Galois-Azumaya extensions and the Brauer-Galois group of a commutative ring

Philippe Nuss

Abstract

For any commutative ring R, we introduce a group attached to R, the *Brauer-Galois group of* R, defined to be the subgroup of the Brauer group of R consisting of the classes of the Azumaya R-algebras which can be represented, via Brauer equivalence, by a Galois extension of R. We compute this group for some particular commutative rings.

Introduction.

Galois extensions of noncommutative rings were introduced in 1964 by Teruo Kanzaki [13]. These algebraic objects generalize to noncommutative rings the classical Galois extensions of fields and the Galois extensions of commutative rings due to Auslander and Goldman [1]. At the same time they also turn out to be fundamental examples of Hopf-Galois extensions; these were first considered by Kreimer-Takeuchi [18] as a noncommutative analogue of the torsors in algebraic geometry. Since Galois extensions are separable (Corollary 2.4) and since the class of central Galois extensions $\psi : R \longrightarrow S$ over a fixed commutative ground ring R behaves well under tensor product (Theorem 3.1), we may introduce a subgroup of the Brauer group of R, that we designate by *Brauer-Galois group of* R. The purpose of the present paper is to compute this object in some particular cases.

Received by the editors August 2004.

Communicated by M. Van den Bergh.

2000 *Mathematics Subject Classification :* Primary: 16H05, 16K50, 19C30, 16W22 ; secondary: 16W20.

Key words and phrases : noncommutative ring, Galois-extension, Azumaya algebra, quaternion, Brauer group.

First of all, we need to recall the definitions and collect some basic properties of Galois extensions. This is done in section 1. In the second part, we investigate particular ring extensions such as centralizing, Galois-Azumaya, Frobenius or separable extensions. We observe that Galois extensions are Frobenius and deduce from this fact that there exists a quantum object, called $\mathcal{R}$-matrix, which is in a natural way attached to any Galois-Azumaya extension ψ. Therefore ψ gives rise, for any $n \geq 2$, to a representation of the braid groups B_n (§ 2.3). The quaternion algebras furnish an important family of examples of Galois-Azumaya extensions over their centre. We show that the "n'th power norm residue algebras" — a generalization of quaternion algebras originate from Class Field Theory — are also Galois-Azumaya extensions over their centre (Theorem 2.11). In the last section, we prove that the category of centralizing Galois extensions over a fixed ground ring R is stable under tensor product (Theorem 3.1). This property enables us to introduce $\mathrm{Br}_{\mathrm{Gal}}(R)$, the Brauer-Galois group of a commutative ring R: it is the subgroup of the Brauer group of R consisting of those classes $\xi \in \mathrm{Br}(R)$ for which there exists a finite group G and a G-Galois-Azumaya extension $\psi : R \longrightarrow S$, such that ξ is equal to the class $[S]$ of S modulo stable isomorphisms. The computation of this object is in general at least as difficult as the determination of the classical Brauer group is. However, when n is a positive integer and the ring R is a field F with some arithmetic conditions with respect to n satisfied, we may use results by Merkurjev and Suslin in order to identify the n-torsion of $\mathrm{Br}_{\mathrm{Gal}}(F)$ with that of $\mathrm{Br}(F)$ (Theorem 3.4). The main point lies in the fact that the n'th power norm residue algebras generate the n-torsion of $\mathrm{Br}_{\mathrm{Gal}}(F)$ and are Galois-Azumaya extensions over their centre. As as consequence, for some particular fields of characteristic zero the Brauer group and the Brauer-Galois group coincide (Corollary 3.5).

1 Reminder on noncommutative Galois extensions

Let k be a commutative ring, fixed throughout the paper (possibly $k = \mathbf{Z}$, the ring of integers). By *algebra* we mean an associative unital k-algebra. A *division algebra* is either a commutative field or a skew-field. If R is an algebra, an *R-ring* S is an algebra S coming along with a morphism of algebras $\psi : R \longrightarrow S$. We call $\psi : R \longrightarrow S$ a *(ring-)extension*. A morphism of extensions from $\psi : R \longrightarrow S$ to $\psi' : R' \longrightarrow S'$ is a pair $(\varphi, \tilde{\varphi})$, where $\varphi : S \longrightarrow S'$ and $\tilde{\varphi} : R \longrightarrow R'$ are two morphisms of algebras verifying $\varphi \circ \psi = \psi' \circ \tilde{\varphi}$. An R-ring S carries always the R-bimodule structure $r \cdot s \cdot r' = \psi(r)s\psi(r')$ (with $r, r' \in R$ and $s \in S$).

For any extension $\psi : R \longrightarrow S$, the group $S \otimes_R S$ inherits an S-bimodule (hence an R-bimodule, via ψ) structure by $s_1 \cdot (s_2 \otimes s_3) \cdot s_4 = s_1 s_2 \otimes s_3 s_4$, with $s_1, s_2, s_3, s_4 \in S$. A tensor $\eta \in S \otimes_R S$ is called a *Casimir element* in $S \otimes_R S$ if it is symmetric in the S-bimodule $S \otimes_R S$, that is, if it verifies, for all $s \in S$, the equality $\eta s = s\eta$.

An R-ring S is endowed with an R-algebra structure if and only if R is commutative and the morphism ψ factors through the centre $\mathcal{Z}(S)$ of S. An extension $\psi : R \longrightarrow S$ is *centralizing* if the ring R is embedded in the centre $\mathcal{Z}(S)$ of S (in this event R is commutative and S is an R-algebra). The extension $\psi : R \longrightarrow S$ is *central* if there is a bijection between the ring R and the centre $\mathcal{Z}(S)$ of S (this means that S is a faithful R-algebra and that we can identify R with $R \cdot 1$). An extension

$\psi : R \longrightarrow S$ is said to be *commutative* if the rings R and S are commutative.

1.1 The definition of noncommutative Galois-extensions

Before we recall the definition of noncommutative Galois-extensions, we need to introduce some notations. Let S be an algebra and G be a finite group. Denote by $S(G)$ the algebra of all maps from G to S, the sum and the product of two maps being calculated pointwise. Let $\delta_g : G \longrightarrow S$ be the Dirac function at the point $g \in G$. It is defined by $\delta_g(h) = \boldsymbol{\delta}_{g,h}1$, for any $h \in G$ ($\boldsymbol{\delta}_{g,h}$ stands for the Kronecker symbol of g and h). View $S(G)$ as the free left S-module of rank $|G|$ (the order of the group G) with basis $\{\delta_g, g \in G\}$, and with the product

$$(s\delta_g)(t\delta_h) = st\boldsymbol{\delta}_{g,h}\delta_g,$$

for $s, t \in S$, and $g, h \in G$. The family $(\delta_g)_{g\in G}$ is then a collection of orthogonal idempotents, the sum of which $\sum_{g\in G} \delta_g$ being equal to the unit of the ring $S(G)$.

Suppose now that G acts by ring automorphisms on S. Denote by $g(s)$ the result of the action of $g \in G$ on an element $s \in S$. Endow $S(G)$ with the S-bimodule structure given, for $g \in G$ and $s_g, s, t \in S$, by the equality

$$s \cdot \sum_{g\in G} s_g\delta_g \cdot t = \sum_{g\in G} ss_g g(t)\delta_g. \tag{1}$$

For any subalgebra R of S contained in the algebra S^G of the invariant elements of S under G, define the map $\Gamma_{S/R} : S\otimes_R S \longrightarrow S(G)$ by

$$\Gamma_{S/R}(s\otimes t) = \sum_{g\in G} sg(t)\delta_g = \sum_{g\in G} s \cdot \delta_g \cdot t,$$

with $s\otimes t \in S\otimes_R S$. This map $\Gamma_{S/R}$, sometimes denoted by Γ_ψ or simply by Γ, is a morphism of S-bimodules (hence of R-bimodules). Equipped with all these notations, we are now able to state the definition of Galois extensions.

Definition 1.1. A *G-Galois extension* $\psi : R \longrightarrow S$ is a morphism of algebras $\psi : R \longrightarrow S$, together with a finite group G acting by ring automorphisms on S and trivially on $\psi(R)$ such that:

- the morphism ψ is faithfully flat (that is S is, via ψ, a faithfully flat left R-module),
- the morphism of S-bimodules $\Gamma_{S/R} : S\otimes_R S \longrightarrow S(G)$, called in this case *Galois morphism of S/R*, is an isomorphism.

The group G is called a *Galois group of* ψ. A G-Galois extension $\psi : R \longrightarrow S$ is *centralizing*[1] (respectively *central*, respectively *commutative*) if the underlying extension is centralizing (respectively central, respectively commutative). A G-Galois extension $\psi : R \longrightarrow S$ is said to be *strict* if the order of the group G is invertible in the ring S.

[1]Here the terminology differs with the one adopted in [27], where we called such extensions *central*.

1.2 Preliminary results

Galois extensions verify many nice properties. We restate those which are necessary in the rest of this paper.

1) If $\psi : R \longrightarrow S$ is a G-Galois extension, the algebra of invariants S^G is exactly $\psi(R)$ and the morphism ψ is injective [20]. Thus one may identify $\psi(R)$ with R and treat ψ as an inclusion.

2) The abelian group S is, via ψ, also faithfully flat as a right R-module, and R is a direct summand as well of the right R-module S as of the left R-module S ([27], Proposition 1.2).

3) The left R-module S is, via ψ, a left R-progenerator, that is a finitely generated projective left R-module which is also a left R-generator ([27], Lemme 1.4).

3') The same sentence as 3) but with "left" replaced everywhere by "right".

The proof of these statements call in a crucial way on a morphism of R-bimodules $S \longrightarrow R$, the *trace map*, which appears as some kind of R-linear section of the inclusion ψ. Let $\psi : R \longrightarrow S$ be a G-Galois extension. Since S^G is exactly R, the map from S to R denoted by $\mathrm{tr}_{S/R}$ or tr and given by

$$\mathrm{tr}(s) = \sum_{g \in G} g(s)$$

is well defined. It is a morphism of R-bimodules, called the *trace map*, and clearly verifies $\mathrm{tr} \circ \psi = |G| \cdot \mathrm{id}_R$.

Galois extensions as Hopf-Galois extensions. Let G be a finite group and let $\mathcal{H} = k^G$ be the Hopf algebra with k-basis $\{\delta_g\}_{g \in G}$, with multiplication $\cdot$ and comultiplication $\Delta_{\mathcal{H}}$ defined by the formulae

$$\delta_g \cdot \delta_{g'} = \boldsymbol{\delta}_{g,g'} \delta_g \quad \text{and} \quad \Delta_{\mathcal{H}}(\delta_g) = \sum_{ab=g} \delta_a \otimes \delta_b$$

(the unit in $\mathcal{H} = k^G$ is the element $1 = \sum_{g \in G} \delta_g$ and the counit is the map defined by $\epsilon(\delta_g) = 0$ if $g \neq e$ and $\epsilon(\delta_e) = 1$). A Galois extension $\psi : R \longrightarrow S$ with Galois group G is then an $\mathcal{H}$-Hopf-Galois extension (we refer to [18] for the definition), where S is an $\mathcal{H}$-comodule algebra with the coaction $\Delta_S : S \longrightarrow S \otimes \mathcal{H}$ given by $\Delta_S(s) = \sum_{g \in G} g(s) \otimes \delta_g$.

Examples 1.2. The prototypical examples of Galois extensions are:

- The classical finite Galois extensions of commutative fields.

- The Galois extensions of commutative rings, introduced by Auslander and Goldman [1], studied by Chase, Harrison, A. Rosenberg and Sweedler ([4], [6], see also [17]).

