Une introduction au groupe de Brauer

Bruno Deschamps

Le Mans - Caen - Paris - New York - Berlin

— 2012 —

à Juillet l'universelle
à Octobre, pleine d'espoir...

Table des matières

1 Structure des algèbres simples centrales

L'objectif de cette partie est d'établir un théorème de structure sur la nature des algèbres simples centrales, notion centrale dans la théorie du groupe de Brauer. Nous allons voir que les algèbres simples centrales sont exactement les algèbres de matrices.

On considère dans la suite un corps commutatif k et une k-algèbre unitaire A de dimension finie sur k. On notera A_g (resp. A_d) la structure de A-module gauche (resp. droite) de A. Pour tout A-module (droite ou gauche) M on notera $\mathscr{L}_A(M)$ l'ensemble des endomorphismes de M que l'on considérera avec sa structure de k-algèbre. Les modules que nous considérons seront toujours supposés de type fini. En particulier, ils seront de dimension finie en tant que k-espace vectoriel, posséderont toujours des sous-modules minimaux et maximaux et verront toutes sommes directes posséder se ramener à un nombre fini de facteurs.

Etant donnée une k-algèbre A rapportée à une base $\{a_1, \cdots a_n\}$, pour tout couple d'indices $(i,j) \in \{1, \cdots, n\}^2$ il existe un unique vecteur $\lambda^{(i,j)} = (\lambda_1^{(i,j)}, \cdots, \lambda_n^{(i,j)}) \in k^n$ tel que

$$a_i a_j = \sum_{k=1}^{n} \lambda_k^{(i,j)} a_k$$

Les vecteurs $\lambda^{(i,j)}$ sont appelés les *constantes de structure* de la k-algèbre A (relativement à la base $\{a_1, \cdots a_n\}$). On voit alors qu'étant données deux k-algèbres A et B, les deux propriétés suivantes

i) A et B sont isomorphes en tant que k-algèbres,

ii) il existe un entier $n \geq 1$ et des bases de A et B de cardinal n tels que les constantes de structure de A et B relativement à ces bases soient égales,

sont équivalentes.

Etant donnée une k-algèbre A, on notera A^{op} *l'algèbre opposée de* A, qui est l'ensemble A munie des même lois de compositions que l'algèbre A ormis le produit que l'on remplace par le produit opposé $*$ défini, pour $a, b \in A$, par $a * b = ba$.

1.1 Modules simples et semi-simples

1.1.1 Modules simples

Définition 1.— *1/ Un A-module M est dit simple, s'il est non trivial et s'il ne possède aucun sous-module stricte.*

2/ Un A-module M est dit semi-simple s'il est égal à la somme de sous-modules simples de M.

Exemple 2.— Considérons un corps K (non nécessairement commutatif) de dimension finie sur k et $A = \mathscr{M}_n(K)$ la k-algèbre des matrices $n \times n$ à coefficients dans K. Pour tout $i = 1, \cdots, n$ on note

$$M_i = \left\{ \left(\begin{array}{ccc} & \overset{\text{i-ème}}{a_1} & \\ 0 & \vdots & 0 \\ & a_n & \end{array} \right) / \; a_1, \cdots a_n \in K \right\}$$

l'ensemble des matrices de $\mathscr{M}_n(K)$ dont toutes les colonnes, sauf peut-être la i-ème, sont nulles. Il est clair que M_i est un $\mathscr{M}_n(K)$-module à gauche (pour la multiplication des matrices). C'est un module simple. En effet, soit N un sous-module non nul de M_i et $\left(\begin{array}{ccc} & \overset{\text{i-ème}}{a_1} & \\ 0 & \vdots & 0 \\ & a_n & \end{array} \right) \in N$ une matrice non nulle (par exemple $a_j \neq 0$). Soit $\left(\begin{array}{ccc} & \overset{\text{i-ème}}{b_1} & \\ 0 & \vdots & 0 \\ & b_n & \end{array} \right) \in M_i$, on alors

$$\left(\begin{array}{ccc} & \overset{\text{i-ème}}{b_1} & \\ 0 & \vdots & 0 \\ & b_n & \end{array} \right) = \left(\begin{array}{ccc} & \overset{\text{j-ème}}{b_1/a_j} & \\ 0 & \vdots & 0 \\ & b_n/a_j & \end{array} \right) \left(\begin{array}{ccc} & \overset{\text{i-ème}}{a_1} & \\ 0 & \vdots & 0 \\ & a_n & \end{array} \right)$$

ce qui prouve que $N = M_i$. Maintenant, il est clair que $A_g = \bigoplus_{i=1}^{n} M_i$ et ainsi, A_g est un A-module semi-simple. On va voir un peu plus loin que l'existence d'une écriture en somme directe de sous-modules simples d'un module semi-simple n'est pas spécifique à $\mathscr{M}_n(K)$.

Proposition 3.— *Soit $f : M \longrightarrow N$ un homomorphisme de A-modules. Si M et N sont simples, alors f est soit l'homomorphisme nul, soit un isomorphisme. En conséquence de quoi :*

1/ Si M et N sont deux modules simples non isomorphes, alors tout homomorphisme de M vers N est nul.

2/ Si M est un A-module simple alors l'anneau $\mathscr{L}_A(M)$ est un corps. (Cet énoncé est habituellement appelé lemme de Schur.*)*

Preuve : Si f est non nulle, alors $f(M)$ est un sous module non nul de N et donc $f(M) = N$ puisque N est simple. Ainsi, f est surjective. De même, toujours puisque f est non nulle, $f^{-1}(0)$ est un sous-module de M distinct de M. Comme M est simple, on a $f^{-1}(0) = \{0\}$ et donc f est injective.

Exemple 4.— Reprenons l'exemple précédent et décrivons $\mathscr{L}_A(M_i)$. Pour tout couple d'indice (p,q) on note $X_{p,q}$ la matrice composée de 0 partout sauf en coordonnées (p,q) où il y a un 1. Soit $f \in \mathscr{L}_A(M_i)$ non nulle. Pour tout $X \in M_i$ il existe $T \in A$ tel que $X = TX_{1,i}$, et comme $f(X) = f(TX_{1,i}) = Tf(X_{1,i})$ pour décrire f il suffit d'expliciter $f(X_{1,i})$. Pour $T = X_{1,1}$ on a

$$f(X_{1,i}) = f(X_{1,1}X_{1,i}) = X_{1,1}f(X_{1,i}) = X_{1,i}.\lambda I \text{ pour un certain } \lambda \in K$$

Ainsi, pour tout $X \in M_i$, on a $f(X) = f(TX_{1,i}) = Tf(X_{1,i}) = TX_{1,i}\lambda I = X.\lambda I$ et donc f est de la forme

$$\begin{array}{rccc} f_\lambda : & M_i & \longrightarrow & M_i \\ & X & \longmapsto & X.\lambda I \end{array}$$

Réciproquement, pour tout $\lambda \in K$ l'application f_λ est bien un élément de $\mathscr{L}_A(M_i)$. Par ailleurs, comme pour tout $\lambda, \mu \in K$, $f_\lambda \circ f_\mu = f_{\mu\lambda}$ on en déduit finalement que $\mathscr{L}_A(M_i) \simeq K^{\mathrm{op}}$.

1.1.2 Type de modules simples

Proposition 5.— *1/ Soit J un idéal à gauche (resp. à droite) de A. Les propositions suivantes*

i) A_g/J (resp. A_d/J) est un A-module à gauche (resp. à droite) simple,

ii) J est maximal,

sont équivalentes.

2/ Tout A-module à gauche (resp. à droite) simple est isomorphe à un module quotient A_g/J (resp. A_d/J), J étant maximal.

Preuve : 1/ Les sous-modules de A_g/J correspondent bijectivement aux sous-modules de A_g qui contiennent J, c'est-à-dire aux idéaux à gauches de A contenant J. L'équivalence annoncée découle de cette correspondance.

2/ Soit M un A-module gauche et $x \in A$ non nul. L'ensemble Ax est un sous-module non trivial de M et donc, si M est simple, on a $M = Ax$. Dans cette situation, on considère l'application

$$\begin{array}{rccc} f : & A & \longrightarrow & M \\ & a & \longmapsto & ax \end{array}$$

Cette application est visiblement un homomorphisme de A-modules gauches surjectif. Son noyau J est un sous-module de A_g, c'est-à-dire un idéal à gauche de A. En application des théorèmes d'isomorphismes, on a alors $M \simeq A_g/J$ et J est alors maximal en vertu du 1/.

On considère la classe des modules simples à gauche (resp. à droite), quotient de A_g (resp. A_d). Sur cette classe on considère les classes d'équivalences

pour la relation d'isomorphisme de A-module à gauche (resp. à droite). On appelle *type* de A-modules simples à gauhe (resp. à droite) ces classes. La proposition précédente assure que tout A-module à gauche (resp. à droite) M simple est isomorphe aux modules d'un type donné. Ce type sera appelé *le type de* M. La collection des types forme donc un ensemble, paramétré par les quotients A_g/J.

Exemple 6.— Les modules M_i des exemples précédents ont tous le même type. Ils sont, en effet, tous isomorphes en tant que A-modules à gauche. Pour tout $i = 1, \cdots, n$, le noyau de l'application

$$\begin{array}{ccc} A_g & \longrightarrow & M_i \\ X & \longmapsto & XX_{1,i} \end{array}$$

est égal à $J = \left\{ \begin{pmatrix} 0 & \cdots & \\ \vdots & \vdots & \vdots \\ 0 & \cdots & \end{pmatrix} \right\}$ donc les M_i sont tous isomorphes en tant que A-modules gauche à A_g/J.

Définition 7.— *Soit M un A-module à gauche (resp. à droite) et λ un type. On appelle composante isotypique de M le sous-module noté M_λ obtenu en prenant la somme des tous les sous-modules de M de type λ.*

1.1.3 Structures des modules semi-simples

Les modules semi-simples sont des sommes de modules simples. Puisque l'on a supposé que A était de dimension finie sur k et qu'on ne considère ici que des A-modules de type fini, un module semi-simple pourra donc toujours être écrit comme une somme finie de modules simples (si ce n'était pas le cas, un tel module serait de dimension infinie en tant que k-espace vectoriel).

Proposition 8.— *Soit M un A-module semi-simple et $M = N_1 + \cdots + N_n$ une écriture de M en somme de sous-modules simples. Pour tout sous-module N de M il existe un ensemble ordonné d'indices $i_1 < \cdots < i_k$ tel que*

$$M = N \oplus N_{i_1} \oplus \cdots \oplus N_{i_k}$$

Preuve : Si $N = M$ on prend l'ensemble vide. Si $N \neq M$, alors tous les N_i ne peuvent être inclus dans N, sinon leur somme, c'est-à-dire M, le serait aussi. Il existe alors un plus petit indice i_1 tel que $N_{i_1} \not\subset N$. Alors, $N \cap N_{i_1}$ est un sous-module strict de N_{i_1}, il donc nulle et par suite N et N_{i_1} sont en somme directe.

Supposons posséder un indice $h \geq 1$ et une suite d'indices $i_1 < \cdots < i_h$ de $\{1, \cdots, n\}$ telle que

$$N_1 + N_2 + \cdots + N_{i_h} \subset N \oplus N_{i_1} \oplus \cdots \oplus N_{i_h}$$

Si cette somme directe vaut M, la proposition est aquise. Sinon, il existe un plus petit indice $i_{h+1} > i_h$ tel que $N_{i_{h+1}} \not\subset N \oplus N_{i_1} \oplus \cdots \oplus N_{i_h}$ (sinon $M = N_1 + N_2 + \cdots + N_n \subset N_{i_1} \oplus \cdots \oplus N_{i_h}$ ce qui est contraire à l'hypothèse). Alors, $N_{i_{h+1}} \cap N \oplus N_{i_1} \oplus \cdots \oplus N_{i_h}$ est un sous-module strict de $N_{i_{h+1}}$ et est donc nul. Par ailleurs, par construction, pour tout indice i variant de 1 à $i_{h+1}-1$ on a $N_i \subset N \oplus N_{i_1} \oplus \cdots \oplus N_{i_h}$ et par suite

$$N_1 + N_2 + \cdots + N_{i_{h+1}} \subset N \oplus N_{i_1} \oplus \cdots \oplus N_{i_{h+1}}$$

Comme ce procédé récursif est limité à un ensemble fini d'indices, il est fini et il existe donc un indice k tel que

$$M = N \oplus N_{i_1} \oplus \cdots \oplus N_{i_k}$$

Corollaire 9.— *Tout sous-module et tout module quotient d'un module semi-simple est semi-simple.*

Plus précidément, si M est un A-module semi-simple et $M = N_1 + \cdots + N_n$ est une écriture de M en somme de sous-modules simples, alors tout sous-module et tout module quotient de M est isomorphe à une somme directe de la forme

$$N_{i_1} \oplus \cdots \oplus N_{i_k}$$

En particulier, tout sous-module simple de M est isomorphe à un N_i.

Preuve : Soit M/N un module quotient. En appliquant la proposition 8, on peut écrire $M = N \oplus N_{i_1} \oplus \cdots \oplus N_{i_k}$ et, par suite,

$$M/N \simeq N_{i_1} \oplus \cdots \oplus N_{i_k}$$

Soit N un sous-module de M. Comme M est de type fini, N possède un supplémentaire F. En appliquant la proposition 8, on peut écrire $M = F \oplus N_{i_1} \oplus \cdots \oplus N_{i_k}$ et, par suite,

$$N \simeq N \oplus F/F = M/F \simeq N_{i_1} \oplus \cdots \oplus N_{i_k}$$

Le sous-module $N_{i_1} \oplus \cdots \oplus N_{i_k}$ de M est simple si et seulement si $k = 1$, et donc un sous-module simple de M est bien isomorphe à un N_i.

Corollaire 10.— *Un module semi-simple M est somme directe de ses composantes isotypiques.*

Preuve : Comme M est semi-simple, il est somme de ses sous-modules simples, il est donc somme de ses composantes isotypiques. Supposons que pour un type λ on ait $M_\lambda \cap \sum_{\mu \neq \lambda} M_\mu \neq \{0\}$, alors ce sous-module intersection contient un sous-module simple N. Le module M_λ est somme directe de sous-modules de type λ et donc, d'après le corollaire 9, N est de type λ. De même, $\sum_{\mu \neq \lambda} M_\mu$ est

somme directe de sous-modules de types $\mu \neq \lambda$, toujours d'après le corollaire 9, N est de type différent de λ, ce qui est absurde. Ainsi, on a $M = \bigoplus_\lambda M_\lambda$.

———

Passons maintenant à l'étude des endomorphismes des modules semi-simples et commençons par regarder l'image des composantes isotypiques par un homomorphisme :

Lemme 11.— *Soit $f : M \longrightarrow N$ un homomorphisme de A-modules. Pour tout type de A-modules simples λ, on a*

$$f(M_\lambda) \subset N_\lambda$$

Preuve : Si on pose $M_\lambda = \bigoplus_{i=1}^n S_i$ où les S_i sont des sous-modules de type λ de M, alors on a

$$f(M_\lambda) = \bigoplus_{i=1}^n f(S_i)$$

et comme S_i est simple, on a $f(S_i) = \{0\}$ ou alors $f : S_i \longrightarrow f(S_i)$ est un isomorphisme et donc $f(S_i)$ est un sous-module simple de N de type λ. Ainsi, $f(M_\lambda) \subset N_\lambda$.

———

Théorème 12.— *Soit M un A-module semi-simple. Si $M = \bigoplus_{\lambda\in\Lambda} M_\lambda$ est la décomposition en composantes isotypiques de M alors*

$$\mathscr{L}_A(M) \simeq \prod_{\lambda\in\Lambda} \mathscr{L}_A(M_\lambda)$$

Par ailleurs, si $M_\lambda = \bigoplus_{i=1}^n S_i$ où les S_i sont des sous-modules de type λ de M alors

$$\mathscr{L}_A(M_\lambda) \simeq \mathscr{M}_n(K)$$

où $K = \mathscr{L}_A(S)$, S étant un représentant de λ. En conséquence de quoi, $\mathscr{L}_A(M)$ est isomorphe à un produit d'algèbres de matrices à coefficients dans des extensions finies de k.

