Bull. Soc. math. France,
126, 1998, p. 1–49.

UN FONCTEUR NORME

PAR DANIEL FERRAND (*)

RÉSUMÉ. — Pour R-algèbre S, finie et localement libre, nous proposons une nouvelle définition du foncteur norme : S-**Mod** $\to$ R-**Mod**, qui en étend l'existence (S peut être ramifiée sur R) et qui en facilite l'emploi (car il est vu comme la solution d'un problème universel).

ABSTRACT. — A NORM FUNCTOR. — Let S be a finite and locally free R-algebra, and let norm : $S \to R$ be the usual norm map. We construct a functor N : S-**Mod** $\to$ R-**Mod** which extends both the "Corestriction" introduced by C. Riehm when S/R is a finite separable fields extension, and its generalisation by Knus and Ojanguren in case where S is étale over R. Unlike these, the definition we give does not rely upon descent methods, but it rather uses a universal property : $N(F)$ is equipped with a R-polynomial law $\nu_F : F \to N(F)$ satisfying the relations $\nu_F(sx) = \mathrm{norm}(s)\nu_F(x)$, for $s \in S$ and $x \in F$, and the couple $(N(F), \nu_F)$ is universal for these properties. We thus get a well defined functor even if S is ramified over R, but then the image of a projective S-module may fail to be projective over R. Nevertheless, the norm of an invertible S-module is always invertible and for these modules our construction gives the classical one. Moreover, if S is locally of the form $R[X]/(P)$, then $N(F)$ is projective over R for any projective S-module (of finite type); but that fails to be true if $R \to S$ is only supposed to be a complete intersection morphism. These points are discussed in some details before we focus on the etale case in order to emphasize the isomorphism between the "Weil restriction" and the norm functor (when applied to commutative algebras), and the intricate relations between $N(S \otimes E)$ and $E^{\otimes d}$ for a R-module E.

(*) Texte reçu le 24 décembre 1996, révisé le 6 février 1998, accepté le 2 mars 1998.
D. FERRAND, Institut Mathématique de Rennes, Campus de Beaulieu, 35042 Rennes CEDEX (France). Email : ferrand@univ-rennes1.fr.

Mots clés : corestriction, norme, transfert, restriction de Weil, algèbre d'Azumaya, puissances divisées.

Classification AMS : 13 B 40, 14 E 22, 14 F 20, 55 R 12.

0. Introduction

0.1. — Vue de loin, une norme (au sens algébrique) transforme une somme d'objets en leur produit ou, ce qui revient au même, une norme associe à un morphisme l'ensemble de ses sections (un morphisme $X \to S$ décompose X en la somme $\coprod X_s$ de ses fibres X_s, et une section de $X \to S$ est un élément du produit $\prod X_s$). Cet aspect géométrique, dans l'esprit de la restriction de Weil, éloquent pour les revêtements, réapparaîtra après le détour algébrique nécessaire pour prendre en compte la ramification.

Voici le point de départ algébrique : pour un anneau commutatif R et la R-algèbre $R \to R^d$, l'application norme transforme l'élément $(x_1, \ldots, x_d) \in R^d$ en le produit $x_1 \cdots x_d$ de ses composantes, et le foncteur norme transforme un R^d-module, c'est-à-dire une suite $(E_1, \ldots, E_d)$ de R-modules, en leur produit tensoriel $E_1 \otimes_R \cdots \otimes_R E_d$.

0.2. — Le but de ce travail est de construire, pour un morphisme $R \to S$ fini localement libre, un foncteur

$$N_{S/R} : S\text{-}\mathbf{Mod} \longrightarrow R\text{-}\mathbf{Mod}$$

qui généralise le précédent.

Cette généralisation est guidée par l'application de corestriction, qui est bien définie sur les groupes de cohomologie (étale) de $\mathbf{G}_m$; en dimensions 0, 1 et 2, ces groupes classifient respectivement les éléments inversibles, les modules inversibles et les algèbres d'Azumaya, objets sur lesquels peut porter le foncteur en question ; il serait souhaitable que la corestriction soit induite par le foncteur norme, dans les situations où cela a un sens. Il n'est pas nécessaire d'expliciter ce souhait car deux propriétés « minimales » s'imposent immédiatement et s'avèreront suffisantes pour caractériser un « foncteur norme » :

(N1) $N_{S/R}(S) = R$, et l'image par $N_{S/R}$ de la multiplication par $s \in S$ est la multiplication dans R par la norme usuelle

$$\operatorname{norm}_{S/R}(s) := \det(x \mapsto sx).$$

(N2) Le foncteur norme commute aux changements de base sur R : pour toute R-algèbre R', notant $S' = R' \otimes_R S$, les foncteurs suivants sont isomorphes :

$$F \mapsto R' \otimes_R N_{S/R}(F) \quad \text{et} \quad F \mapsto N_{S'/R'}(R' \otimes_R F).$$

Ces deux propriétés de bon sens imposent, à elles seules, la définition introduite dans ce texte : supposons, en effet, qu'il existe un foncteur N vérifiant (N1) et (N2) ; la fonctorialité et (N1) impliquent, pour tout S-module F, l'existence d'une application

$$F = \operatorname{Hom}_S(S, F) \longrightarrow \operatorname{Hom}_R(NS, NF) = \operatorname{Hom}_R(R, NF) = NF\,;$$

cette application, notée $\nu_F : F \to NF$, possède, toujours d'après (N1), la propriété suivante

$$\nu_F(sx) = \operatorname{norm}_{S/R}(s)\nu_F(x), \quad \text{pour } s \in S \text{ et } x \in F. \tag{0.2.1}$$

On dira, faute de mieux, qu'une application est *normique* si, après tout changement de base $R \to R'$, la relation (0.2.1) est vérifiée.

L'application $\nu_F : F \to NF$ ne peut être linéaire (pour $F = S$, c'est l'application norme) ; le mieux que l'on puisse prescrire est que ν_F soit polynomiale, ou, plus exactement, une loi polynôme, c'est-à-dire qu'elle soit compatible à tous les changements de base sur R : pour tout morphisme de R-algèbres $R' \to R''$ le carré suivant doit être commutatif (on a posé $F' = R' \otimes_R F$, $S' = R' \otimes_R S$, *etc.*)

$$\begin{array}{ccccc}
R' \otimes_R F = F' & \xrightarrow{\nu_{F'}} & N_{S'/R'}(F') & \xrightarrow{\sim} & R' \otimes_R N_{S/R}(F) \\
{\scriptstyle \mathrm{can}}\Big\downarrow & & & & \Big\downarrow{\scriptstyle \mathrm{can}} \\
R'' \otimes_R F = F'' & \xrightarrow{\nu_{F''}} & N_{S''/R''}(F'') & \xrightarrow{\sim} & R'' \otimes_R N_{S/R}(F).
\end{array}$$

Cela justifie la caractérisation suivante :

Le foncteur norme $N_{S/R}$ associe à tout S-module F un R-module $N_{S/R}(F)$, muni d'une loi polynôme normique

$$\nu_F : F \longrightarrow N_{S/R}(F),$$

le couple $(N_{S/R}(F), \nu_F)$ étant universel pour ces propriétés.

0.3. — Qu'une notion aussi générale soit cependant féconde fut une première surprise. Ce foncteur est isomorphe, en effet, à celui évoqué plus haut lorsque $S = R^d$; mieux, il est aussi isomorphe au foncteur corestriction introduit par Riehm lorsque S/R est une extension finie séparable de corps ; mais la corestriction de Riehm est définie comme le sous-espace des invariants sous l'action d'un groupe de Galois, c'est-à-dire comme un noyau, ce qui rend son maniement beaucoup plus malaisé que celui du foncteur norme proposé ici ; ainsi, la méthode à peu près constante pour établir les propriétés du foncteur norme est d'une désarmante simplicité (du moins lorsque $R \to S$ est étale) ; elle consiste à :

1) établir l'existence d'un morphisme en utilisant la propriété universelle ;

2) faire un changement de base fidèlement plat pour décomposer S en R^d ;

3) montrer que le morphisme exhibé en 1) est alors un isomorphisme par des arguments essentiellement combinatoires portant sur l'ensemble fini $\{1, \ldots, d\}$.

0.4. — Autre surprise, mais désagréable, celle-là : si le morphisme $R \to S$ est trop ramifié, le foncteur norme ne préserve plus la projectivité des modules ; c'est cependant le cas si la R-algèbre S est localement monogène, en particulier, bien sûr, si elle est étale ; mais on donne un exemple de morphisme fini d'intersection complète, libre de rang 4, pour lequel $N(S^2)$ n'est pas libre.

Je remercie le rapporteur pour ses questions ; elles m'ont conduit à modifier certaines parties et à en ajouter d'autres ; en particulier, 4.4 et le § 7 ne figuraient pas dans un état antérieur de ce texte.

1. Liste des principales propriétés du foncteur norme

Pour tout morphisme $R \to S$, fini et localement libre, il existe un foncteur
$$N_{S/R} : S\text{-}\mathbf{Mod} \longrightarrow R\text{-}\mathbf{Mod}$$
ayant les propriétés suivantes :

(N1) $N_{S/R}(S) = R$, et l'image par $N_{S/R}$ de la multiplication par $s \in S$ est la multiplication dans R par la norme usuelle
$$\operatorname{norm}_{S/R}(s) := \det(x \mapsto sx).$$

(N2) Le foncteur norme commute aux changements de base sur R : pour toute R-algèbre $R \to R'$, notant $S' = R' \otimes_R S$, les foncteurs suivants, en le S-module F, sont isomorphes
$$F \longmapsto R' \otimes_R N_{S/R}(F) \quad \text{et} \quad F \longmapsto N_{S'/R'}(R' \otimes_R F).$$

(N3) Le foncteur norme est caractérisé par la propriété suivante : $N_{S/R}$ associe à tout S-module F un R-module $N_{S/R}(F)$, muni d'une loi polynôme
$$\nu_F : F \longrightarrow N_{S/R}(F),$$
vérifiant après tout changement de base la relation (analogue à)
$$\nu_F(sx) = \operatorname{norm}_{S/R}(s)\nu_F(x), \quad \text{pour } s \in S \text{ et } x \in F,$$
le couple $(N_{S/R}(F), \nu_F)$ étant universel pour ces propriétés.

(N4) Lorsque $S = R^d$, et que le S-module F s'écrit $F = E_1 \times \cdots \times E_d$, on a
$$N_{S/R}(F) = E_1 \otimes_R \cdots \otimes_R E_d.$$

(N5) Si L est un S-module inversible (et si S est de rang d), on a un isomorphisme fonctoriel
$$N_{S/R}(L) \simeq \operatorname{Hom}_R(\wedge^d S, \wedge^d L).$$

(N6) Si F' et F'' sont des S-modules, il existe un morphisme fonctoriel

$$\varphi_{F',F''} : N_{S/R}(F') \otimes_R N_{S/R}(F'') \longrightarrow N_{S/R}(F' \otimes_S F'')\,;$$

en particulier, pour une S-algèbre B, $N_{S/R}(B)$ est une R-algèbre. Si S est étale sur R, alors $\varphi_{F',F''}$ est un isomorphisme.

(N7) Si F' et F'' sont des S-modules, il existe un morphisme fonctoriel

$$\psi : N_{S/R}\big(\mathrm{Hom}_S(F', F'')\big) \longrightarrow \mathrm{Hom}_R\big(N_{S/R}F', N_{S/R}F''\big).$$

C'est un isomorphisme si S est étale sur R, et si F' est un S-module projectif de type fini.

(N8) Lorsque S est une R-algèbre localement monogène de rang d, et que F est un S-module projectif de rang m, alors $N_{S/R}(F)$ est un R-module projectif de rang m^d.

2. Puissances divisées

2.1 Conventions et notations.

2.1.1. — Les anneaux considérés dans ce texte sont commutatifs et unitaires. Et, à part cela, quelconques. En particulier, il n'y a pas de restriction de caractéristique avant le § 7.

Les constructions et résultats présentés ici s'étendent immédiatement au cas d'un morphisme de schémas, fini, de présentation finie et plat.

2.1.2. — Deux adverbes sont utilisés fréquemment :

• « *Localement sur R* » signifie le plus souvent « *après un changement de base fidèlement plat $R \to R'$* » ; dans certains cas, notamment lorsque des constructions dépendent du rang de S sur R, et que ce rang n'est pas constant, il faut penser à une « *localisation* » un peu plus fine : « *il existe une famille finie (R_i) de R-algèbres telle que le morphisme $R \to \prod R_i$ soit fidèlement plat, et telle que la propriété envisagée soit vraie après chaque changement de base $R \to R_i$* ». Pour un module de type fini, être localement libre équivaut à être projectif de type fini, ou encore à être facteur direct d'un module libre de rang fini.

• « *Universellement* » signifie « *après tout changement de base* ».

2.1.3. — Pour un ensemble I, on note $\mathbb{N}^{(I)}$ l'ensemble des applications $\boldsymbol{a} : I \to \mathbb{N}$ à support fini (appelées parfois *multiindices*). Pour un entier d, on note $\Gamma_d I \subset \mathbb{N}^{(I)}$ l'ensemble des multiindices $\boldsymbol{a}$ dont le poids $\sum a(i)$ est égal à d. Pour I fini, on a :

$$\operatorname{Card}(\Gamma_d I) = \binom{\operatorname{Card} I + d - 1}{d}.$$

2.1.4. — Pour un multiindice $\boldsymbol{a} : I \to \mathbb{N}$, on pose

$$((\boldsymbol{a})) = \frac{\left(\sum a(i)\right)!}{\prod\left(a(i)!\right)}.$$

C'est un entier, appelé le *coefficient multinomial* de $\boldsymbol{a}$. En particulier, pour deux entiers $p, q \geq 0$, on a $((p, q)) = \binom{p+q}{q}$.

2.1.5. — Pour une famille $(x_i)_{i \in I}$ d'éléments d'un anneau (commutatif unitaire), et $\boldsymbol{a} \in \mathbb{N}^{(I)}$, on pose :

$$x^{\boldsymbol{a}} = \prod_{i \in I} x_i^{a(i)}.$$

Si I est fini, la formule du multinôme s'écrit :

$$\Big(\sum_{i \in I} x_i\Big)^d = \sum_{\boldsymbol{a} \in \Gamma_d I} ((\boldsymbol{a})) x^{\boldsymbol{a}}.$$

En particulier, si $\operatorname{Card} I = m$, et si $x_i = 1$, pour tout i, on trouve

$$m^d = \sum_{\boldsymbol{a} \in \Gamma_d I} ((\boldsymbol{a})).$$

2.1.6. — Si X et Y sont deux ensembles, on écrira, suivant Tate, $\mathbf{M}(X, Y)$ plutôt que $\operatorname{Hom}_{\mathbf{Ens}}(X, Y)$, pour désigner l'ensemble des applications de X vers Y. La notation plus compacte Y^X évoque trop les invariants pour être utilisable ici.

2.1.7. — Un morphisme d'anneaux sera dit *fini étale* s'il est localement de la forme $R \to R^d$; intrinsèquement, c'est un morphisme fini, localement libre et non ramifié (on dit aussi : *net*). Ainsi, pour un idempotent e, le morphisme $R \to R/eR$ est considéré comme fini étale.

2.2 Lois polynômes et algèbre à puissances divisées.

Les définitions et propriétés rappelées dans les §§ 2.2, 2.3 et 2.4 seront constamment utilisées dans la suite ; elles sont standard (voir par exemple l'article de Roby [17], ou les exercice dans Bourbaki [3], A IV, p. 87–90) ; le lecteur averti est donc invité à passer directement au § 2.5, après, peut-être, un coup d'œil à l'utile lemme 2.3.1 qui ne figure pas ailleurs.

2.2.1. (Roby, p. 219). — Soient R un anneau commutatif, et E et F deux R-modules ; on note $\underline{E}$ le foncteur covariant

$$\underline{E} : R\text{-}\mathbf{Alg} \longrightarrow \mathbf{Ens}, \quad R' \longmapsto R' \otimes_R E.$$

Une *loi polynôme* de E vers F est, par définition, un morphisme de foncteurs

$$f : \underline{E} \longrightarrow \underline{F}.$$

Plus prosaïquement, c'est la donnée, pour toute R-algèbre R', d'une application d'ensembles

$$f_{R'} : R' \otimes_R E \longrightarrow R' \otimes_R F,$$

soumise à la seule condition de dépendre fonctoriellement de R' : pour tout morphisme de R-algèbres, $R' \to R''$ le carré suivant est commutatif

$$\begin{array}{ccc} R' \otimes_R E & \xrightarrow{f_{R'}} & R' \otimes_R F \\ {\scriptstyle \text{can}}\big\downarrow & & \big\downarrow{\scriptstyle \text{can}} \\ R'' \otimes_R E & \xrightarrow{f_{R''}} & R'' \otimes_R F. \end{array}$$

Dans la suite, on se permettra le plus souvent de parler d'une loi polynôme comme d'une application entre deux modules — alors que c'est en fait un morphisme de foncteurs —, lorsque le caractère fonctoriel sera évident.