– *The algebra of diagonal matrices.* For any division ring D and any non-negative integer n, the diagonal map $\psi : D \longrightarrow D^n$ defines a $\mathbf{Z}/n\mathbf{Z}$-Galois extension ([27], § 2.2).

– *The trivial Galois extensions.* Given any (non)commutative ring R and any finite group G, then G is realizable over R, that is one may construct a (non)commutative Galois extension $\psi : R \longrightarrow S$ having G as Galois group. Do it in the following way: set $S = R(G)$, embed R into $R(G)$ via the diagonal map $\psi(r) = \sum_{g\in G} r\delta_g$ $(r \in R)$, and let G act on $R(G)$ by the formula

$$g(r\delta_h) = r\delta_{hg^{-1}},$$

for $r \in R$ and $g, h \in G$. Such a Galois extension is called *trivial*. It is straightforward to see that when one identifies both $R(G)\otimes_R R(G)$ and $R(G)(G)$ with $R(G \times G)$, then the isomorphism $\Gamma : R(G \times G) \longrightarrow R(G \times G)$ deduced from the Galois isomorphism Γ_ψ is given by

$$\Gamma(r\delta_{(g,h)}) = r\delta_{(g,g^{-1}h)},$$

for any $r \in R$ and $(g, h) \in G \times G$.

– *The quaternion algebras over a field of characteristic different from* 2. Let F be a commutative field of characteristic different from 2. Fix two elements $a, b \in F^\times$. Denote by $(\frac{a,b}{F})$ the quaternion algebra over F. It is obtained by dividing the free associative F-algebra on two generators i and j by the relations $i^2 = a$, $j^2 = b$ and $ij = -ji$. It is well known (see [30] for example) that $(\frac{a,b}{F})$ is a central simple algebra of dimension 4 isomorphic either to the algebra of matrices $M_2(F)$ or to a skew field, depending whether the Hilbert symbol $(a, b)_F$ is equal to 1 or to -1 (when F is the field $\mathbf{R}$ of the real numbers and $a = b = -1$, then $(\frac{-1,-1}{\mathbf{R}})$ is the skew field $\mathbf{H}$ of Hamilton's quaternions). The Klein's *Vierergruppe* $V = (\mathbf{Z}/2\mathbf{Z})^2$ acts on $(\frac{a,b}{F})$ by $\alpha(i) = i$, $\alpha(j) = -j$, $\beta(i) = -i$, $\beta(j) = j$, where α and β are two generators of V. In [26] (Lemma 4.3.2) we proved that the extension $F \longrightarrow (\frac{a,b}{F})$ is V-Galois (see also [27], § 2.3).

– *A counter-example: The quaternion algebras over a field of characteristic* 2. Let F be a commutative field of characteristic 2. Fix two elements $a, b \in F$. Denote by $H_{a,b} = [\frac{a,b}{F})$ the quaternion algebra over F (see [2]). It is obtained by dividing the free associative F-algebra on two generators e_1 and e_2 by the relations $e_1^2 = e_1 + a$, $e_2^2 = b$ and $e_2e_1 = e_1e_2 + e_2$. The ring $H_{a,b}$ is a skew field if and only if the polynomial $X_0^2 + X_0X_1 + aX_1^2 + b(X_2^2 + X_1X_2 + aX_3^2) \in F[X_0, X_1, X_2, X_3]$ has only one root, namely $(0, 0, 0, 0)$. When $H_{a,b}$ is a skew field, with $b = c^2$ a square in F, we have shown ([26], § 2.4) that the extension $\psi : F \longrightarrow H_{a,b}$ can never be Galois.

For the sake of completeness, we state again an important result, proved in [27] (Théorème 1.9), which we need in the sequel:

Theorem 1.3. *Let G be a finite group and $\psi : R \longrightarrow S$ be a strict G-Galois extension. For any subgroup H of G, denote by $U = S^H$ the ring of fixed elements of S under H, and by $\theta : U \longrightarrow S$ the canonical inclusion map. The morphism θ is then a strict H-Galois extension. Moreover, if H is normal in G, the canonical inclusion map $\theta' : R \longrightarrow U$ is a strict G/H-Galois extension.*

1.3 The Galois element

Let $\psi : R \longrightarrow S$ be a G-Galois extension. For any $g \in G$, denote by η_g the element $\Gamma^{-1}(\delta_g)$ in $S \otimes_R S$. The identity (1) implies the equality

$$\eta_g s = g(s)\eta_g,$$

which holds in $S \otimes_R S$, for all $s \in S$. Denote by e the neutral element of the group G. Then $\eta_e \in S \otimes_R S$ is called the *Galois element for* ψ; it is in particular a Casimir element. Fix once and for all a decomposition $\sum_{i=1}^{m} x_i \otimes y_i$ of the Galois element $\eta_e \in S \otimes_R S$. The $2m$-tuple $(x_1, \ldots, x_m;\ y_1, \ldots, y_m)$ is called a *Galois basis of* ψ. The equality $\Gamma(\eta_e) = \delta_e$ can be expressed by $\sum_{i=1}^{m} x_i g(y_i) = \boldsymbol{\delta}_{g,e}$. We state now, without proof, the properties verified by the elements $\eta_g \in S \otimes_R S$, which we need here (for details, see [27]).

The element η_g can be recovered from the Galois element $\eta_e = \sum_{i=1}^{m} x_i \otimes y_i$, namely $\eta_g = \sum_{i=1}^{m} x_i \otimes g^{-1}(y_i)$, which implies the equality $\sum_{i=1}^{m} x_i g h^{-1}(y_i) = \boldsymbol{\delta}_{g,h}$. Finally the collection of all η_g (for $g \in G$) form a "partition of the unity" in the following sense: one has $\sum_{g \in G} \eta_g = 1 \otimes 1$.

Lemma 1.4. *Let G be a finite group and $\psi : R \longrightarrow S$ be a G-Galois extension. The opposite morphism $\psi^{\mathrm{o}} : R^{\mathrm{o}} \longrightarrow S^{\mathrm{o}}$ defines then a G-Galois extension, G acting on S^{o} via*

$$g(s^{\mathrm{o}}) = (g(s))^{\mathrm{o}}.$$

Proof. It is clear that $(S^{\mathrm{o}})^G = (S^G)^{\mathrm{o}} = R^{\mathrm{o}}$. By [27] (Théorème 1.5), it remains to show that the morphism $\Gamma_{\psi^{\mathrm{o}}}$ from $S^{\mathrm{o}} \otimes_{R^{\mathrm{o}}} S^{\mathrm{o}}$ to $S^{\mathrm{o}}(G)$ given by

$$\Gamma_{\psi^{\mathrm{o}}}(s^{\mathrm{o}} \otimes t^{\mathrm{o}}) = \sum_{g \in G} s^{\mathrm{o}} g(t^{\mathrm{o}}) \delta_g = \sum_{g \in G} (g(t)s)^{\mathrm{o}} \delta_g$$

is surjective. To this end, choose a Galois basis $(x_1, \ldots, x_m;\ y_1, \ldots, y_m)$ of ψ. Then

$$\Gamma_{\psi^{\mathrm{o}}}\Big(\sum_{i=1}^{m} y_i^{\mathrm{o}} \otimes g^{-1} x_i^{\mathrm{o}}\Big) = \sum_{g \in G} \Big(\sum_{i=1}^{m} h g^{-1}(x_i) y_i\Big)^{\mathrm{o}} \delta_h,$$

which is equal to δ_g, according to the identity (5') in [27]. ∎

Notice that the quaternion algebras $(\frac{a,b}{F})$ over a commutative field F of characteristic different from 2 are isomorphic to their opposite algebras.

1.4 The categories $\mathfrak{Gal}$ and $\mathfrak{Gal}(G)$

First introduce the category $\mathfrak{Gal}$ of Galois extensions: its objects are the couples $(G, \psi : R \longrightarrow S)$, with G a finite group and $\psi : R \longrightarrow S$ a G-Galois extension; a morphism in $\mathfrak{Gal}$ from $(G, \psi : R \longrightarrow S)$ to $(G', \psi' : R' \longrightarrow S')$ is a triple $(f, \varphi, \tilde{\varphi})$, where $f : G' \longrightarrow G$ is morphism of groups, and $(\varphi : S \longrightarrow S', \tilde{\varphi} : R \longrightarrow R')$ is a morphism of extensions (that is $\varphi \circ \psi = \psi' \circ \tilde{\varphi}$) verifying $\varphi \circ f(g') = g' \circ \varphi$, for all $g' \in G'$. Necessarily $\tilde{\varphi}$ is then the restriction of φ to R. In a similar manner, define the full subcategories $\mathfrak{Galstr}$, $\mathfrak{Galcent}$, $\mathfrak{GalAzum}$ or $\mathfrak{Galcom}$ of $\mathfrak{Gal}$; their objects are respectively the strict, centralizing, central or commutative Galois extensions.

Let $\mathfrak{Gpf}$ be the category of finite groups and $\pi^{gr} : \mathfrak{Gal} \longrightarrow \mathfrak{Gpf}$ be the contravariant functor defined by $\pi^{gr}(G, \psi : R \longrightarrow S) = G$. The fibre category of π^{gr} over a fixed group G is denoted by $\mathfrak{Gal}(G)$; its objects are therefore the G-Galois extensions $\psi : R \longrightarrow S$; a morphism from $(\psi : R \longrightarrow S)$ to $(\psi' : R' \longrightarrow S')$ in $\mathfrak{Gal}(G)$ is a couple $(\varphi : S \longrightarrow S', \tilde{\varphi} : R \longrightarrow R')$ of morphisms of algebras such that φ is G-equivariant (that is $\varphi \circ g = g \circ \varphi$ for all $g \in G$) and $\psi' \circ \tilde{\varphi} = \varphi \circ \psi$. Observe that $\tilde{\varphi}$ is induced by restriction by φ. Starting with $\mathfrak{Gal}(G)$, one may define in an obvious way the full subcategories $\mathfrak{Galstr}(G)$, $\mathfrak{Galcent}(G)$, $\mathfrak{GalAzum}(G)$ or $\mathfrak{Galcom}(G)$ of $\mathfrak{Gal}(G)$.

Proposition 1.5. *Let $(\varphi, \tilde{\varphi})$ be a morphism from $(\psi : R \longrightarrow S)$ to $(\psi' : R' \longrightarrow S')$ in $\mathfrak{Gal}(G)$. Then*

$$\tilde{\varphi} \circ \Gamma = \Gamma' \circ (\varphi \otimes \varphi).$$

Here Γ (respectively Γ') stands for the Galois isomorphism of S/R (respectively of S'/R'), and $\tilde{\varphi}$ is the morphism of left R-modules from $S(G)$ to $S'(G)$ defined by $\tilde{\varphi}(\sum_{g \in G} s_g \delta_g) = \sum_{g \in G} \varphi(s_g)\delta_g$.