Preuve : D'après le lemme précédent, pour tout $f \in \mathscr{L}_A(M)$ la restriction f_λ de f à M_λ est un élément de $\mathscr{L}_A(M_\lambda)$. Ceci permet de définir une application

$$\begin{array}{rccc} \Omega : & \mathscr{L}_A(M) & \longrightarrow & \prod_{\lambda\in\Lambda} \mathscr{L}_A(M_\lambda) \\ & f & \longmapsto & (f_\lambda)_{\lambda\in\Lambda} \end{array}$$

qui est visiblement un homomorphisme d'algèbres. Pour tout $\lambda \in \Lambda$, notons $\pi_\lambda : M \longrightarrow M_\lambda$ la projection canonique. Comme pour tout $x \in M$ on a

$$f(x) = \sum_\lambda f_\lambda(\pi_\lambda(x))$$

on en déduit que Ω est injective. Par ailleurs, pour un élément $(f_\lambda)_{\lambda\in\Lambda}$ donné, la formule précédente définit clairement un élément f dont l'image par Ω est $(f_\lambda)_{\lambda\in\Lambda}$. Ceci prouve la surjectivité de Ω et, par suite, l'isomorphisme annoncé.

Venons-en maintenant à l'isomorphisme $\mathscr{L}_A(M_\lambda) \simeq \mathscr{M}_n(K)$. On s'intéresse donc à la structure de l'algèbre $\mathscr{L}_A(S^n)$. Pour tout $i = 1,\cdots,n$ notons respectivement $\pi_i : S^n \longrightarrow S$ et $\gamma_i : S \longrightarrow S^n$ la i-èmè projection canonique et la i-ème injection canonique.

Pour tout $i,j \in \{1,\cdots,n\}$ et tout $f \in \mathscr{L}_A(S^n)$ l'application $f_{i,j} = \pi_i \circ f \circ \gamma_j$ est un élément de $\mathscr{L}_A(S) = K$. Ainsi, on définit une application

$$\begin{array}{rccc} \Theta : & \mathscr{L}_A(S^n) & \longrightarrow & \mathscr{M}_n(K) \\ & f & \longmapsto & (f_{i,j})_{i,j} \end{array}$$

Remarquons que $\sum_i \gamma_i \circ \pi_i$ est la fonction identité sur S^n, on a donc pour tout $f \in \mathscr{L}_A(S^n)$

$$f = \sum_{i,j} \gamma_i \circ \pi_i \circ f \circ \gamma_j \circ \pi_j = \sum_{i,j} \gamma_i f_{i,j} \circ \pi_j$$

Ceci montre, en particulier, que Θ est injective. De même, en prenant un élément $(f_{i,j})_{i,j} \in \mathscr{M}_n(K)$, on voit que la formule précédente permet de définir un élément $f \in \mathscr{L}_A(S^n)$ dont l'image par Θ est $(f_{i,j})_{i,j}$, ce qui prouve que Θ est surjective.

Il reste à montrer que Θ est un homomorphisme de A-algèbre. Comme les applications π_i et γ_j sont des homomorphisme de A-modules, pour tout $f,g \in \mathscr{L}_A(S^n)$ et tout $a \in A$, on a

$$\begin{array}{rcl} af+g & = & \sum_{i,j} \gamma_i \circ \pi_i \circ (af+g) \circ \gamma_j \circ \pi_j \\ & = & a\sum_{i,j} \gamma_i \circ \pi_i \circ f \circ \gamma_j \circ \pi_j + \sum_{i,j} \gamma_i \circ \pi_i \circ g \circ \gamma_j \circ \pi_j \\ & = & a\sum_{i,j} \gamma_i f_{i,j} \circ \pi_j + \sum_{i,j} \gamma_i g_{i,j} \circ \pi_j \\ & = & \sum_{i,j} \gamma_i (af_{i,j} + g_{i,j}) \circ \pi_j \end{array}$$

On en déduit que pour tout i,j on a $(af+g)_{i,j} = af_{i,j} + g_{i,j}$ et donc que Θ est un homomorphisme de A-modules.

Soient $f,g \in \mathscr{L}_A(S^n)$, on a

$$\begin{array}{rcl} f \circ g & = & \left(\sum_{i,j} \gamma_i f_{i,j} \circ \pi_j\right) \circ \left(\sum_{p,q} \gamma_p g_{p,q} \circ \pi_q\right) \\ & = & \sum_{i,j,p,q} \gamma_i f_{i,j} \circ (\pi_j \circ \gamma_p) \circ g_{p,q} \circ \pi_q \\ & = & \sum_{i,j,q} \gamma_i f_{i,j} \circ g_{j,q} \circ \pi_q \end{array}$$

On a donc

$$(f \circ g)_{i,q} = \sum_j f_{i,j} g_{j,q}$$

et donc $\Theta(f \circ g) = \Theta(f)\Theta(g)$ ce qui prouve, pour finir, que Θ est un isomorphisme d'algèbre.

Exemple 13.— L'algèbre $A = \mathscr{M}_n(K)$, vue comme module à gauche sur elle-même, est semi-simple et ne possède qu'une seule composante isotypique. En effet, d'après les résultats établis dans les exemples 2 et 6 on a $\mathscr{M}_n(K) = \bigoplus_{i=1}^{n} M_i$ et les M_i ont tous même type S. D'après le résultat établi dans l'exemple 4, on a $\mathscr{L}_A(S) \simeq K^{\mathrm{op}}$. Ainsi, si l'on applique le théorème 12, on trouve que

$$\mathscr{L}_A(\mathscr{M}_n(K)) \simeq \mathscr{M}_n(K^{\mathrm{op}})$$

Maintenant, la transposition

$$\begin{array}{ccc} \mathscr{M}_n(K^{\mathrm{op}}) & \longrightarrow & \mathscr{M}_n(K)^{\mathrm{op}} \\ M & \longmapsto & {}^tM \end{array}$$

est visiblement un isomorphisme et on a donc pour finir

$$\mathscr{L}_A(\mathscr{M}_n(K)) \simeq \mathscr{M}_n(K)^{\mathrm{op}}$$

Les résultats précédents permettent d'obtenir le résultat important suivant :

Proposition 14.— *Soit K_1 et K_2 deux corps de dimensions finies sur k et n_1, n_2 deux entiers ≥ 1. Les propositions suivantes*

i) Les k-algèbres $\mathscr{M}_{n_1}(K_1)$ et $\mathscr{M}_{n_2}(K_2)$ sont isomorphes,

ii) $K_1 \simeq K_2$ et $n_1 = n_2$,

sont équivalentes.

Preuve : Si $A_1 = \mathscr{M}_{n_1}(K_1)$ et $A_2 = \mathscr{M}_{n_2}(K_2)$ sont isomorphes alors elles sont isomorphes en tant que modules à gauche sur elle-même. Elles ne possèdent toutes deux qu'une seule composante isotypique et ces deux composantes sont relatives au même type λ. Soit S_1 et S_2 des sous-modules simples de $\mathscr{M}_{n_1}(K_1)$ et $\mathscr{M}_{n_2}(K_2)$. Ils sont tous les deux de type λ et donc

$$K_1 = K_1^{\mathrm{op}\ \mathrm{op}} \simeq \mathscr{L}_{A_1}(S_1)^{\mathrm{op}} \simeq \mathscr{L}_{A_2}(S_2)^{\mathrm{op}} \simeq K_2^{\mathrm{op}\ \mathrm{op}} = K_2$$

Maintenant, on a $[A_1 : k] = n_1^2[K_1 : k]$ et $[A_2 : k] = n_2^2[K_2 : k]$ et comme par ailleurs on a $[A_1 : k] = [A_2 : k]$ et $[K_1 : k] = [K_2 : k]$, on en déduit que $n_1 = n_2$.

1.2 Algèbres simples

1.2.1 Structures des algèbres simples et semi-simples

On rappelle que les k-algèbres que l'on étudie ici sont supposées de dimensions finies.

Définition 15.— *Une algèbre est dite simple si elle ne possède aucun idéal bilatère non trivial. Une algèbre est dite semi-simple si elle est isomorphe à un produit direct d'algèbres simples.*

Exemples 16.— • Un corps K contenant k dans son centre, extension finie de k, est bien sur une k-algèbre simple. Mais plus généralement, pour tout entier $n \geq 1$, la k-algèbre $\mathscr{M}_n(K)$ des matrices carrées $n \times n$ à coefficients dans K est une algèbre simple.

En effet, considérons un idéal bilatère non nul J de $\mathscr{M}_n(K)$ et prenons une matrice $H = (h_{i,j})_{i,j} \in J$ non nulle, disons par exemple $h_{i_0,j_0} \neq 0$. Pour tout couple d'indice (i,j) notons $\Gamma_{i,j}$ la matrice dont tous les coefficients sont nuls, sauf celui d'indice (i,j) qui vaut 1. Pour tout i,j on a

$$\Gamma_{i,j} = h_{i_0,j_0}^{-1} \Gamma_{i,i_0} H \Gamma_{j_0,j}$$

et, par suite, $\Gamma_{i,j} \in J$, mais comme la collection des $\Gamma_{i,j}$ engendre toutes les matrices, on en déduit que $J = \mathscr{M}_n(K)$.

• Le théorème 12 assure, avec le résultat précédent, que l'algèbre des endomorphismes d'un module semi-simple est une algèbre semi-simple.

Lemme 17.— *Soit A une k-algèbre. Si $f \in \mathscr{L}_A(A_g)$ alors f est la multiplication à droite sur A par un certain élément. En conséquence de quoi, on a*

$$A^{\mathrm{op}} \simeq \mathscr{L}_A(A_g)$$

Preuve : Pour tout $\alpha \in A$ on $f(\alpha) = f(\alpha.1) = \alpha f(1)$. Donc f est la multiplication à droite par $f(1)$. Réciproquement, si on note m_x la multiplication à droite par $x \in A$, il est clair que $m_x \in \mathscr{L}_A(A_g)$. Par ailleurs, pour tout $x,y \in A$ on a $m_x \circ m_y = m_{yx}$, d'où l'isomorphisme annoncé.

———

Dans la cas de $A = \mathscr{M}_n(K)$, on retrouve directement le résultat de l'exemple 13.

On rappelle qu'un idéal J d'un anneau A est dit nilpotent s'il existe un entier $n \geq 1$ tel que $J^n = \{0\}$. On dira d'une algèbre qu'elle est sans idéaux nilpotents si son seul idéal bilatère nilpotent est $\{0\}$. Remarquons qu'une algèbre sans idéaux nilpotents ne contient aucun idéal gauche ou droite non trivial qui soit nilpotent. En effet, si J est un idéal (par exemple gauche) de A non trivial nilpotent, disons $J^n = \{0\}$, alors JA est l'idéal bilatère engendré par J. Puisque $AJ = J$ on a alors

$$(JA)^n = J(AJ)^{n-1}A = J^n A = \{0\}$$

et donc A contient un idéal bilatère nilpotent non trivial. Commençons par établir quelques résultats techniques sur les algèbres sans idéaux nilpotents.

Proposition 18.— *Soit A une k-algèbre sans idéaux nilpotents.*

1/ A est somme directe d'idéaux à gauche minimaux, en particulier, A_g est un A-module à gauche semi-simple.

2/ Soit Λ l'ensemble des types de A-modules simples. On a

$$A^{op} \simeq \prod_{\lambda \in \Lambda} \mathscr{M}_{n_\lambda}(K_\lambda)$$

où les K_λ sont des corps contenant k dans leurs centres.

Preuve : 1/ Considérons pour commencer un idéal à gauche minimal J de A. Puisque A est sans idéaux nilpotents, on a $J^2 \neq \{0\}$ et donc il existe $a \in J$ tel que $Ja \neq \{0\}$. Comme J est minimal et que Ja est un idéal à gauche non nul inclus dans J on a $J = Ja$. Ainsi, il existe $e \in J$ tel que $a = ea$ et on a, par suite, $ea = e^2a$. La multiplication à droite par a dans J est un homomorphisme non trivial, donc son noyau est un sous-idéal à gauche de J différent de J. Il est donc réduit à $\{0\}$ et, par suite la multiplication à droite dans J est injective. On en déduit que $e = e^2$. Par ailleurs, e engendre bien J, puisque e est non nul et que Ae est un idéal à gauche inclus dans J qui est minimal. Nous venons donc de montrer que tout idéal à gauche minimal peut-être engendré par un élément idempotent.

Considérons un idéal à gauche minimal J_1 de A engendré par un élément idempotent e_1. Supposons que pour un indice $h \geq 1$ on ait trouvé des idéaux à gauche minimaux $J_1, \cdots, J_h$ en somme directe engendrés rexpectivement par des idempotents $e_1, \cdots, e_h$ vérifiant pour tout $i \neq j$, $e_i e_j = 0$. Si $A = J_1 \oplus \cdots \oplus J_h$, alors la proposition est démontrée. Sinon, on remarque que les deux éléments $e_1 + \cdots + e_h$ et $1 - e_1 - \cdots - e_h$ sont des idempotents et que pour tout $x \in A$, on a

$$x = xe_1 + \cdots + xe_h + x(1 - e_1 - \cdots - e_h)$$

Ainsi, l'idéal à gauche B engendré par $(1 - e_1 - \cdots - e_h)$ est un supplémentaire de $J_1 \oplus \cdots \oplus J_h$. On considère alors un idéal à gauche minimal J_{h+1} inclus dans B et ε un générateur idempotent de J_{h+1}. On pose

$$e_{h+1} = (1 - e_1 - \cdots - e_h)\varepsilon$$

Puisque B est engendré par $(1 - e_1 - \cdots - e_h)$ et que cet élément est un idempotent, la multiplication à droite par $(1 - e_1 - \cdots - e_h)$ dans B est donc l'identité. Ainsi, on a

$$\varepsilon e_{h+1} = \varepsilon(1 - e_1 - \cdots - e_h)\varepsilon = \varepsilon^2 = \varepsilon$$

et donc $e_{h+1} \neq 0$. Comme $e_{h+1} \in J_{h+1}$ et que J_{h+1} est minimal, on en déduit que e_{h+1} est générateur de J_{h+1}. Par ailleurs, on a aussi :

$$\begin{aligned} e_{h+1}^2 &= (1 - e_1 - \cdots - e_h)\varepsilon(1 - e_1 - \cdots - e_h)\varepsilon \\ &= (1 - e_1 - \cdots - e_h)\varepsilon^2 \\ &= (1 - e_1 - \cdots - e_h)\varepsilon \\ &= e_{h+1} \end{aligned}$$

et donc e_{h+1} est un idempotent. De même, pour tout $i \leq h$,

$$e_i e_{h+1} = e_i(1 - e_1 - \cdots - e_h)\varepsilon = (e_i - e_i)\varepsilon = 0$$

Par ailleurs, puisque $e_{h+1} \in B$, il existe $x \in A$ tel que $e_{h+1} = x(1 - e_1 - \cdots - e_h)$ et donc, pour tout $i \leq h$,

$$e_{h+1}e_i = x(1 - e_1 - \cdots - e_h)e_i = x(e_i - e_i)\varepsilon = 0$$

Ainsi, on a construit un idéal J_{h+1} engendré par un idempotent e_{h+1} tel que $J_1, \cdots, J_{h+1}$ soit en somme directe et tel que pour tout $i \neq j$, $e_i e_j = 0$. Pour des raisons de dimension, ce procédé récursif est forcément fini, d'où le résultat.

2/ Les sous-modules simples de A_g correspondants aux idéaux à gauche minimaux de A, le 1/ implique que A_g est un A-module semi-simple. La proposition 5 que les types de A-modules à gauche simples sont décrit par les quotients de A par des idéaux à gauche minimaux. Les corollaires 9 et 10 assure que

$$A_g = \bigoplus_{\lambda \in \Lambda} A_{g\,\lambda}$$

et que tous les types participent à cette somme. Le lemme 17 montre que

$$A^{\mathrm{op}} \simeq \mathscr{L}_A(A_g) = \mathscr{L}_A\left(\bigoplus_{\lambda \in \Lambda} A_{g\,\lambda}\right)$$

et le théorème 12 prouve finalement que

$$A^{\mathrm{op}} \simeq \prod_{\lambda \in \Lambda} \mathscr{M}_{n_\lambda}(K_\lambda)$$

où les K_λ sont des corps contenant k dans leurs centres.