2.2.2. (Roby, p. 226 et 220). — On dit que la loi polynôme f est *homogène de degré* d si, pour toute algèbre R', tout $r \in R'$ et tout $x \in R' \otimes_R E$, on a $f(rx) = r^d f(x)$.

Supposons f homogène de degré d. Soit $(x_i)_{i \in I}$ une famille à support fini d'éléments de E ; désignons par R' la R-algèbre de polynômes en la famille $(T_i)_{i \in I}$ d'indéterminées ; il existe une unique famille $(y_{\boldsymbol{a}})$ d'éléments de F, indexée par $\mathbb{A} := \Gamma_d I$ (voir 2.1.3), telle que, dans $R' \otimes F$, on ait :

$$f\Big(\sum_{i \in I} T_i \otimes x_i\Big) = \sum_{\boldsymbol{a} \in \mathbb{A}} T^{\boldsymbol{a}} \otimes y_{\boldsymbol{a}}.$$

Cette famille $(y_{\boldsymbol{a}})$ a la propriété suivante : pour toute R-algèbre S, et toute famille (t_i) d'éléments de S, on a

$$f\Big(\sum_{i \in I} t_i x_i\Big) = \sum_{\boldsymbol{a} \in \mathbb{A}} t^{\boldsymbol{a}} y_{\boldsymbol{a}}.$$

Cette expression justifie l'emploi du terme : « loi polynôme ». On voit, en particulier, qu'une loi polynôme homogène de degré 1 n'est autre qu'une application linéaire.

2.2.3. L'algèbre à puissances divisées, ou algèbre gamma, d'un R-module E (Roby, p. 248). — Pour un R-module E, il existe une R-algèbre commutative graduée à degrés positifs, notée $\Gamma_R(E) = \bigoplus_d \Gamma_R^d(E)$, ou simplement ΓE (et notée souvent DE par les anglo-saxons), munie d'applications $\gamma^d : E \to \Gamma_R^d(E)$, telles que, en notant $\times$ le produit dans ΓE, on ait, pour tout $x, y \in E$ et $r \in R$,

$$\begin{gathered}
\Gamma_R^0(E) = R \text{ et } \gamma^0(x) = 1, \\
\Gamma_R^1(E) = E \text{ et } \gamma^1(x) = x, \\
\gamma^p(rx) = r^p \gamma^p(x), \\
\gamma^p(x+y) = \sum \gamma^r(x) \times \gamma^{p-r}(y), \\
\gamma^p(x) \times \gamma^q(x) = ((p,q))\gamma^{p+q}(x).
\end{gathered}$$

Soient $x = (x_i)_{i \in I}$ une famille d'éléments d'un module E et $\boldsymbol{a} \in \mathbb{N}^{(I)}$; on pose, par analogie avec la convention 2.1.5,

$$\gamma^{\boldsymbol{a}}(x) = \prod_{i \in I} \gamma^{a(i)}(x_i), \tag{2.2.3.1}$$

le produit étant celui de l'algèbre ΓE, noté aussi $\times$; $\gamma^{\boldsymbol{a}}(x)$ est donc un élément de $\Gamma^d E$, où d est le poids de $\boldsymbol{a}$.

2.2.4. Propriété universelle de $\Gamma_R^d(E)$ (Roby, p. 266). — Pour tout R-module F, l'application $u \mapsto u \circ \gamma^d$ établit une bijection entre $\mathrm{Hom}(\Gamma_R^d(E), F)$ et l'ensemble des lois polynômes homogènes de degré d de E vers F.

2.2.5. Décomposition (Roby, p. 262). — Si $E = E' \oplus E''$, pour tout couple d'entiers positifs (d', d''), l'application

$$E \longrightarrow \Gamma_R^{d'}(E') \otimes \Gamma_R^{d''}(E''), \quad x = x' + x'' \longmapsto \gamma^{d'}(x') \otimes \gamma^{d''}(x'')$$

définit une loi polynôme homogène de degré $d' + d''$, et s'étend donc en une application linéaire $\Gamma_R^{d'+d''}(E) \to \Gamma_R^{d'}(E') \otimes \Gamma_R^{d''}(E'')$; pour un entier d, et en prenant la somme de ces applications pour les couples (d', d'') tels que $d = d' + d''$, on obtient l'isomorphisme suivant où, dans le second membre, la somme est directe

$$\Gamma^d_R(E'\oplus E'') \xrightarrow{\sim} \sum_{d'+d''=d} \Gamma^{d'}_R(E')\otimes\Gamma^{d''}_R(E''),$$
$$\gamma^d(x'+x'') \longmapsto \sum_{d'+d''=d} \gamma^{d'}(x')\otimes\gamma^{d''}(x'').$$

Poussant l'argument jusqu'au bout, et en utilisant la notation $\gamma^{\boldsymbol{a}}$ (2.2.3.1), on voit que si $(e_i)_{i\in I}$ une base de E (resp. un système générateur), alors la famille $(\gamma^{\boldsymbol{a}}(e))$ indexée par les multiindices $\boldsymbol{a}\in\Gamma_d I$, est une base (resp. un système générateur) de $\Gamma^d E$.

2.2.6. (Roby, p. 282). — Toute suite exacte de modules

$$E' \overset{u}{\underset{v}{\rightrightarrows}} E \xrightarrow{w} E''$$

se prolonge en une suite exacte de R-algèbres

$$\Gamma E' \overset{\Gamma u}{\underset{\Gamma v}{\rightrightarrows}} \Gamma E \xrightarrow{\Gamma w} \Gamma E''$$

(*i.e.* Γw est surjectif et son noyau est l'idéal engendré par les éléments $\gamma^n(v(x'))-\gamma^n(u(x'))$ pour $n\geq 1$ et $x'\in E'$).

2.2.7. (Roby, p. 262). — Pour toute R-algèbre S, on a un isomorphisme de S-algèbres graduées

$$S\otimes_R\Big(\bigoplus\Gamma^d_R(E)\Big)\simeq\bigoplus\big(\Gamma^d_S(S\otimes_R E)\big).$$

2.3. Un lemme.

En général, le R-module $\Gamma^d_R(E)$ n'est pas engendré par le sous-ensemble $\gamma^d(E)$. C'est déjà faux pour $\Gamma^3_{\mathbb{Z}}(\mathbb{Z}^2)$ comme on le voit en réduisant modulo 2. Le lemme qui suit, et qui ne semble pas figurer dans la littérature, montre que ce défaut est corrigé par un changement de base fini et libre, qui dépend de d mais pas de E ; cela simplifie certaines vérifications.

On se fixe un entier $d\geq 1$ et on pose $\Lambda=\mathbb{Z}[T]/(P)$, où P est le polynôme unitaire (au signe près)

$$P(T)=\prod_{0\leq i<j\leq d}(T^i-T^j)-1.$$

Si on désigne par t la classe de T dans Λ, les différences t^i-t^j sont donc inversibles dans Λ, pour $0\leq i<j\leq d$; par suite, si e est un entier tel que $1\leq e\leq d$, la matrice de Vandermonde $(t^{ij})_{0\leq i,j\leq e}$ est inversible.

Lemme 2.3.1. — *Si R est une Λ-algèbre, pour tout R-module E, le R-module $\Gamma^d_R(E)$ est engendré par l'ensemble $\gamma^d(E)$. En particulier, pour R quelconque, si on pose $R' = \Lambda \otimes_{\mathbb{Z}} R$, le R'-module*

$$\Lambda \otimes_{\mathbb{Z}} \Gamma^d_R(E) \simeq \Gamma^d_{R'}(\Lambda \otimes_{\mathbb{Z}} E)$$

est engendré par l'ensemble $\gamma^d(\Lambda \otimes_{\mathbb{Z}} E)$.

Démonstration. — On suppose que R est une Λ-algèbre, et on va démontrer un peu plus : le R-module $\Gamma^e_R(E)$ est engendré par l'ensemble $\gamma^e(E)$, pour tout entier e tel que $1 \leq e \leq d$. Tout élément de $\Gamma^e_R(E)$ est combinaison linéaire d'éléments de la forme

$$\xi = \gamma^{a}(x) := \gamma^{a(1)}(x_1) \times \gamma^{a(2)}(x_2) \times \cdots \times \gamma^{a(m)}(x_m)$$

où $\boldsymbol{a} = (a(1), a(2), \ldots, a(m))$ est une suite d'entiers > 0 de somme égale à e. On procède par récurrence sur m ; on peut donc supposer que $m \geq 2$, et que l'élément $\gamma^{a(2)}(x_2) \times \cdots \times \gamma^{a(m)}(x_m) \in \Gamma^{e-a(1)}E$ est combinaison linéaire d'éléments de la forme $\gamma^{e-a(1)}(y)$; on est donc ramené au cas $m = 2$, c'est-à-dire à prouver ceci : pour deux éléments $x, y \in E$, et pour $0 \leq i \leq e$, alors $z_i := \gamma^i(x) \times \gamma^{e-i}(y)$ est combinaison linéaire d'éléments de $\gamma^e(E)$. Or, on a, pour $j = 0, 1, \ldots, e$,

$$\gamma^e(t^j x + y) = \sum_{i=0}^{e} \gamma^i(t^j x) \times \gamma^{e-i}(y) = \sum_{i=0}^{e} t^{ij} z_i.$$

L'inversibilité de la matrice de Vandermonde (t^{ij}) permet de conclure. ∎

On aura remarqué que dans la démonstration qui précède, les éléments z_0 et z_e sont déjà dans $\gamma^e(E)$, et que cela permet visiblement d'affaiblir les hypothèses ; nous n'avons pas herché l'énoncé optimum ; signalons toutefois que si $d = 2$ la conclusion est toujours vraie (car $x \times y = \gamma^2(x+y) - \gamma^2(x) - \gamma^2(y)$), et que lorsque $d = 3$, il suffit que R contienne un élément t tel que t et $1 - t$ soient inversibles.

2.4. L'algèbre $\boldsymbol{\Gamma^m S}$.

2.4.1. — Soient F, F' deux R-modules et m un entier ≥ 1 ; il y a une unique application linéaire

$$\mu : \Gamma^m F' \otimes \Gamma^m F'' \longrightarrow \Gamma^m(F' \otimes F'')$$

qui envoie $\gamma^m(x') \otimes \gamma^m(x'')$ sur $\gamma^m(x' \otimes x'')$: pour le voir, on fixe d'abord $x' \in F'$, et on constate que l'application

$$F'' \longrightarrow \Gamma^m(F' \otimes F''), \quad x'' \longmapsto \gamma^m(x' \otimes x''),$$

est une loi polynôme homogène de degré m, et qu'elle s'étend donc (2.2.4) en une application linéaire $\Gamma^m\Gamma'' \to \Gamma^m(F' \otimes F'')$; on définit ainsi une application $F' \to \mathrm{Hom}(\Gamma^m F'', \Gamma^m(F' \otimes F''))$ qui a les vertus requises pour se prolonger en une application linéaire

$$\Gamma^m F' \longrightarrow \mathrm{Hom}\big(\Gamma^m F'', \Gamma^m(F' \otimes F'')\big);$$

on conclut par la propriété universelle du produit tensoriel. $\square$

La formule suivante qui explicite l'application μ de 2.4.1, ne sera utilisée que dans quelques exemples. (L. Breen me signale qu'il connaissait cette formule depuis longtemps, et qu'elle figure aussi dans un manuscrit ancien de Bousfield. On la trouve aussi dans [18].)

FORMULE 2.4.2. — *Soient $x = (x_i)_{i\in I}$ et $y = (y_j)_{j\in J}$ deux familles d'éléments de F' et F'' respectivement, et soient $\boldsymbol{a} \in \Gamma_m I$, $\boldsymbol{b} \in \Gamma_m J$ deux multiindices de poids m. Désignons par $\mathbb{C}(\boldsymbol{a}, \boldsymbol{b}) \subset \Gamma_m(I \times J)$ l'ensemble des applications $\boldsymbol{c} : I \times J \to \mathbb{N}$ de « sommes partielles » $\boldsymbol{a}$ et $\boldsymbol{b}$, c'est-à-dire telles que $\sum\limits_{j\in J} c(i,j) = a(i)$ pour tout $i \in I$, et $\sum\limits_{i\in I} c(i,j) = b(j)$ pour tout $j \in J$. Alors, avec la notation de* 2.2.3.1, *l'application* (2.4.1),

$$\mu : \Gamma^m F' \otimes \Gamma^m F'' \longrightarrow \Gamma^m(F' \otimes F''),$$

est précisée par la formule

$$\mu\big(\gamma^{\boldsymbol{a}}(x) \otimes \gamma^{\boldsymbol{b}}(y)\big) = \sum_{\boldsymbol{c}\in\mathbb{C}(a,b)} \gamma^{\boldsymbol{c}}(x \otimes y). \quad \square$$

2.4.3. — Si F' est un R-module libre, alors l'application

$$\mu : \Gamma^m F' \otimes \Gamma^m F'' \longrightarrow \Gamma^m(F' \otimes F'')$$

admet une rétraction (application linéaire φ telle que $\varphi \circ \mu = \mathrm{id}$). En effet, soit $(e_i)_{i\in I}$ une base de F' ; tout élément de $F' \otimes F''$ s'écrit de façon unique sous la forme $\sum e_i \otimes x_i$, pour une famille convenable (x_i) d'éléments de F''. Alors, avec les notations compactées de 2.2.3.1, l'application $f : F' \otimes F'' \to \Gamma^m F' \otimes \Gamma^m F''$ définie par

$$f\Big(\sum e_i \otimes x_i\Big) = \sum \gamma^{\boldsymbol{a}}(e) \otimes \gamma^{\boldsymbol{a}}(x),$$

pour $\boldsymbol{a}$ parcourant $\Gamma_m I$, est une loi polynôme homogène de degré m, et s'étend donc (2.2.4) en une application linéaire

$$\varphi : \Gamma^m(F' \otimes F'') \longrightarrow \Gamma^m F' \otimes \Gamma^m F'' ;$$

c'est une rétraction de μ.

Pour le voir, il faut vérifier que $f(x' \otimes x'') = \gamma^m(x') \otimes \gamma^m(x'')$; or, si on écrit $x' = \sum r_i e_i$, avec $r_i \in R$, on a, par définition de f,

$$\begin{aligned} f(x' \otimes x'') &= f\Big(\sum e_i \otimes r_i x''\Big) \\ &= \sum \gamma^{\boldsymbol{a}}(e) \otimes \gamma^{\boldsymbol{a}}(rx'') \ \text{ (somme pour } \boldsymbol{a} \in \Gamma_m I) ; \end{aligned}$$

d'autre part, en posant $r^{\boldsymbol{a}} = \prod r_i^{a(i)}$, on a :

$$\begin{aligned} \sum \gamma^{\boldsymbol{a}}(e) \otimes \gamma^{\boldsymbol{a}}(rx'') &= \sum \gamma^{\boldsymbol{a}}(e) \otimes r^{\boldsymbol{a}} \gamma^m(x'') \\ &= \Big(\sum r^{\boldsymbol{a}} \gamma^{\boldsymbol{a}}(e)\Big) \otimes \gamma^m(x'') = \gamma^m(x') \otimes \gamma^m(x''). \quad \square \end{aligned}$$

Soit L un module inversible ; on a donc un isomorphisme

$$L^{\otimes m} \xrightarrow{\sim} \Gamma^m L.$$

On déduit de ce qui précède que pour tout module F, on a un isomorphisme

$$\Gamma^m(L \otimes F) \xrightarrow{\sim} L^{\otimes m} \otimes \Gamma^m F, \tag{2.4.3.1}$$

tel que l'image de $\gamma^m(\lambda \otimes x)$ soit $\lambda^{\otimes m} \otimes \gamma^m(x)$. $\square$

2.4.4. — Si S est une R-algèbre, $\Gamma^m S$ est muni, d'après ce qui précède, d'une structure de R-algèbre pour laquelle le produit de $\gamma^m(s)$ par $\gamma^m(s')$ est égal à $\gamma^m(ss')$; le produit dans $\Gamma^m S$ de deux éléments $x, y \in \Gamma^m S$ sera noté par simple juxtaposition ou par le symbole $*$, pour le distinguer du produit « externe »

$$\Gamma^p S \times \Gamma^{m-p} S \longrightarrow \Gamma^m S, \quad \text{noté } (z,t) \mapsto z \times t.$$

L'élément unité de l'algèbre $\Gamma^m S$ est $\gamma^m(1)$, et le morphisme canonique $R \to \Gamma^m S$ est $r \mapsto r\gamma^m(1)$, et non pas $r \mapsto \gamma^m(r) = r^m \gamma^m(1)$, qui en diffère si $m > 1$.