Proof. For any element $s \otimes t \in S \otimes_R S$, one has the equality $\Big(\Gamma' \circ (\varphi \otimes \varphi)\Big)(s \otimes t) = \sum_{g \in G} \varphi(s) g\Big(\varphi(t)\Big)\delta_g$, whereas $(\tilde{\varphi} \circ \Gamma)(s \otimes t) = \sum_{g \in G} \varphi(s)\varphi\Big(g(t)\Big)\delta_g$. The proposition is then a consequence of the G-equivariance of φ. ∎

Corollary 1.6. *Let $(\varphi, \tilde{\varphi})$ be a morphism from $(\psi : R \longrightarrow S)$ to $(\psi' : R' \longrightarrow S')$ in $\mathfrak{Gal}(G)$. If η_e (respectively η'_e) is the Galois element for ψ (respectively for ψ'), then*

$$(\varphi \otimes \varphi)(\eta_e) = \eta'_e.$$

Proof. One has $\Big(\Gamma' \circ (\varphi \otimes \varphi)\Big)(\eta_e) = (\tilde{\varphi} \circ \Gamma)(\eta_e) = \tilde{\varphi}(\delta_e) = \delta_e$. The result follows from the fact that Γ' is an isomorphism. ∎

2 Galois-Azumaya extensions

2.1 Separable extensions

Let $\psi : R \longrightarrow S$ be a morphism of algebras and $S^e = S \otimes_k S^o$ the enveloping algebra of S over the ground ring k. Define the multiplication $\bar{\mu} : S^e \longrightarrow S$ to be the S^e-linear map given by $\bar{\mu}(s \otimes t^o) = st$, and denote by $\Omega_{\bar{\mu}}$ the kernel of $\bar{\mu}$. One easily sees that $\Omega_{\bar{\mu}}$ is generated by the elements $s \otimes t^o - st \otimes 1^o$ indistinctly as a left or as a right S-module. An element $\eta \in S \otimes_R S$ is then Casimir if and only if $\Omega_{\bar{\mu}} \cdot \eta = 0$.

Proposition 2.1. *Let $\psi : R \longrightarrow S$ be a morphism of algebras. The following conditions are equivalent:*

(i) *The multiplication $\mu : S \otimes_R S \longrightarrow S$ splits as an S^e-module morphism.*

(ii) *There exists a Casimir element η in $S \otimes_R S$ such that $\mu(\eta) = 1$.*

If moreover R coincides with the (commutative) ground ring k, one of the two previous conditions is equivalent to the following assertion:

(iii) *The k-module S is projective as a left S^e-module.*

Definition 2.2. A morphism of algebras $\psi : R \longrightarrow S$ is called *separable* if it satisfies the equivalent conditions of Proposition 2.1. A Casimir element η in $S \otimes_R S$ verifying $\mu(\eta) = 1$ is called a *separability element of S*. If moreover the extension ψ is centralizing, then S is a *separable R-algebra.* Furthermore, if ψ is central, then S is a central separable R-algebra, or an *Azumaya R-algebra*[2].

Remarks:

1.– One may also characterize separable extensions using derivations or Hochschild cohomology (see for example [5], 1.3, Theorem 3]).

2.– When R is the commutative ground ring k, the separability element η viewed as an element of S^e is necessarily an idempotent of the algebra S^e. This means: fix a decomposition $\sum_{i=1}^{m} u_i \otimes v_i$ of $\eta \in S \otimes_R S$ and set $e(\eta) = \sum_{i=1}^{m} u_i \otimes v_i^o \in S^e$. Then $e(\eta)^2 = e(\eta)$. Indeed, $e(\eta)^2 - e(\eta) = e\Big(e(\eta) \cdot e - (1 \otimes 1^o)\eta\Big) \in e(\Omega_{\bar{\mu}} \cdot \eta) = 0$.

Proof of Proposition 2.1.

(i) $\Longrightarrow$ (ii) Let σ be an S^e-linear section of μ and $\eta = \sigma(1)$. Then $\mu(\eta) = \mu \circ \sigma(1) = 1$. For $s \otimes t^o - st \otimes 1^o \in \Omega_{\bar{\mu}}$, one has $(s \otimes t^o - st \otimes 1^o) \cdot \eta = (s \otimes t^o)\sigma(1) - (st \otimes 1^o)\sigma(1) = \sigma(st) - \sigma(st) = 0$, hence $\Omega_{\bar{\mu}} \cdot \eta = 0$.

(ii) $\Longrightarrow$ (i) Since $\Omega_{\bar{\mu}} \cdot \eta = 0$, one defines a map σ from S to $S \otimes_R S$ by $\sigma(s) = (s \otimes 1^o) \cdot \eta$. Thus $\sigma(s) = s \cdot \eta = (1 \otimes s^o) \cdot \eta = \eta \cdot s$. Then $\mu \circ \sigma(s) = \mu(s \cdot \eta) = s\mu(\eta) = s$, and σ is S^e-linear since $\sigma((s \otimes t^o) \cdot u) = \sigma(sut) = (sut \otimes 1^o) \cdot \eta = (su \otimes 1^o)(t \otimes 1^o) \cdot \eta = (su \otimes 1^o)(1 \otimes t^o) \cdot \eta = (su \otimes t^o) \cdot \eta = (s \otimes t^o)(u \otimes 1^o) \cdot \eta = (s \otimes t^o)\sigma(u)$.

(i) $\Longleftrightarrow$ (iii) is well known (see [7]). ∎

Examples of separable extensions are ([7], [15], [17]):

i) A finite product $\prod L_i/K$ of separable finite commutative field extensions L_i/K (recall that a field extension L/K is separable if and only if the minimal polynomials of the elements of L have simple zeroes);

[2] We follow here the terminology proposed by Bourbaki [3]. Some authors deal only with Azumaya algebras over a field. These are central simple algebras [7] (as an example take quaternion algebras over a field). Recall that an Azumaya R-algebra is simple if and only if R is a field.

ii) The n-fold product $R \times R \ldots \times R$ of a commutative ring R is separable over R;

iii) Let A be a commutative algebra and Σ be a multiplicative subset of A. The localized ring $\Sigma^{-1}A$ is separable over A;

iv) The ring $M_n(R)$ of all $n \times n$-matrices over a commutative ring R is separable over R;

v) Let G be a finite group whose order n is invertible in a commutative ring R. The group algebra $R[G]$ is separable over R;

vi) Any Azumaya algebra.

Definition 2.3. A morphism of rings $\psi : R \longrightarrow S$ is called *a G-Galois-Azumaya extension* if ψ is a G-Galois extension, R is a commutative ring and S is an R-Azumaya algebra, that is a central separable R-algebra.

For instance, the quaternion extension $F \longrightarrow (\frac{a,b}{F})$ (Example 1.2) is V-Galois-Azumaya, with $V = (\mathbf{Z}/2\mathbf{Z})^2$.

Galois-Azumaya extensions verify nice properties in view of cohomology theories. On the one side, the group of automorphisms of an Azumaya algebra is well controlled ([17], IV). For instance, if S is an Azumaya algebra over a ring R, then $\mathrm{Aut}(S/R)$ fits into an exact sequence of groups $1 \longrightarrow R^\times \longrightarrow S^\times \longrightarrow \mathrm{Aut}(S/R) \longrightarrow \mathrm{Pic}(R)$, known as the Rosenberg-Zelinsky exact sequence [17]. Therefore, if the Picard group $\mathrm{Pic}(R)$ is trivial (what happens when R is a local ring or a principal ideal domain for example), one obtains the Skolem-Noether theorem, which asserts that any automorphism of S leaving R pointwise invariant is inner. On the other side, any G-Galois-Azumaya (or, more generally, centralizing G-Galois) extension $\psi : R \longrightarrow S$ provides a natural crossed module of G-groups obtained from $S^\times \longrightarrow \mathrm{Aut}(S/R)$ which can be taken as coefficients for nonabelian hypercohomology [27].

We restate now a well-known and straightforward result [20] that furnishes further examples of separable extensions.

Corollary 2.4. *Any Galois extension is separable.*

Indeed, if $\psi : R \longrightarrow S$ is a G-Galois extension, the Galois element η_e is a separability element for S, hence ψ is separable. *Therefore a central Galois extension amounts to a Galois-Azumaya extension.* We remark now that Galois extensions own another interesting structure, that of a Frobenius extension.

2.2 Frobenius extensions

A morphism of algebras $\psi : R \longrightarrow S$ is called a *Frobenius extension* if there exists a morphism $\tau : S \longrightarrow R$ of R-bimodules and a finite set of couples $(u_i, v_i)_{i=1,\ldots,m}$, with $u_i, v_i \in S$, which verify for all $s \in S$ the *Frobenius normalizing conditions*, that is

$$\sum_{i=1}^{m} u_i \tau(v_i s) = s \quad \text{and} \quad \sum_{i=1}^{m} \tau(s u_i) v_i = s.$$

The collection $((u_i, v_i)_{i=1,\dots,m})$ allows us to construct the tensor $\eta = \sum_{i=1}^{m} u_i \otimes v_i \in S \otimes_R S$, called the *Frobenius element of the extension* $\psi : R \longrightarrow S$. The datum $((u_i, v_i)_{i=1,\dots,m}, \tau)$ or (η, τ) is a *Frobenius system*. If R lies in the centre of S, the extension $\psi : R \longrightarrow S$ is *centralizing Frobenius* (S is then a *Frobenius R-algebra*).

As examples of Frobenius extensions, let us mention, with Kadison, morphisms of integral group algebras $\psi : \mathbf{Z}[H] \longrightarrow \mathbf{Z}[G]$ (where H is a subgroup of G of finite index ℓ, such that $G = \coprod g_i H$, with $g_1 = e, g_2, \dots, g_\ell \in G$) ([12], Example 1.7), and the Frobenius extensions obtained from certain types of von Neumann $*$-algebras ([12], Example 1.8). To this list, add the Galois extensions:

Lemma 2.5. *Let G be a finite group. Any G-Galois extension $\psi : R \longrightarrow S$ is Frobenius. As a Frobenius system one may choose the datum $((x_i, y_i)_{i=1,\dots,m}, \mathrm{tr})$, where $(x_1, \dots, x_m; y_1, \dots, y_m)$ is a Galois basis of ψ, and* tr *is the trace morphism. As a Frobenius element one may take the Galois element $\eta_e = \sum_{i=1}^{m} x_i \otimes y_i \in S \otimes_R S$.*

Proof. This assertion comes as an immediate consequence from the definitions and from the following two equalities, showed in [27] (Démonstration du lemme 1.4), namely: for all $s \in S$, one has

$$\sum_{i=1}^{m} x_i \mathrm{tr}(y_i s) = \sum_{i=1}^{m} \mathrm{tr}(s x_i) y_i = s.$$

■

Let $\psi : R \longrightarrow S$ be a G-Galois extension. Denote by $C_R(S) = \{s \in S \mid sr = rs, \ \forall r \in R\} = S^R$ the centralizer of R in S. Clearly the group G acts on the algebra $C_R(S)$ and $C_R(S)^G = \mathcal{Z}(R)$. The general theory of Frobenius extensions ([12], 1.3) shows that once a Frobenius system $((u_i, v_i)_{i=1,\dots,m}, \tau)$ is fixed, there is an automorphism $\nu : C_R(S) \longrightarrow C_R(S)$, called the *Nakayama automorphism of* ψ, which verifies

$$\tau(\nu(d)s) = \tau(sd),$$

for any $s \in S$ and $d \in C_R(S)$. If the automorphism ν is inner, the Frobenius extension is called *symmetric.*

In the Galois case, taking as Frobenius system $((x_i, y_i)_{i=1,\dots,m}, \mathrm{tr})$, where $(x_1, \dots, x_m; y_1, \dots, y_m)$ is a Galois basis of ψ, the Nakayama automorphism is given by the formula

$$\nu(d) = \sum_{i=1}^{m} \mathrm{tr}(x_i d) y_i = \sum_{g \in G} \sum_{i=1}^{m} g(x_i d) y_i,$$

for any $d \in C_R(S)$. If $\psi : R \longrightarrow S$ is a centralizing G-Galois extension, then $C_R(S) = S$, and the Nakayama automorphism is defined on the whole ring S.