Venons-en maintenant à la classification des algèbres simples et semi-simples.

Théorème 19.— *Soit A une k-algèbre. Les propriétés suivantes*

i) A est semi-simple,

ii) A est sans idéaux nilpotents,

iii) A est isomorphe à un produit d'algèbres de matrices sur des corps contenant k dans leurs centres.

Preuve : $i) \Longrightarrow ii)$ Il est déjà clair qu'un algèbre simple est sans idéaux nilpotents. Soit A une algèbre semi-simple, $A = A_1 \times \cdots \times A_n$ une décomposition de A en produit d'algèbres simples et J un idéal non nul. Soit $x = (x_1, \cdots, x_n)$ un élément non nul de J, disons $x_i \neq 0$. Notons J_i l'idéal de A_i engendré par x_i. Pour tout entier $k \geq 1$, on a $J_i^k \subset J^k$. On en déduit que si J est nilpotent alors J_i l'est aussi, mais comme $J_i \neq \{0\}$ et A_i est simple, cela est impossible. Donc A est sans idéaux nilpotents.

$ii) \Longrightarrow iii)$ soit A une algèbre sans idéaux nilpotents. Il est clair que l'algèbre opposée A^{op} est aussi sans idéaux nilpotents et si on applique la proposition 18-2 à A^{op}, on en déduit que A est isomorphe à un produit d'algèbres de matrices sur des corps contenant k dans leurs centres.

iii) $\Longrightarrow$ *i*) Le premier exemple de 16 montre qu'une algèbre de matrices sur un corps est simple. Donc A est semi-simple.

Théorème 20.— *Soit A une k-algèbre. Les propriétés suivantes*

i) A est simple,

ii) A est isomorphe à une algèbre de matrices $\mathscr{M}_n(K)$ où K est un corps contenant k dans son centre,

iii) A est sans idéaux nilpotents et il n'existe qu'un seul type de A-modules à gauche simples,

iii)$'$ A est semi-simple et il n'existe qu'un seul type de A-modules à gauche simples,

sont équivalentes.

Preuve : *i*) $\Longrightarrow$ *ii*) Si A est simple, alors A est semi-simple et donc d'après le théorème 19 l'algèbre A est isomorphe à un produit d'algèbres de matrices. Il est clair que si ce produit contient plus d'un facteur non trivial alors A n'est pas simple.

ii) $\Longrightarrow$ *iii*) $A = \mathscr{M}_n(K)$ est simple (exemple 16) donc est sans idéaux nilpotent. Par ailleurs, A^{op} est aussi simple et donc ne peut être isomorphe à aucun produit de plus d'un facteur d'algèbres de matrices. La proposition 18-2 implique alors qu'il n'y a qu'un seul type de A-modules à gauche simples.

iii) $\Longrightarrow$ *i*) Sous les hypothèses, la proposition 18-2 assure que $A^{\text{op}} \simeq \mathscr{M}_n(K)$ où K est un corps contenant k dans son centre et donc $A \simeq \mathscr{M}_n(K^{\text{op}})$ qui est simple (exemple 16).

Proposition 21.— *Si A est une k-algèbre semi-simple alors tout A-module à gauche est semi-simple. Si A est simple alors tout A-module à gauche est semi-simple isotypique, en particulier, si M et N sont deux A-modules alors les propriétés suivantes*

i) $M \simeq N$ en tant que A-modules,

ii) $[M : k] = [N : k]$,

sont équivalentes.

Preuve : D'après la proposition 18 le A-module A_g est semi-simple et donc, pour tout $n \geq 1$, A_g^n est aussi semi-simple. Si M est un A-module à gauche alors A est module quotient de A_g^n pour un certain entier n. En effet, M étant supposé de type fini, on se donne $x_1, \cdots, x_n$ une famille génératrice. L'application

$$\begin{array}{ccc} A_g^n & \longmapsto & M \\ (\lambda_1, \cdots, \lambda_n) & \longrightarrow & \displaystyle\sum_{i=1}^{n} \lambda_i x_i \end{array}$$

définit un épimorphisme de A_g^n sur M et donc, M est bien isomorphe à un quotient du module A_g^n. Le corollaire 9 assure alors que M est semi-simple.

Dans le cas où A est simple, le théorème 20 assure qu'il n'existe qu'un seul type de A-modules simples et donc que tout A-module est semi-simple isotypique.

Pour l'équivalence, si M et N sont des A-modules gauches, ils sont isotypiques. Le type λ des sous-modules simples de N et M est le même, puisque quotient de A_g. Soit S, un A-module simple de type λ, il existe donc deux entiers n, m tels que $M \simeq S^n$ et $N \simeq S^m$. On a alors,

$$M \simeq N \Longleftrightarrow S^n \simeq S^m \Longleftrightarrow n = m \Longleftrightarrow n[S:k] = m[S:k] \Longleftrightarrow [M:k] = [N:k]$$

Définition 22.— *Etant donné un corps commutatif k, on appelle k-algèbre simple centrale, toute k-algèbre A de dimension finie telle que $Z(A) = k$.*

Remarque 23.— Le théorème 20 et la proposition 14 assurent donc, qu'à isomorphisme près, les k-algèbres simples centrales sont biunivoquement décrites par les algèbres de matrices $\mathscr{M}_n(K)$ où K décrit les corps de dimension finie sur leur centre k et $n \in \mathbb{N}^*$.

Par ailleurs, étant donnée un k-algèbre simple centrale A, on a $A \simeq \mathscr{M}_n(K)$. On peut retrouver les éléments caractéristiques n et K de la manière suivante : il n'y a qu'un seul type de A-modules simples. Un tel module S est donc isomorphe aux M_i de l'exemple 2. On voit alors que la dimension de S sur k est l'entier n. Le corps K est lui égal à $\mathscr{L}_A(S)^{\mathrm{op}}$ d'après le théorème 12.

1.3 Algèbres tensorielles

On considère dans cette partie, un corps commutatif k. Dans le paragraphe 1.3.1 et le paragraphe 1.3.2 jusqu'à l'exemple 32, on ne suppose pas forcément que les espaces vectoriels et les algèbres que l'on considère soient de dimensions finies sur k.

1.3.1 Produit tensoriel

Théorème 24.— *Soit E et F deux k-espaces vectoriels. Il existe un k-espace vectoriel T, unique à isomorphisme près, muni d'une application bilinéaire $\varphi : E \times F \longrightarrow T$ tel que pour tout k-e.v. G et toute application bilinéaire $f : E \times F \longrightarrow G$ il existe une unique application linéaire $\tilde{f} : T \longrightarrow G$ telle que :*

$$\forall (x,y) \in E \times F,\ f(x,y) = \tilde{f} \circ \varphi(x,y)$$

Preuve : On considère le k-espace vectoriel $\mathscr{M}$ de base $\{x,y\}_{(x,y)\in E\times F}$ et le sous-espace N engendré par les éléments

$$\begin{gathered}(x_1+x_2,y)-(x_1,y)-(x_2,y)\\(x,y_1+y_2)-(x,y_1)-(x,y_2)\\\alpha(x,y)-(\alpha x,y)\\\alpha(x,y)-(x,\alpha y)\end{gathered}$$

où x,x_1,x_2 parcourent E, y,y_1,y_2 parcourent F et α parcourt k. On pose $T=\mathscr{M}/N$ et φ la restriction à $E\times F$ de la sujection canonique de $\mathscr{M}$ sur $\mathscr{M}/N$. L'application φ est bilinéaire. En effet, soit $(x_1,y),(x_2,y)\in E\times F$ et $\alpha\in k$, on a $\alpha(x_1,y)+(x_2,y)-(\alpha x_1+x_2,y)\in N$ et donc $\varphi(\alpha(x_1,y)+(x_2,y))=\alpha\varphi((x_1,y))+\varphi(x_2,y))$ ce qui assure que φ est linéaire à droite. On montre de même que φ est linéaire à gauche.

Soit G un k-espace vectoriel et $f:E\times F\longrightarrow G$ une application bilinéaire. Comme $\{x,y\}_{(x,y)\in E\times F}$ est une k-base de $\mathscr{M}$, f induit une unique application linéaire de $\mathscr{M}$ sur G. Puisque f est bilinéaire, il s'ensuit que N est contenu dans le noyau de l'application induite par f et donc f définit, par passage au quotient, une application linéaire $\tilde{f}:T\longrightarrow G$ qui vérifie $f(x,y)=\tilde{f}\circ\varphi(x,y)$ pour tout $(x,y)\in E\times F$.

L'unicité de T (à isomorphisme) près, découle de l'unicité de $\tilde{f}$ à f donnée.

———

Définition 25.— *Le k-espace vectoriel G du théorème précédent s'appelle le produit tensoriel sur k des espaces E et F. Il se note $E\otimes_k F$. Pour tout $(x,y)\in E\times F$ on note $x\otimes y$ l'élément $\varphi(x,y)$.*

Proposition 26.— *Soient E et F deux k-espaces vectoriels. Si $\{x_i\}_{i\in I}$ et $\{y_j\}_{j\in J}$ sont des k-bases respectives de E et F alors $\{x_i\otimes y_j\}_{(i,j)\in I\times J}$ est une k-base de $E\otimes_k F$. En particulier, on a*

$$\dim_k E\otimes_k F=\dim_k E.\dim_k F$$

Preuve : Soit $\sum_{i,j}\lambda_{i,j}(x_i\otimes y_j)=0$ une équation de dépendance linéaire. On a $\sum_{i,j}\lambda_{i,j}(x_i\otimes y_j)=\sum_{i,j}(\lambda_{i,j}x_i)\otimes y_j=\sum_{i,j}\varphi\left(\lambda_{i,j}x_i,y_j\right)$ et si l'on considère la première projection $\pi:E\times F\longrightarrow E$, il existe une application $\tilde{\pi}:E\otimes_k F\longrightarrow E$ telle que $\pi=\tilde{\pi}\circ\varphi$. On a donc

———

On obtient alors comme corollaire immédiat :

Corollaire 27.— *Soient E, F et G des k-espaces vectoriels.*

1) Les espaces $E\otimes_k F$ et $F\otimes_k E$ sont isomorphes (commutativité du produit tensoriel).

2) Les espaces $(E\otimes_k F)\otimes_k G$ et $E\otimes_k(F\otimes_k G)$ sont isomorphes (associativité du produit tensoriel).

Corollaire 28.— *Soient E et F deux k-espaces vectoriels et E_0 un sous-espace de E. On a $E \otimes_k F = E_0 \otimes_k F$ si et seulement si $E_0 = E$.*

Preuve : Soit $\{y_i\}_{i\in I}$ une k-base de F, $\{x_i\}_{i\in I_0}$ une k-base de E_0 et $\{x_i\}_{i\in I_0}$ une k-base de E qui complète celle de E_0. D'après la proposition 26 les ensembles $\{x_i \otimes y_j\}_{(i,j)\in I_0\times J} \subset \{x_i \otimes y_j\}_{(i,j)\in I\times J}$ sont des bases respectives de $E_0 \otimes_k F$ et $E \otimes_k F$. Ces deux espaces sont donc égaux si et seulement si les bases considérées sont égales, c'est-à-dire si et seulement si $I_0 = I$.

———

1.3.2 Produit tensoriel d'algèbres

Proposition 29.— *Soient A et B deux k-algèbres. Sur le k-espace vectoriel $A \otimes_k B$ il existe une unique loi de composition interne qui fait de $A \otimes_k B$ une k-algèbre et qui vérifie pour tout $x, y \in A$ et tout $u, v \in B$*

$$(x \otimes u)(y \otimes v) = (xy) \otimes (uv)$$

Preuve : Unicité : Le produit dans une k-algèbre est entièrement déterminé par les valeurs des produits des vecteurs d'une k-base fixée par ce produit. Notons $(a_i)_i$ et $(b_j)_j$ des k-bases de A et de B. La proposition 26 montre que $(a_i \otimes b_j)_{i,j}$ est une k-base de $A \otimes_k B$. Si $\perp_1$ et $\perp_2$ sont deux lois de compositions vérifiant les hypothèses de la proposition, pour tout i, i', j, j' on a

$$(a_i \otimes b_j) \perp_1 (a_{i'} \otimes b_{j'}) = (a_i a_{i'}) \otimes (b_j b_{j'}) = (a_i \otimes b_j) \perp_2 (a_{i'} \otimes b_{j'})$$

ce qui prouve que $\perp_1 = \perp_2$.

Existence : Fixons un couple $(y, v) \in A \times B$ et considérons l'application

$$\begin{array}{rccc} f_{y,v} : & A \times B & \longrightarrow & A \otimes_k B \\ & (x, u) & \longmapsto & (xy) \otimes (uv) \end{array}$$

Cette application est clairement bilinéaire, il existe donc (théorème 24) un unique élément $\tilde{f}_{y,v} \in \mathscr{L}(A \otimes_k B)$ tel que pour tout $(x, u) \in A \otimes_k B$,

$$\tilde{f}_{y,v}(x \otimes u) = (xy) \otimes (uv)$$

Maintenant l'application

$$\begin{array}{ccc} A \times B & \longrightarrow & \mathscr{L}(A \otimes_k B) \\ (y, v) & \longmapsto & \tilde{f}_{y,v} \end{array}$$

est visiblement bilinéaire, ainsi (théorème 24) il existe une unique application

$$\varphi : A \otimes_k B \longrightarrow \mathscr{L}(A \otimes_k B)$$

telle que pour tout $(y,v) \in A \times B$,

$$\tilde{f}_{y,v} = \varphi(y \otimes v)$$

Pour $(x \otimes u), (y \otimes v) \in A \otimes_k B$, on pose

$$(x \otimes u)(y \otimes v) = (\varphi(x \otimes u))(y \otimes v)$$

Ceci définit une loi de composition interne sur $A \otimes B$, qui vérifie pour tout $x, y \in A$ et tout $u, v \in B$

$$(x \otimes u)(y \otimes v) = (xy) \otimes (uv)$$

On vérifie sans peine avec la définition qu'on en a donné, que cette loi fait finalement de $A \otimes_k B$ une k-algèbre.

———

Dans la suite, quand on tensorisera deux algèbres on considérera toujours la multiplication introduite plus haut pour faire du produit tensoriel une algèbre. On voit alors que, compte tenu des résultats sur les constantes de structures d'une algèbre, les isomorphismes établis dans le corollaire 27 restent vrais si l'on suppose que E, F et G sont des k-algèbres.

Dans une algèbre tensorisée $A \otimes_k B$, on identifie les algèbres A et B aux sous-algèbres $A \otimes 1$ et $1 \otimes B$ et l'on voit alors que tout élément de A commute avec tout élément de B. Cette propriété se transfère aux morphismes :

Proposition 30.— *Soient A, B, C trois k-algèbres et $\theta_A : A \longrightarrow C$ et $\theta_B : B \longrightarrow C$ deux morphismes de k-algèbres. Pour qu'il existe un morphisme de k-algèbre $\theta : A \otimes_k B \longrightarrow C$ vérifiant que $\theta_{|A} = \theta_A$ et $\theta_{|B} = \theta_B$, il faut et il suffit que tout élément de $\theta_A(A)$ commute avec tout élément de $\theta_B(B)$ dans C. Dans ces conditions, le morphisme θ est unique et il est défini par la relation tensorielle*

$$\theta(x \otimes y) = \theta_A(x)\theta_B(y)$$

Preuve : Si θ existe alors pour tout tenseur $x \otimes y \in A \otimes_k B$, on a

$$\theta(x \otimes y) = \theta((x \otimes 1).(1 \otimes y)) = \theta(x \otimes 1)\theta(1 \otimes y) = \theta_A(x)\theta_B(y)$$

ceci prouve, par linéarité, l'unicité de θ. Puisque $(x \otimes 1).(1 \otimes y) = (y \otimes 1).(1 \otimes x)$, on voit aussi que $\theta_A(x)\theta_B(y) = \theta_B(y)\theta_A(x)$ pour tout $(x,y) \in A \times B$.