2.4.5. — Voici les formules donnant le produit de deux éléments dans $\Gamma^2 S$. Pour $s, s', t, t' \in S$, on a :

$$\begin{gathered} \gamma^2(s) * \gamma^2(s') = \gamma^2(ss'), \\ \gamma^2(s) * (t \times t') = (st) \times (st'), \\ (s \times t) * (s' \times t') = ss' \times tt' + st' \times s't. \end{gathered}$$

2.4.6. — Enfin, si F est un S-module, alors $\Gamma^m F$ est un $\Gamma^m S$-module...

2.5. Lois multiplicatives.

Si S et S' sont deux anneaux, une application $g : S \to S'$ est dite *multiplicative* si elle est compatible aux produits :

$$g(1) = 1, \quad g(st) = g(s)g(t).$$

Si S et S' sont des R-algèbres, une loi polynôme de S vers S' sera dite *multiplicative* si pour toute R-algèbres R', l'application $R' \otimes S \to R' \otimes S'$ est multiplicative.

La loi polynôme

$$\gamma^m : S \to \Gamma^m S$$

est multiplicative ; elle est universelle :

Proposition 2.5.1. — *Soient S et S' deux R-algèbres ; alors l'application $f \mapsto f \circ \gamma^m$ établit une bijection entre l'ensemble* $\mathrm{Hom}_{R\text{-}\mathbf{Alg}}(\Gamma^m S, S')$ *et l'ensemble des lois polynômes, définies sur R, de S vers S', homogènes de degré m et multiplicatives.*

Démonstration. — Il est clair que si $f : \Gamma^m S \to S'$ est un morphisme de R-algèbres, alors $f \circ \gamma^m$ définit une loi polynôme, homogène de degré m et multiplicative. Réciproquement, d'après 2.2.4, une loi polynôme $g : S \to S'$ homogène de degré m se factorise en $g = f \circ \gamma^m$, où $f : \Gamma^m S \to S'$ est une application R-linéaire ; il s'agit de voir que si g est multiplicative, alors f est un morphisme. Notons que pour $s, t \in S$, on a par définition du produit dans $\Gamma^m S$,

$$\begin{aligned} f\big(\gamma^m(s) * \gamma^m(t)\big) &= f\big(\gamma^m(st)\big) \\ &= g(st) = g(s)g(t) \\ &= f\big(\gamma^m(s)\big) \cdot f\big(\gamma^m(t)\big). \end{aligned}$$

Comme f est R-linéaire, on aura encore, par distributivité,

$$f(s' * t') = f(s')f(t')$$

si s' et t' sont dans le sous-R-module de $\Gamma^m S$ engendré par l'ensemble $\gamma^m(S)$; le lemme 2.3.1 permet de se ramener à ce cas. $\square$

(Cet énoncé se trouve aussi dans [18], mais avec une démonstration peut-être un peu courte.)

Remarque 2.5.2. — Pour deux entiers positifs a et b, l'application $s \mapsto \gamma^a(s) \otimes \gamma^b(s)$ a les propriétés requises par l'énoncé précédent pour se prolonger en un morphisme de R-algèbres

$$\Gamma^{a+b} S \longrightarrow \Gamma^a S \otimes \Gamma^b S,$$

qui envoie $\gamma^{a+b}(s)$ sur $\gamma^a(s) \otimes \gamma^b(s)$. Par contre, l'application associée au produit « externe »

$$\Gamma^a S \otimes \Gamma^b S \longrightarrow \Gamma^{a+b} S, \quad \gamma^a s \otimes \gamma^b t \longmapsto \gamma^a s \times \gamma^b t,$$

n'est pas un morphisme d'anneaux.

2.5.3. — Soient S et R' deux R-algèbres et f une loi polynôme multiplicative et homogène de degré m, de S vers R' ; notons encore f l'application (relative à $R[X]$),

$$f_{R[X]} : S[X] \longrightarrow R'[X] ;$$

alors, pour tout $s \in S$, $f(X - s)$ est un polynôme unitaire de degré m ; en effet, c'est l'image par un morphisme de R-algèbres du polynôme suivant de $(\Gamma^m S)[X]$ (*cf.* 2.2.3)

$$\gamma^m(X - s) = \sum_{i=0}^{m} \big(\gamma^i(1) \times \gamma^{m-i}(-s)\big) X^i = \gamma^m(1) X^m - \cdots .$$

Or, $\gamma^m(1)$ est l'élément unité de $\Gamma^m S$.

2.6 Cas des algèbres décomposées.

Sera dite *décomposée* une R-algèbre de la forme $R \to R^d$; il est préférable de la voir, plus intrinsèquement, comme l'algèbre $\mathbf{M}(T, R)$ formée des applications d'un ensemble fini T de cardinal d, vers R. C'est le modèle local pour les algèbres finies étales.

Rappelons (2.1.3) que l'on note $\Gamma_n T$ l'ensemble des applications $\boldsymbol{a} : T \to \mathbb{N}$ telles que $|\boldsymbol{a}| := \sum a(t) = n$; cette notation est justifiée ici :

Proposition 2.6.1. — *Pour un ensemble fini T, et un entier $d \geq 0$, l'application*

$$\mathbf{M}(T, R) \longrightarrow \mathbf{M}(\Gamma_d T, R), \quad m \longmapsto \Big(\boldsymbol{a} \mapsto \prod m(t)^{a(t)}\Big)$$

se prolonge en un isomorphisme de R-algèbres

$$\Gamma^d \mathbf{M}(T, R) \simeq \mathbf{M}(\Gamma_d T, R).$$

Démonstration. — L'application indiquée est une loi polynôme multiplicative homogène de degré d ; elle se prolonge donc (2.5.1) en un morphisme d'algèbres

$$\Gamma^d\mathbf{M}(T,R) \longrightarrow \mathbf{M}(\Gamma_d T, R).$$

Pour vérifier que c'est un isomorphisme, on considère la base (e_t) de $\mathbf{M}(T,R)$ formée des idempotents habituels, de sorte que, par 2.2.5, la famille des $(\gamma^{\boldsymbol{a}}(e))$, pour $\boldsymbol{a} \in \Gamma_d T$, forme une base du membre de gauche ; pour évaluer l'image de $\gamma^{\boldsymbol{a}}(e)$ par le morphisme considéré, on introduit des indéterminées $(X_t)_{t\in T}$; l'image de $\gamma^{\boldsymbol{a}}(e)$ dans $\mathbf{M}(\Gamma_d T, R)$ apparaît alors comme le coefficient de $X^{\boldsymbol{a}} := \prod X_t^{a(t)}$ dans l'image de $\gamma^d(\sum X_t e_t)$. Comme $\sum X_t e_t$ est l'application $t \mapsto X_t$, le morphisme ci-dessus envoie $\gamma^d(\sum X_t e_t) = \sum X^{\boldsymbol{a}}\gamma^{\boldsymbol{a}}(e)$ sur l'application $\boldsymbol{b} \mapsto \prod X_t^{b(t)} = X^{\boldsymbol{b}}$; l'image de $\gamma^{\boldsymbol{a}}(e)$ dans $\mathbf{M}(\Gamma_d, T, R)$ est donc l'application $\Gamma_d T \to R$ nulle sauf en $\boldsymbol{a}$, où elle vaut 1. On retrouve bien la base canonique de $\mathbf{M}(\Gamma_d T, R)$; le morphisme considéré est donc un isomorphisme. □

3. Définition du foncteur norme

3.1 La norme et le morphisme $\boldsymbol{\pi} : \boldsymbol{\Gamma^d_R}(\boldsymbol{S}) \to \boldsymbol{R}$.

3.1.1. — Soit S une R-algèbre finie localement libre de rang d ; la norme

$$\operatorname{norm}_{S/R} : S \to R$$

associe à $s \in S$ le déterminant de l'endomorphisme R-linéaire de S défini par la multiplication par s :

$$\operatorname{norm}(s) = \det(x \mapsto sx).$$

Le déterminant commute aux changements de base, si bien que la norme est une loi polynôme.

C'est toujours sous cet aspect fonctoriel que la norme sera considérée dans la suite.

Cette loi polynôme est multiplicative et homogène de degré d.

3.1.2. — D'après 2.5.1, il existe un unique morphisme de R-algèbres

$$\pi : \Gamma^d_R(S) \longrightarrow R$$

tel que

$$\pi \circ \gamma^d = \operatorname{norm}_{S/R}.$$

En un sens, ce morphisme π « linéarise » la norme ; il joue un rôle central dans la suite. Soulignons donc la propriété qui le caractérise : pour toute R-algèbre R', l'application composée

$$R' \otimes S \xrightarrow{\gamma^d} \Gamma^d_{R'}(R' \otimes S) \xrightarrow{\sim} R' \otimes \Gamma^d_R(S) \xrightarrow{1\otimes\pi} R'$$

est égale à l'application norme relative au morphisme $R' \to R' \otimes S$.

3.1.3. Exemples.

a) Voici d'abord le cas le plus simple : celui d'un morphisme de rang 2. L'application $S \to S$, $s \mapsto s^2$ est aussi une loi polynôme multiplicative de degré 2 ; on a donc un morphisme

$$\Gamma^2 S \longrightarrow R \times S,$$

caractérisé par

$$\gamma^2(s) \longmapsto \big(\operatorname{norm}(s), s^2\big).$$

C'est un isomorphisme si $S = R^2$, donc aussi lorsque S est étale sur R (la réciproque est vraie).

Poussons les calculs lorsque

$$S = R[X]/(X^2 - \delta),$$

en notant $x =$ classe de X. La norme est donnée par la formule

$$\operatorname{norm}(a + bx) = a^2 - b^2\delta.$$

La R-algèbre $\Gamma^2_R(S)$ est libre de rang 3, de base $\{1, u, v\}$, où $u = 1 \times x$ et $v = \gamma^2(x)$; les formules 2.4.5 conduisent aux relations

$$u^2 = 2v + 2\delta, \quad v^2 = \delta^2, \quad uv = \delta u.$$

Le morphisme π est défini par $\pi(u) = 0$, $\pi(v) = -\delta$. Le morphisme $\kappa : \gamma^2 S \to S$, associé au carré, est donné par

$$\kappa(u) = 2x, \quad \kappa(v) = \delta.$$

Le noyau $\operatorname{Ker}(\pi)$ est un R-module libre de base $\{u, v+\delta\}$; si $2 = 0$ dans R, auquel cas $R \to S$ est radiciel, alors l'idéal $\operatorname{Ker}(\pi)$ est de carré nul.

b) Considérons la R-algèbre décomposée $\mathbf{M}(T, R)$ formée des applications d'un ensemble T de cardinal d, vers R ; la norme est ici le produit des composants

$$\operatorname{norm} : \mathbf{M}(T, R) \longrightarrow R, \quad \operatorname{norm}(m : T \to R) = \prod m(t).$$

Tenant compte de l'isomorphisme 2.6.1, on voit que le morphisme

$$\pi : \Gamma^d \mathbf{M}(T, R) \simeq \mathbf{M}(\Gamma_d T, R) \longrightarrow R$$

consiste à associer à une application $\Gamma_d T \to R$ sa valeur en l'application constante $(t \mapsto 1) \in \Gamma_d T$.

3.1.4. — Lorsque S est fini localement libre, son rang n'est pas nécessairement constant, mais on peut décomposer R en un produit fini d'anneaux tels que le rang de S soit constant au dessus de chaque facteur ; la norme est encore définie, elle est homogène mais son degré varie d'un facteur à l'autre.

3.2. Le foncteur norme.

DÉFINITION 3.2.1. — *Soient S une R-algèbre finie localement libre, F un S-module et E un R-module. Une loi normique est une loi polynôme φ de F vers E, définie sur R, telle que pour toute R-algèbre R', on ait, pour $s \in R' \otimes_R S$ et $x \in R' \otimes_R F$,*

$$\varphi(sx) = \operatorname{norm}_{R' \otimes_R S/R'}(s)\varphi(x).$$

Si S est de rang constant d, une loi normique est homogène de degré d.

3.2.2. Exemples.

a) Supposons S de rang constant d. Soit F un S-module, et prenons pour E le R-module $\operatorname{Hom}_R(\wedge^d S, \wedge^d F)$, où les puissances extérieures sont effectuées sur R ; à tout $x \in F$ est associée l'application $S \to F$, $s \mapsto sx$, qui est (en particulier) R-linéaire ; posons

$$\varphi(x) = \wedge^d (s \mapsto sx);$$

on définit ainsi une loi normique de F vers E (*cf.* 3.3).

b) Supposons que E soit une R-algèbre (commutative), de sorte qu'on dispose de l'application norme $S \otimes E \to E$; à tout S-module F et toute application S-linéaire $u : F \to S \otimes_R E$, on associe la loi normique composée

$$F \xrightarrow{u} S \otimes_R E \xrightarrow{\text{norm}} E;$$

cette loi normique servira à relier le foncteur norme au foncteur restriction de Weil (6.2).

c) Considérons la R-algèbre décomposée $S = \mathbf{M}(T, R)$; un S-module F se décompose en le produit $F = \prod F_t$ d'une famille de $R-$modules, indexée par T ; posons $E = \otimes F_t$; alors l'application

$$\begin{aligned} \varphi : \prod F_t &\longrightarrow \otimes F_t, \\ (x_t) &\longmapsto \otimes x_t, \end{aligned}$$

se prolonge en une loi normique.

Théorème 3.2.3. — *Soient $f : R \to S$ un morphisme fini localement libre et F un S-module. Alors il existe un R-module, noté $N_f(F)$ ou $N_{S/R}(F)$ ou même $N(F)$, et une loi normique*

$$\nu_F : F \longrightarrow N(F)$$

qui sont universels au sens suivant : pour tout R-module E et toute loi normique v de F vers E, il existe une unique application R-linéaire $u : N(F) \to E$ telle que $v = u \circ \nu_F$.

La propriété universelle entraîne que le couple $(N(F), \nu_F)$ dépend fonctoriellement de F ; ce foncteur $N_{S/R} : \mathbf{Mod}\text{-}S \to \mathbf{Mod}\text{-}R$ sera nommé dans la suite le *foncteur norme.*

Pour la démonstration de 3.2.3, on peut, en décomposant R en un produit convenable, se ramener au cas où S est de rang constant d. On pose alors

$$N_{S/R}(F) = \Gamma_R^d(F) \otimes_{\Gamma^d(S)} R, \quad \nu_F(x) = \gamma^d(x) \otimes 1$$

où la structure de $\Gamma_R^d(S)$-algèbre sur R est celle associée au morphisme $\pi : \Gamma_R^d(S) \to R$ déduit de la norme 3.1.2.

Montrons d'abord que $\nu_F : F \to N(F)$ est une loi normique, ce qui impliquera immédiatement que pour toute application R-linéaire $u : N(F) \to E$, le composé $u \circ \nu_F$ définira une loi normique de F vers E. Par construction, ν_F est une loi polynôme homogène de degré d. Pour $s \in S$ et $x \in F$, on a dans $\Gamma_R^d(F) \otimes_{\Gamma^d(S)} R$,

$$\begin{aligned} v(sx) &= \gamma^d(sx) \otimes 1 = \gamma^d(s)\gamma^d(x) \otimes 1 \\ &= \gamma^d(x) \otimes \pi\gamma^d(s) = \mathrm{norm}(s)v(x), \end{aligned}$$

et après tout changement de base, la relation analogue reste vraie ; ν_F est donc normique.

Montrons que ν_F est universelle : soit $v : F \to E$ une loi normique ; comme v est, en particulier, une loi polynôme homogène de degré d, elle se factorise en $v = w \circ \gamma^d$ où $w : \Gamma^d F \to E$ est une application R-linéaire, et il s'agit de vérifier que pour $t \in \Gamma^d S$ et $y \in \Gamma^d F$, on a

$$w(ty) = \pi(t)w(y). \tag{*}$$

Quitte à faire le changement de base fidèlement plat évoqué dans 2.3.1, on peut supposer que les R-modules $\Gamma^d S$ et $\Gamma^d F$ sont engendrés respectivement par les sous-ensembles $\gamma^d(S)$ et $\gamma^d(F)$; utilisant la distributivité, on est alors ramené à vérifier (*) lorsque $t = \gamma^d(s)$ et $y = \gamma^d(x)$, avec $s \in S$ et $x \in F$; mais l'égalité (*) est alors la traduction du fait que v est normique. ∎

Il est clair que $N_{S/R}(S) = R$ et que la loi normique universelle de S vers R est l'application norme usuelle.