Lemma 2.6. *Let $\psi : R \longrightarrow S$ be a G-Galois-Azumaya extension such that the Picard group* $\mathrm{Pic}(R)$ *is trivial. Then S is a symmetric Frobenius R-algebra.*

Proof. Denote by $\mathrm{Inn}(S)$ the group of inner automorphisms of S. When R has trivial Picard group, the Rosenberg-Zelinsky exact sequence asserts that $\mathrm{Inn}(S) =$

$\mathrm{Aut}(S/R)$. It remains to show that the Nakayama automorphism leaves R pointwise invariant. For $r \in R$, one gets

$$\nu(r) = \sum_{g\in G}\sum_{i=1}^{m} g(x_i r)y_i = \sum_{i=1}^{m}\Big(\sum_{g\in G} g(x_i)r\Big)y_i = r\sum_{g\in G}\sum_{i=1}^{m} g(x_i)y_i = r.$$

■

2.3 Galois representations of the braid groups

Let R be a commutative algebra and $\psi : R \longrightarrow S$ be a Frobenius R-algebra. For any $X = \sum_{i=1}^{m} x_i \otimes y_i \in S\otimes_R S$, define three elements X_{12}, X_{23}, X_{13} in $S\otimes_R S\otimes_R S$ by the formulae

$$X_{12} = \sum_{i=1}^{m} x_i\otimes y_i\otimes 1, \quad X_{23} = \sum_{i=1}^{m} 1\otimes x_i\otimes y_i \quad \text{and} \quad X_{13} = \sum_{i=1}^{m} x_i\otimes 1\otimes y_i.$$

The properties satisfied by a Frobenius element η attached to the extension $\psi : R \longrightarrow S$ lead to the fact that η satifies the *Frobenius-separability equation* $X_{12}X_{23} = X_{23}X_{13} = X_{13}X_{12}$ [5] (Definition 18), which obviously implies the Yang-Baxter equation $X_{12}X_{23}X_{12} = X_{23}X_{12}X_{23}$ (this result appears in [12], Theorem 4.7). Therefore, when η is invertible in $S\otimes_R S$, it defines a representation of E. Artin's braid group B_n on n strings. Recall that B_n is the group generated by symbols $\sigma_1, \ldots, \sigma_{n-1}$ subject to the relations $\sigma_i\sigma_j = \sigma_j\sigma_i$ $(1 \le i, j \le n-1$ and $|i-j| > 1)$ and $\sigma_{i+1}\sigma_i\sigma_{i+1} = \sigma_i\sigma_{i+1}\sigma_i$ $(1 \le i < n-1)$.

Proposition 2.7. *For any centralizing G-Galois extension $\psi : R \longrightarrow S$, the Galois element $\eta_e = \sum_{i=1}^{m} x_i\otimes y_i$ verifies the Frobenius-separability equation and therefore the Yang-Baxter equation. For any G-Galois-Azumaya extension $\psi : R \longrightarrow S$, the Galois element η is invertible in $S\otimes_R S$, hence defines for any $n \ge 2$ a representation $\rho^n_\psi : B_n \longrightarrow \mathrm{Aut}(S^{\otimes_R n})$ of the braid group B_n.*

Proof. The proposition is a consequence of Lemma 2.5, of the observation stated above, and of a crucial result of Kadison [12] (Theorem 5.14) asserting that a Frobenius algebra S/R is central separable if and only if the Frobenius element is invertible in $S\otimes_R S$. Now an invertible solution η of the Yang-Baxter equation defines an element ℓ_η in $\mathrm{Aut}_R(S\otimes S)$, the left multiplication by η. This automorphism ℓ_η is then a solution of the Yang-Baxter equation for endomorphisms, a so-called $\mathcal{R}$-matrix, hence gives rise, for any $n \ge 2$, to a representation ρ^n_ψ of the braid group B_n in $S^{\otimes_R n}$ given by $\rho^n_\psi(\sigma_i) = \mathrm{id}_S^{\otimes(i-1)}\otimes\ell_\eta\otimes\mathrm{id}_S^{\otimes(n-i-1)}$ [14] (Corollary X.6.9). ■

Definition 2.8. For any G-Galois-Azumaya extension $\psi : R \longrightarrow S$, the representation ρ^n_ψ is called the *Galois representation of B_n attached to ψ.*

Corollary 2.9. *A morphism $(\varphi, \tilde{\varphi})$ from $(\psi : R \longrightarrow S)$ to $(\psi' : R' \longrightarrow S')$ in $\mathfrak{GalAzum}(G)$ induces, for any $n \ge 2$, a morphism $\rho^n_\psi \longrightarrow \rho^n_{\psi'}$ of Galois representations of the braid group B_n.*

Proof. Fix $n \geq 2$. From Corollary 1.6, one deduces that the diagram

$$\begin{array}{ccc} S^{\otimes_R n} & \xrightarrow{\rho_\psi^n} & S^{\otimes_R n} \\ {\scriptstyle \varphi^{\otimes n}}\downarrow & & \downarrow{\scriptstyle \varphi^{\otimes n}} \\ S'^{\otimes_{R'} n} & \xrightarrow[\rho_{\psi'}^n]{} & S'^{\otimes_{R'} n} \end{array}$$

is commutative. ∎

Example 2.10. Let $H = (\dfrac{a,b}{F})$ be a quaternion algebra. In [27] (§ 2.3), we have seen that

$$\eta = \frac{1}{4}(1\otimes 1 + \frac{i\otimes i}{a} + \frac{j\otimes j}{b} - \frac{k\otimes k}{ab})$$

is the Galois element of the V-Galois-Azumaya extension $\psi : F \longrightarrow H$. Let us mention on the way that the Nakayama automorphism ν is in this case equal to the identity of H. Indeed, the trace map $\mathrm{tr} : H \longrightarrow F$ is given by $\mathrm{tr}(c_0+c_1i+c_2j+c_3k) = 4c_0$, where $c_0 + c_1i + c_2j + c_3k \in H$. Take as Galois basis $x_1 = 1$, $x_2 = i$, $x_3 = j$, $x_4 = k$; $y_1 = 1/4$, $y_2 = i/4a$, $y_3 = j/4b$, $y_4 = -k/4ab$. Then $\nu(c) = \sum_{i=1}^{m} \mathrm{tr}(x_i c)y_i = c$.

Let us now describe the automorphism ℓ_η with more details. Decompose the 16-dimensional F-vector space $H\otimes_F H$ into four subspaces V_1, V_i, V_j, V_k each of them of dimension 4 in the following way.

Vector space	Basis
V_1	$(1\otimes 1, i\otimes i, j\otimes j, k\otimes k)$
V_i	$(1\otimes i, i\otimes 1, j\otimes k, k\otimes j)$
V_j	$(1\otimes j, j\otimes 1, k\otimes i, i\otimes k)$
V_k	$(1\otimes k, k\otimes 1, i\otimes j, j\otimes i)$

Then $H\otimes_F H = V_1 \oplus V_i \oplus V_j \oplus V_k$ and each of the subspaces V_1, V_i, V_j, V_k is stable under ℓ_η. In the given bases, ℓ_η is represented by the matrix Ξ_u in V_u $(u = 1, i, j, k)$, where

$$\Xi_1 = \frac{1}{4}\begin{pmatrix} 1 & a & b & -ab \\ \frac{1}{a} & 1 & \frac{-1}{ab} & \frac{1}{b} \\ \frac{1}{b} & \frac{-1}{ab} & 1 & \frac{1}{a} \\ \frac{-1}{ab} & \frac{1}{b} & \frac{1}{a} & 1 \end{pmatrix}, \qquad \Xi_i = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & \frac{-1}{ab} \\ 1 & 1 & \frac{-1}{ab} & 1 \\ \frac{-1}{b} & \frac{-1}{ab} & 1 & \frac{-1}{a} \\ \frac{-1}{ab} & \frac{-1}{b} & \frac{-1}{a} & 1 \end{pmatrix},$$

$$\Xi_j = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & \frac{1}{ab} \\ \frac{1}{ab} & \frac{1}{a} & 1 & \frac{-1}{b} \\ \frac{1}{a} & \frac{1}{ab} & \frac{-1}{b} & 1 \end{pmatrix}, \qquad \text{and} \quad \Xi_k = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ \frac{-1}{a} & \frac{1}{b} & 1 & \frac{1}{ab} \\ \frac{1}{b} & \frac{-1}{a} & \frac{1}{ab} & 1 \end{pmatrix}.$$

The quaternionic extension $F \longrightarrow H$ gives moreover rise to a representation of the symmetric groups $\mathfrak{S}_n$ $(n \geq 2)$. Indeed the square of η in the F-algebra $H\otimes_F H$ is

$$\eta^2 = \frac{1}{4}(1\otimes 1).$$

Thus $(2\eta)^2 = 1 \otimes 1$, that is to say that $\ell_{2\eta}$ is involutive. The assertion follows from Moore's presentation of the symmetric groups: for any $n \geq 2$, $\mathfrak{S}_n$ is the group generated by symbols $\sigma_1, \ldots, \sigma_{n-1}$ subject to the relations $\sigma_i \sigma_j = \sigma_j \sigma_i$ $(1 \leq i, j \leq n-1$ and $|i-j| > 1)$, $\sigma_{i+1}\sigma_i\sigma_{i+1} = \sigma_i\sigma_{i+1}\sigma_i$ $(1 \leq i < n-1)$ and $\sigma_i^2 = 1$ $(1 \leq i \leq n-1)$.

2.4 A fundamental example of a Galois-Azumaya extension: the n'th power norm residue algebra

Let F be a commutative field and $n \geq 2$ an integer. Suppose that the multiplicative group $F^\times$ of F contains a primitive n-th root of unity ζ, that is an element of order n in $F^\times$. Choose once and for all two elements $a, b \in F^\times$. With these datas, following Milnor [24] (§ 15) (we refer also to [8] (§ 11) or to [29] (15.4)), one explicitly constructs a central simple associative algebra in which n plays the same rôle as 2 does for quaternion algebras. This is done in the following way (see [21] (16.22, iv)):

Let Q be the quotient ring $F[X]/(X^n - a)$ of the polynomial ring $F[X]$ in one indeterminate X by the ideal $(X^n - a)$. Denote by x the image of X by the canonical projection $F[X] \longrightarrow Q$. By the euclidian division algorithm, $\{1, x, x^2, \ldots, x^{n-1}\}$ is a basis of the F-vector space Q. The F-algebra homomorphism $s : F[X] \longrightarrow F[X]$ defined by $s(X) = \zeta X$ induces a F-algebra automorphism $\sigma : Q \longrightarrow Q$ that is of order n in $\mathrm{Aut}(Q)$. Identify the cyclic group $\langle\sigma\rangle$ generated by σ with $\mathbf{Z}/n\mathbf{Z}$. Take now the free Q-module S based on the set $\{u^m \mid m = 0, \ldots, n-1\}$ indexed by the group $\mathbf{Z}/n\mathbf{Z}$. As an F-vector space, S has the basis $\{x^m u^{m'} \mid m, m' = 0, \ldots, n-1\}$. Put on S the multiplication determined by the relations

$$x^n = a, \quad u^n = b, \quad \text{and} \quad ux = \zeta xu.$$

The F-vector space S becomes an algebra S, called the *n'th power norm residue algebra* (or a *symbol algebra* [16]) and denoted by $(a, b, \zeta)_F$. It is an Azumaya algebra of degree n ([8], § 11).

Remark: The n'th power norm residue algebra clearly generalize quaternion algebras: let F be a field of characteristic different from 2 and $a, b \in F^\times$. Then $(\dfrac{a, b}{F})$ is isomorphic to $(a, b, -1)_F$ [29]. Therefore, following Pierce, one denotes $(a, b, \zeta)_F$ also by $(\dfrac{a, b}{F, \zeta})$.

