 0$ has a non trivial solution in k. The map from $k^* \times k^*$ to $(\operatorname{Br} k)[2]$ that sends a pair a, b to (a, b) is therefore bilinear.

Let K be the fraction field of a discrete valuation ring A with residue field κ whose characteristic does not divide n. There is a residue map $\partial_A : (\operatorname{Br} K)[n] \to H^1(\kappa, \mathbf{Z}/n)$. The following result relates the cup-product with this residue map:

Proposition 5.8 *Let $\alpha \in H^1(A, \mathbf{Z}/n)$ with image $\alpha_0 \in H^1(\kappa, \mathbf{Z}/n)$. Let $b \in K^*$, denote by $v_A(b) \in \mathbf{Z}$ its valuation and by β its image in $H^1(K, \mu_n) = K^*/K^{*^n}$. Then*

$$\partial_A(\alpha \cup \beta) = v_A(b)\alpha_0 \in H^1(\kappa, \mathbf{Z}/n).$$

Proof : See [1], §1.4.1., Formula (1.18).

□

Corollary 5.9 *Assume that the characteristic of κ is not 2. Let $a \in A^*$ and $b \in K^*$. Then the residue $\partial_A((a, b))$ of the symbol $(a, b) \in (\operatorname{Br} K)[2]$ is zero as soon as $v_A(b)$ is even or the image of a in κ^* is a square.*

Theorem 5.10 (D.H., 1994) *Let $a \in \mathbf{C}^*$. Let V be the $\mathbf{C}$-variety defined in the affine space $\mathbf{A}^4$ by the equation*

$$y^2 - tz^2 = (x^2 + a)(1 + t^2 - t(x^2 + a + 2)).$$

Then $(t, x^2 + a)$ is a non-zero element of $\operatorname{Br}_{\mathrm{nr}}(\mathbf{C}(V))$.

This yields an example of a $\mathbf{C}$-variety which is not stably rational. Nevertheless V is unirational. Indeed it is dominated by the rational variety V' obtained via the change of variables $t = u^2$, which is rational: by the change of variables $y' = y - uz$, $z' = y + uz$, V' is birational to a variety given by the equation $y'z' = Q(x, u)$, where Q is a polynomial.

Proof : (See also [4]). Set

$$f(x) := (x^2 + a);\ \ g(x,t) := (1 + t^2 - t(x^2 + a + 2)).$$

To show that $(t, f(x)) \neq 0$, observe that V is fibered over the affine plane (via t, x), the generic fibre being a conic X over $F := \mathbf{C}(x,t)$ with function field $F(X) = \mathbf{C}(V)$. The equation of X is

$$y^2 - tz^2 = f(x)g(x,t),$$

A general property of conics (see the exercises) is that the kernel of $\mathrm{Br}\, F \to \mathrm{Br}\,(F(X))$ is of order at most 2, generated by $(t, f(x)g(x,t))$. Therefore, to show that $(t, f(x))$ is not in this kernel, it is sufficient to show that $(t, f(x))$ and $(t, g(x,t))$ are both non zero in $\mathrm{Br}\, F$, that is that $f(x)$ and $g(x,t)$ are not norms of the extension $F(\sqrt{t})/F$, which is not difficult to check.

We now have $(t, f(x)) = (t, g(x,t))$ in $\mathrm{Br}\,(\mathbf{C}(V))$. To show that $(t, f(x))$ is in $\mathrm{Br}_{\mathrm{nr}}\,(\mathbf{C}(V))$, the method consists of proving that all its residues (associated to discrete valuation rings A containing $\mathbf{C}$ and with fraction field $\mathbf{C}(V)$) are zero. We use Corollary 5.9. Let $\mathcal{M}$ be the maximal ideal of A and κ its residue field. If the valuation $v(x)$ of x is > 0, then $v(x^2 + a) = 0$ and $x^2 + a$ coincide with a modulo $\mathcal{M}$, hence is a square in κ and the residue is zero. The case $v(x) < 0$ is similar, as $(t, x^2 + a) = (t, 1 + a/x^2)$, so we can assume $v(x) = 0$. Now it $v(t) > 0$, then $v(g(x,t)) = 0$ and $g(x,t)$ coincides with 1 modulo $\mathcal{M}$, hence the residue is again zero; the case $v(t) < 0$ is similar as the coefficient of t^2 is a square. Finally, the only possibility to obtain a non trivial residue is when $v(t) = v(x) = 0$, with $v(f(x))$ and $v(g(x,t))$ both odd, hence strictly positive. But this implies that $(t-1)^2 = 0$ modulo $\mathcal{M}$, hence t becomes a square in κ and the residue is again trivial.