Lemme 3.2.4 (*Produit d'algèbres*). — *Soient $S_1, \dots, S_m$ une famille de R-algèbres finies localement libres de rang $d(1), \dots, d(m)$ respectivement, et un module $F = F_1 \times F_2 \times \cdots \times F_m$ sur $S = S_1 \times \cdots \times S_m$. On a alors un isomorphisme*

$$N_{S/R}(F_1 \times F_2 \times \cdots \times F_m) \xrightarrow{\sim} N_{S_1/R}(F_1) \otimes \cdots \otimes N_{S_m/R}(F_m).$$

En particulier, soit $S = \mathbf{M}(T, R)$ une R-algèbre décomposée. Un $\mathbf{M}(T, R)$-module F est une famille $F = (E_t)$ de R-modules, indexée par T, et sa norme est

$$N_{S/R}\big((E_t)\big) = \otimes E_t.$$

Démonstration. — Posons $d = \sum d(i)$; vu comme R-module, F est la somme directe des F_i ; par suite, en appliquant 2.2.5, on trouve un isomorphisme de R-modules

$$\Gamma^d F \xrightarrow{\sim} \prod_{a \in \mathbb{A}} \Gamma^{\boldsymbol{a}} F, \tag{$*$}$$

où $\boldsymbol{a}$ parcourt l'ensemble $\mathbb{A} \subset \mathbb{N}^m$ des multiindices de poids $\sum a(i) = d$, et où $\Gamma^{\boldsymbol{a}} F := \bigotimes_i \Gamma^{a(i)} F_i$. On a de même un isomorphisme de R-algèbres

$$\Gamma^d S \xrightarrow{\sim} \prod \Gamma^{\boldsymbol{a}} S\,;$$

il est clair que pour tout $\boldsymbol{a} \in \mathbb{A}$, le changement de base $\Gamma^d S \to \Gamma^{\boldsymbol{a}} S$ transforme $\Gamma^d F$ en $\Gamma^{\boldsymbol{a}} F$. Comme la norme d'un élément de S est le produit des normes de ses composantes, le morphisme $\pi : \Gamma^d S \to R$ se factorise par la projection $\Gamma^d S \to \Gamma^{\boldsymbol{a}} S$, avec $\boldsymbol{a} = (d(1), \dots, d(m))$. D'où le résultat. ∎

Proposition 3.2.5.

a) (*Compatibilités*) *Pour deux* S*-modules* F' *et* F'' *on a des applications* R*-linéaires fonctorielles*

$$\varphi : N(F') \otimes_R N(F'') \longrightarrow N(F' \otimes_S F''),$$

$$\psi : N\big(\mathrm{Hom}_S(F', F'')\big) \longrightarrow \mathrm{Hom}_R(NF', NF''),$$

uniquement déterminées par les conditions suivantes : pour $x' \in F'$, $x'' \in F''$ *et* $u : F' \to F''$, *on a :*

$$\varphi\big(\nu(x') \otimes \nu(x'')\big) = \nu(x' \otimes x'') \quad \text{et} \quad \psi\big(\nu(u)\big) = N(u).$$

En particulier, si B *est une* S*-algèbre, alors* NB *est une* R*-algèbre et la loi normique universelle* $\nu_B : B \to NB$ *est multiplicative.*

b) (*Transitivité*) *Soit* $S \to T$ *un second morphisme fini localement libre. Pour tout* T*-module* F, *il existe une application* R*-linéaire, fonctorielle en* F,

$$\theta : N_{T/R}(F) \longrightarrow N_{S/R}\big(N_{T/S}(F)\big).$$

c) Si S *est étale sur* R, *alors* φ *et* θ *sont des isomorphismes ; si, de plus,* F' *est un* S*-module projectif de type fini, alors* ψ *lui-même est un isomorphisme.*

Démonstration. — Il est clair que l'application R-linéaire composée

$$\Gamma^d F' \otimes_R \Gamma^d F'' \xrightarrow{(2.4.1)} \Gamma^d(F' \otimes_R F'') \xrightarrow{\text{can}} \Gamma^d(F' \otimes_S F'')$$

se factorise à travers une application $\Gamma^d S$-linéaire

$$\Gamma^d F' \otimes_{\Gamma^d S} \Gamma^d F'' \longrightarrow \Gamma^d(F' \otimes_S F'')$$

qui envoie $\gamma^d(x') \otimes \gamma^d(x'')$ sur $\gamma^d(x' \otimes x'')$; on obtient φ par le changement de base $\pi : \Gamma^d S \to R$.

L'existence de ψ provient de la propriété universelle du foncteur norme et du fait que l'application $\mathrm{Hom}_S(F', F'') \to \mathrm{Hom}_R(NF', NF'')$, $u \mapsto N(u)$ est normique.

Pour obtenir la flèche de transitivité considérons la loi normique universelle (sur le S-module $N_{T/S}(F)$) $v' : N_{T/S}(F) \to N_{S/R}(N_{T/S}(F))$; en la composant avec la loi $\nu_F : F \to N_{T/S}(F)$ on obtient une loi polynôme définie sur R, $F \to N_{T/S}(F) \to N_{S/R}(N_{T/S}(F))$, qui est normique relativement au morphisme composé $R \to T$, en vertu de la transitivité des applications normes ; l'application θ s'en déduit par la propriété universelle du foncteur norme.

Supposons que $R \to S$ soit étale ; un changement de base fidèlement plat sur R permet de supposer de plus que S est décomposée, et on constate qu'alors φ est un isomorphisme en utilisant le lemme 3.2.4 ; en ce qui concerne ψ, il faut, de plus, utiliser le résultat de compatibilité entre $\otimes$ et Hom énoncé par exemple dans (Bourbaki, A II, Alg. lin., § 4, n$^{\mathrm{o}}$ 4, p. 113). Pour l'application de transitivité, il suffit de remarquer que la S-algèbre T se décompose en un produit $T = T_1 \times \cdots \times T_d$, et que le morphisme composé $R \to S \to T$ se récrit $R \to R \times \cdots \times R \to T_1 \times \cdots \times T_d$; il suffit donc d'appliquer 3.2.4.

3.3 La norme d'un module inversible.

Proposition 3.3. — *Soit $R \to S$ un morphisme fini localement libre de rang d, et L un S-module inversible. Alors l'application*

$$L \longrightarrow \mathrm{Hom}_R(\wedge^d S, \wedge^d L), \quad x \longmapsto \wedge^d(s \mapsto sx)$$

est la loi normique universelle ; *autrement dit, on a un isomorphisme*

$$N_{S/R}(L) \simeq \mathrm{Hom}_R(\wedge^d S, \wedge^d L);$$

en particulier, $N_{S/R}(L)$ est donc un R-module inversible. Pour tout S-module F l'application (3.2.5)

$$\varphi : N(L) \otimes_R N(F) \longrightarrow N(L \otimes_S F),$$

est un isomorphisme.

Démonstration. — Comme S est fini sur R, il existe un changement de base fidèlement plat $R \to R'$ qui trivialise le S-module $L \ldots$ et la vérification ! □

Pour les modules inversibles, le foncteur N est donc isomorphe au foncteur norme introduit dans EGA II, 6.5.

4. Projectivité de $N(S^m)$

Pour tout entier m, le R-module $N(S^m)$ se décompose canoniquement en le produit des modules $\mathbf{P}^{\boldsymbol{a}}(S)$ introduits plus bas, si bien que la question de la projectivité de $N(S^m)$ est ramenée à celle des $\mathbf{P}^{\boldsymbol{a}}(S)$. Or, chaque $\mathbf{P}^{\boldsymbol{a}}(S)$ est muni naturellement d'une structure de R-algèbre, et cette dernière « paramétrise » certaines factorisations de l'application norme. Cette interprétation permet de montrer que les $\mathbf{P}^{\boldsymbol{a}}(S)$ — donc aussi les $N(S^m)$ — sont des R-modules libres lorsque S est une R-algèbre monogène ; elle conduit aussi à l'exemple d'une R-algèbre intersection complète S telle que $N(S^2)$ ne soit pas libre.

4.1. Un critère de projectivité.

Soit S une R-algèbre finie localement libre de rang d. Considérons une suite de m entiers $\boldsymbol{a} \in \mathbb{N}^m$ de poids $\sum a(i) = d$. D'après (2.5.1) on dispose d'un morphisme de R-algèbres

$$\Gamma^d S \to \Gamma^{\boldsymbol{a}} S := \Gamma^{a(1)} S \otimes \Gamma^{a(2)} S \otimes \cdots \otimes \Gamma^{a(m)} S.$$

Posons

$$\mathbf{P}^{\boldsymbol{a}}(S) = \Gamma^{\boldsymbol{a}} S \otimes_{\Gamma^d S} R$$

Lemme 4.1.1. — *Soient* $\mathbf{M}(T,R)$ *une* R*-algèbre décomposée, de rang* d, *et* $\boldsymbol{a} \in \mathbb{N}^m$ *un multiindice de poids* d. *Alors, on a un isomorphisme de* R*-algèbres*

$$\mathbf{P}^{\boldsymbol{a}}\big(\mathbf{M}(T,R)\big) \xrightarrow{\sim} \mathbf{M}(\mathbf{P}_{\boldsymbol{a}} T, R),$$

où $\mathbf{P}_{\boldsymbol{a}} T$ *désigne l'ensemble des partitions* $T = T_1 \coprod \cdots \coprod T_m$ *en parties* T_i *de cardinal* $a(i)$; *l'ensemble* $\mathbf{P}_{\boldsymbol{a}} T$ *est de cardinal* $((\boldsymbol{a}))$ (*voir* 2.1.4).

En particulier, si S *est une* R*-algèbre finie étale de rang* d, *alors* $\mathbf{P}^{\boldsymbol{a}}(S)$ *est une algèbre finie étale de rang* $((\boldsymbol{a}))$.

Démonstration. — Pour un ensemble fini T, vu comme espace topologique discret, et pour une R-algèbre R', on a clairement une bijection

$$\mathrm{Hom}_{R\text{-}\mathbf{Alg}}\big(\mathbf{M}(T,R), R'\big) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cont}}\big(\mathrm{Spec}(R'), T\big).$$

Par suite, si $T \to V$ et $U \to V$ sont deux applications entre ensembles finis, on a un isomorphisme de R-algèbres

$$\mathbf{M}(T,R) \otimes_{\mathbf{M}(V,R)} \mathbf{M}(U,R) \xrightarrow{\sim} \mathbf{M}(T \times_V U, R).$$

Ceci permet de déterminer $\mathbf{P}^{\boldsymbol{a}}(S)$: d'après 2.6.1, on a

$$\Gamma^d S = \mathbf{M}(\Gamma_d T, R) \quad \text{et} \quad \Gamma^{\boldsymbol{a}} S = \mathbf{M}(\Gamma_{\boldsymbol{a}} T, R),$$

où $\Gamma_{\boldsymbol{a}} T := \prod_i \Gamma_{a(i)} T$; le morphisme $\Gamma^d S \to \Gamma^{\boldsymbol{a}} S$ est associé à l'application somme

$$\sigma : \prod_i \Gamma_{a(i)} T \to \Gamma_{\Sigma a(i)} T, \quad (p_i)_i \mapsto \sum p_i.$$

Le morphisme $\pi : \Gamma^d S \to R$ correspond à l'inclusion $\{*\} \to \Gamma_d T$ d'image l'application constante c de valeur 1 ; le produit fibré, qui définit $\mathbf{P}^{\boldsymbol{a}}(S)$, est donc l'ensemble $\sigma^{-1}(c)$ formé des suites $(p_1, \ldots, p_m) \in \prod_i \Gamma_{a(i)} T$ telles que $\sum_i p_i(t) = 1$ pour tout $t \in T$; les p_i sont donc les fonctions caractéristiques de parties $T_i \subset T$ formant une partition de T, celle d'indice i étant de cardinal $a(i)$; un comptage standard, utilisant l'action du groupe symétrique $\mathfrak{S}_T$, montre que le nombre de telles partitions est

$$((\boldsymbol{a})) = \big((a(1), \ldots, a(m)\big) = \frac{\big(\sum a(i)\big)!}{\prod\big(a(i)!\big)} \cdot \qquad \square$$

Revenons au cas général où S est localement libre de rang d. Si $\mathbb{A} \subset \mathbb{N}^m$ désigne l'ensemble des multiindices de poids d, on a d'après 2.2.5, un isomorphisme

$$\Gamma^d S^m \xrightarrow{\sim} \prod_{\boldsymbol{a} \in \mathbb{A}} \Gamma^{\boldsymbol{a}} S.$$

Par le changement de base $\pi : \Gamma^d S \to R$ on obtient un isomorphisme de R-modules

$$N(S^m) \xrightarrow{\sim} \prod_{\boldsymbol{a} \in \mathbb{A}} \mathbf{P}^{\boldsymbol{a}}(S). \tag{4.1.2}$$

Compte-tenu de la relation $\sum_{\boldsymbol{a} \in \mathbb{A}} ((\boldsymbol{a})) = m^d$, on obtient donc la

Proposition 4.1.3. — *Soit S une R-algèbre finie localement libre de rang d. On suppose que pour tout multiindice $\boldsymbol{a} \in \mathbb{N}^m$ de poids d, la R-algèbre $\mathbf{P}^{\boldsymbol{a}}(S)$ est localement libre de rang $((\boldsymbol{a}))$, ce qui est le cas si S est étale. Alors, pour tout S-module F, projectif de rang m, la norme $N(F)$ est un R-module projectif de rang m^d.*

4.2 Factorisations de l'application norme.

Soient, comme ci-dessus, S une R-algèbre finie localement libre de rang d, et $\boldsymbol{a} \in \mathbb{N}^m$ un multiindice de poids $\sum a(i) = d$. Pour chaque i, l'application composée

$$\begin{aligned} \boldsymbol{p}_i : S &\longrightarrow \Gamma^{a(i)} S \longrightarrow \Gamma^{\boldsymbol{a}} S \longrightarrow \mathbf{P}^{\boldsymbol{a}}(S), \\ x &\longmapsto \text{classe de } 1 \otimes \cdots \otimes \gamma^{a(i)}(x) \otimes \cdots \otimes 1, \end{aligned}$$

est une loi polynôme multiplicative, homogène de degré $a(i)$, et, par définition de $\mathbf{P}^{\boldsymbol{a}}(S)$, on a :

$$\operatorname{norm}_{S/R} = \prod_i \boldsymbol{p}_i. \tag{4.2.1}$$

Cette factorisation est universelle :

Proposition 4.2.2. — *Soient R' une R-algèbre et $(f_1,\ldots,f_m)$ une suite de lois polynômes de S vers R' multiplicatives, homogènes de degré $a(1),\ldots,a(m)$ respectivement, et telles qu'on ait universellement*

$$\operatorname{norm}_{S/R} = \prod f_i.$$

Alors, il existe un unique morphisme de R-algèbres $g : \mathbf{P}^{\boldsymbol{a}}(S) \to R'$ tel que pour tout i, on ait $f_i = g \circ \boldsymbol{p}_i$. $\square$

(Rappelons que l'unique loi polynôme multiplicative homogène de degré 0 est l'application constante de valeur 1, et qu'une loi polynôme multiplicative homogène de degré 1 est simplement un morphisme de R-algèbres.)

Règle 4.2.3. — *Soient $R \to S$ et $R \to S'$ deux R-algèbres, et f, g et h des lois polynômes de S vers S'. On suppose que S est localement libre de rang fini, et que l'on a universellement*

$$\operatorname{norm}_{S/R} = fg = fh,$$

Alors $g = h$; si, de plus, f est multiplicative, g l'est aussi.

Démonstration. — Les hypothèses étant stables par changement de base sur R, il suffit de montrer que pour tous $x, y \in S$, on a

$$g(x) = h(x),$$

et, si f est multiplicative,

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

Ces égalités sont claires si $f(x)$ et $f(y)$ sont des éléments réguliers de S' ; on va se ramener à ce cas par le changement de base $R \to R[X]$; en effet, $\operatorname{norm}_{S/R}(X + x)$ est un polynôme unitaire (2.5.3) ; son image dans $S'[X]$ est donc un élément régulier, ainsi que son facteur $f(X + x)$; on a donc $g(X + x) = h(X + x)$. Utilisant maintenant le changement de base $R[X] \to R$, $X \mapsto 0$, on trouve $g(x) = h(x)$.

Supposons maintenant que f est multiplicative ; dans $S'[X]$, $f(X + x)$ et $f(X + y)$ sont des éléments réguliers, de produit égal à

$$f\big(X^2 + X(x + y) + xy\big) ;$$

on a donc

$$g\big(X^2 + X(x + y) + xy\big) = g(X + x)g(X + y) ;$$

le morphisme associé à $X \mapsto 0$ permet encore de conclure. $\square$

Il est clair que $\mathbf{P}^{(d)}(S) = R$, et que si $\boldsymbol{b} \in \mathbb{N}^m$ se déduit de $\boldsymbol{a}$ par une permutation, alors $\mathbf{P}^{\boldsymbol{a}}(S)$ est canoniquement isomorphe à $\mathbf{P}^{\boldsymbol{b}}(S)$.

Le théorème de Hamilton-Cayley conduit à un isomorphisme

$$\mathbf{P}^{(d-1,1)}(S) \xrightarrow{\sim} S,$$

utilisé dans un autre contexte par Iversen (*cf.* [12, I.3.1, I.4.4, II.2.2]) ; pour le définir, on introduit le « co-transposé » cotrans(x) d'un élément $x \in S$: considérons le polynôme caractéristique de la multiplication par x dans le R-module S :

$$P(X) = \operatorname{norm}(X - x) = X^d - \sigma_1(x)X^{d-1} + \cdots + (-1)^d\sigma_d(x)$$

Le coefficient σ_i est une loi polynôme homogène de degré i de S vers R ; posons

$$\operatorname{cotrans}(x) = (-x)^{d-1} + \sigma_1(x)(-x)^{d-2} + \cdots + \sigma_{d-1}(x).$$

On définit ainsi une loi polynôme de S vers S, homogène de degré $d-1$.