Réciproquement, la donnée de θ_A et θ_B, définie par propriété universelle du produit tensoriel une unique application k-linéaire $\theta : A \otimes_k B \longrightarrow C$ vérifiant $\theta(x \otimes y) = \theta_A(x)\theta_B(y)$. Le fait que θ soit un morphisme d'algèbre résulte, par linéarité, de l'égalité sur les produits de tenseurs suivante :

$$\begin{aligned} \theta((x \otimes y).(u \otimes v)) &= \theta(xu \otimes yv) = \theta_A(xu)\theta_B(yv) = \theta_A(x)\theta_A(u)\theta_B(y)\theta_B(v) \\ &= \theta_A(x)\theta_B(y)\theta_A(u)\theta_B(v) = \theta(x \otimes y)\theta(u \otimes v) \end{aligned}$$

Remarque 31.— On considère deux algèbres A et B et V un A-B-bimodule, c'est-à-dire un ensemble qui est A-module à gauche et B-module à droite et tel que pour tout $(a,b,x) \in A \times B \times V$ on ait $a.(x.b) = (a.x).b$. Comme V est un B-module à droite, on peut aussi le voir comme B^{op}-module à gauche pour la même action. Pour $x \in V$, on définit

$$\begin{array}{rccc} f_x : & A \times B^{\mathrm{op}} & \longrightarrow & V \\ & (a,b) & \longmapsto & (a.x).b \end{array}$$

Cette application étant visiblement bilinéaire, on peut lui faire correspondre une application linéaire $\widetilde{f_x} : A \otimes_k B^{\mathrm{op}} \longrightarrow V$ qui vérifie

$$\widetilde{f_x}\left(\sum_i a_i \otimes b_i\right) = \sum_i (a_i.x).b_i$$

Maintenant, on a

$$\widetilde{f_x}((a\otimes b)(c\otimes d)) = \widetilde{f_x}((ac \otimes db)) = ac.x.db = \widetilde{f}_{\widetilde{f_x}(c\otimes d)}(a\otimes d)$$

et l'on voit ainsi qu'en posant $\left(\sum_i a_i \otimes b_i\right).x = \sum_i (a_i.x).b_i$ on définit une action qui confère à V une structure de $A \otimes_k B^{\mathrm{op}}$-module gauche sur V.

Réciproquement, si V est un $A \otimes_k B^{\mathrm{op}}$-module gauche alors comme $A, B^{\mathrm{op}} \subset A \otimes_k B^{\mathrm{op}}$ c'est aussi un A-mobule gauche et un B^{op}-module gauche, donc un B-module droite. Du fait que les éléments de A commutent avec ceux de B^{op} dans $A \otimes_k B^{\mathrm{op}}$, on en déduit que V est aussi un A-B-bimodule.

Exemple 32.— Si A est une k-algèbre et $n \geq 1$ un entier, l'algèbre $A \otimes_k \mathscr{M}_n(k)$ est isomorphe à $\mathscr{M}_n(A)$.

En effet, considérons $(a_r)_r$ une k-base de A et $(\gamma_{i,j})_{i,j}$ la base canonique de $\mathscr{M}_n(k)$. En tant que k-espace vectoriel, $\mathscr{M}_n(A)$ possède $(a_r\gamma_{i,j})_{r,i,j}$ pour base et donc la correspondance

$$\gamma_{i,j} \otimes a_r \longrightarrow a_r\gamma_{i,j}$$

définit un isomorphisme de k-espace vectoriel ψ. Par ailleurs, on a

$$\begin{array}{rcl} \psi((\gamma_{i,j}\otimes a_r)(\gamma_{p,q}\otimes a_s)) & = & \psi((\gamma_{i,j}\gamma_{p,q})\otimes(a_r a_s)) \\ & = & a_r a_s \gamma_{i,j}\gamma_{p,q} \\ & = & a_r \gamma_{i,j} a_s \gamma_{p,q} \\ & = & \psi(\gamma_{i,j}\otimes a_r)\psi(\gamma_{p,q}\otimes a_s) \end{array}$$

ce qui assure que ψ est bien un isomorphisme d'algèbre (cf. ???).

Ainsi, si l'on prend $A = \mathscr{M}_p(k)$, on a

$$\mathscr{M}_p(k) \otimes_k \mathscr{M}_n(k) \simeq \mathscr{M}_n(\mathscr{M}_p(k)) \simeq \mathscr{M}_{np}(k)$$

Intéressons-nous maintenant au cas des algèbres simples.

Lemme 33.— *Soient K un corps contenant k dans son centre $Z(K)$ et A une k-algèbre. Tout idéal bilatère de $K \otimes_k A$ est engendré par un idéal bilatère de $Z(K) \otimes_k A$.*

En conséquence de quoi, si K est de centre k et si A est simple, alors $K \otimes_k A$ est une k-algèbre simple.

Preuve : Soit $\{e_1, \cdots, e_n\}$ une k-base de A. Si l'on considére $K \otimes_k A$ comme K-espace vectoriel gauche ($x \in K$ opérant sur $K \otimes_k A$ par multiplication par $x \otimes 1$), la famille $\{1 \otimes e_1, \cdots, 1 \otimes e_n\}$ est alors une K-base de $K \otimes_k A$. On a donc $n = [A : k] = [K \otimes_k A : K]$.

Si J est un idéal bilatère de $K \otimes_k A$ alors J est un sous-K-espace vectoriel de $K \otimes_k A$, de sorte que $K \otimes_k A/J$ est aussi un K-espace vectoriel à gauche. Ainsi, il existe une partie $I \subset \{1, \cdots, n\}$ telle que les images modulo J de $\{1 \otimes e_i\}_{i \in I}$ forment une K-base de $K \otimes_k A/J$. Pour tout indice $j \notin I$, il existe une unique famille $\{x_{i,j}\}_{i \in I}$ d'éléments de K telle que

$$1 \otimes e_j = \sum_{i \in I} x_{i,j} \otimes e_i \bmod J$$

On pose alors

$$\varepsilon_j = 1 \otimes e_j - \sum_{i \in I} x_{i,j} \otimes e_i$$

de sorte que la famille $\{\varepsilon_j\}_{j \notin I}$ forme une K-base de J.

Considérons $x \in K$, pour tout $j \notin I$, on a

$$(x \otimes 1)\varepsilon_j(x^{-1} \otimes 1) = 1 \otimes e_j - \sum_{i \in I} x x_{i,j} x^{-1} \otimes e_i \in J$$

et donc, $(x \otimes 1)\varepsilon_j(x^{-1} \otimes 1) - \varepsilon_j = \sum_{i \in I}(x_{i,j} - x x_{i,j} x^{-1}) \otimes e_i \in J$. On en déduit que $x_{i,j} = x x_{i,j} x^{-1}$, et ce, pour tout $x \in K$. Ainsi, $x_{i,j} \in Z(K)$ et l'idéal J qui est engendré par les ε_j est donc engendré par l'idéal bilatère de $Z(K) \otimes_k A$ engendré par les tenseurs $x_{i,j} \otimes e_i$.

Supposons maintenant que $Z(K) = k$ et A soit simple. Si J désigne un idéal bilatère de $K \otimes_k A$, alors il est engendré par un idéal bilatère J_0 de $Z(K) \otimes_k A = k \otimes_k A \simeq A$. Ainsi, par simplicité de A, on en déduit que $J_0 = \{0\}$ ou $Z(K) \otimes_k A$ et donc $J = \{0\}$ ou $K \otimes_k A$. Ainsi, $K \otimes_k A$ est bien une algèbre simple.

Théorème 34.— *Soient A et B deux k-algèbres simples. Si l'une de ces deux algèbres est de centre k, alors $A \otimes_k B$ est une k-algèbre simple.*

Preuve : Le théorème 20 assure que $A \simeq \mathscr{M}_n(K_1)$ et $B \simeq \mathscr{M}_p(K_2)$ où K_1 et K_2 sont des corps contenant k dans leurs centres. Si on suppose que A est centrale, alors K_1 est exactement de centre k. D'après les résultats de l'exemple 32, on a alors

$$A \otimes_k B \simeq \mathscr{M}_n(K_1) \otimes_k \mathscr{M}_p(K_2) \simeq \mathscr{M}_n(k) \otimes_k K_1 \otimes_k \mathscr{M}_p(k) \otimes_k K_2 \simeq \mathscr{M}_{np}(K_2) \otimes_k K_1$$

et comme $\mathscr{M}_{np}(K_2)$ est une k-algèbre simple, le lemme 33 permet de conclure que $A \otimes_k B$ est simple.

———

Corollaire 35.— *Soit K un corps de dimension n sur son centre k. L'algèbre $K \otimes_k K^{op}$ est isomorphe à $\mathscr{M}_n(k)$.*

Preuve : Le corps K est de manière évidente un K-K-bimodule. On peut donc considérer K comme $K \otimes_k K^{op}$-module à gauche (remarque 31). On en déduit donc l'existence d'un morphisme non trivial de k-algèbre $\omega : K \otimes_k K^{op} \longrightarrow \mathscr{L}_k(K)$. Maintenant, le théorème 34 assure que $K \otimes_k K^{op}$ est simple et donc ω est injective. Comme $K \otimes_k K^{op}$ et $\mathscr{L}_k(K) (\simeq \mathscr{M}_n(k))$ ont même dimension sur k, on conclu que ω est un isomorphisme.

———

1.3.3 Extension des scalaires

Considérons une k-algèbre A, un surcorps commutatif K de k et l'application

$$\begin{array}{ccc} K & \longrightarrow & A \otimes_k K \\ x & \longmapsto & 1 \otimes x \end{array}$$

Il s'agit d'un homomorphisme qui permet d'identifier K en un sous-anneau (qui est donc un corps) de $A \otimes_k K$. Visiblement, puisque K est commutatif son image est contenue dans le centre de $A \otimes_k K$. Ainsi, $A \otimes_k K$ a naturellement une structure de K-algèbre.

Définition 36.— *La K-algèbre $A \otimes_k K$ s'appelle l'algèbre obtenue à partir de A par extension des scalaires de k à K.*

Si $(a_i)_i$ désigne une k-base de A, alors $(a_i \otimes 1)_i$ est une K-base de $A \otimes_k K$ et l'on en déduit en particulier que $[A \otimes_k K : K] = [A : k]$. Lemme 46 à venir assure que $Z(A \otimes_k K) = Z(A) \otimes_k K$ et l'on en déduit donc

Proposition 37.— *Si K/k désigne une extension de corps commutatifs et A une k-algèbre simple centrale alors $A \otimes_k K$ est une K-algèbre simple centrale de même dimension sur K que A sur k.*

On remarque, part ailleurs, que les multiplications dans A et $A \otimes_k K$ ont même constantes de structures dans ces bases. On en déduit que :

Proposition 38.— *Soit $L/K/k$ une tour d'extensions de corps commutatifs.*

1/ Si A et B sont deux k-algèbres isomorphes, alors $A \otimes_k K$ et $B \otimes_k K$ sont deux K-algèbres isomorphes.

2/ Si A est une k-algèbre, alors les deux L-algèbres $(A \otimes_k K) \otimes_K L$ et $A \otimes_k L$ sont isomorphes.

3/ Si A et B sont deux k-algèbres, alors les deux K-algèbres $(A \otimes_k K) \otimes_K (B \otimes_k K)$ et $(A \otimes_k B) \otimes_k K$ sont isomorphes.

Preuve : Conséquence de l'étude des constantes de structure des algèbres considérées.

———

Bien que A et $A \otimes_k K$ aient des constantes de structures identiques dans les bases décrites précédemment, il ne faut pas en déduire trop rapidement quelque chose de structurel sur $A \otimes_k K$ à partir de A. Pour illustrer cette mise en garde, considérons une extension algébrique stricte K/k et un élément $x \in K$ qui n'est pas dans k. Notons alors $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in k[X]$ son polynôme minimal. Dans l'algèbre $K \otimes_k K$, pour tout $k \geq 1$, on a

$$(x \otimes 1)^k - (1 \otimes x)^k = (x \otimes 1 - 1 \otimes x)(x^{k-1} \otimes 1 + x^{k-2} \otimes x + \cdots + 1 \otimes x^{k-1})$$

et donc

$$\begin{aligned} P(x \otimes 1) - P(1 \otimes x) &= (x \otimes 1)^n - (1 \otimes x)^n + a_{n-1}((x \otimes 1)^{n-1} - (1 \otimes x)^{n-1}) + \\ &\quad \cdots + a_1(x \otimes 1 - 1 \otimes x) \\ &= (x \otimes 1 - 1 \otimes x)\Big((x^{n-1} \otimes 1 + \cdots + 1 \otimes x^{n-1}) + \\ &\quad a_{n-1}(x^{n-2} \otimes 1 + \cdots + 1 \otimes x^{n-2}) + \cdots + a_1(1 \otimes 1)\Big) \end{aligned}$$

Maintenant, comme $\{1, x, \cdots, x^{n-1}\}$ est une famille k-libre de K, la famille $\{x^i \otimes x^j\}_{i,j<n}$ est k-libre. Dans l'expression

$$(x^{n-1} \otimes 1 + \cdots + 1 \otimes x^{n-1}) + a_{n-1}(x^{n-2} \otimes 1 + \cdots + 1 \otimes x^{n-2}) + \cdots + a_1(1 \otimes 1)$$

les tenseurs $x^i \otimes x^j$ n'apparaissent chacun qu'une seule fois, ce qui assure que cette expression est non nulle. Pour les mêmes raisons, on a $(x \otimes 1 - 1 \otimes x) \neq 0$. Pourtant, $P(x \otimes 1) = P(1 \otimes x) = 0$ et on a ainsi trouvé un produit de deux éléments non nuls qui est nul. Ainsi, $K \otimes_k K$ n'est pas intègre au contraire de K.

De manière générale, le produit tensoriel de deux corps peut être ou non un corps. Nous allons examiner dans la suite le cas des corps commutatifs.

On se donne donc deux extensions L/k et M/k de corps commutatifs. La théorie générale des corps commutatifs montre que l'on peut plonger L et M dans un même corps Ω. Dans Ω le compositum $L.M$ est, par définition, le plus petit sous-corps de Ω contenant L et M. Il peut être décrit comme le corps des fractions de l'anneau $R = \{\sum_{i \in I} \lambda_i \mu_i / \ I \text{ fini}, \ \lambda_i, \mu_i \in L \times M\}$. La construction de $L.M$ dépend fortement des plongements de L et M ainsi que du corps Ω. Par exemple, si l'on prend $L = k(x)$, $M = k(y)$ et $\Omega = k(u, v)$, et que l'on plonge les

corps en appliquant $x \mapsto u$ et $y \mapsto v$ on a $L.M = \Omega$, alors que si l'on prend $x \mapsto u$ et $y \mapsto u$ on a $L.M = k(u)$ qui ne peut définitivement pas être k-isomorphe au précédent compositum. On ne peut donc pas parler du compositum $L.M$ dans l'absolu. Dans la suite, quand on parlera d'un compositum $L.K$ on sous-entendra la donnée d'un corps Ω muni de plongements de L et K dans Ω.

Etant donné un compositum $L.M$, par propriété universelle du produit tensoriel, l'application $(\lambda, \mu) \in L \times M \longmapsto \lambda\mu \in L.K$ définit un morphisme de k-algèbre $\varphi : L \otimes_k M \longrightarrow L.M$ associé au choix du compositum $L.K$. Ce dernier est donné par ses images sur les tenseurs : $\varphi(\lambda \otimes \mu) = \lambda\mu$. On voit que l'image par φ de $L \otimes_k M$ dans $L.M$ est égale à l'anneau R décrit précédemment. On en déduit la proposition suivante :

Proposition 39.— *Avec les notations précédentes, pour tout compositum $L.K$, les propositions suivantes*

i) le k-morphisme φ est un isomorphisme,

ii) $L \otimes_k M$ est un corps,

sont équivalentes et, dans cette situation, le corps $L \otimes_k M$ est alors isomorphe au compositum $L.M$.