Theorem 2.11. *Let F be a commutative field. Take two elements a and b in $F^\times$, and $n \geq 2$ an integer. Suppose that the multiplicative group $F^\times$ of F has an element ζ of order n and that the characteristic of F either is equal to zero or is positive and does not divide n. Let $(a, b, \zeta)_F$ be the n'th power norm residue algebra. Then the extension $F \longrightarrow (a, b, \zeta)_F$ is $(\mathbf{Z}/n\mathbf{Z})^2$-Galois-Azumaya with Galois element*

$$\eta = \sum_{r,s=0}^{n-1} \frac{\zeta^{rs}}{abn^2} x^r u^s \otimes x^{n-r} u^{n-s}.$$

Proof. Set $S = (a, b, \zeta)_F$ and $G = (\mathbf{Z}/n\mathbf{Z})^2$. It is already known that S is an Azumaya F-algebra ([21], Proposition 16.24). It remains to show that the extension $F \longrightarrow S$ is G-Galois.

Denote by (i,j), with $0 \leq i,j \leq n-1$, the elements of G. It is easy to see that the formula

$$(i,j) \cdot (qu^m) = \sigma^j(q)\zeta^{im}u^m$$

defines an action of G on S (here $0 \leq i,j,m \leq n-1$ and $q \in Q$). Thus, if $\alpha = (1,0)$ and $\beta = (0,1)$ are the two canonical generators of G, one gets $\alpha(x) = x$, $\alpha(u) = \zeta u$, $\beta(x) = \zeta x$, and $\beta(u) = u$. Suppose now that $\sum_{m=0}^{n-1} q_m u^m \in S^G$. Then, in particular $(0,1) \cdot \sum_{m=0}^{n-1} q_m u^m = \sum_{m=0}^{n-1} q_m u^m$, that is $\sum_{m=0}^{n-1} \sigma(q_m) u^m = \sum_{m=0}^{n-1} q_m u^m$. But $(u^m)_{0\leq m\leq n-1}$ is a Q-basis of S, thus, for any m, one has $\sigma(q_m) = q_m$.

Pick now an element $q = \sum_{k=0}^{n-1} a_k x^k \in Q$ which is invariant under σ. This means that $\sum_{k=0}^{n-1} a_k x^k = \sum_{k=0}^{n-1} a_k \zeta^k x^k$. Again $(x^k)_{0\leq k\leq n-1}$ is an F-basis of Q, therefore $a_k = a_k\zeta^k$, for all k, thus $a_k = 0$ as soon as $k \geq 1$. So q belongs to F. Conversely, it is clear that an element $a_0 \in F$ is invariant under G. Hence $S^G = F$.

Before we end the proof, we write down an important formula that is readily deduced from the multiplication law in S given above. For any $r,s,i,j,k,l \in \{0,\ldots,n-1\}$, an easy computation gives

$$x^r u^s (i,j)(x^k u^l) = \zeta^{il+jk+ks} x^{r+k} u^{s+l}.$$

In particular,

$$x^r u^s (i,j)(x^{n-r} u^{n-s}) = \zeta^{-(is+jr+rs)} ab. \tag{2}$$

Having this rule of calculus in view, we claim that the following equality is true:

$$\Gamma\Big(\sum_{r,s=0}^{n-1} \frac{\zeta^{rs}}{abn^2} x^r u^s \otimes x^{n-r} u^{n-s}\Big) = \delta_{(0,0)}. \tag{3}$$

This is then sufficient to show that $\psi : F \longrightarrow S$ is G-Galois, since formula (3) exactly means that there exists a Galois basis (see [27], Définition 1.6 and Théorème 1.5). Let us prove (3).

According to (2), the left-hand side is equal to $\dfrac{1}{n^2} \sum_{(i,j)\in G} \sum_{r,s=0}^{n-1} \zeta^{-(jr+is)} \delta_{(i,j)}$. The coefficient of $\delta_{(i,j)}$ is $\sum_{r,s=0}^{n-1} \zeta^{-(jr+is)} = \sum_{r=0}^{n-1} \zeta^{-jr} (\sum_{s=0}^{n-1} (\zeta^{-i})^s)$. But the cyclotomic sum $\sum_{t=0}^{n-1} (\zeta^{-k})^t$ is equal either to 0, when k is different from 0, or to n, when $k = 0$. ∎

Remark: Taking $n = 2$, $x = i$, $u = j$, $xu = k$, one verifies that the tensor decomposition of the Galois element in Theorem 2.11 coincides with that of the V-Galois-Azumaya extension $\psi : F \longrightarrow H$ given in Example 2.10.

Similarly to the case of Hamilton's quaternion, where Theorem 1.3 shows that the inclusions $\mathbf{R} \longrightarrow \mathbf{C}$ and $\mathbf{C} \longrightarrow \mathbf{H}$ are both $\mathbf{Z}/2\mathbf{Z}$-Galois extensions, one deduce, with the notations adopted above, the following result:

Corollary 2.12. *Let F be a commutative field. Take two elements a and b in $F^\times$, and $n \geq 2$ an integer. Suppose that the multiplicative group $F^\times$ of F has an element ζ of order n and that the characteristic of F either is equal to zero or is positive and does not divide n. Let Q be the quotient ring $F[X]/(X^n - a)$. Then the extensions $F \longrightarrow Q$ and $Q \longrightarrow (a, b, \zeta)_F$ are $\mathbf{Z}/n\mathbf{Z}$-Galois. Moreover Q is the maximal commutative subring of $(a, b, \zeta)_F$.*

The maximality of Q in $(a, b, \zeta)_F$ is shown in [21] (Proposition 16.24). The definition of Q is in fact the usual cyclic extension performed over an n-kummerian ring ([10], Chapter 0, § 5) (recall that an *n-kummerian ring* is a commutative ring which contains n^{-1} and a root of the n-cyclotomic polynomial).

Corollary 2.13. *Let $n \geq 2$ be an integer and F be a commutative field such that the characteristic of F either is equal to zero or is positive and does not divide n. Then the extension $F \longrightarrow M_n(F)$ is $(\mathbf{Z}/n\mathbf{Z})^2$-Galois-Azumaya.*

Proof. The matrix algebra $M_n(F)$ is a particular case of n'th power norm residue algebras: choose a primitive n-th root of unity ζ and $a, b \in F^\times$, then $M_n(F)$ is isomorphic to $(a, b, \zeta)_F$ if (and only if) $b \in N_{E/F}(E^\times)$ or equivalently if (and only if) $a \in N_{K/F}(K^\times)$, where $E = F(a^{\frac{1}{n}})$, $K = F(b^{\frac{1}{n}})$, and $N_{L/F}$ is the norm map $L^\times \longrightarrow F^\times$ for any finite extension L/F ([21], Chapter 16). For instance $(1, b, \zeta)_F \cong M_n(F)$. ∎

3 The Brauer-Galois group of a commutative ring

3.1 The category $\mathfrak{Gal}_R$

We study some properties of the two subcategories of $\mathfrak{Gal}$ obtained by fixing a Galois group, or by fixing simultaneously a base ring and a Galois group (of course, an analogue work can be done starting with one of the categories $\mathfrak{Galstr}$, $\mathfrak{Galcent}$ or $\mathfrak{Galcom}$).

The functor $\pi_{alg} : \mathfrak{Gal} \longrightarrow \mathfrak{Alg}_k$, given on objects by $\pi_{alg}(G, \psi : R \longrightarrow S) = R$, enables us to consider the fibre category over a fixed algebra R. Denote it by $\mathfrak{Gal}_R$. Its objects are the couples $(G, \psi : R \longrightarrow S)$; a morphism from $(G, \psi : R \longrightarrow S)$ to $(G', \psi' : R \longrightarrow S')$ in $\mathfrak{Gal}_R$ is a couple (f, φ), where $f : G' \longrightarrow G$ is a morphism of groups and $\varphi : S \longrightarrow S'$ a morphism of algebras. These data are subject to the two conditions: $\varphi \circ \psi = \psi'$ and $\varphi \circ f(g') = g' \circ \varphi$, for any $g' \in G'$. Necessarily, φ is a morphism of R-rings.

Theorem 3.1. *Let R be a commutative algebra. Suppose that $(G, \psi : R \longrightarrow S)$ and $(G', \psi' : R \longrightarrow S')$ are two objects in $\mathfrak{Galcent}_R$ (repectively in $\mathfrak{GalAzum}_R$). Then the canonical extension $\psi'' : R \longrightarrow S \otimes_R S'$ is a centralizing (respectively central) $G \times G'$-Galois extension that we denote by $\psi \otimes \psi'$.*

Proof. Let $(G, \psi : R \longrightarrow S)$ and $(G', \psi' : R \longrightarrow S')$ be two centralizing Galois extensions. Since the ring R is commutative, the tensor product $S \otimes_R S'$ comes with the multiplication given by $(s \otimes s').(t \otimes t') = st \otimes s't'$, with $s, t \in S$ and $s', t' \in S'$. The group $K = G \times G'$ acts on $U = S \otimes_R S'$ by $(g, g') \cdot (s \otimes s') = g(s) \otimes g'(s')$, for $(g, g') \in K$ and $s \otimes s' \in U$. We must show that $\psi'' : R \longrightarrow U$ is K-Galois. In order to do that,

we successively prove that R can be identified with the ring U^K of invariants of U under K, that the associated morphism $\Gamma : U\otimes_R U \longrightarrow U(K)$ is an isomorphism, and finally that the extension $R \longrightarrow U$ is faithfully flat.

1) The inclusion $R \subseteq U^K$ is obvious. In order to prove $U^K \subseteq R$, we use an argument inspired by Chase-Harrison-Rosenberg [4] (Lemma 1.7) which involves descent. By [27] (Lemme 1.4.2), the trace morphisms $\mathrm{tr}_{S/R}$ and $\mathrm{tr}_{S'/R}$ are surjective. Choose $s_0 \in S$ and $s'_0 \in S'$ with $\mathrm{tr}_{S/R}(s_0) = \mathrm{tr}_{S'/R}(s'_0) = 1$. For any $u \in U^K$, the following equalities hold

$$u = \Big((\mathrm{tr}_{S/R}\otimes\mathrm{tr}_{S'/R})(s_0\otimes s'_0)\Big).u = \Big(\sum_{g\in G} g(s_0)\otimes \sum_{g'\in G'} g'(s'_0)\Big).u$$
$$= \sum_{(g,g')\in K}\Big(g(s_0)\otimes g'(s'_0)\Big).u = \sum_{(g,g')\in K}(g,g')\Big((s_0\otimes s'_0).u\Big) = (\mathrm{tr}_{S/R}\otimes\mathrm{tr}_{S'/R})\Big((s_0\otimes s'_0).u\Big),$$

that belongs to $\mathrm{Im}(\mathrm{tr}_{S/R}\otimes\mathrm{tr}_{S'/R}) = R\otimes_R R \cong R$.

2) The morphism $\Gamma : U\otimes_R U \longrightarrow U(K)$ defined by

$$\Gamma\Big((s\otimes s')\otimes(t\otimes t')\Big) = \sum_{(g,g')\in K}\Big(sg(s')\otimes tg'(t')\Big)\delta_{(g,g')}$$

is an isomorphism of left R-modules. Indeed, one may easily see that Γ is the composition $\beta \circ (\Gamma_S\otimes\Gamma_{S'}) \circ \alpha$, where $\alpha : U\otimes_R U \longrightarrow (S\otimes_R S)\otimes_R(S'\otimes_R S')$ and $\beta : S(G)\otimes_R S'(G') \longrightarrow (S\otimes_R S')(K)$ are the canonical isomorphisms.