Proposition 4.2.4. — *Avec les notations ci-dessus, on a universellement*

$$\operatorname{norm}(x) = \operatorname{cotrans}(x)x,$$

et la loi polynôme cotrans *est multiplicative. Le morphisme*

$$\mathbf{P}^{(d-1,1)}(S) \longrightarrow S$$

associé à cette factorisation est un isomorphisme.

Démonstration. — L'application σ_d est la norme, de sorte que l'égalité $\operatorname{norm}(x) = \operatorname{cotrans}(x)x$ n'est autre que le théorème de Hamilton-Cayley : $P(x) = 0$. La relation

$$\operatorname{cotrans}(xy) = \operatorname{cotrans}(x)\operatorname{cotrans}(y)$$

est une conséquence de 4.2.3. Il reste à vérifier que S, muni des lois cotrans et id, est « universel » ; soient donc R' une R-algèbre munie de deux lois polynôme $p, q : S \rightrightarrows R'$, homogènes de degré respectif $d-1$ et 1, multiplicatives, et telles que l'on ait universellement

$$\operatorname{norm}(x) = p(x)q(x).$$

Remarquons d'abord que q n'est autre qu'un morphisme de R-algèbres et qu'il s'agit de montrer que $p = q \circ \mathrm{cotrans}$. Or, en prenant l'image de l'égalité $\mathrm{norm}(x) = \mathrm{cotrans}(x)x$, par le morphisme de R-algèbres q, on trouve

$$\mathrm{norm}(x) = q\big(\mathrm{cotrans}(x)\big)q(x);$$

il suffit donc, pour conclure, d'appliquer la règle de simplification 4.2.3.

Pour une algèbre décomposée $S = \mathbf{M}(T,R)$, factoriser l'application norme $m \mapsto \prod m(t)$ consiste simplement à prendre une partition de T et à effectuer d'abord les produits des $m(t)$ pour les t dans chaque bloc de la partition. Une fois précisé, cela donnerait une autre vérification de 4.1.1.

4.3. Cas des algèbres monogènes.

Dans ce paragraphe, on montre essentiellement que pour

$$S = R[X]/(P),$$

où P est un polynôme unitaire, $\mathbf{P}^{\boldsymbol{a}}(S)$ est libre de rang $(\!(\boldsymbol{a})\!)$; la première étape consiste à montrer que $\mathbf{P}^{\boldsymbol{a}}(S)$ « représente » les factorisations de multidegré $\boldsymbol{a}$ du polynôme P. Le passage de la norme à P repose sur le

Fait 4.3.0. — *Notant s la classe de X dans $S = R[X]/(P)$, on a :*

$$\mathrm{norm}_{S[T]/R[T]}(T - s) = P(T). \quad \square$$

Le lemme suivant est classique (par exemple, [5, 6.3.10]).

Lemme 4.3.1. — *Soient T une R-algèbre localement libre de rang d, t un élément de T et $P(X) = \mathrm{norm}_{T/R}(X - t)$ le polynôme caractéristique de t ; désignons par s la classe de X dans $S = R[X]/(P)$; le théorème de Hamilton-Cayley assure l'existence d'un morphisme de R-algèbres $h : S \to T$ tel que $h(s) = t$. Alors le morphisme h est universellement compatible aux normes, autrement dit on a l'égalité suivante entre lois polynômes*

$$\mathrm{norm}_{S/R} = \mathrm{norm}_{T/R} \circ h.$$

Démonstration. — Il suffit de montrer que pour tout $x \in S$, on a

$$\mathrm{norm}_{S/R}(x) = \mathrm{norm}_{T/R}\big(h(x)\big).$$

La définition de P et 4.3.0 donnent

$$\mathrm{norm}_{S/R}(X - s) = P(X) = \mathrm{norm}_{T/R}\big(h(X - s)\big).$$

En particulier, pour tout $r \in R$, on a

$$\operatorname{norm}_{S/R}(r-s) = \operatorname{norm}_{T/R}\bigl(h(r-s)\bigr).$$

Compte tenu de la multiplicativité des normes, il reste donc à vérifier que tout élément de S peut se décomposer, au moins localement, en un produit d'éléments de la forme $r_i - s$. Or, un élément $x \in S$ s'écrit sous la forme $x = Q(s)$, où $Q \in R[X]$ est un polynôme de degré $< d$; puisque $P(s) = 0$, on peut aussi l'écrire sous la forme $x = Q(s) + P(s)$, c'est-à-dire sous la forme $x = F(s)$ où F est un polynôme *unitaire* de degré d; mais d'après [3, A IV, p. 68], un changement de base libre $R \to R'$ permet alors de supposer que F est décomposé : $F(X) = (X - r_1) \cdots (X - r_d)$, donc que $x = (s - r_1) \cdots (s - r_d)$. $\square$

4.3.2. — Soient $P \in R[X]$ un polynôme unitaire de degré d, $S = R[X]/(P)$, et $\boldsymbol{a} \in \mathbb{N}^m$ un multiindice de poids d. Désignons encore par s la classe de X dans S, et posons

$$P_i(T) = \boldsymbol{p}_i(T - s)\,;$$

c'est un polynôme unitaire de degré $a(i)$. D'après 4.2.1, on a dans $\mathbf{P}^{\boldsymbol{a}}(S)[T]$ la factorisation

$$P(T) = \operatorname{norm}_{S/R}(T - s) = \prod_i P_i(T).$$

Cela définit, pour toute R-algèbre R', une application

$$\operatorname{Hom}_{R-\mathbf{Alg}}\bigl(\mathbf{P}^{\boldsymbol{a}}(S), R'\bigr) \longrightarrow \Bigl\{(P_1, \ldots, P_m) \in R'[T]^m\,; \; P_i \text{ unitaire de degré } a(i) \text{ et } P = \prod_i P_i\Bigr\}.$$

Lemme 4.3.3. — *Cette application est bijective.*

Indiquons l'application réciproque : soit $P = \prod_i P_i$ une factorisation dans $R'[T]$ du type indiqué; pour chaque i, considérons l'application composée

$$f_i : S = R[X]/(P) \longrightarrow R'[X]/(P_i) \xrightarrow{\text{norm}} R'.$$

C'est une loi polynôme multiplicative, homogène de degré $\deg(P_i) = a(i)$, et l'on a universellement $\operatorname{norm}_{S/R} = \prod f_i$, comme on le voit en appliquant 4.3.1 à l'anneau produit $T = \prod R'[X]/(P_i)$, et à l'élément $t = (x_1, \ldots, x_m) \in T$, où x_i désigne la classe de X dans $R'[X]/(P_i)$. La propriété universelle de $\mathbf{P}^{\boldsymbol{a}}(S)$ (4.2.2) donne le morphisme cherché $\mathbf{P}^{\boldsymbol{a}}(S) \to R'$. $\square$

Une R-algèbre localement libre S est dite *localement monogène* si elle est localement isomorphe à $R[X]/(P)$, où P est un polynôme unitaire.

THÉORÈME 4.3.4. — *Soit S une R-algèbre localement libre de rang d et localement monogène. Alors pour tout S-module F, projectif de rang m, $N_{S/R}(F)$ est un R-module projectif de rang m^d.*

Démonstration. — En vertu du critère 4.1.3, il suffit de montrer que pour tout $\boldsymbol{a} \in \mathbb{N}^m$ de poids d, la R-algèbre $\mathbf{P}^{\boldsymbol{a}}(S)$ est localement libre de rang $((\boldsymbol{a}))$; quitte à faire un changement de base convenable, on peut supposer que $S = R[X]/(P)$, où P est un polynôme unitaire de degré d. Posons $E = \mathbf{P}^{\boldsymbol{a}}(S)$; dans $E[X]$, on a, d'après 4.3.2, une factorisation

$$P(X) = P_1(X) \cdots P_m(X),$$

où le polynôme P_i est unitaire et de degré $a(i)$; il admet donc une « algèbre de décomposition universelle » $E \to D_i$, libre de rang $a(i)!$ sur E (*cf.* [3, A IV, p. 68]) ; on va montrer que $D_1 \otimes_E D_2 \otimes_E \cdots \otimes_E D_m$ est une R-algèbre de décomposition universelle de P, donc qu'elle est libre de rang $d\,!$ sur R ; comme elle est libre de rang $\prod a(i)!$ sur E, on en tirera que $E = \mathbf{P}^{\boldsymbol{a}}(S)$ est localement libre sur R, de rang $d\,!/\prod a(i)! = ((\boldsymbol{a}))$, ce qui entraînera la conclusion.

Soit donc $R \to C$ une R-algèbre telle que le polynôme P se décompose complètement dans $C[X]$:

$$P(X) = (X - c_1) \cdots (X - c_d), \quad c_i \in C.$$

En regroupant les $a(1)$ premiers facteurs $(X - c_1) \cdots (X - c_{a(1)})$, puis les $a(2)$ suivants, *etc.*, on définit une factorisation de P dans $C[X]$, de multidegré $\boldsymbol{a}$, donc, d'après 4.3.3, un morphisme de R-algèbres $f : E = \mathbf{P}^{\boldsymbol{a}}(S) \to C$ tel que l'image de $P_1(X)$ soit égale à $(X - c_1) \cdots (X - c_{a(1)})$, celle de P_2 soit le produit des $a(2)$ facteurs suivants, *etc.* ; les images des P_i étant décomposées, on a bien le morphisme cherché

$$D_1 \otimes_E D_2 \otimes_E \cdots \otimes_E D_m \longrightarrow C. \quad \square$$

4.4. Un exemple.

Il s'agit du morphisme

$$R = \mathbb{Z}[U, V] \longrightarrow S = \mathbb{Z}[X, Y]$$

défini par

$$U = X^2 \quad \text{et} \quad V = Y^2 \,;$$

il est fini localement libre de rang 4, et d'intersection complète. Cependant, $N(S^2)$ n'est pas un R-module localement libre car son rang n'est pas constant : il est égal à $2^4 = 16$ au point générique ; mais lorsque $U = V = 0$, (et qu'on considère donc le morphisme $\mathbb{Z} \to \mathbb{Z}[X,Y]/(X^2,Y^2)$), ce rang est égal à 17 au dessus de tout corps de caractéristique $\neq 2$, et est égal à 20 en $\mathbb{F}_2$. Comme ce morphisme est le composé de deux morphismes monogènes, cela montre aussi que l'application de transitivité (3.2.5) n'est pas toujours un isomorphisme.

Ce morphisme étant génériquement étale, le rang 16 provient de 4.1.3 ; tout revient donc à calculer le rang au dessus de la « section origine ». Malgré plusieurs tentatives anciennes, ce calcul me semblait inextricable jusqu'à ce que je fasse appel à Fabrice Rouillier, un expert en calcul formel (INRIA Lorraine), qui m'a immédiatement donné le résultat ; en examinant en détail la base de Gröbner fournie par sa machine, j'ai enfin compris ce qui était en jeu, et que ce calcul était conceptuellement assez facile ; il est esquissé ci-dessous.

On considère donc, dans la suite, le morphisme

$$R \longrightarrow S = R[X,Y]/(X^2,Y^2),$$

où R est un anneau pour l'instant quelconque. La formule 4.1.2 donne ici

$$N(S^2) \xrightarrow{\sim} \mathbf{P}^{(4)}(S) \times \mathbf{P}^{(3,1)}(S) \times \mathbf{P}^{(2,2)}(S) \times \mathbf{P}^{(1,3)}(S) \times \mathbf{P}^{(4)}(S).$$

Compte-tenu de 4.2.4, cela se récrit

$$N(S^2) \xrightarrow{\sim} R \times S \times \mathbf{P}^{(2,2)}(S) \times S \times R,$$

et il s'agit de déterminer $\mathbf{P}^{(2,2)}(S)$; on utilise pour cela sa propriété universelle (4.2.2) : cette algèbre représente les factorisations de la norme en produit de 2 lois polynômes multiplicatives homogènes de degré 2 ; en particulier, il y a donc deux telles lois $\boldsymbol{p}_i : S \to \mathbf{P}^{(2,2)}(S)$ telles que $\mathrm{norm} = \boldsymbol{p}_1\boldsymbol{p}_2$.

Soit M l'idéal de S engendré par les classes x et y ; il est libre sur R, de rang 3, de base $\{x, y, xy\}$. Un élément de S s'écrit $t + z$, avec $t \in R$, $z \in M$. En utilisant l'identification $\Gamma^2 S = R \oplus M \oplus \Gamma^2 M$, on écrit

$$\gamma^2(t+z) = t^2 + tz + \gamma^2(z)$$

à la place de $t^2\gamma^2(1) + t1 \times z + \gamma^2(z)$ (mais il vaut mieux se souvenir de cette dernière écriture plus bas !).

Lemme 4.4.1. — *Soit $I \subset \Gamma^2 M$ le sous-R-module engendré par les éléments de la forme $z \times z^2$, pour z parcourant M. Alors I est un idéal de l'anneau $\Gamma^2 S$. Posons $P := \Gamma^2(S)/I = R \oplus M \oplus (\Gamma^2(M)/I)$, et soient $p, q : S \rightrightarrows P$ les lois polynômes de degré 2 définies par*

$$\begin{aligned} p(t+z) &= \text{classe de } \gamma^2(t+z) = t^2 + tz + \text{classe}\big(\gamma^2(z)\big), \\ q(t+z) &= t^2 + (z^2 - tz) + \text{classe}\big(\gamma^2(z)\big). \end{aligned}$$

Alors, p et q sont multiplicatives, on a $\mathrm{norm} = p \cdot q$, *et cette égalité est la factorisation universelle; autrement dit (P, p, q) est isomorphe à $(\mathbf{P}^{(2,2)}(S), \boldsymbol{p}_1, \boldsymbol{p}_2)$.*

Si on écrit un élément $z \in M$ sur la base citée :

$$z = ax + by + cxy,$$

alors, compte-tenu de ce que $M^2 = Rxy$ et $M^3 = 0$, on a

$$z \times z^2 = 2a^2bx \times xy + 2ab^2y \times xy + 2abcxy \times xy.$$

On en déduit immédiatement que

$$2(x \times xy + y \times xy) \in I$$

et que $2xy \times xy \in I$. Par suite,

$$\gamma^2(z^2) = \gamma^2(2abxy) = 4a^2b^2\gamma^2(xy) = 2a^2b^2xy \times xy \in I.$$

La vérification des assertions du lemme utilise les relations 2.4.5. Voici leur traduction en notant $*$ le produit de l'algèbre $\Gamma^2 S$: on a pour $z, z', u, u' \in M$,

$$\begin{aligned} z * z' &= zz' + z \times z', \\ z * (u \times u') &= zu \times u' + u \times zu', \\ z * \gamma^2(z') &= zz' \times z', \\ (z \times z') * (u \times u') &= zu \times z'u' + zu' \times z'u, \\ \gamma^2(z) * \gamma^2(z') &= \gamma^2(zz'). \end{aligned}$$

Ceci étant précisé la vérification de ce que I est un idéal est immédiate, ainsi que le fait que l'on a universellement

$$t^4 = \mathrm{norm}(t+z) = p(t+z) * q(t+z).$$

Comme p est évidemment multiplicative, la règle 4.2.3 entraîne que q l'est aussi. Pour la propriété universelle, on part de deux morphismes de R-algèbres $f, g : \Gamma^2 S \rightrightarrows R'$ tels que l'on ait, universellement,

$$\mathrm{norm} = f \circ \gamma^2 \cdot g \circ \gamma^2,$$

c'est-à-dire

$$t^4 = \mathrm{norm}(t + z) = \big(t^2 + tf(z) + f(\gamma^2(z))\big)\big(t^2 + tg(z) + g(\gamma^2(z))\big).$$

Comme cette égalité est vraie universellement, il faut la voir comme une égalité entre polynômes en t ; d'où, pour tout $z \in M$, les relations :

(i) $$f(z) + g(z) = 0,$$

(ii) $$f(\gamma^2(z)) + f(z)g(z) + g(\gamma^2(z)) = 0,$$

(iii) $$f(z)g(\gamma^2(z)) + g(z)f(\gamma^2(z)) = 0,$$

(iv) $$f(\gamma^2(z))g(\gamma^2(z)) = 0.$$

Les relations (i) et (ii) impliquent que pour tout $z \in M$, on a

$$g(z) = -f(z), \quad g(\gamma^2(z)) = f\big(z^2 + \gamma^2(z)\big).$$

La relation (iii), compte-tenu de (i) et de (ii), et du fait que l'idéal M de S vérifie $M^2 = Rxy$, $M^3 = 0$, devient $f(z \times z^2) = 0$; par symétrie, on a aussi $g(z \times z^2) = 0$; autrement dit, les morphisme f et g se factorisent par $P = \Gamma^2(S)/I$; si on note $h : P \to R'$ le morphisme déduit de f, il devient aisé de vérifier que $f \circ \gamma^2 = h \circ p$ et que $g \circ \gamma^2 = h \circ q$. $\square$

Si R est un corps de caractéristique $\neq 2$, alors I est sous-espace de dimension 3 de $\Gamma^2 M$ (de base $x \times xy$,$y \times xy$, $xy \times xy$) ; par suite, $\mathbf{P}^{(2,2)}(S)$ est de rang 7, et non 6, et $N(S^2)$ est de rang 17. Si R est un corps de caractéristique 2, alors $I = 0$, l'égalité $\mathrm{norm}(s) = (\gamma^2(s))^2$ (pour $s \in S$) est la factorisation universelle de la norme, et $N(S^2)$ est de rang 20.