Preuve : L'implication $i) \Rightarrow ii)$ et ce qui en découle est immédiate. Réciproquement, si $L \otimes_k M$ est un corps alors son image par φ est un sous-corps de $L.K$ contenant L et K. Par définition du compositum, on en déduit qu'elle est égale à $L.K$ tout entier.

———

Corollaire 40.— *Si le produit tensoriel $L \otimes_k M$ est un corps alors tous les compositums $L.K$ sont k-isomorphes.*

L'exemple donné précédemment montre que $k(x) \otimes_k k(y)$ n'est pas un corps.

Caractérisons maintenant l'injectivité du morphisme φ :

Proposition 41.— *Soit $L.M$ un compositum. Les propriétés suivantes*

i) le k-morphisme φ est injectif,

ii) les images de L et M dans $L.M$ sont des corps linéairement disjoints sur k,

sont équivalentes. De plus, l'existence d'un compositum $L.K$ vérifiant ces propriétés équivaut à la propriété suivante :

iii) $L \otimes_k M$ est une k-algèbre intègre.

Preuve : Pour l'équivalence $i) \Longleftrightarrow ii)$ on se donne un compositum $L.K$ et l'on identifie L et M à leurs images dans $L.K$.

$i) \Longrightarrow ii)$ Supposons que L et M ne soit pas linéairement disjoints sur k. Il existe donc une famille k-libre $\{y_1, \cdots, y_n\}$ d'éléments de M et une famille non triviale $\{x_1, \cdots, x_n\}$ d'éléments de M telles que $x_1y_1 + \cdots + x_ny_n = 0$. L'élément

$\alpha = x_1 \otimes y_1 + \cdots + x_n \otimes y_n \in L \otimes_k M$ n'est certainement pas nul puisque $\{y_1, \cdots, y_n\}$ est k-libre et qu'au moins un des x_i est non nul. Ainsi, φ n'est pas injectif.

$ii) \Longrightarrow i)$ Si φ n'est pas injectif alors il existe un élément non nul $\alpha = x_1 \otimes y_1 + \cdots + x_n \otimes y_n \in L \otimes_k M$ tel que $\varphi(\alpha) = 0$. Quitte à écrire les éléments y_i dans une k-base donnée de M et à utiliser la propriété de k-bilinéarité du produit tensoriel, on peut supposer que la famille $\{y_1, \cdots, y_n\}$ est k-libre (éventuellement l'entier n change lui aussi). Puisque $\varphi(\alpha) = x_1 y_1 + \cdots + x_n y_n = 0$ et que la famille $\{x_1, \cdots, x_n\}$ n'est pas triviale, on en déduit que la famille $\{y_1, \cdots, y_n\}$ est L-liée, ce qui prouve que L et M ne sont pas linéairement disjointes sur k.

$i) \Longrightarrow iii)$ Puisque la k-algèbre $L \otimes_k M$ s'identifie par φ à une sous-k-algèbre du corps $L.M$, elle est nécessairement intègre.

$iii) \Longrightarrow i)$ Si $R = L \otimes_k M$ est un anneau intègre, alors il possède un corps de fractions Ω dans lequel R s'injecte par un k-morphisme φ. Les corps $L = L \otimes_k k$ et $M = k \otimes_k M$ se plongent par φ dans Ω, et l'on peut donc considérer le compositum $L.M \subset \Omega$ relativement à ces plongements. Puisque $\varphi(L \otimes_k M) \subset L.M$, le k-morphisme φ est donc bien celui défini par la propriété universelle du produit tensoriel et il est injectif.

———

Puisque, vus dans $k(x, y)$, les corps $k(x)$ et $k(y)$ sont visiblement linéairement disjoints sur k, on voit que $k(x) \otimes_k k(y)$ est une k-algèbre intègre, mais qui n'est pas un corps en vertu de ce qui précède.

Cherchons maintenant une condition suffisante sur les corps M et L pour que la k-amgèbre $L \otimes_k M$ soit un corps. Commençons par le cas des extensions algébriques :

Lemme 42.— *Si L/k et M/k désignent deux extensions algébriques linéairement disjointes sur k, alors la k-algèbre $L \otimes_k M$ est un corps.*

En particulier, si L/k et M/k désignent deux extensions finies sur k alors $L \otimes_k M$ est un corps si et seulement si $[L.M : k] = [L.k].[M.k]$.

Preuve : On considère L et M dans une même clôture algébrique $\overline{k}$ de k. Les éléments du compositum $L.M$ sont des rapports de la forme $\sum_i \lambda_i \mu_i / \sum_j \lambda_j \mu_j$ avec $\lambda_i, \lambda_j \in L$ et $\mu_i, \mu_j \in M$. Vu que l'ensemble des sommes $\sum_i \lambda_i \mu_i$ correspond précisément à l'image dans $L.M$ de φ, montrer que $L \otimes_k M$ est un corps (c'est-à-dire montrer que φ est surjectif) revient à prouver que l'inverse dans $L.K$ de toute somme non nulle $s = \sum_i \lambda_i \mu_i$ s'écrit encore sous la forme $\sum_p \lambda_p \mu_p$. Puisque les extensions L et M sont algébriques sur k, il en est de même de $L.M$. Ainsi, une somme $s = \sum_i \lambda_i \mu_i \neq 0$ est un élément algébrique sur k et il existe donc un polynôme $P \in k[x]$ tel que $s^{-1} = P(s)$ (le polynôme P s'obtient, par exemple, en prenant $P(x) = (1 - H(0)^{-1} H(x))/x$ où H désigne le polynôme minimal de s sur k). Par composition, on voit que $s^{-1} = P(\sum_i \lambda_i \mu_i) = \sum_p \lambda_p \mu_p$ pour des $\lambda_p, \mu_p \in L \times M$ bien choisis.

La dernière partie du lemme provient du fait que l'égalité $[L.M : k] =$

$[L.k].[M.k]$ caractérise le fait que L et M sont linéairement disjointes sur k.

Lemme 43.— *Soit $L = k(x_i)_i$ une extension transcendante pure de k de base de transcendance $\{x_i\}_{i\in I}$. Si M/k désigne une extension algébrique alors la k-algèbre $L \otimes_k M$ est un corps, isomorphe à $M(x_i)_i$.*

Preuve : Il est clair que, canoniquement plongés dans $M(x_i)_i$, les corps L et M sont linéairement disjoints sur k et que leur compositum est égal à $M(x_i)_i$. Tout revient donc à montrer que φ est surjectif et, comme on l'a expliqué dans la preuve du lemme précédent, il s'agit en fait de montrer que si l'on prend une somme non nulle $s = \sum_{p=1}^{n} \mu_p r_p(x_i)_i$ avec $\mu_p \in p$ et $r_p \in k(x_i)$ alors s^{-1} s'écrit sous la forme d'une somme de la même nature. En écrivant chaque r_p sous forme d'un rapport de polynômes et en réduisant au même dénominateur, on voit que s s'écrit sous la forme $P(x_i)_i/Q(x_i)_i$ avec $P \in M[x_i]_i$ et $Q \in k[x_i]_i$. On va montrer que P^{-1} peut s'écrire sous la forme $P_0(x_i)_i/Q_0(x_i)_i$ avec $P_0 \in M[x_i]_i$ et $Q_0 \in k[x_i]_i$, ce qui montrera bien ce que l'on veut.

On considère $\alpha_0, \cdots, \alpha_n \in M$ les coefficients non nuls du polynôme P. Si l'un des α_i n'est pas séparable sur k, alors la caractéristique de k est égale à un nombre premier $p > 0$ et il existe un entier h_i tel que $\alpha_i^{p^{h_i}}$ soit séparable. Ainsi, il existe un entier h tel que, pour tout $i = 0, \cdots, n$, $\alpha_i^{p^h}$ soit séparable. Maintenant, les $\alpha_i^{p^h}$ sont exactement les coefficients non nuls du polynôme P^{p^h}. Quitte à écrire $P^{-1} = P^{p^h-1}/P^{p^h}$, on peut donc supposer que tous les α_i sont séparables.
On note M_0 la clôture galoisienne su k du corps $k(\alpha_0, \cdots, \alpha_n)$. L'extension M_0/k est donc galoisienne finie et l'on note G son groupe de Galois. Le groupe G est aussi le groupe de Galois de l'extension $M_0(x_i)_i/k(x_i)_i$, l'action des éléments de G sur $M_0(x_i)_i$ étant simplement l'action sur les coefficients des fractions rationnelles. On peut alors écrire

$$\frac{1}{P} = \frac{\displaystyle\prod_{\sigma\in G-\{Id\}} P^\sigma}{\displaystyle\prod_{\sigma\in G} P^\sigma}$$

L'action des éléments de G laissant visiblement invariant $Q_0 = \prod_{\sigma\in G} P^\sigma$, on en déduit que $Q_0 \in k[x_i]_i$. Le polynôme $P_0 = \prod_{\sigma\in G-\{Id\}} P^\sigma$ est *a priori* élément de $M_0(x_i)_i$. Pour montrer qu'il est élément de $M(x_i)_i$, il suffit de vérifier que, pour tout $\sigma_0 \in H = \mathrm{Gal}(M_0/k(\alpha_0, \cdots, \alpha_n))$, on a $P_0^{\sigma_0} = P_0$. Or,

$$P_0^{\sigma_0} = \prod_{\sigma\in G-\{\sigma_0^{-1}\}} P^\sigma = \frac{Q_0}{P^{\sigma_0^{-1}}}$$

Par construction, on a $P \in k(\alpha_0, \cdots, \alpha_n)$ et donc, $P^{\sigma_0^{-1}} = P$. Ainsi, $P_0^{\sigma_0}) = Q_0/P =$

P_0 et l'on a bien réussi à écrire $P(x_i)_i^{-1} = P_0(x_i)_i/Q_0(x_i)_i$ avec $P_0 \in M[x_i]_i$ et $Q_0 \in k[x_i]_i$.

———

Théorème 44.— *Soient L/k et M/k deux extensions de corps commutatifs linéairement disjointes sur k dans un certain compositum $L.K$. Pour que la k-algèbre $L \otimes_k M$ soit un corps, il suffit que l'une des deux extensions soit algébrique.*

Preuve : Supposons que M/k soit algébrique. La théorie des corps commutatifs dit que L est une extension algébrique d'une extension transcendante pure $k(x_i)_i$. Le lemme 43 assure que $M(x_i)_i = M \otimes_k k(x_i)_i$ et la proposition 38 prouve alors que

$$M \otimes_k L = (M \otimes_k k(x_i)_i) \otimes_{k(x_i)_i} L = M(x_i)_i \otimes_{k(x_i)_i} L$$

Les corps $M(x_i)_i$ et L sont des extensions algébriques de $k(x_i)_i$, visiblement linéairement disjointes. En appliquant le lemme 42 on en déduit que $M \otimes_k L = M(x_i)_i \otimes_{k(x_i)_i} L$ est bien un corps.

———

1.3.4 Commutant

Définition 45.— *Etant donné une sous-algèbre B d'une k-algèbre A, on appelle commutant de B l'ensemble noté $\widetilde{B}$ et composé des éléments de A qui commutent avec tous les éléments de B.*

Il est clair que pour toute sous-algèbre B de A, l'ensemble $\widetilde{B}$ est une sous-algèbre de A. Nous allons nous intéresser aux commutants dans le cas où les algèbres sont simples centrales.

Lemme 46.— *Soient A et B deux k-algèbres, C et D des sous-algèbres respectives de A et B, et $\widetilde{C}$ et $\widetilde{D}$ les commutants de C et D dans A et B. Dans l'algèbre $A \otimes_k B$, on a $\widetilde{C \otimes_k D} = \widetilde{C} \otimes_k \widetilde{D}$.*

En particulier, on a $Z(A \otimes_k B) = Z(A) \otimes_k Z(B)$.

Preuve : Il est déjà clair que $\widetilde{C} \otimes_k \widetilde{D} \subset \widetilde{C \otimes_k D}$. Considérons un élément $\sum_i x_i \otimes y_i \in A \otimes_k B$ où l'on a pris soin de prendre la famille $\{y_i\}_i$, k-libre. Si cet élément commute avec tous les éléments de $C \otimes_k D$, alors il commute en particulier avec les $z \otimes 1$, $z \in C$. Ainsi, pour tout $z \in C$ on a

$$\sum_i (zx_i - x_i z) \otimes y_i$$

Comme les y_i sont supposés k-linéairement indépendants, on en déduit que $zx_i - x_i z = 0$, c'est-à-dire $x_i \in \widetilde{C}$ pour tout i. Ainsi, on a $\widetilde{C \otimes_k D} \subset \widetilde{C} \otimes_k B$. Un raisonnement analogue montre que $\widetilde{C \otimes_k D} \subset A \otimes_k \widetilde{D}$. Si l'on choisit une base de A (resp. B) contenant une base de $\widetilde{C}$ (resp. $\widetilde{D}$), on constate que $(\widetilde{C} \otimes_k B) \cap (A \otimes_k \widetilde{D}) = \widetilde{C} \otimes_k \widetilde{D}$ et donc que $\widetilde{C \otimes_k D} \subset \widetilde{C} \otimes_k \widetilde{D}$.

Le centre d'une algèbre n'est rien d'autre que son commutant dans elle-même. Le relation $Z(A \otimes_k B) = Z(A) \otimes_k Z(B)$ découle alors du choix $C = A$ et $D = B$ dans ce qui précède.

Théorème 47.— *Soit A une k-algèbre simple centrale et B une sous-algèbre simple de A. On a :*

1/ L'algèbre $\widetilde{B}$ est simple.

2/ $[B : k].[\widetilde{B} : k] = [A : k]$.

3/ $\widetilde{\widetilde{B}} = B$.

Preuve : Commençons par montrer ce résultat lorsque $A \simeq \mathscr{M}_n(k)$.

Comme B est supposée simple, d'après le théorème 20, B est isomorphe à $\mathscr{M}_p(K)$ où K est un corps contenant k dans son centre.

Soit S un A-module simple. On a $[S : k] = n$ et $A = \mathscr{L}_k(S)$. Maintenant, S a aussi une structure de B-module et donc d'après la proposition 21 S est isotypique sur B. Si S_B est un B-module simple, alors $S = \bigoplus_q S_B$. D'après l'exemple 2 et le théorème 20 on a $[S_B : k] = p[K : k]$ et donc $n = [S : k] = pq[K : k]$.

Puisque $A = \mathscr{L}_k(S)$, on voit que $\widetilde{B} = \mathscr{L}_B(S)$. En effet, si l'on note $B = \{f_\omega \in \mathscr{L}_k(S) / \ \omega \in \Omega\}$, alors

$$\begin{array}{rcl} f \in \widetilde{B} & \iff & \forall \omega \in \Omega,\ f \circ f_\omega = f_\omega \circ f \iff \forall \omega \in \Omega,\ \forall s \in S,\ f \circ f_\omega(s) = f_\omega \circ f(s) \\ & \iff & \forall \omega \in \Omega,\ \forall s \in S,\ f(f_\omega.s) = f_\omega.f(s) \\ & \iff & \forall b \in B,\ \forall s \in S,\ f(b.s) = b.f(s) \iff f \in \mathscr{L}_B(S) \end{array}$$

La combinaison du théorème 12 et de l'exemple 4 montre que $\widetilde{B} = \mathscr{L}_B(S) \simeq \mathscr{M}_q(K^{\mathrm{op}})$. Ainsi, $\widetilde{B}$ est bien une algèbre simple. Par ailleurs, on a $[\widetilde{B} : k] = q^2[K^{\mathrm{op}} : k]$ et donc

$$[B : k][\widetilde{B} : k] = p^2[K : k]q^2[K^{\mathrm{op}} : k] = (pq[K : k])^2 = n^2 = [A : k]$$

L'algèbre $\widetilde{B}$ étant simple, en appliquant ce qui précède, on trouve

$$[B : k][\widetilde{B} : k] = [A : k] = [\widetilde{B} : k][\widetilde{\widetilde{B}} : k]$$

Ainsi, $[B : k] = [\widetilde{\widetilde{B}} : k]$ mais comme on a visiblement $B \subset \widetilde{\widetilde{B}}$, on en déduit finalement que $\widetilde{\widetilde{B}} = B$.