3) Proposition 1.2 in [27] asserts that when $U^K = R$ and when $\Gamma : U\otimes_R U \longrightarrow U(K)$ is an isomorphism, then the extension $R \longrightarrow U$ is faithfully flat if and only if R is a direct summand of the (right or left) R-module U. The extension $R \longrightarrow S$ (respectively $R \longrightarrow S'$) being Galois, R is a direct summand of the R-module S (respectively S'). Hence $S\otimes_R S'$ contains $R\otimes_R R \cong R$ as a direct summand, because the tensor product preserves direct limits and consequently also direct sums.

Suppose now that $(G, \psi : R \longrightarrow S)$ and $(G', \psi' : R \longrightarrow S')$ are Galois-Azumaya. Since the centre $\mathcal{Z}(S\otimes_R S')$ of $S\otimes_R S'$ is isomorphic to $\mathcal{Z}(S)\otimes_R\mathcal{Z}(S')$ [7], the extension $\psi'' : R \longrightarrow S\otimes_R S'$ is $G\times G'$-Galois-Azumaya. ∎

Examples.

1.– Let F be a commutative field of characteristic different from 2 and let a_m, b_m $(m = 1, \ldots, n)$ be $2n$ non zero elements in F. Denote by H_m the quaternion algebra $(\dfrac{a_m, b_m}{F})$. By Theorem 3.1, the n-fold tensor product extension $F \longrightarrow H_1\otimes_F \ldots \otimes_F H_n$ is V^n-Galois. Observe that the tensor product $H_1 \otimes_F H_2$ of two quaternion algebras may be not a skew field. For instance, let F be the field $\mathbf{R}$ of the real numbers and $a = b = -1$. Thus $(\dfrac{-1,-1}{\mathbf{R}})$ is the field $\mathbf{H}$ of Hamilton's quaternions. The algebra $\mathbf{H}\otimes_{\mathbf{R}}\mathbf{H}$ is not a skew field, but is isomorphic to the matrix algebra $M_2(\mathbf{R})$ (see for example [8] (§ 14)). So, in the Brauer group $\mathrm{Br}(F)$, the class of $\mathbf{H}\otimes_{\mathbf{R}}\mathbf{H}$ is equal to the class of the quaternion algebra $(\dfrac{1,1}{\mathbf{R}})$. In fact, $H_1 \otimes_F H_2$ is not a skew field if and only if H_1 and H_2 have a common splitting field which is separable quadratic over F [8] (§ 14, Theorem 6).

2.– Let F be a commutative field of characteristic different from 2 and A central simple algebra of degree 4 and exponent 2 (recall that the exponent of an F-Azumaya algebra is the order, in the sense of Group Theory, of its class $[A]$ in the Brauer group $\mathrm{Br}(F)$). Then the extension $F \longrightarrow A$ is V^2-Galois-Azumaya. Indeed, following a well-known result of Albert [16], A is necessarily a biquaternion algebra, that is a tensor product of two quaternion algebras over F.

Proposition 3.2. *Fix a commutative algebra R. Let $\psi : R \longrightarrow S$ (respectively $\psi' : R \longrightarrow S'$) be a centralizing Galois extension with Galois group G (respectively G') of order n (respectively n'). Assume that the integer nn' is invertible in $S \otimes_R S'$. Then the extension $\varepsilon_1 : S \longrightarrow S \otimes_R S'$ given by $\varepsilon_1(s) = s \otimes 1$ $(s \in S)$ is G-Galois and the extension $\varepsilon_2 : S' \longrightarrow S \otimes_R S'$ given by $\varepsilon_2(s') = 1 \otimes s'$ $(s' \in S')$ is G'-Galois.*

Proof. Because of the condition on nn', the $G \times G'$-Galois extension $\psi \otimes \psi' : R \longrightarrow S \otimes_R S'$ becomes strict. Take the subgroup $H = \{1\} \times G'$ of $G \times G'$. By Theorem 1.3, the inclusion $\theta : U = (S \otimes_R S')^H \longrightarrow S \otimes_R S'$ is H-Galois. It is enough to show that $(S \otimes_R S')^H \cong S$.

Consider the right S'-module $M' = S \otimes_R S'$. Identifying $\{1\} \times G'$ with G', the group action on M' is given by $g'(s \otimes s') = s \otimes g'(s')$ $(g' \in G', s \in S, s' \in S')$. So M' is a G'-Galois module. By Galois descent for modules [26] (Corollary 4.16), the module $N' = {M'}^{G'}$ is such that $N' \otimes_R S' \cong M'$, that is $(S \otimes_R S)^{G'} \otimes_R S' \cong S \otimes_R S'$. By faithfully flatness of ψ', one concludes that $(S \otimes_R S)^{G'} \cong S$ and that $\varepsilon_2 : S' \longrightarrow S \otimes_R S'$ is G'-Galois. Similarly $\varepsilon_1 : S \longrightarrow S \otimes_R S'$ is G-Galois. ∎

Example. Take $F \longrightarrow H$ a quaternionic extension over a field F of characteristic different from 2. By Proposition 3.2, the two extensions $\varepsilon_i : H \longrightarrow H \otimes_F H$ $(i = 1, 2)$ are both V-Galois.

3.2 The Brauer-Galois group

Corollary 3.3. *Let R be a commutative algebra. Denote by $\mathrm{Br}_{\mathrm{Gal}}(R)$ the subset of the Brauer group of R consisting of those classes $\xi \in \mathrm{Br}(R)$ for which there exists a finite group G and a G-Galois-Azumaya extension $\psi : R \longrightarrow S$, such that ξ is equal to the class $[S]$ of S modulo stable isomorphisms. Then $\mathrm{Br}_{\mathrm{Gal}}(R)$ is a subgroup of $\mathrm{Br}(R)$.*

This group $\mathrm{Br}_{\mathrm{Gal}}(R)$ is called the *Brauer-Galois group of R.*

Proof. The neutral element of $\mathrm{Br}(R)$ is the class $[R]$. Since $\mathrm{id} : R \longrightarrow R$ is a $\{1\}$-Galois-Azumaya extension, $[R]$ belongs to $\mathrm{Br}_{\mathrm{Gal}}(R)$, and this set is therefore non-empty.

Let $\xi_1, \xi_2 \in \mathrm{Br}(R)$. Represent these classes by $\psi_1 : R \longrightarrow S_1$ and $\psi_2 : R \longrightarrow S_2$, two Galois-Azumaya extensions with Galois groups G_1 and G_2. The product $\xi_1.\xi_2 \in \mathrm{Br}(R)$ can then be represented by the R-Azumaya algebra $S_1 \otimes_R S_2$ (the multiplication in $S_1 \otimes_R S_2$ being given by $(s_1 \otimes s_2) \cdot (t_1 \otimes t_2) = s_1 t_1 \otimes s_2 t_2$, for any $s_1, t_1 \in S_1$ and $s_2, t_2 \in S_2$, is well defined since R is commutative and ψ_i $(i = 1, 2)$ is central). By Theorem 3.1, $\psi_1 \otimes \psi_2 : R \longrightarrow S_1 \otimes_R S_2$ is a $G_1 \times G_2$-Galois extension. Hence the set $\mathrm{Br}_{\mathrm{Gal}}(R)$ is stable under the product in $\mathrm{Br}(R)$.

The symmetric element of $[S]$ can be represented by the opposite algebra S^{o}. But if $\psi : R \longrightarrow S$ is a G-Galois-Azumaya extension, the group G acts on S^{o} by $g(s^{\mathrm{o}}) = \Big(g(s)\Big)^{\mathrm{o}}$. Since R is the centre of S, the map $\psi^{\mathrm{o}} : R \longrightarrow S^{\mathrm{o}}$ is well defined. It is a G-Galois extension by Lemma 1.4. ∎

Remark: A similar construction can be provided in the Hopf-Galois context when one replaces Galois-Azumaya extensions by Hopf-Galois-Azumaya extensions. This gives rise to a group $\mathrm{Br}_{\mathrm{HopfGal}}(R)$, the *Brauer-Hopf-Galois group of* R, which should be less interesting than $\mathrm{Br}_{\mathrm{Gal}}(R)$ since it is bigger: the inclusions $\mathrm{Br}_{\mathrm{Gal}}(R) \subseteq \mathrm{Br}_{\mathrm{HopfGal}}(R) \subseteq \mathrm{Br}(R)$ hold.

3.3 Some straightforward facts about the Brauer-Galois group

1) The Brauer-Galois group $\mathrm{Br}_{\mathrm{Gal}}(S)$ is obviously trivial when $\mathrm{Br}(S)$ is trivial. Therefore the group $\mathrm{Br}_{\mathrm{Gal}}(S)$ is trivial for any finite field $S = \mathbf{F}_q$ (by Wedderburn's Theorem on finite division rings), as well as for any algebraic extension of $\mathbf{F}_q$. It is also trivial for any algebraically closed field or for any field of transcendence degree one over an algebraically closed field (Tsen's Theorem) [9]. Other examples of commutative fields with trivial Brauer group can be found in [31] (p. 170).

2) Let F be a commutative field of characteristic different from 2 and $a, b \in F^{\times}$. Since $(\dfrac{a,b}{F})^{\mathrm{o}} \cong (\dfrac{a,b}{F})$, the quaternion algebra $(\dfrac{a,b}{F})$ is an element of order at most 2 in $\mathrm{Br}_{\mathrm{Gal}}(F)$. It is exactly of order two if and only if the Hilbert symbol $(a,b)_F$ is equal to 1, in other words if and only if $(\dfrac{a,b}{F})$ is not isomorphic to the matrix algebra $M_2(F)$ [30].

3) For any commutative field F of characteristic different from 2, the Brauer-Galois group $\mathrm{Br}_{\mathrm{Gal}}(F)$ contains the quaternion group $\mathrm{Quat}(F)$, that is the subgroup of $\mathrm{Br}(F)$ generated by the quaternion algebras (these lie in the 2-torsion). Under suitable conditions on the characteristic of F (see Theorem 2.11), the Brauer-Galois group $\mathrm{Br}_{\mathrm{Gal}}(F)$ contains the subgroup of $\mathrm{Br}(F)$ generated by the n'th power norm residue algebras (these lie in the n-torsion).

Next we shall use a deep result due to Merkurjev and Suslin in order to discuss the relationship between the n-torsion of $\mathrm{Br}_{\mathrm{Gal}}(F)$ and the n'th power norm residue algebras, for any $n \geq 2$. Before doing that, we have to make a short digression into K-theory.

3.4 Connection with Milnor's K_2 and the main Theorem

For any abelian group A and any integer $n \geq 2$, denote by ${}_nA$ the n-torsion subgroup of A, that is the part of A annihilated by the multiplication by n. Let F be a commutative field. Following a famous result of Matsumoto [21] (16.49), the Milnor's K_2-group $K_2(F)$ is generated by the symbols $\{a, b\}$ (with $a, b \in F^{\times}$) subject to the relations

$$\{ab, c\} = \{a, c\}\ \{b, c\}, \quad \{a, bc\} = \{a, b\}\ \{a, c\}, \quad \text{and} \quad \{a, b\} = 1 \ \text{ if } \ a + b = 1.$$

Suppose that the field F is such that the multiplicative group $F^\times$ has an element ζ of finite order n and such that its characteristic char$F$ does not divide n. Then the assignment $F^\times \otimes_{\mathbf{Z}} F^\times \longrightarrow \mathrm{Br}(F)$ defined by $r_{n,F}(\{a,b\}) = [(a,b,\zeta)_F]$ is a Steinberg symbol, hence defines a homomorphism of groups $R_{n,F} : K_2(F) \longrightarrow \mathrm{Br}(F)$. Furthermore $R_{n,F}$ annihilates ${}_nK_2(F)$ and takes its values in ${}_n\mathrm{Br}(F)$ (for all these facts, see [24]). Thus there exists a homomorphism $\bar{R}_{n,F} : K_2(F)/nK_2(F) = K_2(F) \otimes_{\mathbf{Z}} (\mathbf{Z}/n\mathbf{Z}) \longrightarrow {}_n\mathrm{Br}(F)$, called the *Galois symbol*, which is, following a celebrated and difficult Theorem proved by Merkurjev and Suslin [23], an isomorphism of groups (for the formulation we use, see [21]).