5. Comparaison avec les constructions dues à Riehm, Gabber, et Knus-Ojanguren.

5.1. — Pour une extension L/K finie séparable de corps, C. Riehm a défini un foncteur « corestriction »

$$\mathrm{Cor}_{L/K} : L\text{-}\mathbf{Mod} \longrightarrow K\text{-}\mathbf{Mod}$$

(*cf.* [16], et aussi [7] et [21] ; c'est dans un manuscrit de N. Bourbaki, daté de 1972 et non publié, que j'ai découvert et compris cette construction ; elle présente de très fortes analogies avec «l'induction tensorielle» introduite par L. Evens en théorie des représentations).

On va montrer que ce foncteur $\mathrm{Cor}_{L/K}$ est isomorphe au foncteur norme introduit plus haut.

Soit $K \to K'$ une extension finie galoisienne, de groupe G, trivialisant $K \to L$; posant

$$T = \mathrm{Hom}_{K\text{-}\mathbf{Alg}}(L, K'),$$

on a donc un isomorphisme de K'-algèbres

$$K' \otimes_K L \xrightarrow{\sim} \mathbf{M}(T, K'), \quad \alpha \otimes \beta \longmapsto \big(t \mapsto \alpha \cdot t(\beta)\big).$$

Si V est un L-espace vectoriel, on a de même la décomposition

$$K' \otimes_K V \xrightarrow{\sim} (K' \otimes_K L) \otimes_L V \xrightarrow{\sim} \oplus V_t, \tag{5.1.1}$$

où V_t désigne le K'-espace obtenu par le changement de base $t : L \to K'$; notons $j_t : V \to V_t$ l'application K-linéaire canonique, de sorte qu'on a

$$j_t(\lambda x) = t(\lambda) j_t(x), \quad \text{pour } \lambda \in L \text{ et } x \in V.$$

Posons

$$W = \bigotimes_{t \in T} V_t,$$

(produit tensoriel sur K'), et soit

$$j : V \longrightarrow W$$

l'application donnée par $j(x) = \otimes j_t(x)$; comme la norme relative à L/K est ici le produit des conjugués : $\mathrm{norm}(\lambda) = \prod t(\lambda)$, on a

$$j(\lambda x) = \mathrm{norm}(\lambda) j(x). \tag{5.1.2}$$

Chaque automorphisme $g \in G$ induit un isomorphisme g-semi-linéaire

$$V_t \longrightarrow V_{gt}$$

qui envoie $j_t(x)$ sur $j_{gt}(x)$; le produit tensoriel de ces isomorphismes est donc un isomorphisme g-semi-linéaire

$$g_W : W \longrightarrow W,$$

qui laisse invariants les éléments $j(x)$. On a défini ainsi une opération de G sur W, et on pose

$$\mathrm{Cor}_{L/K}(V) = W^G.$$

Voici comment on peut construire un isomorphisme de foncteurs

$$N_{L/K} \xrightarrow{\sim} \mathrm{Cor}_{L/K}\,.$$

L'application $j : V \to \mathrm{Cor}(V) = W^G$ s'étend en une loi polynôme qui est normique d'après 5.1.2 ; la propriété universelle du foncteur norme entraîne donc l'existence d'une application K-linéaire fonctorielle

$$N_{L/K}(V) \longrightarrow \mathrm{Cor}_{L/K}(V). \tag{5.1.3}$$

Pour constater que c'est un isomorphisme, on fait le changement de base $K \to K'$, pour se ramener au cas décomposé (3.2.4), et on utilise 5.1.1 ; on obtient donc les isomorphismes

$$K' \otimes_K N(V) \xrightarrow{\sim} N(K' \otimes_K V) \xrightarrow{\sim} \bigotimes_{t\in T} V_t.$$

Or, par descente galoisienne (*cf.* [3, AV, § 10, n° 4]), on a aussi un isomorphisme

$$K' \otimes_K W^G \xrightarrow{\sim} W.$$

La vérification, immédiate, que ces deux isomorphismes sont compatibles avec (5.1.3), permet de conclure. □

5.2. — O. Gabber m'a signalé oralement, il y a quelques années, une construction qui généralise celle de Riehm, et qui me semble très proche du transfert des topologues (*cf.* [1, § 4.2]) ; sauf malentendu de ma part, Gabber doit, lui aussi, supposer que le morphisme est localement monogène pour pouvoir démontrer que son foncteur transforme projectif en projectif.

Soit S une R-algèbre finie localement libre de rang d, et

$$D = \mathbf{P}^{(1,\dots,1)}(S)$$

« l'anneau de décomposition » pour les polynômes caractéristiques des éléments de S (4.2) ; D est donc le quotient $S^{\otimes d}/I$, où l'idéal I est défini comme suit : notons $q_1, q_2, \dots q_d$ les d morphismes $S \to S^{\otimes d}$, ($q_1(s) = s \otimes 1 \otimes \dots \otimes 1$, *etc.*), et $\sigma_m(s)$ le polynôme symétrique élémentaire de degré m en les $q_1(s), q_2(s), \dots, q_d(s)$. Le polynôme caractéristique d'un élément $s \in S$ s'écrit

$$Pc(X,s) = X^d - a_1(s)X^{d-1} + \cdots + (-1)^i a_i(s)X^{d-i} + \cdots + (-1)^d a_d(s).$$

L'idéal I est engendré par les $a_m(s) - \sigma_m(s)$, pour $m = 1, \dots d$, et pour s parcourant S ; on a donc la décomposition

$$Pc(X,s) = \prod \big(X - q_i(s)\big)$$

dans $D[X]$, et $(D, q_1, q_2, \dots q_d)$ est universel pour cette propriété. Partant d'un S-module F, le groupe symétrique $\mathfrak{S}_d$ opère sur le D-module $F^{\otimes d}/IF^{\otimes d}$, et on pose

$$N'(F) = (F^{\otimes d}/IF^{\otimes d})^{\mathfrak{S}_d}.$$

L'application $x \mapsto x^{\otimes d}$ définit une application $F \to N'(F)$, qui est normique ; on dispose donc d'un morphisme de foncteurs $N \to N'$; c'est un isomorphisme lorsque S est étale sur R, et probablement aussi lorsque S est localement monogène.

5.3. — Pour un morphisme $R \to S$ fini étale, Knus et Ojanguren ont construit un foncteur $N'' : S\text{-}\mathbf{Mod} \to R\text{-}\mathbf{Mod}$ par descente à partir du cas décomposé [14] ; la liste de ses propriétés est donnée dans leur théorème 3.2 (il faut oublier la propriété (2)) ; les propriétés (6) et (7) montrent qu'il existe un morphisme de foncteurs $N \to N''$, et la propriété (1) entraîne que c'est un isomorphisme.

5.4. — L'isomorphisme — dans le cas étale — entre ces trois foncteurs et celui qui est l'objet de cet article ne doit pas faire oublier la différence radicale entre leur construction : ils sont tous les trois définis comme noyau, tandis que le foncteur norme est un quotient, solution d'un problème universel ; l'usage de ce dernier est ainsi plus naturel (fonctoriel), et la plupart des vérifications qu'il requiert sont complètement formelles, comme le lecteur a pu le constater.

6. Norme d'algèbres commutatives

La plupart des exposés sur le foncteur corestriction, relatif à une extension L/K finie séparable, culminent dans son application aux algèbres centrales simples (voir [7], [16], [21],...) : en effet, ce foncteur «incarne» parfaitement la corestriction cohomologique

$$\mathrm{Br}(L) = H^2(H, \overline{K}^\times) \longrightarrow \mathrm{Br}(K) = H^2(G, \overline{K}^\times).$$

(Ici, $\overline{K}$ est une clôture algébrique de K contenant $L, G = \mathrm{Gal}(\overline{K}/K)$ et $H = \mathrm{Gal}(\overline{K}/L)$, *cf.* [19, ch. X]). Cet aspect important est bien connu, et ne sera pas abordé (voir cependant 7.3) ; par contre, le foncteur norme est appliqué ici aux algèbres commutatives, d'une part pour mettre en évidence sa ressemblance avec la restriction de Weil et le « transfert », et d'autre part pour montrer certaines de ses propriétés pathologiques lorsque L est radiciel sur K.

6.1. — Dans tout ce qui suit on considère une R-algèbre S finie localement libre de rang d, et la restriction du foncteur norme à la catégorie des S-algèbres commutatives :

$$N_{S/R} : S\text{-}\mathbf{Alg} \longrightarrow R\text{-}\mathbf{Alg}\,.$$

Rappelons (2.5.1 et 3.2.5) que pour une R-algèbre A et une S-algèbre B, on établit une bijection entre $\mathrm{Hom}_{R\text{-}\mathbf{Alg}}(N_{S/R}(B), A)$ et l'ensemble des lois polynômes $B \to A$ multiplicatives et qui prolongent norm : $S \to R$, en composant un morphisme de R-algèbres f et la loi normique universelle ν,

$$B \xrightarrow{\nu} N_{S/R}(B) \xrightarrow{f} A.$$

6.2 Foncteur norme et restriction de Weil.

La restriction de Weil est le foncteur

$$\mathbf{R}_{S/R} : S\text{-}\mathbf{Alg} \longrightarrow R\text{-}\mathbf{Alg}$$

adjoint à gauche au changement de base (*cf.* [2, p. 191], [6, p. 30], [15, p. 82]) ; on a donc une bijection fonctorielle en les R-algèbres A et les S-algèbres B,

$$\mathrm{Hom}_{R\text{-}\mathbf{Alg}}(\mathbf{R}_{S/R}(B), A) \xrightarrow{\sim} \mathrm{Hom}_{S\text{-}\mathbf{Alg}}(B, S \otimes_R A).$$

Par ailleurs, en composant un morphisme de S-algèbres $B \to S \otimes A$ avec l'application norme $S \otimes A \to A$, on obtient une loi polynôme multiplicative qui prolonge la norme ; d'où une application fonctorielle en A et B,

$$\mathrm{Hom}_{S\text{-}\mathbf{Alg}}(B, S \otimes_R A) \longrightarrow \mathrm{Hom}_{R\text{-}\mathbf{Alg}}(N(B), A).$$

Par composition avec l'isomorphisme qui caractérise $\mathbf{R}_{S/R}$, on trouve

$$\mathrm{Hom}_{R\text{-}\mathbf{Alg}}(\mathbf{R}_{S/R}(B), A) \to \mathrm{Hom}_{R\text{-}\mathbf{Alg}}(N(B), A)\,;$$

comme c'est une application fonctorielle en A et B, il y a un morphisme de foncteurs

$$N_{S/R} \longrightarrow \mathbf{R}_{S/R}. \tag{6.2.1}$$

Proposition 6.2.2. — *Lorsque S est étale sur R, le morphisme* (6.2.1) *est un isomorphisme.*

Vérification. — Comme ces deux foncteurs commutent aux changements de base sur R, on peut supposer que S est décomposée, donc de la forme $S = \mathbf{M}(T, R)$; une S-algèbre B est alors une famille (B_t), indexée par T, de R-algèbres, et on a des bijections

$$\mathrm{Hom}_{S\textbf{-Alg}}(B, S \otimes_R A) \xrightarrow{\sim} \prod_t \mathrm{Hom}_{R\textbf{-Alg}}(B_t, A) \xrightarrow{\sim} \mathrm{Hom}_{R\textbf{-Alg}}(\otimes_t B_t, A);$$

par ailleurs,

$$N_{S/R}(B) = \bigotimes_t B_t.$$

6.2.3. Remarques. — Lorsque $R \to S$ est une extension radicielle de corps, de degré 2, le morphisme (6.2.1) n'est pas un isomorphisme, même si on se restreint à la catégorie des S-algèbres finies étales (voir 6.4.3).

6.2.4. — En termes géométriques, $\mathrm{Spec}(\mathbf{R}_{S/R}(B))$ représente le foncteur des sections de $\mathrm{Spec}(B) \to \mathrm{Spec}(S)$, au dessus de schémas sur $\mathrm{Spec}(R)$; la première phrase de l'introduction fait allusion à cet énoncé, et à ses analogues topologiques.

6.3 Norme d'algèbres étales ; description galoisienne.

Dans ce paragraphe, on se fixe une extension de corps $K \to L$, finie séparable, et une clôture séparable K_s de L ; on pose $G = \mathrm{Gal}(K_s/K)$ et $H = \mathrm{Gal}(K_s/L)$; la norme considérée ici, $N = N_{L/K}$, ne portera que sur des L-algèbres finies étales.

6.3.1. — La catégorie K-**Etf** des K-algèbres finies étales est anti-équivalente à celle des G-ensembles finis (avec, bien entendu, action continue de G) (*cf.* [3, A, V, p. 73]). Plus précisément, à une K-algèbre finie étale A est associé le G-ensemble

$$X = \mathrm{Hom}_{K\textbf{-Alg}}(A, K_s).$$

L'accouplement $A \times X \to K_s$, $(a, \xi) \mapsto \xi(a)$, donne un isomorphisme

$$A \xrightarrow{\sim} \mathbf{M}_G(X, K_s),$$

où le membre de droite désigne l'anneau des applications de G-ensembles de X vers K_s. Mis en regard du précédent, l'isomorphisme, (*cf.* [3, A, V, p. 61]),

$$K_s \otimes_K A \xrightarrow{\sim} \mathbf{M}(X, K_s)$$

montre l'équivalence entre les trois démarches suivantes : localiser, passer à la clôture séparable, oublier l'action de G.

PROPOSITION 6.3.2. — *Sous les hypothèses précédentes, le foncteur norme*

$$N_{L/K} : L\text{-}\mathbf{Etf} \longrightarrow K\text{-}\mathbf{Etf},$$

correspond, via les anti-équivalences rappelées ci-dessus, au foncteur

$$H\text{-}\mathbf{Ens} \longrightarrow G\text{-}\mathbf{Ens}, \quad Y \longmapsto \mathbf{M}_H(G, Y).$$

Ce foncteur $\mathbf{M}_H(G, -)$ est l'adjoint à droite de la restriction de G à H : pour un G-ensemble X et un H-ensemble Y, on a une bijection

$$\mathbf{M}_H(X, Y) \xrightarrow{\sim} \mathbf{M}_G(X, \mathbf{M}_H(G, Y)).$$

La structure de G-ensemble à gauche sur $\mathbf{M}_H(G, Y)$ est donnée par la multiplication à droite dans G : $({}^g u)(g') = u(g'g)$. (L'adjoint *à gauche* de la restriction est donné, quant à lui, par le produit contracté $Y \mapsto G \wedge^H Y$; ces deux foncteurs ne sont pas isomorphes).

Ceci étant précisé, la vérification de 6.3.2 est formelle en utilisant la restriction de Weil. $\square$

6.4 Contre-exemples relatifs à une extension radicielle.

Dans ce paragraphe on se place en caractéristique positive p, et on considère une extension de corps $K \subset L$ radicielle de degré p, de sorte que $L^p \subset K$, et que l'on a pour $x \in L$, $\operatorname{norm}_{L/K}(x) = x^p$.

Soit $L \to L'$ une extension finie séparable de degré p ; on sait que si K' est la clôture séparable de K dans L', on a un isomorphisme

$$K' \otimes_K L \xrightarrow{\sim} L' ;$$

en particulier, $L'^p \subset K'$; cela fournit une loi normique $L' \to K'$, $x \mapsto x^p$.

$$\begin{array}{ccc} K' & \longrightarrow & L' \\ \uparrow & & \uparrow \\ K & \longrightarrow & L. \end{array}$$

Pour éviter des confusions, on posera

$$\lambda = \mathrm{norm}_{L'/L} : L' \longrightarrow L\,;$$

il se trouve que c'est aussi une loi normique relativement à $K \to L$, puisque pour $x \in L$ et $y \in L'$, on a

$$\lambda(xy) = x^p \lambda(y) = \mathrm{norm}(x)\lambda(y).$$

LEMME 6.4.1. — *Sous les hypothèses précédentes, le morphisme d'algèbres*

$$N_{L/K}(L') \longrightarrow L \times K',$$

déduit de la loi normique $x \mapsto (\lambda(x), x^p)$ *est surjectif; si* $p = 2$, *il est même bijectif.*

En particulier, la norme d'une algèbre étale n'est donc pas toujours étale !