Paçons-nous maintenant dans le cas général. L'algèbre A est isomorphe à une algèbre de matrice $\mathscr{M}_n(K)$ où K est un corps de centre k. Posons $r = [K : k]$ et considérons l'algèbre (simple) $A \otimes_k K^{\mathrm{op}}$. Elle est isomorphe à $\mathscr{M}_n(k) \otimes_k K \otimes_k K^{\mathrm{op}}$ et donc, d'après le corollaire 35 et l'exemple 32, on a

$$A \otimes_k K^{\mathrm{op}} \simeq \mathscr{M}_n(k) \otimes_k K \otimes_k K^{\mathrm{op}} \simeq \mathscr{M}_n(k) \otimes_k \mathscr{M}_r(k) \simeq \mathscr{M}_{nr}(k)$$

Dans $A \otimes_k K^{op}$ considérons l'algèbre $B \otimes_k k$ qui, étant isomorphe à B, est simple. D'après le lemme 46 son commutant dans $A \otimes_k K^{op}$ est $\widetilde{B} \otimes_k K^{op}$. D'après le cas particulier, on en déduit que $\widetilde{B} \otimes_k K^{op}$ est une algèbre simple et que $[B : k][\widetilde{B} \otimes_k K^{op} : k] = n^2 r^2$. Comme $[\widetilde{B} \otimes_k K^{op} : k] = [\widetilde{B} : k][K^{op} : k] = [\widetilde{B} : k]r$, on en déduit que $[B : k][\widetilde{B} : k] = n^2 r = [A : k]$.

Par ailleurs, d'après le théorème 34, l'algèbre $B \otimes_k K^{op}$ est aussi simple et, d'après le lemme 46, son commutant dans $A \otimes_k K^{op}$ vaut $\widetilde{B} \otimes_k k$ qui est isomorphe à $\widetilde{B}$. D'après ce qui précède, $\widetilde{B}$ est donc simple.

Enfin, comme dans le cas particulier, l'égalité $\widetilde{\widetilde{B}} = B$ s'obtient en constatant que $B \subset \widetilde{\widetilde{B}}$ et, qu'en utilisant le 2/, $[B : k] = [\widetilde{\widetilde{B}} : k]$.

Remarque 48.— Soient B est une sous-k-algèbre simple d'une k-algèbre simple centrale A et $\widetilde{B}$ le commutant de B dans A. Considérons un élément $x \in Z(\widetilde{B})$, x est alors dans le commutant de $\widetilde{B}$, qui vaut B lui-même, d'après ce qui précède. Mais maintenant, puisque $x \in \widetilde{B}$, il est dans le centre de B. On en déduit que $Z(\widetilde{B}) \subset Z(B)$, mais puisque $\widetilde{\widetilde{B}} = B$, on en déduit finalement que $Z(\widetilde{B}) = Z(B)$.

En particulier, si B est une sous-k-algèbre simple centrale de A alors $\widetilde{B}$ est aussi une sous-k-algèbre simple centrale de A.

Exemple 49.— Considérons une k-algèbre simple A et M un A-module à gauche simple. D'après le lemme de Schur (proposition 3-2), l'algèbre $\mathscr{L}_A(M)$ est un corps, c'est donc une sous-k-algèbre simple de $\mathscr{L}_k(M)$ qui est elle une k-algèbre simple centrale (car isomorphe à $\mathscr{M}_n(k)$, où $n = \dim_k M$). Considérons le morphisme $\varphi : A \longrightarrow \mathscr{L}_A(M)$ défini pour $a \in A$ par

$$\begin{array}{rccc} \varphi(a) : & M & \longrightarrow & M \\ & x & \longmapsto & ax \end{array}$$

Il s'agit d'un plongement puisque φ est non nulle et que $\ker(\varphi)$ est un idéal bilatère de A qui est supposée simple par hypothèse. Ainsi, l'algèbre $\Omega = \varphi(A)$ est une sous-k-algèbre isomorphe à A et pour $f \in \mathscr{L}_k(M)$, on a

$$f \in \widetilde{\Omega} \Longleftrightarrow \forall a \in A,\ \forall x \in M,\ f(ax) = af(x) \Longleftrightarrow f \in \mathscr{L}_A(M)$$

Ainsi, $\widetilde{\Omega} = \mathscr{L}_A(M)$ et comme A est supposée simple, on en déduit en application du théorème 47-2, que le commutant dans $\mathscr{L}_k(M)$ du corps $\mathscr{L}_A(M)$ est (isomorphe à) l'algèbre A.

Corollaire 50.— *Soit A une k-algèbre simple centrale et B une sous-algèbre commutative de A qui est simple (e.g. B un corps commutatif). Les propriétés suivantes*

i) B est une sous-algèbre commutative maximale de A,

ii) $B = \widetilde{B}$,

iii) $[B : k]^2 = [A : k]$,

sont équivalentes.

Preuve : $i) \Longleftrightarrow ii)$ Puisque B est commutative toute sur-algèbre commutative de B est incluse dans $\widetilde{B}$. Si $x \in \widetilde{B}$ alors l'algèbre $B(x)$ engendrée par B et x dans A est une sur-algèbre commutative de B. L'équivalence annoncée découle alors de ces deux propriétés.

$ii) \Longleftrightarrow iii)$ Puisque $B \subset \widetilde{B}$, l'équivalence découle immédiatement du théorème 47.

Corollaire 51.— *Soit K un corps de dimension finie sur son centre k et L un corps intermédiaire. Les propriétés suivantes*

i) L est une sous-algèbre commutative maximale de K,

ii) L est un sous-corps commutatif maximal de K,

iii) $[L : k]^2 = [K : k]$,

sont équivalentes.

Preuve : $i) \Longleftrightarrow iii)$ C'est le corollaire 50 pour $A = K$.

$i) \Longleftrightarrow ii)$ Immédiat, compte tenu du fait que K est un corps et donc que les sous-algèbres de K sont des sous-corps.

Corollaire 52.— *Soit A une k-algèbre simple centrale. La dimension $[A : k]$ est un carré parfait.*

Preuve : Commençons par le cas où $A = K$ est un corps. Comme $[K : k]$ est finie et que k est commutatif, il existe un sous-corps commutatif maximal L de K. En effet, pour des raisons évidentes de dimension, toute suite croissante de sous-corps commutatifs de K est stationnaire. En application du corollaire précédent on a $[A : k] = [L : k]^2$ qui est donc un carré parfait.

Maintenant; si A est quelconque, A est isomorphe à une algèbre de matrices $\mathscr{M}_n(K)$ sur un corps K de centre k. On a donc $[A : k] = n^2[K : k] = n^2 r^2$ où r est la dimension d'un sous-corps commutatif maximal de K.

1.3.5 Le théorème de Skolem-Nœther

C'est le théorème suivant :

Théorème 53.— (Skolem-Nœther) *Soit A une k-algèbre simple centrale et B_1, B_2 deux sous-algèbres simples de A. S'il existe un k-isomorphisme $f : B_1 \longrightarrow B_2$, alors f est relevable en un automorphisme intérieur de A.*

Preuve : On sait que A est isomorphe à $\mathscr{M}_n(K)$ où K est le corps des A-endomorphismes d'un A-module à gauche, disons $K = \mathscr{L}_A(M)$. Les deux k-algèbres simples centrales $B_1 \otimes_k K$ et $B_2 \otimes_k K$ sont k-isomorphes par $\alpha \otimes \beta \longrightarrow f(\alpha) \otimes \beta$.

On peut donc confèrer à M une structure de $B_1 \otimes_k K$-module de deux manières différentes :

$$\begin{array}{rcl}(\alpha \otimes \beta)x & = & \alpha.\beta(x) = \beta(\alpha.x) \\ (\alpha \otimes \beta) * x & = & f(\alpha).\beta(x) = \beta(f(\alpha).x)\end{array}$$

Puisque $B_1 \otimes_k K$ est simple, tous les modules à gauche sur $B_1 \otimes_k K$ sont semi-simples isotypiques. Par ailleurs, pour ces deux structures, M a même dimension sur k, on en déduit qu'il existe un k-automorphisme, $g \in \mathscr{L}_k(M)$ qui est un $B_1 \otimes_k K$-isomorphisme de modules entre ces deux structures. On a donc pour tout $\alpha \in B_1$, $\beta \in K$ et $x \in M$

$$g(\beta(\alpha.x) = f(\alpha).\beta(g(x))$$

Si $\alpha = 1$, on a alors $g \circ \beta = \beta \circ g$ et ce pour tout $\beta \in K$. Ainsi, g est dans le commutant de $K = \mathscr{L}_A(M)$ dans $\mathscr{L}_k(M)$. D'après le résultat établi dans l'exemple 49, on en déduit qu'il existe $a \in A$ inversible (car g est un automorphisme) tel que pour tout $x \in M$, $g(x) = ax$. On a alors, pour tout $\alpha \in B_1$, $\beta \in K$ et $x \in M$,

$$a\alpha.\beta(x) = f(\alpha)a.\beta(x)$$

En prenant $\beta = Id$, on en déduit que $f(\alpha) = a\alpha a^{-1}$, et donc l'automorphisme intérieur associé à a^{-1} prolonge f sur A.

Corollaire 54.— *Les automorphismes d'une k-algèbre simple centrale sont intérieurs. En particulier les k-automorphismes d'un corps gauche de dimension finie sur son centre k, sont intérieurs.*

Preuve : Immédiat.

Application aux corps finis : le théorème de Wedderburn. Considérons un corps fini K de centre k. Puisque tous les sous-corps commutatifs maximaux de K ont même dimension, ils possèdent donc le même cardinal et sont donc isomorphes. En appliquant le théorème de Skolem-Noether, on en déduit que ces corps sont conjugués par automorphismes intérieurs dans K. Notons L un sous-corps commutatif maximal. Puisque tout élément de K est inclus dans un sous-corps commutatif on a $K^* = \bigcup_{x \in K^*} xLx^{-1}$.

Maintenant, le normalisateur de L^* contient évidemment L^*, il s'ensuit que le nombre des xL^*x^{-1} est plus petit que $[K^* : L^*]$. Mais comme $\sharp xL^*x^{-1} = \sharp L^*$, il est donc nécessaire que les xL^*x^{-1} soient disjoints deux à deux, mais comme il possède tous 1, cela n'est possible que s'il n'y en a qu'un... Ainsi $K = L$ est commutatif.

2 Groupe de Brauer

2.1 Généralités.

2.1.1 Définitions, exemples.

Étant donné un corps commutatif k et deux k-algèbres simples centrales A et B, on sait d'après le théorème 20 et la proposition 14 qu'il existe deux uniques entiers $n_A, n_B \geq 1$ et deux uniques corps (à isomorphisme près) K_A, K_B de centres k et de dimensions finies sur k tels que $A \simeq \mathscr{M}_{n_A}(K_A)$ et $B \simeq \mathscr{M}_{n_B}(K_B)$. On dira que A et B sont semblables (ou Brauer-équivalentes) si $K_A \simeq K_B$. On a alors :

Proposition 55.— *Soit A et B deux k-algèbres simples centrales. Les propositions suivantes*

i) A et B sont semblables,

ii) il existe deux entiers n et p tels que $\mathscr{M}_n(k) \otimes_k A \simeq \mathscr{M}_p(k) \otimes_k B$,

iii) il existe deux entiers n et p tels que $\mathscr{M}_n(A) \simeq \mathscr{M}_p(B)$,

sont équivalentes.

Preuve : $i) \Rightarrow ii)$ Il existe deux entiers $n, p \geq 1$ et un corps K un corps de centre k tels que $A \simeq \mathscr{M}_p(K)$ et $B \simeq \mathscr{M}_n(K)$. On a, d'après les résultats de l'exemple 32,

$$\mathscr{M}_n(k) \otimes_k A \simeq \mathscr{M}_n(k) \otimes_k \mathscr{M}_p(k) \otimes_k K \simeq \mathscr{M}_p(k) \otimes_k \mathscr{M}_n(k) \otimes_k K \simeq \mathscr{M}_p(k) \otimes_k B$$

$ii) \Rightarrow i)$ On a $A \simeq \mathscr{M}_{n_A}(K_A)$ et $B \simeq \mathscr{M}_{n_B}(K_B)$, on en déduit d'après l'exemple 32, que

$$\begin{array}{rcl} \mathscr{M}_{nn_A}(K_A) & \simeq & \mathscr{M}_{nn_A}(k) \otimes_k K_A \simeq \mathscr{M}_n(k) \otimes_k \mathscr{M}_{n_A}(k) \otimes_k K_A \\ & \simeq & \mathscr{M}_n(k) \otimes_k \mathscr{M}_{n_A}(K_A) \simeq \mathscr{M}_n(k) \otimes_k A \simeq \mathscr{M}_p(k) \otimes_k B \\ & \simeq & \mathscr{M}_p(k) \otimes_k \mathscr{M}_{n_B}(K_B) \simeq \mathscr{M}_{pn_B}(K_B) \end{array}$$

La proposition 14 assure alors que $nn_A = pn_B$ et surtout que $K_A \simeq K_B$, ce qui équivaut à dire que A et B sont semblables.

$ii) \iff iii)$ Immédiat, compte tenu des résultats établis dans l'exemple 32.

———

Etant donné une k-algèbre simple centrale A, la classe de A est l'ensemble des k-algèbres simples centrales semblables à A. Ainsi, toute k-algèbre simple centrale appartient à une unique classe, les classes de k-algèbres simples centrales sont donc en correspondance biunivoque avec l'ensemble de classe d'isomorphisme de corps de centres k et de dimensions finies sur k.

Définition 56.— *Etant donné un corps commutatif k, on appelle groupe de Brauer de k l'ensemble, noté* $\mathrm{Br}(k)$, *composé des classes de k-algèbres simples centrales. Si A désigne une k-algèbre simple centrale, on notera $[A]$ sa classe dans* $\mathrm{Br}(k)$.

Lemme 57.— *Soit $A, A^{'}$ et $B, B^{'}$ deux paires de k-algèbres simples centrales semblables. Les algèbres simples centrales $A \otimes_k B$ et $A^{'} \otimes_k B^{'}$ sont semblables.*

Preuve : Par hypothèses il existe des corps K_1 et K_2 de centre k et de dimensions finies sur k tels que $A \simeq \mathscr{M}_n(K_1)$, $A^{'} \simeq \mathscr{M}_{n^{'}}(K_1)$, $B \simeq \mathscr{M}_m(K_2)$ et $B^{'} \simeq \mathscr{M}_{m^{'}}(K_2)$ avec $n, n^{'}, m$ et $m^{'}$ des entiers ≥ 1. Puisque $K_1 \otimes_k K_2$ est une k-algèbre simple centrale, il existe un corps K_3 de centre k et de dimension finie sur k et un entier $q \geq 1$ tel que $K_1 \otimes_k K_2 \simeq \mathscr{M}_q(K_3)$. D'après ce qui précède, on a

$$\begin{array}{rcl} A \otimes_k B & \simeq & \mathscr{M}_n(K_1) \otimes_k \mathscr{M}_m(K_2) \simeq \mathscr{M}_n(k) \otimes_k K_1 \otimes_k \mathscr{M}_m(k) \otimes_k K_2 \\ & \simeq & \mathscr{M}_n(k) \otimes_k \mathscr{M}_m(k) \otimes_k K_1 \otimes_k K_2 \simeq \mathscr{M}_{nm}(k) \otimes_k \mathscr{M}_q(K_3) \\ & \simeq & \mathscr{M}_{nm}(k) \otimes_k \mathscr{M}_q(k) \otimes_k K_3 \simeq \mathscr{M}_{nmq}(k) \otimes_k K_3 \\ & \simeq & \mathscr{M}_{nmq}(K_3) \end{array}$$

De même, on obtient que $A^{'} \otimes_k B^{'} \simeq \mathscr{M}_{n^{'}m^{'}q}(K_3)$ ce qui prouve bien que $A \otimes_k B$ et $A^{'} \otimes_k B^{'}$ sont semblables.

Théorème 58.— *Le produit tensoriel des algèbres induit une loi de groupe abélien sur* $\mathrm{Br}(k)$.