Theorem 3.4. *Let F be a commutative field, and $n \geq 2$ an integer. Suppose that the multiplicative group $F^\times$ of F has an element ζ of order n and that the characteristic of F either is equal to zero or is positive and does not divide n. Then the Steinberg symbol $F^\times \otimes_{\mathbf{Z}} F^\times \longrightarrow \mathrm{Br}(F)$ factorizes through $\mathrm{Br}_{\mathrm{Gal}}(F)$, hence*

$$ {}_n\mathrm{Br}_{\mathrm{Gal}}(F) = {}_n\mathrm{Br}(F). $$

In particular, if F is a commutative field of characteristic different from 2, then ${}_2\mathrm{Br}_{\mathrm{Gal}}(F) = {}_2\mathrm{Br}(F) = \mathrm{Quat}(F)$.

Proof. This result comes readily from Theorem 2.11, Corollary 3.3 and the Theorem of Merkurjev-Suslin. ∎

The case $n = 2$ already follows from a theorem of Merkurjev [22], which shows that the 2-torsion of the Brauer group is $\mathrm{Quat}(F)$. This result implies in particular that

- The Brauer-Galois group $\mathrm{Br}_{\mathrm{Gal}}(\mathbf{R})$ of the real numbers is equal to $\mathbf{Z}/2\mathbf{Z}$, since $\mathrm{Br}(\mathbf{R})$ is equal to $\mathbf{Z}/2\mathbf{Z}$ and is generated by Hamilton's quaternions $\mathbf{H}$ [28] (Example 3.8);
- The Brauer-Galois group $\mathrm{Br}_{\mathrm{Gal}}(\mathbf{Q})$ of the rational numbers is infinite, since $\mathrm{Quat}(\mathbf{Q})$ is infinite (see the classification of quaternion algebras via quadratic forms [9]).

Corollary 3.5. *Let F be a commutative field of characteristic zero such that, for any $n \geq 2$, the multiplicative group $F^\times$ of F has an element of order n. Then*

$$ \mathrm{Br}_{\mathrm{Gal}}(F) = \mathrm{Br}(F). $$

Proof. The group $\mathrm{Br}(F)$ is torsion ([9], Corollary 4.15), hence as sets

$$ \mathrm{Br}(F) = \bigcup_{n\geq 1} {}_n\mathrm{Br}(F) = \bigcup_{n\geq 1} {}_n\mathrm{Br}_{\mathrm{Gal}}(F) = \mathrm{Br}_{\mathrm{Gal}}(F). $$

∎

Notice that the conditions that have to be satisfied by the field F do not imply that F is algebraically closed (in which case Corollary 3.5 would be vacuous, the Brauer group of an algebraically closed field being trivial). For example take $F = \mathbf{Q}_{\mathrm{ab}} = \bigcup_{n\geq 1} \mathbf{Q}(\boldsymbol{\mu}_n(\mathbf{C}))$, the field obtained by adjoining all roots of unity

to the rationals. Then F is of characteristic zero and is strictly contained in the algebraic closure $\bar{\mathbf{Q}}$ of $\mathbf{Q}$. Indeed, in the absolute Galois group $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, the only non-trivial torsion elements have order 2 ([19], VI, § 9, Example 1), whereas $\mathrm{Gal}(\mathbf{Q}_{\mathrm{ab}}/\mathbf{Q}) = \varprojlim_n \mathrm{Gal}\Big(\mathbf{Q}(\boldsymbol{\mu}_n(\mathbf{C}))/\mathbf{Q}\Big) = \varprojlim_n (\mathbf{Z}/n\mathbf{Z})^\times$ is isomorphic to the group $\hat{\mathbf{Z}}^\times$ of invertible elements of the Prüfer ring $\hat{\mathbf{Z}} = \varprojlim_n (\mathbf{Z}/n\mathbf{Z}) = \prod_{p \text{ prime}} \mathbf{Z}_p$; therefore $\mathrm{Gal}(\mathbf{Q}_{\mathrm{ab}}/\mathbf{Q}) \cong \prod_{p\neq 2 \text{ prime}} \mathbf{Z}/(p-1)\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ ([25], VI, Satz 5.1).

Question. Does there exist a commutative field – or even a ring – K such that $\mathrm{Br}_{\mathrm{Gal}}(K)$ is strictly contained in $\mathrm{Br}(K)$?

This problem looks rather difficult to solve since very few is known in general about Brauer groups. A natural candidate seems to be an infinite field K of characteristic 2. Indeed, there exists then a central simple K-algebra which is not Galois over K (namely the quaternion algebra $H_{a,b} = [\frac{a,b}{K})$ over K of counter-example 1.2). The technics involved here however do not allow to show that under suitable conditions none of the representants of $[H_{a,b}] \in \mathrm{Br}(K)$ is Galois.

3.5 The category $\mathfrak{Gal}_R(G)$ and base change

Denote by π^{gr}_{alg} the functor from $\mathfrak{Gal}$ to $\mathfrak{Gpf}^{\mathrm{o}} \times \mathfrak{Alg}_k$ defined by $\pi^{gr}_{alg}(G, \psi : R \longrightarrow S) = (G, R)$. Introduce the fibre category, denoted by $\mathfrak{Gal}_R(G)$, of π^{gr}_{alg} over (G, R). Its objects are the G-Galois extensions $\psi : R \longrightarrow S$, with R and G fixed. A morphism from $\psi : R \longrightarrow S$ to $\psi : R \longrightarrow S'$ in $\mathfrak{Gal}_R(G)$ is G-equivariant morphism of R-rings $\varphi : S \longrightarrow S'$. The full subcategories $\mathfrak{Galstr}_R(G)$, $\mathfrak{Galcent}_R(G)$, $\mathfrak{GalAzum}_R(G)$ and $\mathfrak{Galcom}_R(G)$ of $\mathfrak{Gal}_R(G)$ are defined in an obvious way.

Le Bruyn, van den Bergh and van Oystaeyen proved that if $\psi : R \longrightarrow S$ is a Galois extension of *commutative* rings for some finite group G, and if T is an arbitrary R-algebra, then $T \longrightarrow S \otimes_R T$ is also a G-Galois extension ([20], Lemma II.5.1.13). Next we state another version of base change, assuming that the initial Galois extension is centralizing or central and the algebra T is commutative.

Proposition 3.6. *(Base change over an extension of commutative rings). Let R be a commutative algebra and G a finite group. A morphism of commutative algebras $\varrho : R \longrightarrow T$ induces two* "extension of the scalars by T" *functors $\varrho_! : \mathfrak{Galcent}_R(G) \longrightarrow \mathfrak{Galcent}_T(G)$ and ${}_!\varrho : \mathfrak{Galcent}_R(G) \longrightarrow \mathfrak{Galcent}_T(G)$ (resp. $\varrho_! : \mathfrak{GalAzum}_R(G) \longrightarrow \mathfrak{GalAzum}_T(G)$ and ${}_!\varrho : \mathfrak{GalAzum}_R(G) \longrightarrow \mathfrak{GalAzum}_T(G)$) defined by*

$$\varrho_!(\psi : R \longrightarrow S) = (\psi_T : T \longrightarrow T \otimes_R S) \text{ and } {}_!\varrho(\psi : R \longrightarrow S) = ({}_T\psi : T \longrightarrow S \otimes_R T),$$

where, for any $t \in T$,

$$\psi_T(t) = t \otimes 1 \quad \text{and} \quad {}_T\psi(t) = 1 \otimes t.$$

Proof. We show the proposition for instance for the left extension of the scalars by T. The proof paraphrases the one of Theorem 3.1. The group G acts on $U = T \otimes_R S$

by $g(t\otimes s) = t\otimes g(s)$, for $g \in G$ and $t\otimes s \in U$. The abelian group $U = T\otimes_R S$ is clearly a left T-module. Let it also be a right T-module by the formula $(t\otimes s)\cdot t' = tt'\otimes s$, for $t, t' \in T$ and $s \in S$. Since T is commutative, U becomes symmetric as a T-module.

1) It is clear that $T \cong T\otimes_R R \subseteq U^G$. A descent argument analogue to the one used in Theorem 3.1 shows that if $u \in U^G$, then $u \in \mathrm{Im}(\mathrm{id}_T\otimes \mathrm{tr}_{S/R}) = T\otimes_R R \cong T$, because $u = (\mathrm{id}_T\otimes \mathrm{tr}_{S/R})\Big((1\otimes s_0)u\Big)$, for any fixed $s_0 \in S$ which verifies $\mathrm{tr}_{S/R}(s_0) = 1$. Indeed, set $u = \sum_{i=1}^{m} t_i\otimes s_i$. For any $g \in G$, one has $u = \sum_{i=1}^{m} t_i\otimes g(s_i)$. So

$$u = (1\otimes 1)\cdot u = (\mathrm{id}_T\otimes \mathrm{tr}_{S/R})\Big((1\otimes s_0)u\Big) = (\mathrm{id}_T\otimes \mathrm{tr}_{S/R})\Big(\sum_{i=1}^{m}(t_i\otimes s_0 s_i)\Big)$$
$$= \sum_{g\in G}\sum_{i=1}^{m}\Big(t_i\otimes g(s_0)g(s_i)\Big) = \sum_{g\in G}\Big(1\otimes g(s_0)\Big)\Big(\sum_{i=1}^{m} t_i\otimes g(s_i)\Big) = \sum_{g\in G}\Big(1\otimes g(s_0)\Big)u.$$

2) The morphism $\Gamma : U\otimes_T U \longrightarrow U(G)$ defined by

$$\Gamma(u\otimes u') = \sum_{g\in G} ug(u')\delta_g$$

is an isomorphism of left T-modules as a composition $\beta \circ (\mathrm{id}_T\otimes\Gamma_S) \circ \alpha$, where $\alpha : U\otimes_R U \longrightarrow T\otimes_R S\otimes_R S$ and $\beta : T\otimes_R\Big(S(G)\Big) \longrightarrow U(G)$ are the canonical isomorphisms.

3) At last, T is a direct summand in U, since R is a direct summand in S and the base change functor $T\otimes_R -$ preserves direct limits, hence direct sums. ∎

Applications 3.7.

– *Localization.* Let $\psi : R \longrightarrow S$ be a centralizing G-Galois extension and Σ be a multiplicative subset of R. Then G acts on the localized algebra $\Sigma^{-1}S = \Sigma^{-1}R\otimes_R S$ of S by Σ via the formula

$$g(\frac{s}{u}) = \frac{g(s)}{u},$$

for $s \in S$ and $u \in \Sigma$. The localized morphism $\Sigma^{-1}\psi : \Sigma^{-1}R \longrightarrow \Sigma^{-1}S$ remains a centralizing G-Galois extension. In particular, for any prime ideal $\wp \in \mathrm{Spec}(R)$ (respectively maximal ideal $\mathfrak{m} \in \mathrm{Max}(R)$), the morphism of local rings $\psi_\wp : R_\wp \longrightarrow S_\wp$ (respectively $\psi_\mathfrak{m} : R_\mathfrak{m} \longrightarrow S_\mathfrak{m}$) is G-Galois.