Démonstration. — D'après le théorème chinois, il suffit de montrer que chacun des morphismes $N_{L/K}(L') \to L$ et $N_{L/K}(L') \to K'$ est surjectif puisque les extensions L/K et K'/K ne sont pas isomorphes ; par ailleurs, quitte à faire une extension finie de K, on peut supposer que K', et L', sont décomposées, donc de la forme $K' = \mathbf{M}(T, K)$ et $L' = \mathbf{M}(T, L)$, où T est un ensemble de cardinal p (la notation plus légère K^p prêterait vraiment à confusion dans ce contexte !).

Pour voir que $N_{L/K}(L') \to L$ est surjectif, il suffit de constater que l'application λ elle-même est déjà surjective (c'est l'application $\mathbf{M}(T, L) \to L$ donnée par le produit des composantes). Pour montrer que le second morphisme $N_{L/K}(L') \to K'$ est surjectif, il suffit, puisqu'il est K-linéaire, de montrer que son image contient les idempotents de $K' = \mathbf{M}(T, K)$; or, soient e un idempotent et $\nu_{L'} : L' \to N_{L/K}(L')$ la loi normique universelle ; comme $e \in K' \subset L'$, on a $e = e^p =$ image de $\nu_{L'}(e)$.

Si, de plus, $p = 2$, alors $N_{L/K}(L')$ est de rang 4, puisque l'extension $K \to L$ est monogène (5.2.3), ce qui implique que le morphisme surjectif donné est un isomorphisme. $\square$

6.4.2 La norme ne commute pas toujours au produit tensoriel. — Autrement dit, l'application φ de 3.2.5 n'est pas toujours un isomorphisme. Pour le voir, on reprend les notations de 6.4.1, avec $p = 2$, et on va vérifier que le morphisme

$$\varphi : N_{L/K}(L') \otimes_K N_{L/K}(L') \longrightarrow N_{L/K}(L' \otimes_L L')$$

n'est pas un isomorphisme. Comme $K \to K'$ est étale de degré 2, on a les décompositions

$$K' \otimes_K K' \xrightarrow{\sim} K' \times K' \quad \text{et} \quad L' \otimes_L L' \xrightarrow{\sim} L' \times L'.$$

Par suite, on a une décomposition en produit d'anneaux

$$N(L' \otimes_L L') \xrightarrow{\sim} N(L') \times E \times N(L'),$$

où E est une algèbre qu'il est inutile d'expliciter ; d'après 6.4.1, l'anneau $N(L')$ admet un quotient isomorphe à L, donc $N(L' \otimes_L L')$ admet un quotient isomorphe à $L \times L$; par ailleurs, toujours d'après 6.4.1, on a des isomorphismes

$$N(L')\otimes N(L') \xrightarrow{\sim} (L\times K')\otimes(L\times K') \xrightarrow{\sim} L\otimes L\times L\otimes K'\times K'\otimes L\times K'\otimes K'$$

(tous les produits tensoriels sont effectués sur K). Cette K-algèbre n'admet pas de quotient isomorphe à $L \times L$. $\square$

6.4.3. La norme et la restriction de Weil ne sont pas toujours isomorphes. — En effet, restons toujours dans la situation de 6.4.1, avec $p = 2$. On va montrer que $\mathbf{R}_{L/K}(L')$ et K' représentent le même foncteur, ce qui entraînera qu'ils sont isomorphes.

Comme $L' = K' \otimes_K L$, on a, pour une K-algèbre M, des isomorphismes

$$\begin{aligned}\mathrm{Hom}_{K\textbf{-Alg}}(\mathbf{R}_{L/K}(L'), M) &\xrightarrow{\sim} \mathrm{Hom}_{L\textbf{-Alg}}(L', L \otimes_K M)\\ &\xrightarrow{\sim} \mathrm{Hom}_{K\textbf{-Alg}}(K', L \otimes_K M).\end{aligned}$$

Montrons qu'on a aussi un isomorphisme

$$\mathrm{Hom}_{K\textbf{-Alg}}(K', L \otimes_K M) \xrightarrow{\sim} \mathrm{Hom}_{K\textbf{-Alg}}(K', M),$$

c'est-à-dire que tout morphisme $u : K' \to L \otimes_K M$ est à valeurs dans M ; or, la sous-M-algèbre de $L \otimes_K M$ engendrée par $u(K')$ est à la fois non ramifiée sur M comme quotient de $K' \otimes_K M$, et radicielle sur M, comme sous-anneau de $L \otimes_K M$; c'est donc M !

7. Calculs de $N_{S/R}(S \otimes_R E)$.

Ce paragraphe, où S désigne une R-algèbre finie étale de rang d, est consacré aux relations, pour un R-module E, entre $N_{S/R}(S\otimes_R E)$ et $E^{\otimes d}$; elles ne sont pas simples.

Si S est décomposé, il y a, bien sûr, un isomorphisme fonctoriel en E entre $N(S\otimes E)$ et $E^{\otimes d}$ (3.2.4). Pour S quelconque mais si E est inversible on a encore un isomorphisme canonique $N_{S/R}(S\otimes_R E) \xrightarrow{\sim} E^{\otimes d}$. Mais en général, il n'y a pas de tels isomorphismes; d'ailleurs, un phénomène analogue apparaît aussi avec le transfert en topologie (*cf.* [1, p. 99]).

Cependant, si A est une R-algèbre d'Azumaya, alors les algèbres $N_{S/R}(S\otimes_R A)$ et $A^{\otimes d}$ sont isomorphes localement pour la topologie de Zariski sur $\mathrm{Spec}(R)$ (7.3.4). Un résultat analogue reste vrai pour un module E quelconque, au moins en caractéristique nulle (7.4) : il y a des décompositions canoniques en somme directe de $N(S\otimes E)$ et de $E^{\otimes d}$, indexées par les partages de l'entier d, et dont les facteurs de même indice sont isomorphes localement pour la topologie de Zariski. Ces décompositions sont liées aux foncteurs de Schur comme on pouvait le pressentir en remarquant que les R-schémas en groupes $\mathbf{GL}(E)$ et $\mathbf{Aut}(S/R)$ opèrent sur (le faisceau étale associé à) $N(S\otimes E)$, et que le groupe $\mathrm{Aut}(S/R)$ est localement isomorphe au groupe constant $\mathfrak{S}_d$. Ces développements sont précédés de calculs explicites dans deux cas simples.

L'adverbe « *localement* » renvoie toujours à la topologie étale; lorsqu'il s'agira de la topologie de Zariski, cela sera mentionné explicitement.

7.1. Cas où E est une R-algèbre finie étale.

Considérons d'abord une situation proche de la topologie : celle des ensembles finis munis d'une action continue d'un groupe de Galois. On se replace donc sous les hypothèses et les notations de 6.3 (norme d'algèbres finies étales, relative à une extension finie séparable de corps L/K).

Une K-algèbre finie étale est isomorphe à $C^{\otimes d}$ si son G-ensemble est de la forme $\mathbf{M}(T,X)$ où $X=\mathrm{Hom}_{K\text{-}\mathbf{Alg}}(C,K_s)$ et où T est un ensemble de cardinal d, avec action *triviale* de G. Considérons une K-algèbre finie étale A, et son G-ensemble associé $Y=\mathrm{Hom}_{K\text{-}\mathbf{Alg}}(A,K_s)$.

La bijection $\mathrm{Hom}_{K\text{-}\mathbf{Alg}}(A,K_s)=\mathrm{Hom}_{L\text{-}\mathbf{Alg}}(L\otimes_K A,K_s)$ montre que le H-ensemble associé à la L-algèbre $L\otimes_K A$ n'est autre que l'ensemble Y, mais muni de l'action de H obtenue par restriction de celle de G. D'après 6.3.1, le G-ensemble associé à $N_{L/K}(L\otimes_K A)$ est $\mathbf{M}_H(G,Y)$. Or, si une application $u : G \longrightarrow Y$ est H-invariante, alors en posant $v(g)=g^{-1}u(g)$, ce qui a un sens puisque G opère sur Y, l'application v passe au quotient en une application $H\backslash G \rightarrow Y$ (on note $H\setminus G$ l'ensemble des classes à droite Hg; c'est un G-ensemble à droite de cardinal $d = [L : K]$) ; on a donc une application

$$\mathbf{M}_H(G, Y) \longrightarrow \mathbf{M}(H \setminus G, Y)\,;$$

c'est une bijection. Mais, par transport, l'action à gauche de G sur $\mathbf{M}(H\backslash G, Y)$ est alors associée aux actions de G, à gauche sur Y, *et à droite sur* $H \setminus G$. Cette dernière n'est pas triviale, donc l'algèbre $N_{L/K}(L \otimes_K A)$ n'est en général pas isomorphe à $A^{\otimes d}$.

7.2. Cas où *S* est de rang 2.

On suppose ici que S est une R-algèbre finie étale de rang 2, et que 2 est inversible dans R. On a alors un isomorphisme fonctoriel en le R-module E

$$N_{S/R}(S \otimes_R E) \xrightarrow{\sim} \Gamma^2 E \times \wedge^2 S \otimes \wedge^2 E. \tag{7.2.1}$$

Les hypothèses entraînent en effet que le noyau L de la trace $\mathrm{Tr} : S \to R$ est un supplémentaire de R (isomorphe, donc, à $\wedge^2 S$), et que le produit dans $S = R \oplus L$ est déterminée par un isomorphisme $q : L^{\otimes 2} \xrightarrow{\sim} R$; avec ces notations, on a pour $r \in R$ et $\lambda \in L$,

$$\mathrm{norm}(r + \lambda) = r^2 - q(\lambda^{\otimes 2}).$$

Pour un R-module (quelconque) E, on a, d'après (2.4.3.1), un isomorphisme $\Gamma^2(L \otimes E) \xrightarrow{\sim} L^{\otimes 2} \otimes \Gamma^2 E$; il existe donc une loi polynôme

$$\varphi : S \otimes E = E \oplus L \otimes E \longrightarrow \Gamma^2 E$$

telle que

$$\varphi(x + \lambda \otimes y) = \gamma^2(x) - q(\lambda^{\otimes 2})\gamma^2(y)\,;$$

c'est une loi normique, comme on peut le constater en se ramenant au cas où $L = R$. On définit une autre loi normique

$$\psi : S \otimes E \to L \otimes \wedge^2 E$$

en posant

$$\psi(x + \lambda y) = \lambda \otimes x \wedge y.$$

La propriété universelle du foncteur norme donne alors l'application (7.2.1) ; en se ramenant au cas où S est isomorphe à $R \times R$, on vérifie que cette application est un isomorphisme.

Comme 2 est inversible dans R, l'application

$$\Gamma^2 E \times \wedge^2 E \to E^{\otimes 2}$$

définie par

$$\big(\gamma^2(x), y \wedge z\big) \longmapsto x \otimes x + y \otimes z - z \otimes y$$

est un isomorphisme ; il est donc clair que c'est la présence du module inversible $\wedge^2 S$ qui empêche les modules $N_{S/R}(S \otimes_R E)$ et $E^{\otimes 2}$ d'être isomorphes.

7.3. Cas des algèbres d'Azumaya.

Si A est une R-algèbre d'Azumaya on va montrer qu'il existe un $A^{\otimes d}$-module à droite L, localement isomorphe à $A^{\otimes d}$, et un isomorphisme de R-algèbres

$$N_{S/R}(S \otimes_R A) \xrightarrow{\sim} \mathrm{End}_{A^{\otimes d}}(L).$$

En particulier, les R-algèbres $N_{S/R}(S \otimes_R A)$ et $A^{\otimes d}$ sont donc isomorphes localement pour la topologie de Zariski sur $\mathrm{Spec}(R)$.

Ce dernier résultat a été établi par Tignol dans [21], pour une extension séparable de corps, en utilisant la définition de Riehm et des techniques galoisiennes assez fines ; sa méthode est donc différente de celle suivie ici qui utilise le langage des torseurs tel qu'il est introduit, par exemple, dans [20, p. 43 et 44] (mais nous nommons torseur ce que Serre appelle « espace principal homogène », et nous notons $P \wedge^A F$ ce qu'il écrit $P \times^A F$; c'est le quotient de $P \times F$ par l'action diagonale du groupe A).

Commençons, pour un R-module E, par décrire $N_{S/R}(S \otimes_R E)$ comme le module $E^{\otimes d}$ tordu par le $\mathfrak{S}_d$-torseur qui définit S. Soit

$$\mathcal{U} = \underline{\mathrm{Isom}}_{R\text{-}\mathbf{Alg}}(S, R^d)$$

le faisceau (pour la topologie étale sur $\mathrm{Spec}(R)$) défini par

$$\mathcal{U}(R') = \mathrm{Isom}_{R'\text{-}\mathbf{Alg}}(R' \otimes_R S, R'^d) ;$$

c'est un torseur à droite sous le groupe $\underline{\mathrm{Aut}}_{R\text{-}\mathbf{Alg}}(R^d)$ dont l'ensemble des sections au-dessus d'un R' connexe est égal au groupe symétrique $\mathfrak{S}_d$; nous le noterons encore $\mathfrak{S}_d$; précisons qu'un élément de $\mathcal{U}(R')$ est une suite $u = (u_1, \ldots, u_d)$ de morphismes de R-algèbres $u_i : S \to R'$, et que pour $\sigma \in \mathfrak{S}_d$, on a $u^\sigma := (u_{\sigma 1}, \ldots, u_{\sigma d})$.

Pour un R-module F, rappelons que l'on note $\underline{F}$ le faisceau $R' \mapsto R' \otimes_R F$. Le résultat suivant est une conséquence immédiate de la théorie de la descente fidèlement plate :

LEMME 7.3.1. — *Soit F un R-module muni d'une action linéaire de $\mathfrak{S}_d$. Alors il existe un R-module, noté (abusivement) $\mathcal{U} \wedge^{\mathfrak{S}_d} F$, tel que le faisceau $\underline{\mathcal{U} \wedge^{\mathfrak{S}^d} F}$ soit le faisceau associé à $R' \mapsto \mathcal{U}(R') \wedge^{\mathfrak{S}_d} R' \otimes_R F$.*

Esquisse de démonstration. — On choisit un R' fidèlement plat tel que $\mathcal{U}(R') \neq \emptyset$, et un $u \in \mathcal{U}(R')$; les deux images de u dans $\mathcal{U}(R' \otimes_R R')$ diffèrent par une section de $\mathfrak{S}_d$ au-dessus de $R' \otimes_R R'$, laquelle opère sur $R' \otimes_R R' \otimes_R F$ et définit donc une donnée de descente sur $R' \otimes F$; le module cherché est celui obtenu par descente. $\square$

PROPOSITION 7.3.2. — *On a un isomorphisme de foncteurs en le R-module E*

$$N_{S/R}(S \otimes_R E) \xrightarrow{\sim} \mathcal{U} \wedge^{\mathfrak{S}_d} E^{\otimes d}.$$

En effet, pour un R' tel que $\mathcal{U}(R') \neq \emptyset$, et un $u \in \mathcal{U}(R')$, c'est-à-dire un isomorphisme de R'-algèbres $u : R' \otimes_R S \xrightarrow{\sim} R'^d$, on a par composition un isomorphisme

$$N(R' \otimes S \otimes E) \xrightarrow{\text{déduit de u}} N(R'^d \otimes E)$$

$$\xrightarrow{3.2.4} R' \otimes E^{\otimes d} R' \otimes E^{\otimes d}$$

$$\xrightarrow{\xi \mapsto \text{classe de } (u,\xi)} \mathcal{U}(R') \wedge^{\mathfrak{S}_d} R' \otimes E^{\otimes d}.$$

On vérifie immédiatement que cet isomorphisme ne dépend pas du choix de u, et ensuite qu'il est fonctoriel en R'. $\square$

On s'intéresse maintenant à une algèbre d'Azumaya, c'est-à-dire une algèbre localement isomorphe à $\mathrm{End}(P)$, où P est un module projectif de type fini.