Preuve : Soient $\alpha, \beta \in \mathrm{Br}(k)$ pour tout $A \in \alpha$ et tout $B \in \beta$, la classe de $A \otimes_k B$ ne dépend que de α et β, d'après le lemme précédent. Donc le produit tensoriel induit une loi de composition sur $\mathrm{Br}(k)$. L'associativité et la commutativité du produit tensoriel assurent que cette loi est associatice et commutative. Comme pour tout k-algèbre simple centrale, on a $A \otimes_k k \simeq A$, on en déduit que la classe de k est bien un neutre. La partie non triviale de l'énoncé consiste donc à montrer que toutes les classes possèdent un inverse.

Soient $\alpha \in \mathrm{Br}(k)$, il existe un unique corps K de dimension finie sur k tel que $K \in \alpha$. Le corollaire 35 assure que $K \otimes_k K^{\mathrm{op}}$ est isomorphe à $\mathscr{M}_n(k)$ qui représente la classe neutre de $\mathrm{Br}(k)$. Ainsi, la classe de K^{op} est l'opposé de α dans $\mathrm{Br}(k)$ et ce dernier est donc bien un groupe abélien.

Notations : Le groupe $\mathrm{Br}(k)$ étant abélien on notera $+$ sa loi de composition et 0 sont élément neutre. Si A désigne une k-algèbre simple centrale, on notera $[A]$ la classe de A dans $\mathrm{Br}(k)$. On a donc :

- Pour tout $n \geq 1$, $[\mathscr{M}_n(k)] = 0$.
- Pour toute paire A, B de k-algèbres simples centrales, $[A \otimes_k B] = [A] + [B]$.
- Pour toute k-algèbres simples centrales A, $-[A] = [A^{\mathrm{op}}]$.

Remarque 59.— On considère un $\mathscr{M}_n(k)$-module simple M et le k-isomorphisme d'algèbres

$$\begin{array}{rccc} \Theta : & \mathscr{M}_n(k) & \longrightarrow & \mathscr{L}_n(M) \\ & \alpha & \longmapsto & f_\alpha : x \longmapsto \alpha.x \end{array}$$

(Θ est injectif puisque $\mathscr{M}_n(k)$ est simple, et surjectif pour des raisons de dimensions).

Considérons alors une sous-k-algèbre simple centrale A de $\mathscr{M}_n(k)$ et notons $\widetilde{A}$ son commutant (qui est alors aussi une sous-k-algèbre simple centrale de $\mathscr{M}_n(k)$ d'après la remarque 48). D'après les résulats de l'exemple 49 l'image de A par Θ a pour commutant $\mathscr{L}_A(M)$ dans $\mathscr{L}_k(M)$.

Maintenant, en tant que A-module, M est semi-simple isotypique : $M = \bigoplus_q S$ où S est un A-module simple. D'après le théorème 12 on a alors $\mathscr{L}_A(M) \simeq \mathscr{M}_q(K)$ où $K = \mathscr{L}_A(S)$. Par ailleurs, en tant qu'algèbre simple centrale, A est isomorphe à une algèbre de matrices $\mathscr{M}_l(K')$. On sait, par exemple d'après le résulat de l'exemple 4, que $K' = \mathscr{L}_A(S)^{op} = K^{op}$. Ainsi, la classe de A dans $\mathrm{Br}(k)$ est celle de K^{op} et celle de $\widetilde{A}$ est celle de K.

Tout ceci montre que A et $\widetilde{A}$ appartiennent à des classes opposées dans $\mathrm{Br}(k)$, c'est-à-dire que $[\widetilde{A}] = -[A]$.

Exemples 60.— 1/ La classe nulle de $\mathrm{Br}(k)$ correspond au corps k lui-même. La nullité de $\mathrm{Br}(k)$ équivaut donc à affirmer qu'il n'existe aucun corps gauche de centre k et de dimension finie sur k. Donnons deux exemples de familles de tels corps :

a/ Si k est séparablement clos, alors $\mathrm{Br}(k) = 0$. En effet, nous verrons au paragraphe suivant (proposition 68) que si K est un corps gauche de centre k et de dimension finie sur k alors il existe dans K une extension séparable non triviale de k.

b/ Si k est un corps fini, alors $\mathrm{Br}(k) = 0$. Plus précisément, le théorème de Wedderburn est équivalent à dire que pour toute puissance q d'un nombre premier, on a $\mathrm{Br}(\mathbb{F}_q) = 0$. En effet, les corps gauches finis sont de dimension finie sur leur centre, ils sont donc entièrement décrits par les éléments non nuls des $\mathrm{Br}(\mathbb{F}_q)$ (q variant).

2/ On s'intéresse ici à $\mathrm{Br}(\mathbb{R})$. Nous allons montrer que $\mathrm{Br}(\mathbb{R})$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ en décrivant précisément les classes de $\mathbb{R}$-algèbres centrales.

Corps des quaternions d'Hamilton. On considère le $\mathbb{C}$-espace vectoriel de dimension 2, $\mathbb{H}$, rapporté à la base formelle $\{1, \omega\}$. Sur D, on considère la multiplication définie, pour $x, y, \alpha, \beta \in \mathbb{C}$, par

$$(x + y\omega).(\alpha + \beta\omega) = (x\alpha - y\overline{\beta}) + (x\beta + y\overline{\alpha})\omega$$

Une petit vérification élémentaire, que nous laissons au lecteur, montre que cette multiplication définit une structure de $\mathbb{R}$-algèbre sur $\mathbb{H}$. Il s'agit en fait d'un corps de centre $\mathbb{R}$ que l'on appelle le *corps des quaternions d'Hamilton*. En effet, si $\lambda = x + y\omega$ est dans $Z(\mathbb{H})$ alors, pour tout $\beta \in \mathbb{C}$, on a

$$-y\overline{\beta} + x\beta\omega = \lambda.\beta\omega = \beta\omega.\lambda = -\beta\overline{y} + \beta\overline{x})\omega$$

En particulier, $y\overline{\beta} = \beta\overline{y}$, et les choix $\beta = 1$ puis $\beta = i$ montrent que $y = 0$. On a donc $x\beta = \beta\overline{x}$ et le choix $\beta = 1$ prouve finalement que $x \in \mathbb{R}$. Ainsi, $Z(\mathbb{H})$ est bien égal à $\mathbb{R}$. Maintenant, on a

$$(x + y\omega).(\overline{x} - y\omega) = x\overline{x} + y\overline{y}$$

et donc, si $\lambda = x + y\omega \neq 0$, alors λ est inversible d'inverse

$$\lambda^{-1} = \frac{\overline{x}}{|x|^2 + |y|^2} - \frac{\overline{y}}{|x|^2 + |y|^2}\omega$$

Ainsi, $\mathbb{H}$ est un corps. Il est nécessairement non commutatif car de dimension finie sur $\mathbb{R}$ plus grande que 2. C'est historiquement le premier exemple de corps non commutatif, il date de 1843. Il représente donc un élément non trivial de $\mathrm{Br}(\mathbb{R})$. Cet élément non trivial est en fait le seul. Pour montrer ce résultat, nous allons établir un théorème datant de 1878 et du à Frobenius qui assure qu'un corps K contenant $\mathbb{R}$ dans son centre et de dimension finie sur $\mathbb{R}$ est obligatoirement isomorphe à $\mathbb{R}$,$\mathbb{C}$ ou $\mathbb{H}$:

Si K est supposé commutatif, alors K est isomorphe à $\mathbb{R}$ ou $\mathbb{C}$. Supposons maintenant que K soit gauche. Son centre $Z(K)$ est obligatoirement égal à $\mathbb{R}$, sinon puisque $Z(K)$ est un corps commutatif il serait isomorphe à $\mathbb{C}$. Mais alors, pour tout $x \in K - Z(K)$, le corps $Z(K)(x)$ serait un surcorps commutatif strict de $Z(K) \simeq \mathbb{C}$ de dimension finie, ce qui est absurde.

Considérons un élément $\alpha \in K$ tel que $\alpha \notin \mathbb{R}$. Le corps $\mathbb{R}(\alpha)$ est une extension commutative stricte de $\mathbb{R}$, il est donc isomorphe à $\mathbb{C}$. Il existe donc un élément $e_1 \in \mathbb{R}(\alpha)$ tel que $e_1^2 = -1$ et $\mathbb{R}(\alpha) = \mathbb{R}(e_1)$.

Maintenant, aucun élément $z \in K - \mathbb{R}(e_1)$ ne peut commuter avec e_1 sinon on disposerait d'une extension commutative stricte et finie de $\mathbb{C}$. Donc le commutant de $\mathbb{R}(e_1)$ dans K vaut $\mathbb{R}(e_1)$ et donc, d'après le théorème 47, on a $[K : \mathbb{R}] = [\mathbb{R}(e_1) : \mathbb{R}]^2 = [\mathbb{C} : \mathbb{R}]^2 = 4$.

Puisque K est gauche, il existe $y \in K$ tel que $y \notin \mathbb{R}(e_1)$ et l'on pose alors $z = ye_1 - e_1y$. Puisque $e_1z = e_1ye_1 + y = -ze_1$, on en déduit que $e_1z^2 = z^2e_1$ et donc $z^2 \in \mathbb{R}(e_1)$. Comme $\mathbb{R}(z) \simeq \mathbb{C}$ et que $\mathbb{R}(z) \neq \mathbb{R}(e_1)$, on en déduit que $\mathbb{R}(z) \cap \mathbb{R}(e_1) = \mathbb{R}$ et, par conséquent, $z^2 \in \mathbb{R}$. Si $z^2 \in \mathbb{R}^+$, alors il existe $a \in \mathbb{R}$ tel que $a^2 = z^2$ et donc $(z - a)(z + a) = 0$ dans K, ce qui est absurde puisque $z \notin \mathbb{R}$ et que K est un corps. En conclusion, $z^2 \in \mathbb{R}^{-*}$.

On pose $\omega = \frac{z}{\sqrt{-z^2}}$. Puisque $e_1z = -ze_1$, pour tout $x = u + ve_1 \in \mathbb{R}(e_1)$ $(u, v \in \mathbb{R})$, on a $x\omega = -\omega\overline{x}$ où $\overline{x} = u - ve_1$. Maintenant, en tant que $\mathbb{R}(e_1)$-espace vectoriel gauche, K est de dimension 2 et, visiblement $\{1, \omega\}$ est une base de K. Si $x, y, \alpha, \beta \in \mathbb{R}(e_1)$, on a alors

$$(x + y\omega).(\alpha + \beta\omega) = (x\alpha - y\overline{\beta}) + (x\beta + y\overline{\alpha})\omega$$

et, compte-tenu du fait que $\mathbb{R}(e_1) \simeq \mathbb{C}$, on en déduit finalement que $K \simeq \mathbb{H}$.

Le théorème de Frobenius assure ainsi qu'il n'y a que deux corps de dimension finie sur leur centre $\mathbb{R}$ (à isomorphisme près) : $\mathbb{R}$ lui-même et $\mathbb{H}$. Le groupe $\mathrm{Br}(\mathbb{R})$ est donc d'ordre 2 et, par suite, $\mathrm{Br}(\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$.

2.1.2 Indice, exposant et degré.

Si A désigne une k-algèbre simple centrale, on a vu que $[A : k]$ est un carré parfait (corollaire 52). On appelle *degré* de A l'entier $\deg(A) = \sqrt{[A : k]}$. Par ailleurs, on sait qu'il existe (à isomorphisme près) un unique corps K de centre k tel que $A \simeq \mathscr{M}_n(K)$ pour un certain entier n. L'entier $[K : k]$ étant aussi un carré parfait, on appelle *indice* de A l'entier $\mathrm{Ind}(A) = \sqrt{[K : k]}$. Enfin, on appellera *exposant* de A l'ordre $\exp(A)$ de $[A]$ dans le groupe $\mathrm{Br}(k)$. Nous verrons plus loin (corollaire 89) que l'exposant de A est toujours un entier naturel.

Si le degré de A dépend intrinséquement de A, on voit que son indice et son exposant ne dépend, en fait, que de sa classe dans $\mathrm{Br}(k)$. Ainsi, on peut parler de l'indice et de l'exposant d'un élément de $\mathrm{Br}(k)$, mais compte-tenu du fait que l'exposant d'un élément de $\mathrm{Br}(k)$ est juste son ordre, on réservera la terminologie d'exposant pour les k-algèbres simples centrales. Voyons maintenant quelques propriétés élémentaires de ces notions :

Proposition 61.— *Soient A et B deux k-algèbres simples centrales. On a :*

a) $\mathrm{Ind}(A) = \sqrt{\min\left\{[A' : k] / \ A' \in [A]\right\}}$.

b) L'entier $\mathrm{Ind}(A)$ *divise l'entier* $\deg(A)$ *et* $\mathrm{Ind}(A) = \deg(A)$ *si et seulement si A est un corps.*

c) $\deg(A \otimes_k B) = \deg(A).\deg(B)$.

d) L'entier $\mathrm{Ind}(A \otimes_k B)$ *divise le produit* $\mathrm{Ind}(A).\mathrm{Ind}(B)$.

e) Si $[A] = [B]$ *alors $A \simeq B$ si et seulement si* $\deg(A) = \deg(B)$.

Preuve : a) Immédiat compte-tenu du fait les algèbres $A' \in [A]$ sont celles de la forme $\mathscr{M}_n(K)$ où K désigne l'unique corps élément de $[A]$.

b) On a $A \simeq \mathscr{M}_n(K)$ pour un certain entier $n \geq 1$. On a $\mathrm{Ind}(A) = \sqrt{[K : k]} | n\sqrt{[K : k]} = \sqrt{[\mathscr{M}_n(K) : k]} = \sqrt{[A : k]} = \deg(A)$. Maintenant,

$$\mathrm{Ind}(A) = \deg(A) \Longleftrightarrow n = 1 \Longleftrightarrow A \simeq D$$

et comme D est l'unique corps dans $[A]$, on en déduit bien l'équivalence.

c) On a $\deg(A \otimes_k B)^2 = [A \otimes_k B : k] = [A : k][B : k] = (\deg(A).\deg(B))^2$.

d) Puisque la propriété porte sur des indices, on peut supposer que A et B sont des corps. En utilisant le b) et le c), on a donc

$$\mathrm{Ind}(A \otimes_k B) | \deg(A \otimes_k B) = \deg(A).\deg(B) = \mathrm{Ind}(A).\mathrm{Ind}(B)$$

e) L'hypothèse $[A] = [B]$ signifie qu'il existe un corps K de centre k et deux entiers n et m tels que $A \simeq \mathscr{M}_n(K)$ et $B \simeq \mathscr{M}_m(K)$. D'après la proposition14, on a $A \simeq B$ si et seulement si $n = m$ et comme $\deg(A) = n\mathrm{Ind}(A)$ (resp. $\deg(B) = m\mathrm{Ind}(A)$) on en déduit bien l'équivalence annoncée.

2.1.3 Extensions commutatives maximales, corps neutralisants.

Étant donnée une extension finie L/k de corps commutatifs, on sait que si A est une k-algèbre simple centrale alors $A \otimes_k L$ est une L-algèbre simple centrale. Par ailleurs, si A et B sont deux k-algèbres semblables d'après la proposition 55 il existe deux entiers n et p tels que $\mathscr{M}_n(k) \otimes_k A \simeq \mathscr{M}_p(k) \otimes_k B$. Donc, en appliquant la proposition 38, on trouve

$$\begin{aligned}
(A \otimes_k L) \otimes_L \mathscr{M}_n(L) &\simeq (A \otimes_k L) \otimes_L (\mathscr{M}_n(k) \otimes_k L) \\
&\simeq (A \otimes_k \mathscr{M}_n(k)) \otimes_k L \\
&\simeq (B \otimes_k \mathscr{M}_p(k)) \otimes_k L \\
&\simeq (B \otimes_k L) \otimes_L (\mathscr{M}_p(k) \otimes_k L) \\
&\simeq (B \otimes_k L) \otimes_L \mathscr{M}_p(L)
\end{aligned}$$

et ainsi les L-algèbres simples centrales $A \otimes_k L$ et $B \otimes_k L$ sont semblables. Ceci permet donc de définir une application

$$\beta_{L/k} : \mathrm{Br}(k) \longrightarrow \mathrm{Br}(L)$$

qui associe à une classe $\mathcal{A} \in \mathrm{Br}(k)$ de représentant A, la classe de $A \otimes_k L$ dans $\mathrm{Br}(L)$.