□

5.3. The Brauer-Manin obstruction

Let k be a number field. Denote by Ω the set of all places of k and by k_v the completion of k at v. Local class field theory gives a one-to-one homomorphism $\mathrm{inv}_v : \mathrm{Br}\, k_v \to \mathbf{Q}/\mathbf{Z}$, which is an isomorphism if v is not archimedean. Global class field theory yields an exact sequence

$$0 \to \mathrm{Br}\, k \to \bigoplus_{v \in \Omega} \mathrm{Br}\, k_v \overset{\sum \mathrm{inv}_v}{\to} \bigoplus_{v \in \Omega} \mathbf{Q}/\mathbf{Z} \to 0. \tag{5}$$

Observe that the injectivity of the first map implies that a projective conic has a point over k as soon as it has a point over every completion of

k: this is the *Hasse principle* for conics (the result holds more generally for quadrics, but is more difficult in dimension 2).

Now let X be a (smooth) k-variety. Set $X(k_\Omega) = \prod_{v \in Omega} X(k_v)$. Define the *Brauer-Manin pairing* (introduced by Manin in 1970):

$$X(k_\Omega) \times \mathrm{Br}_{\mathrm{nr}}\, X \to \mathbf{Q}/\mathbf{Z}, \ ((x_v), \alpha) \mapsto \sum_{v \in \Omega} \mathrm{inv}_v(\alpha(x_v)).$$

The sum is well-defined, because the property $\alpha \in \mathrm{Br}_{\mathrm{nr}}\, X$ implies[8] that $\alpha(x_v) \in \mathrm{Br}\,(\mathcal{O}_v) = 0$ for almost all v: indeed take a smooth compactification Z of X, and spread out X, Z, and $\alpha \in \mathrm{Br}\, Z$ over the ring of S-integers $\mathcal{O}_{k,S}$ for some finite $S \subset \Omega$; then $\alpha(x_v) \in \mathrm{Br}\,(\mathcal{O}_v)$ for $v \notin S$ thanks to the valuative criterion of properness applied to a proper and smooth model of Z over $\mathcal{O}_{k,S}$.

Let $X(k_\Omega)^{\mathrm{Br}}$ be the left kernel of the Brauer-Manin pairing. Denote by $X(k)$ the set of k-points of X, embedded diagonally into $X(k_\Omega)$. Exact sequence (5) yields

$$X(k) \subset X(k_\Omega)^{\mathrm{Br}} \subset X(k_\Omega).$$

Continuity of Brauer-Manin pairing even shows that the closure $\overline{X(k)}$ of $X(k)$ in $X(k_\Omega)$ for the *weak* topology (=direct product topology) satisfies $\overline{X(k)} \subset X(k_\Omega)^{\mathrm{Br}}$. In particular:

-If $X(k_\Omega)^{\mathrm{Br}} = \emptyset$, then $X(k) = \emptyset$: this is the Brauer-Manin obstruction to the existence of a rational point ("failure of the Hasse-principle").

-If $X(k_\Omega)^{\mathrm{Br}} \neq X(k_\Omega)$, then $X(k)$ is not dense in $X(k_\Omega)$: this is the Brauer-Manin obstruction to weak approximation.

Theorem 5.11 (Iskovskih, 1970) *Let V be the smooth $\mathbf{Q}$-variety defined in the affine space by the equation*

$$y^2 + z^2 = (x^2 - 2)(3 - x^2) \neq 0.$$

Then V has points in every completion of $\mathbf{Q}$ but $V(\mathbf{Q}) = \emptyset$. The same holds for every smooth and projective model X of V.

Proof (sketch of): The property that V has points everywhere locally is easy to check via Hensel's lemma. Then the element $\alpha := (-1, x^2 - 2) \in \mathrm{Br}\,(\mathbf{Q}(V))$ actually belongs to $\mathrm{Br}_{\mathrm{nr}}\,(\mathbf{Q}(V)) \simeq \mathrm{Br}\, X$ (one show that all its residues are trivial).