– *The case of commutative rings.* The opposite functor $\pi_{alg}^{opp} : \mathfrak{Galcomm}^{opp} \longrightarrow \mathfrak{Aff}_k$ to the functor π_{alg} defined on $\mathfrak{Galcomm}$ with values in $\mathfrak{Algcom}_k$ enables us to build over any affine k-scheme $\mathrm{Spec}R$ the fibre category of π_{alg} denoted $\mathfrak{Galcomm}_R^{opp}$. Every morphism of affine k-schemes $f : \mathrm{Spec}T \longrightarrow \mathrm{Spec}R$ (or equivalently, every morphism of commutative algebras $\theta : R \longrightarrow T$) induces then a base change functor $f^* = \theta_!^{opp} : \mathfrak{Galcomm}_R^{opp} \longrightarrow \mathfrak{Galcomm}_T^{opp}$. Observe that the collection of these data is coherent in the following sense: if f and g are composable morphisms of affine schemes, there exists a natural transformation $\phi_{f,g} : (f\circ g)^* \simeq g^*\circ f^*$.

Corollary 3.8. *The assignment* $R \longmapsto \mathrm{Br}_{\mathrm{Gal}}(R)$ *defines a functor* $\mathrm{Br}_{\mathrm{Gal}}$ *from the category* $\mathfrak{Algcom}_k$ *of commutative algebras to the category of groups. For each morphism* $\varrho : R \longrightarrow S$ *in* $\mathfrak{Algcom}_k$*, the map* $\mathrm{Br}_{\mathrm{Gal}}(\varrho)$ *is the homomorphism of groups* $\mathrm{Br}_{\mathrm{Gal}}(R) \longrightarrow \mathrm{Br}_{\mathrm{Gal}}(S)$ *induced by the extension of the scalars* $\varrho : R \longrightarrow S$*.*

Proof. Let $\varrho : R \longrightarrow S$ be a morphism in $\mathfrak{Algcom}_k$. The assignment $A \longmapsto A \otimes_R S$ induces a $\mathbf{Z}$-homomorphism $\mathrm{Br}(\varrho) : \mathrm{Br}(R) \longrightarrow \mathrm{Br}(S)$ ([9], Theorem 8.9). By base change over the commutative algebra morphism $R \longrightarrow S$ (Proposition 3.6), the Brauer functor $\mathrm{Br} : \mathfrak{Algcom}_k \longrightarrow \mathfrak{Gp}$ restricts to $\mathrm{Br}_{\mathrm{Gal}}(\varrho) : \mathrm{Br}_{\mathrm{Gal}}(R) \longrightarrow \mathrm{Br}_{\mathrm{Gal}}(S)$. ∎

Example 3.9. Let K be a global field and Ω be a complete set of valuations of K. For each $v \in \Omega$, let K_v be the completion of K at v. The collection of group homomorphisms $\mathrm{Br}_{\mathrm{Gal}}(K) \longrightarrow \mathrm{Br}_{\mathrm{Gal}}(K_v)$ deduced from $K \longrightarrow K_v$ provides a map $\beta : \mathrm{Br}_{\mathrm{Gal}}(K) \longrightarrow \bigoplus_{v \in \Omega} \mathrm{Br}_{\mathrm{Gal}}(K_v)$ which is a monomorphism of groups. Indeed, the injectivity of β immediately results from the short exact sequence

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \bigoplus_{v \in \Omega} \mathrm{Br}(K_v) \longrightarrow \mathbf{Q}/\mathbf{Z} \longrightarrow 0$$

obtained in the classical theory of Hasse-Brauer-Noether-Albert ([11], Chap. 13).

3.6 The relative Brauer-Galois group

Let $\varrho : R \longrightarrow S$ be a morphism of commutative algebras and let $\mathrm{Br}(\varrho)$ be the homomorphism of groups $\mathrm{Br}(R) \longrightarrow \mathrm{Br}(S)$ induced by ψ. The kernel of $\mathrm{Br}(\varrho)$ is called the *relative Brauer group of* ϱ and is denoted by $\mathrm{Br}(S/R)$. If A is an R-Azumaya algebra such that its Brauer class $[A]$ lies in $\mathrm{Br}(S/R)$, one says that S *splits* A. Corollary 3.8 allows us to define the *relative Brauer-Galois group of* $\varrho : R \longrightarrow S$, denoted by $\mathrm{Br}_{\mathrm{Gal}}(S/R)$, to be the kernel of $\mathrm{Br}_{\mathrm{Gal}}(\varrho)$; it is a subgroup of $\mathrm{Br}(S/R)$.

Remarks.
1.– When $R = K$ is a commutative field and A is a K-Azumaya algebra, A is split by some finite commutative Galois extension of K, say L, with Galois group $G = \mathrm{Gal}(L/K)$ ([28], Corollary 3.15). This strong result does not allow any conclusion about conditions whether $K \longrightarrow A$ should be Galois or not.
2.– If $\psi : R \longrightarrow S$ is a finite Galois extension of commutative rings with Galois group $G = \mathrm{Gal}(S/R)$ such that the Picard group $\mathrm{Pic}(S)$ of S is trivial, then there is a well known cohomological characterization of the relative Brauer group ([28], Theorem 7.12): the group $\mathrm{Br}(S/R)$ is isomorphic to the Galois 2-cohomology group $H^2(G, S^\times)$. Hence $\mathrm{Br}_{\mathrm{Gal}}(S/R)$ corresponds to a subgroup $H^2_{\mathrm{Gal}}(G, S^\times)$ contained in $H^2(G, S^\times)$.

Acknowledgments: The author wishes to thank Lars Kadison for many useful comments on an early version of this paper.

References

[1] M. AUSLANDER, O. GOLDMAN: The Brauer group of a commutative ring, *Trans. Amer. Math. Soc.* **97**, (1960), 367 – 409.

[2] A. BLANCHARD: *Les corps non commutatifs*, Presses Universitaires de France, Paris (1972).

[3] N. BOURBAKI: *Algèbre commutative*, Chap. 1 et 2, Hermann, Paris, (1961).

[4] S. CAENEPEEL, G. MILITARU , S. ZHU: *Frobenius and separable functors for generalized module categories and nonlinear equations*, Lecture Notes in Mathematics 1787, Springer-Verlag, Berlin – Heidelberg – New York – Barcelona – Hong-Kong – London – Milan – Paris – Tokyo (2002).

[5] S. U. CHASE, D. K. HARRISON, A. ROSENBERG: Galois theory and cohomology of commutative rings, *Memoirs of the A.M.S.,* Number 52 (1965).

[6] S. U. CHASE, M. E. SWEEDLER: *Hopf algebras and Galois theory*, Lecture Notes in Math. 97, Springer-Verlag, Berlin – Heidelberg – New York (1969).

[7] F. DEMEYER, E. INGRAHAM: *Separable algebras over commutative rings*, Lecture Notes in Mathematics 181, Springer-Verlag, Berlin – Heidelberg – New York (1971).

[8] P. K. DRAXL: *Skew fields*, London Mathematical Society Lecture Note Series **81**, Cambridge University Press, Cambridge (1983).

[9] B. FARB, R.K. DENNIS: *Noncommutative algebra*, Graduate Texts in Mathematics, Vol. 144, Springer-Verlag, Berlin – Heidelberg – New York (1993).

[10] C. GREITHER: *Cyclic Galois extensions of commutative rings*, Lecture Notes in Math. 1534, Springer-Verlag, Berlin – Heidelberg (1992).

[11] A. J. HAHN: *Quadratic algebras, Clifford algebras, and arithmetic Witt groups*, Universitext, Springer-Verlag, Berlin – Heidelberg – New-York (1993).

[12] L. KADISON: *New examples of Frobenius extensions*, University Lecture Series, Vol. 14, American Mathematical Society, Providence R.I. (1999).

[13] T. KANZAKI: On commutator rings and Galois theory of separable algebras, *Osaka J. Math.* **1** (1964), 103 – 115 ; Correction, *ibid.* **1** (1964), 253.

[14] C. KASSEL: *Quantum groups*, Graduate Texts in Mathematics, Vol. 155, Springer-Verlag, Berlin – Heidelberg – New York (1995).

[15] M. A. KNUS: *Quadratic and hermitian forms over rings*, Grundlehren der mathematischen Wissenschaften 294, Springer-Verlag, Berlin – Heidelberg – New York (1991).

[16] M. A. KNUS, A. MERKURJEV, M. ROST, J.-P. TIGNOL: *The Book of Involutions*, American Mathematical Society, Colloquium Publications, Volume 44, Providence (1998).

[17] M. A. KNUS, M. OJANGUREN: *Théorie de la descente et algèbres d'Azumaya*, Lecture Notes in Mathematics 389, Springer-Verlag, Berlin – Heidelberg – New York (1974).

[18] H. F. KREIMER, M. TAKEUCHI: Hopf algebras and Galois extensions of an algebra, *Indiana Univ. Math. J.*, Vol. **30** (1981), 675 – 692.

[19] S. LANG: *Algebra*, Third edition, Addison Wesley (1997).

[20] L. LE BRUYN , M. VAN DEN BERGH, F. VAN OYSTAEYEN: *Graded orders*, Birkhäuser, Boston – Basel (1988).

[21] B. A. MAGURN: *An algebraic introduction to K-Theory*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge (2002).

[22] А. С. МЕРКУРЬЕВ: О гомоморфизме норменного вычета степени два, *Докл. АН СССР*, т. **264**, № 3 (1981), 542 – 547. *English translation:* A. S. MERKUR'EV: On the norm residue symbol of degree 2, *Soviet Math. Dokl.*, Vol. **24(3)** (1981), 546 – 551.

[23] А. С. МЕРКУРЬЕВ , А. А. СУСЛИН: K-когомологии многообразий Севери-Брауэра и гомоморфизм норменного вычета, *Изв. АН СССР, Сер. Мат.*, т. **46**, № 5 (1983), 1011 – 1046, 1135 – 1136. *English translation:* A. S. MERKUR'EV, A. A. SUSLIN: K-cohomology of Severi-Brauer varieties and the norm residue homomorphism, *Math. USSR – Izv.*, Vol. **21(2)** (1983), 307 – 340.

[24] J. MILNOR: *Introduction to algebraic K-Theory*, Annals of Mathematics Studies, Princeton University Press, Princeton (1971).

[25] J. NEUKIRCH: *Algebraische Zahlentheorie*, Springer-Verlag, Berlin – Heidelberg – New York – London (1992).

[26] P. NUSS: Noncommutative descent and nonabelian cohomology, *K-Theory* **12** (1997), 23 – 74.

[27] P. NUSS: Extensions galoisiennes non commutatives : normalité, cohomologie non abélienne, *Communications in Algebra* **28 (7)** (2000), 3223 – 3251.

[28] M. ORZECH, C. SMALL: *The Brauer group of commutative rings*, Lecture Notes in pure and applied Mathematics 11, Marcel Dekker Inc., New York (1975).

[29] R. S. PIERCE: *Associative algebras*, Graduate Texts in Mathematics, Vol. 88, Springer-Verlag, Berlin – Heidelberg – New York (1982).

[30] J. ROSENBERG: *Algebraic K-theory and its applications*, Graduate Texts in Mathematics, Vol. 147, Springer-Verlag, Berlin – Heidelberg – New York (1994).

[31] J.-P. SERRE: *Corps locaux*, Troisième édition corrigée, Hermann, Paris (1968).

Institut de Recherche Mathématique Avancée,
Université Louis-Pasteur et CNRS, 7, rue René-Descartes,
67084 Strasbourg Cedex, France.
e-mail: nuss@math.u-strasbg.fr