PROPOSITION 7.3.3. — *Soit A une R-algèbre d'Azumaya, et $d > 0$ un entier. Alors il existe un homomorphisme de groupes $\theta : \mathfrak{S}_d \to (A^{\otimes d})^\times$ tel que pour toute suite $a_1, \ldots, a_d$ d'éléments de A, et tout $\sigma \in \mathfrak{S}_d$, on ait*

$$\theta(\sigma) \cdot a_1 \otimes \cdots \otimes a_d \cdot \theta(\sigma)^{-1} = a_{\sigma^{-1}1} \otimes \cdots \otimes a_{\sigma^{-1}d}$$

Esquisse de démonstration (*cf.* [11, lemma 1.1]). — Lorsque $A = \mathrm{End}(P)$, avec P projectif de type fini, le produit tensoriel de d applications définit un isomorphisme

$$\varphi : \mathrm{End}(P)^{\otimes d} \xrightarrow{\sim} \mathrm{End}(P^{\otimes d})\,;$$

on prend pour $\theta(\sigma)$ l'élément de $\mathrm{End}(P)^{\otimes d}$ tel que $\varphi(\theta(\sigma))$ soit l'automorphisme de permutation de $P^{\otimes d}$ associé à σ. Cette construction est stable sous l'action de $\mathrm{PGL}(P)$ et se prolonge donc à une algèbre d'Azumaya quelconque. $\square$

Cette propriété, spécifique aux algèbres d'Azumaya, est la seule à être utilisée dans la suite, mais c'est un passage obligé ; d'ailleurs, elle intervient aussi dans la démonstration de Tignol, pourtant fort différente. Cette propriété met en évidence une autre action de $\mathfrak{S}_d$ sur $A^{\otimes d}$, la multiplication à gauche par les $\theta(\sigma)$, et donc la possibilité d'une nouvelle « torsion » ; passer de l'une à l'autre est l'idée cruciale — malgré sa simplicité — pour démontrer le théorème qui suit.

Soient G un groupe, U un G-torseur à droite, et B un anneau muni d'un homomorphisme de groupes $\theta : G \to B^\times$ (pour l'instant, G et U sont des ensembles, et non des faisceaux). Pour $g \in G$, l'application $b \mapsto gb := \theta(g)b$ est un automorphisme du B-module à droite B_d ; on pose :

$$L = U \wedge^G B_d\,;$$

c'est un B-module à droite ; pour tout $u \in U$, l'application

$$B_d \longrightarrow L, \quad b \longmapsto \text{classe de } (u, b),$$

est un isomorphisme de B-modules à droite.

Pour $g \in G$, la conjugaison $b \mapsto gbg^{-1}$ est un automorphisme de l'anneau B ; on note ${}_UB$ l'anneau obtenu en tordant B au moyen de U, relativement à cette action de G ; pour tout $u \in U$, l'application $B \to {}_UB$, $b \mapsto$ classe de (u, b), est un isomorphisme d'anneaux.

Clé 7.3.4. — *On a un isomorphisme canonique d'anneaux*

$${}_UB \xrightarrow{\sim} \mathrm{End}_B(L).$$

Démonstration. — Pour chaque $u \in U$, on a par composition un isomorphisme

$${}_UB \xrightarrow{\sim} B \xrightarrow{\text{mult. à gauche}} \mathrm{End}_B(B_d) \xrightarrow{\sim} \mathrm{End}_B(L).$$

Il ne dépend pas du choix de u puisque tout élément de U est de la forme ug, pour un unique $g \in G$, et qu'on a, pour $b, c \in B$,

$$(gbg^{-1})(gc) = g(bc). \quad \square$$

Théorème 7.3.5. — *Soient S une R-algèbre finie étale de rang d, et A une R-algèbre d'Azumaya. Alors, il existe un $A^{\otimes d}$-module à droite L, localement isomorphe à $A^{\otimes d}$, et un isomorphisme de R-algèbres*

$$N_{S/R}(S \otimes_R A) \xrightarrow{\sim} \mathrm{End}_{A^{\otimes d}}(L). \tag{7.3.5.1}$$

En particulier, les R-algèbres $N_{S/R}(S \otimes_R A)$ et $A^{\otimes d}$ sont isomorphes localement pour la topologie de Zariski sur $\operatorname{Spec}(R)$.

Démonstration. — D'après 7.3.2, $N(S \otimes A)$ est isomorphe à l'algèbre obtenue en tordant $A^{\otimes d}$ par $\mathcal{U}$ relativement à l'action de $\mathfrak{S}_d$ par permutation des facteurs ; notons ${}_{\mathcal{U}}A^{\otimes d}$ cette algèbre.

Choisissons un homomorphisme de groupes $\mathfrak{S}_d \to (A^{\otimes d})^{\times}$ comme dans 7.3.3, et introduisons le $A^{\otimes d}$-module à droite $L = \mathcal{U} \wedge^{\mathfrak{S}_d} A^{\otimes d}$, l'action de $\mathfrak{S}_d$ étant ici la multiplication à gauche ; l'existence de L est assurée par 7.3.1.

Pour un R' connexe et tel que $\mathcal{U}(R') \neq \emptyset$, donc tel que l'ensemble $\mathcal{U}(R')$ soit un torseur sous le groupe $\mathfrak{S}_d$, on a, d'après 7.3.4, un isomorphisme d'anneaux

$$_{\mathcal{U}(R')}(R' \otimes A^{\otimes d}) \xrightarrow{\sim} \operatorname{End}_{R' \otimes A^{\otimes d}}\big(\mathcal{U}(R') \wedge^{\mathfrak{S}_d} (R' \otimes A^{\otimes d})\big).$$

C'est un isomorphisme de préfaisceaux en R' ; en passant aux faisceaux associés, puis à leurs sections au dessus de l'objet final R, on obtient (7.3.5.1).

Si R' est connexe et si $\mathcal{U}(R') \neq \emptyset$, on voit que

$$R' \otimes L = \mathcal{U}(R') \wedge^{\mathfrak{S}_d} R' \otimes A^{\otimes d}$$

est un $R' \otimes A^{\otimes d}$-module à droite libre de rang 1, donc L est isomorphe à $A^{\otimes d}$, localement pour la topologie de Zariski sur $\operatorname{Spec}(R)$ (EGA IV, 2.5.8). □

Remarque 7.3.6. — Le R-module L est projectif de type fini, tout comme $A^{\otimes d}$, et la structure de $A^{\otimes d}$-module à droite sur L donne un morphisme d'algèbres

$$(A^{\otimes d})^{\mathrm{opp}} \longrightarrow \operatorname{End}_R(L)$$

Le commutant de cette sous-algèbre est par définition $\operatorname{End}_{A^{\otimes d}}(L)$; on a donc (*cf.* [13, p. 95, cor. 5.3]) un isomorphisme

$$\operatorname{End}_{A^{\otimes d}}(L) \otimes_R (A^{\otimes d})^{\mathrm{opp}} \xrightarrow{\sim} \operatorname{End}_R(L)$$

Cela montre que $\operatorname{End}_{A^{\otimes d}}(L)$, donc aussi $N(S \otimes A)$, et $A^{\otimes d}$ sont Morita-équivalentes ; en termes du groupe de Brauer, cela se traduit par le fait que le composé $\operatorname{Br}(R) \to \operatorname{Br}(S) \xrightarrow{N} \operatorname{Br}(R)$ est la multiplication par d, ce qu'on savait déjà grâce à la cohomologie étale !

7.4 En caractéristique nulle.

On suppose ici que R est une $\mathbb{Q}$-algèbre mais il y a certainement une façon d'énoncer la proposition 7.4.6 qui la rendrait vraie sans cette restriction ; il faudrait sans doute, utiliser les foncteurs de Schur sur $\mathbb{Z}$, ce qui dépasse mes compétences. Le livre de Fulton et Harris [8], cité FH, sera la référence pour ce qui suit.

Les représentations irréductibles (sur $\mathbb{C}$) du groupe symétrique $\mathfrak{S}_d$ sont définies sur $\mathbb{Q}$, et, à isomorphisme près, elles sont paramétrées par les partages λ de l'entier d (λ est un partage de d, ce qui est noté $\lambda \to d$, si λ est une suite décroissante d'entiers $\lambda = (\lambda(1) \geq \lambda(2) \geq \cdots \geq \lambda(d) \geq 0)$ de somme égale à d)(*cf.* FH, p. 46). Bref, il existe des $\mathbb{Q}$-espaces vectoriels V_λ et un isomorphisme de $\mathbb{Q}$-algèbres

$$\mathbb{Q}[\mathfrak{S}_d] \xrightarrow{\sim} \prod_{\lambda \to d} \mathrm{End}_{\mathbb{Q}}(V_\lambda). \tag{7.4.1}$$

Pour chaque représentation V_λ, le morphisme $\mathbb{Q}\mathfrak{S}_d \to \mathrm{End}_{\mathbb{Q}}(V_\lambda)$ munit $\mathrm{End}_{\mathbb{Q}}(V_\lambda)$ d'une structure de $\mathfrak{S}_d$-module à gauche ; dans la décomposition

$$\mathrm{End}_{\mathbb{Q}}(V_\lambda) \xrightarrow{\sim} V_\lambda \otimes_{\mathbb{Q}} V_\lambda^\vee,$$

cette structure provient de l'action à gauche de $\mathfrak{S}_d$ sur V_λ ; autrement dit, pour un $\mathfrak{S}_d$-module à droite F, on a un isomorphisme

$$F \otimes_{\mathbb{Q}\mathfrak{S}_d} \mathrm{End}(V_\lambda) \xrightarrow{\sim} (F \otimes_{\mathbb{Q}\mathfrak{S}_d} V_\lambda) \otimes_{\mathbb{Q}} V_\lambda^\vee. \tag{7.4.2}$$

Pour un R-module E, en faisant toujours opérer $\mathfrak{S}_d$ à droite sur $E^{\otimes d}$, on définit le R-module de Schur d'indice λ par

$$\mathbb{S}_\lambda(E) := E^{\otimes d} \otimes_{\mathbb{Q}\mathfrak{S}_d} V_\lambda. \tag{7.4.3}$$

En écrivant $E^{\otimes d} = E^{\otimes d} \otimes_{\mathbb{Q}\mathfrak{S}_d} \mathbb{Q}\mathfrak{S}_d$, et utilisant (7.4.1) et (7.4.2), on a donc un isomorphisme

$$E^{\otimes d} \xrightarrow{\sim} \prod_{\lambda \to d} \mathbb{S}_\lambda(E) \otimes_{\mathbb{Q}} V_\lambda^\vee. \tag{7.4.4}$$

Notons que l'action à droite de $\mathfrak{S}_d$ sur $E^{\otimes d}$ correspond, dans le second membre, à l'action de $\mathfrak{S}_d$ sur le dual $V_\lambda^\vee$ (elle est aussi à droite !). Le module de Schur $\mathbb{S}_\lambda(S)$ hérite de la structure de $\Gamma^d S$-module qui provient de celle de $S^{\otimes d}$; utilisant le morphisme habituel $\pi : \Gamma^d S \to R$, posons

$$V_\lambda(S/R) := R \otimes_{\Gamma^d S} \mathbb{S}_\lambda(S) = (R \otimes_{\Gamma^d S} S^{\otimes d}) \otimes_{\mathbb{Q}\mathfrak{S}_d} V_\lambda.$$

LEMME 7.4.5. — *Le R-modules $V_\lambda(S/R)$ est projectif de type fini de rang égal à* $\dim_{\mathbb{Q}}(V_\lambda)$.

Démonstration. — Il suffit de vérifier que les modules $V_\lambda(S/R)$ et $R \otimes_{\mathbb{Q}} V_\lambda$ deviennent isomorphes après un changement de base étale fidèlement plat ; on peut donc supposer que $S = \mathbf{M}(T, R)$; mais alors, d'après 4.1.1, on a un isomorphisme

$$R \otimes_{\Gamma^d S} S^{\otimes d} = \mathbf{P}^{(1..1)}\big(\mathbf{M}(T, R)\big) \xrightarrow{\sim} \mathbf{M}(P, R),$$

où on a noté P l'ensemble $\mathbf{P}_{(1..1)}T$ des bijections de $\underline{d} = \{1, \ldots, d\}$ sur T ; c'est un torseur sous $\mathfrak{S}_d$; le choix d'une bijection de $\underline{d}$ sur T détermine donc un isomorphisme de $\mathbb{Q}\mathfrak{S}_d$-module à droite $\mathbf{M}(P, \mathbb{Q}) \xrightarrow{\sim} \mathbb{Q}\mathfrak{S}_d$; on a donc

$$V_\lambda(S/R) \xrightarrow{\sim} \big(R \otimes_{\mathbb{Q}} \mathbf{M}(P, \mathbb{Q})\big) \otimes_{\mathbb{Q}\mathfrak{S}_d} V_\lambda \xrightarrow{\sim} R \otimes_{\mathbb{Q}} V_\lambda. \quad \square$$

PROPOSITION 7.4.6. — *Soient R une $\mathbb{Q}$-algèbre et S une R-algèbre finie étale de rang d. Avec les notations introduites ci-dessus, on a un isomorphisme fonctoriel en le R-module E*

$$N_{S/R}(S \otimes_R E) \xrightarrow{\sim} \prod_{\lambda \to d} V_\lambda(S/R) \otimes_R \mathbb{S}_\lambda(E).$$

En particulier, localement pour la topologie de Zariski sur $\operatorname{Spec}(R)$, *les foncteurs $E \mapsto N_{S/R}(S \otimes_R E)$ et $E \mapsto E^{\otimes d}$ sont isomorphes.*

Démonstration. — Après identification des algèbres Γ et Sym, ce qui est légitime puisque R est une $\mathbb{Q}$-algèbre, la « décomposition de Cauchy » (*cf.* FH, p. 80) s'écrit, pour tout R-module E,

$$\Gamma^d(S \otimes_R E) \xrightarrow{\sim} \prod_{\lambda \to d} \mathbb{S}_\lambda(S) \otimes_R \mathbb{S}_\lambda(E).$$

L'isomorphisme annoncé s'obtient par le changement de base habituel $\pi : \Gamma^d S \to R$. La dernière partie de l'énoncé provient de 7.4.5 et de 7.4.3, après avoir choisi, pour chaque λ, un isomorphisme $\mathbb{Q}$-linéaire $V_\lambda^\vee \xrightarrow{\sim} V_\lambda$.

BIBLIOGRAPHIE

[1] ADAMS (J.-F.). — *Infinite Loop Spaces*, Annals of Math. Studies, Study **90**, Princeton Univ. Press, 1978.

[2] BOSCH (S.), LÜTKEBOHMERT (W.), RAYNAUD (M.). — *Néron Models*. — Springer-Verlag, 1990.

[3] Bourbaki (N.). — *Algèbre*, ch. 4 à 7. — Masson, Paris, 1981.

[4] Breen (L.). — Bitorseurs et cohomologie non abélienne, in *The Grothendieck Festschrift*, vol. I, Birkhäuser, 1990.

[5] Deligne (P.). — Cohomologie à supports propres, exposé XVII de SGA 4, *Théorie des topos et cohomologie étale des schémas*, Lecture Notes in Math. **305**, Springer-Verlag, 1973.

[6] Demazure (M.), Gabriel (P.). — *Groupes algébriques.* — Masson, 1970.

[7] Draxl (P.). — *Skew Fields.* — London Math. Soc., Lecture Note Series **81**, Cambridge Univ. Press, 1983.

[8] Fulton (W.), Harris (J.). — *Representation Theory.* — Grad. Texts in Math. **129**, Springer-Verlag, 1991.

[9] Grothendieck (A.). — *Technique de descente et théorèmes d'existence en géométrie algébrique, II; Le théorème d'existence en théorie formelle des modules*, Sém. Bourbaki, 1959/60, exposé 195.

[10] Grothendieck (A.). — *Éléments de géométrie algébrique (EGA)*, rédigés avec la collaboration de J. Dieudonné, Publ. Math. I.H.E.S., Paris 1960–1967.

[11] Haile (D.). — *On Central Simple Algebras of Given Exponent*, J. Algebra, t. **57**, 1979, p. 449–465.

[12] Iversen (B.). — *Linear Determinants with Applications to the Picard Scheme of a Family of Algebraic Curves.* — Lecture Notes in Math. **174**, Springer-Verlag, 1970.

[13] Knus (M.-A.), Ojanguren (M.). — *Théorie de la Descente et Algèbres d'Azumaya.* — Lecture Notes in Math. **389**, Springer-Verlag, 1974.

[14] Knus (M.-A.), Ojanguren (M.). — *A Norm for Modules and Algebras*, Math.Z., t. **142**, 1975, p. 34–45.

[15] Oesterlé (M.). — *Nombres de Tamagawa et groupes unipotents en caractéristique p*, Invent. Math., t. **78**, 1984, p. 13–88.

[16] Riehm (C.). — *The Corestriction of Algebraic Structures*, Invent. Math., t. **11**, 1970, p. 73–98.

[17] Roby (N.). — *Lois polynômes et lois formelles en théorie des modules*, Ann. scient. Éc. Norm. Sup., t. **80**, 1963, p. 213–348.

[18] Roby (N.). — *Lois polynômes multiplicatives universelles*, C. R. Acad. Sc. Paris, t. **290**, 1980, p. 869–871.

[19] Serre (J.-P.). — *Corps locaux.* — Hermann, Paris, 1962.

[20] Serre (J.-P.). — *Cohomologie Galoisienne*, 5e éd. — Lecture Notes in Math. **5**, Springer-Verlag, 1994.

[21] Tignol (J.-P.). — *On the Corestriction of Central Simple Algebras*, Math. Z., t. **194**, 1987, p. 267–274.