Local computations (quite similar to the proof of Theorem 5.10) then show that for every local point $P_v \in V(Q_v)$, we have $\alpha(P_v) = 0$, except if

[8] The converse is true, but much more difficult: see [3], Th. 2.1.1.

v is the finite place 2 where $\alpha(P_v) \neq 0$. Hence $V(\mathbf{Q}) = \emptyset$ thanks to the Brauer-Manin obstruction associated to α. The same argument works for X because V (which is smooth) is isomorphic to a Zariski open subset of X, so $V(\mathbf{Q}_v)$ is dense in $X(\mathbf{Q}_v)$ by the implicit function Theorem.

□

Remark 5.12 [4] gives examples (similar to the one of Theorem 5.10) of Brauer-Manin obstruction (to the Hasse principle as well as to weak approximation) given by a *transcendental* element of $\mathrm{Br}\, X$ and not detected by algebraic elements (i.e. elements of $\mathrm{Br}_1 X$).

It is not true in general that for a (proper, smooth, geometrically integral) variety X, we have $X(k_\Omega)^{\mathrm{Br}} = \overline{X(k)}$. The first example with $X(k_\Omega)^{\mathrm{Br}} \neq \emptyset$ and $X(k) = \emptyset$ was given by Skorobogatov in 1997 (see [11], chapter 8). Nevertheless, the following conjecture has been made by Colliot-Thélène:

Conjecture 5.13 *Let X be a proper, smooth, and geometrically integral variety over a number field k. Assume that $\overline{X} := X \times_k \bar{k}$ is rationally connected (e.g. unirational). Then $X(k_\Omega)^{\mathrm{Br}} = \overline{X(k)}$.*

Here are a few known cases of this conjecture:

-Châtelet surfaces, that is: smooth proper models of affine surfaces with equation $y^2 - az^2 = P(x)$, where $a \in k^*$ is a constant and P is a polynomial of degree 4 (Colliot-Thélène, Sansuc, Swinnerton-Dyer, 1987).

-(smooth proper models of) Quotients G/H of a connected linear algebraic group by a connected subgroup (Borovoi, 1996).

-(smooth proper models of) Quotients SL_n/H, where H is constant and supersolvable (Harpaz-Wittenberg, 2020).

Julian Demeio recently announced a generalization of this last result to the case when H is any finite group scheme with $H(\bar{k})$ solvable. It is also known (Demarche-Lucchini Arteche) that the general case of a homogeneous space $X = G/H$ (where G is any linear algebraic group) reduces to dealing with SL_n/H for H a finite group scheme. The latter seems beyond of reach (even if H is assumed to be constant), as (by an argument due to Ekedahl and Colliot-Thélène) it implies the inverse Galois problem for H.

References

[1] J. L. Colliot-Thélène, A. N. Skorobogatov: *The Brauer-Grothendieck group*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. **71**, Springer 2021.

[2] P. Gille, T. Szamuely: *Central simple algebras and Galois cohomology*, second edition, Cambridge studies in advanced mathematics **165**, Cambridge University Press, Cambridge 2017.

[3] D. Harari: *Méthode des fibrations et obstruction de Manin*, Duke Math. J. **75**, 221–260 (1994).

[4] D. Harari: *Obstructions de Manin transcendantes*, Journal du Séminaire de théorie des nombres de Paris 1993-1994 (Éd. S. David), Cambridge Univ. Press, 75–97 (1996).

[5] D. Harari: *Galois cohomology and class field theory* (translated from the 2017 French original by Andrei Yafaev), Universitext, Springer, Cham 2020.

[6] D. Harari: Lectures notes 2023, https://www.imo.universite-paris-saclay.fr/~david.harari/enseignement/m2brauer23/

[7] J.S. Milne: *Étale cohomology*, Princeton Mathematical Series **33**, Princeton University Press, Princeton, N.J., 1980.

[8] J. Neukirch, A. Schmidt, K. Wingberg: *Cohomology of number fields*, second edition, Grundlehren der mathematischen Wissenschaften **323**, Springer-Verlag, Berlin, 2008.

[9] J-P. Serre: *Corps locaux*, quatrième édition, Hermann, Paris, 1968.

[10] J-P. Serre: *Cohomologie galoisienne*, fifth edition, Lecture Notes in Mathematics **5**, Springer-Verlag, Berlin, 1994.

[11] A. N. Skorobogatov: *Torsors and rational points*, Cambridge Tracts in Mathematics **144**, Cambridge University Press, Cambridge, 2001

[12] C. Weibel: *An introduction to Homological Algebra*, Cambridge Studies in Advanced Mathematics **38**, Cambridge University Press, Cambridge, 1994.