Proposition 62.— *Pour toute extension finie L/k, l'application $\beta_{L/k}$ est un morphisme de groupes. Par ailleurs, si $M/L/k$ est une tour d'extensions finies, alors $\beta_{M/k} = \beta_{M/L} \circ \beta_{L/k}$.*

Preuve : Conséquences immédiates de la proposition 38.

Définition 63.— *Soit A une k-algèbre simple centrale. On appelle corps neutralisant de A toute extension commutative finie L/k telle que la L-algèbre $A \otimes_k L$ soit isomorphe à une algèbre de matrices sur L. Dans cette situation on dit aussi que L déploie A ou que L est un corps déployant de A.*

On voit que si L est un corps neutralisant de A et que B est une k-algèbre simple centrale semblable à A alors L est aussi un corps neutralisant de B. On peut donc parler de corps neutralisant d'un élément de $\mathrm{Br}(k)$. Il s'ensuit que L est un corps neutralisant de A si et seulement si la classe de A dans $\mathrm{Br}(k)$ est dans le noyau du morphisme $\beta_{L/k} : \mathrm{Br}(k) \longrightarrow \mathrm{Br}(L)$.

La proposition 62 montre que si L est un corps neutralisant de $\mathcal{A} \in \mathrm{Br}(k)$, alors toute extension algébrique finie de L est aussi un corps neutralisant. On

peut caractériser les corps neutralisants en terme de sous-algèbres commutatives maximales :

Théorème 64.— *Soit A une k-algèbre simple centrale et $L \subset A$ un corps. Si L est une sous-algèbre commutative maximale, alors L est un corps neutralisant de A.*

Réciproquement, si L un corps neutralisant d'une k-algèbre simple centrale A alors L est une sous-algèbre commutative maximale d'une k-algèbre simple centrale C semblable à A (et l'on a alors $[C : k] = [L : k]^2$).

Preuve : L'algèbre A est isomorphe à une algèbre de matrices $\mathscr{M}_n(K)$ sur un corps K de dimension r^2 sur son centre k. Soit M un A-module à gauche simple. Le théorème 20 et l'exemple 4, montrent que M s'identifie à l'espace des colonnes à n éléments et à coefficients dans K de sorte que, $[M : k] = nr^2$. On sait, par ailleurs, que le corps opposé K^{op} s'identifie au corps $\mathscr{L}_A(M)$ (exemple 6). Ainsi, M peut-être vu comme un K-module à droite, mais comme les actions de A et de K sur M commutent visiblement, on en déduit (remarque 31) que M est un $A \otimes_k K^{op}$-module simple. Puisque $A \otimes_k K^{op}$ est simple, elle s'identifie donc en une sous-algèbre de $\mathscr{L}_k(M)$, mais comme $[A \otimes_k K^{op} : k] = [A : k].[K^{op} : k] = n^2r^4 = [M : k]^2 = [\mathscr{L}_k(M) : k]$ on en déduit finalement que $A \otimes_k K^{op}$ est isomorphe à $\mathscr{L}_k(M)$.

Puisque L est maximale dans A, son commutant dans A vaut L (corollaire 50) et donc, le commutant de $L \otimes_k K^{op}$ dans $A \otimes_k K^{op}$ est égal à $L \otimes_k k$ (lemme 46) qui est isomorphe à L. Puisque M est un $L \otimes_k K^{op}$-module, c'est donc aussi un L-espace vectoriel. L'image de L (en fait de $L \otimes_k k$) dans $\mathscr{L}_k(M)$ est le commutant de l'image de $L \otimes_k K^{op}$. D'après le résultat établi dans l'exemple 49, et du fait que le commutant du commutant d'une sous-algèbre simple est égal à elle-même (théorème 47), on en déduit que l'image de $L \otimes_k K^{op}$ dans $\mathscr{L}_k(M)$ est égale à $\mathscr{L}_L(M)$. Puisque $[L : k] = nr]$, on a donc $[M : L] = r$ et ainsi, $L \otimes_k K^{op} \simeq \mathscr{M}_r(L)$.

On vient donc de montrer que L est un corps neutralisant de K^{op}, mais comme $L^{op} = L$, on en déduit que L neutralise aussi K et donc A.

Réciproquement, posons $[A : k] = n^2$ et $[L : k] = q$. Dire que L un corps neutralisant d'une k-algèbre simple centrale A revient à dire que $A \otimes_k L \simeq \mathscr{L}_L(V)$ où V est un L-espace vectoriel de dimension n sur L. Puisque V est un $A \otimes_k L$-module à gauche, c'est aussi un A-module à gauche. Considérons $C = \mathscr{L}_A(V)$, d'après les résultats établis dans l'exemple 49, C est le commutant de A dans $\mathscr{L}_k(V)$. C'est une k-algèbre simple centrale qui contient L et l'on a $[C : k][A : k] = [V : k]^2 = n^2q^2$. Ainsi, $[C : k] = q^2$ et donc, d'après le corollaire 50, L est une sous-agèbre commutative maximale de C.

La première partie de la preuve du théorème 47, montre que le commutant d'une sous-k-algèbre simple centrale de $\mathscr{M}_m(k)$ est un élément de la classe opposée à la classe de cette algèbre dans $\mathrm{Br}(k)$. Ainsi, C^{op} est semblable à A, mais comme L est aussi inclus dans C^{op} on en déduit le résultat annoncé.

L'égalité $[C : k] = [L : k]^2$ découle de la construction de C, mais il ne pouvait en être autrement du fait du corollaire50.

Corollaire 65.— *Soit A une k-algèbre simple centrale. Il existe des corps neutralisants de A et leurs dimensions sur k sont toutes multiples de* $\mathrm{Ind}(A)$.

Preuve : Soit K le corps représentant $[A]$. D'après le corollaire 51 et le théorème 64, si L est une extension commutative de k maximale dans K (une telle extension existant bien) alors L est un corps neutralisant de $\mathcal{A}$ qui vérifie en outre $[L:k] = \mathrm{Ind}(A)\left(= \sqrt{[K:k]}\right)$.

Soit maintenant un corps neutralisant quelconque M de A. D'après le théorème 64 il existe une k-algèbre simple centrale C appartenant à $[A]$ et contenant M qui vérifie $[C:k] = [M:k]^2$. On sait qu'il existe un entier $n \geq 1$ tel que $C \simeq \mathscr{M}_n(K)$ et donc, on a $[M:k] = \sqrt{n^2.[K:k]} = n.\mathrm{Ind}(A)$.

Ces résultats permettent de caractériser les corps neutralisants en termes de plongements :

Corollaire 66.— *Soient k un corps neutralisant, $\alpha \in \mathrm{Br}(k)$, K_α le corps de centre k représentant α et $r = \mathrm{Ind}(\alpha) = \sqrt{[K_\alpha : k]}$ l'indice de α. On considère une extension commutative finie L/k.*

Si $[L:k]$ n'est pas un multiple de r, alors L ne neutralise pas α et si $[L:k] = nr$ pour un certain entier n, alors les propositions suivantes

i) L neutralise α,

ii) L se plonge dans l'algèbre $\mathscr{M}_n(K_\alpha)$,

sont équivalentes.

Preuve : $i) \Longrightarrow ii)$ D'après le théorème 64 il existe une algèbre A dans la classe α telle que L soit une sous-algèbre commutative maximale de A. Or, à isomorphisme près, l'algèbre A est de la forme $\mathscr{M}_m(K_\alpha)$ pour un certain entier m et, toujours d'après le théorème 64, on a $m^2r^2 = [\mathscr{M}_m(K_\alpha) : k] = [L:k]^2 = n^2r^2$ et donc, $m = n$.

$ii) \Longrightarrow i)$ $[\mathscr{M}_m(K_\alpha) : k] = [L:k]^2$ et donc, d'après le corollaire 51, L est une sous-algèbre maximale de $\mathscr{M}_n(K_\alpha)$ ce qui implique, d'après le théorème 64, que L neutralise α.

Remarque 67.— Soient k un corps commutatif, $\alpha \in \mathrm{Br}(k)$ d'indice r et K_α le corps de centre k représentant α. Les corps neutralisants α ont tous un degré de la forme rn (corollaire 65) et ceux qui sont de degré exactement r se plongent tous dans K_α (corollaire 66). On pourrait donc se demander si tous les corps neutralisants de α proviennent de corps neutralisant inclus dans K_α. Plus précisément, étant donné un corps neutralisant L de α existe-t-il un corps neutralisant $L_0 \subset K_\alpha$ tel que L soit une extension de L_0 ? La réponse à cette question est non, comme nous allons le voir dans l'exemple suivant.

On considère le $\mathbb{Q}(i)$-espace vectoriel de dimension 2, D, rapporté à la base formelle $\{1, \omega\}$. Sur D, on considère la multiplication définie, pour $x, y, \alpha, \beta \in \mathbb{Q}(i)$, par

$$(x + y\omega)(\alpha + \beta\omega) = (x\alpha - y\overline{\beta}) + (x\beta + y\overline{\alpha})\omega$$

Il s'agit de la même définition que le corps $\mathbb{H}$ des quaternions d'Hamilton, à la différence près que x, y, α, β vivent dans $\mathbb{Q}(i)$ et non dans $\mathbb{C}$. On vérifie, comme pour $\mathbb{H}$, que D est bien un corps, son centre étant alors $\mathbb{Q}$. Dans l'algèbre $\mathscr{M}_2(D)$ on considère la matrice

$$M = \begin{pmatrix} a^{-1} - a^{-1}ba & -a^{-1}b^2 \\ a & b \end{pmatrix}$$

où $a = -i + (1+i)\omega \in D$ et $b = 7i/2 + (1+2i)\omega \in D$. En calculant les puissances de M on trouve notamment :

$$M^2 = \begin{pmatrix} 0 & -23/4 \\ 1 & 0 \end{pmatrix} \text{ et } M^4 = \frac{-23}{4} I$$

Le polynôme $4T^4 + 23 \in \mathbb{Q}[T]$ étant visiblement irréductible et annulateur de M, on en déduit que M engendre dans $\mathscr{M}_2(D)$ un corps commutatif isomorphe à $L = \mathbb{Q}\left(\sqrt[4]{\frac{-23}{4}}\right)$. Puisque L est de dimension 4 sur $\mathbb{Q}$, d'après le corollaire 66, L neutralise D. Par ailleurs, l'extension $L/\mathbb{Q}$ possède un unique sous-corps strict qui est $\mathbb{Q}\left(\sqrt{-23}\right)$. Nous allons maintenant montrer que $\mathbb{Q}\left(\sqrt{-23}\right)$ n'est isomorphe à aucun sous-corps L_0 de D, ce qui montrera que L ne provient d'aucun corps neutralisant inclus dans D.

Les corps $L_0 \subset D$ tel que $[L_0 : \mathbb{Q}] = 2$ sont commutatifs et donc sont des extensions quadratiques de $\mathbb{Q}$. Ainsi, il existe un élément $\alpha \in \mathbb{Q} - \mathbb{Q}^2$ tel que $L_0 = \mathbb{Q}(\sqrt{\alpha})$. L'élément α est donc la carré d'un élément de D. Réciproquement, si $\alpha \in \mathbb{Q} - \mathbb{Q}^2$ est le carré d'un élément $\lambda \in D$, alors λ engendre dans D un corps isomorphe à $\mathbb{Q}(\sqrt{\alpha})$. Il s'agit donc de montrer que -23 n'est pas le carré d'un élément de D.

Examinons les carrés rationnels dans D. Si l'on pose $\lambda = x + y\omega \in D$ avec $x, y \in \mathbb{Q}(i)$, on a alors

$$\lambda^2 = (x^2 - y\overline{y}) + y(x + \overline{x})\omega$$

et donc, $\lambda^2 \in \mathbb{Q}$ si et seulement si $y = 0$ ou $x = iw$ avec $w \in \mathbb{Q}$.

1/ Si $y = 0$, alors posons $x = u + iv$ avec $u, v \in \mathbb{Q}$. On a $\lambda^2 \in \mathbb{Q}$ si et seulement $u^2 - v^2 + 2iuv = 0$. On en déduit alors que $\lambda^2 \in \pm\mathbb{Q}^2$.

2/ Si $x = iw$, alors posons $y = u + iv$ avec $u, v \in \mathbb{Q}$. On a $\lambda^2 = -u^2 - v^2 - w^2$.

En conclusion, les carrés rationnels de D sont exactement les carrés de $\mathbb{Q}$ et les opposés des sommes de trois carrés de rationnels. Un célèbre théorème dû à Gauss-Davenport-Cassels assure qu'un entier naturel n est somme de trois carrés dans $\mathbb{Q}$ si et seulement si n n'est pas de la forme $4^h(8k+7)$ avec $h, k \in \mathbb{N}$.

Puisque $23 \equiv 7 \bmod(8)$, on en déduit que -23 n'est pas le carré d'un élément de D, ce qui achève la preuve.

L'exemple que nous donnons ici est celui d'un corps neutralisant qui n'est pas une extension galoisienne de $\mathbb{Q}$. Pour un exemple de tel corps qui soit galoisien, il suffit de prendre le même corps gauche D qu'au-dessus et de considérer la matrice

$$M = \begin{pmatrix} 2i+\omega & i \\ -5i & -3i+\omega \end{pmatrix} \in \mathscr{M}_2(D)$$

On a alors $P(M) = 0$ avec $P(X) = X^4+5X^2+5$. Le polynôme P est galoisien sur $\mathbb{Q}$ et engendre l'extension $\mathbb{Q}\left(\sqrt{\frac{-5+\sqrt{5}}{2}}\right)/\mathbb{Q}$ qui est cyclique et dont l'unique corps intermédiaire strict vaut $\mathbb{Q}(\sqrt{5})$. Puisque 5 n'est pas un carré dans D, d'après ce qui précède, on en déduit que $L = \mathbb{Q}\left(\sqrt{\frac{-5+\sqrt{5}}{2}}\right)$ est un corps neutralisant de D, galoisien sur $\mathbb{Q}$, qui n'est extension d'aucun corps neutralisant inclus dans D.

On peut apporter une précision arithmétique sur l'ensemble des corps neutralisants :

Proposition 68.— *Soit K un corps de dimension finie sur son centre k. Il existe un sous-corps commutatif maximal de K qui est une extension séparable de k.*

En particulier, si $k = k^{sep}$ est un corps séparablement clos, alors $\mathrm{Br}(k) = 0$.

Preuve : Commençons par montrer l'existence d'un élément de $K-k$ qui est séparable sur k. En caractéristique 0, tous les éléments de $K-k$ sont séparables. On suppose donc que k est de caractéristique p et on considère un élément $y \in K-k$. Si $k(y)/k$ n'est pas purement inséparable il existe donc un élément dans $k(y)-k$ (et donc dans $K-k$) qui est séparable.

Si maintenant $k(y)/k$ est purement inséparable alors y est radiciel. Dans cette situation, si $X^{p^n}-\lambda$ désigne le polynôme minimal de y sur k, on considère l'élément $u = y^{p^{n-1}}$. Soit alors σ, l'automorphisme intérieur de K défini par u (i.e. $\sigma(z) = u^{-1}zu$ pour tout $z \in K$). Comme u vérifie $u^i \notin k$ pour tout $i = 1, \cdots, p-1$ et $u^p \in k$, on en déduit que σ est d'ordre p et puisque nous sommes en caractéristique p, on a $(\sigma - Id) \neq 0$ et $(\sigma - Id)^p = 0$. Soit alors r le plus grand entier tel que $(\sigma - Id)^r \neq 0$ et $z \in K$ tel que $(\sigma - Id)^r(z) \neq 0$. Posons $v = (\sigma-Id)^{r-1}(z)$ et $w = (\sigma-Id)^r(z)$. On a $(\sigma-Id)(w) = 0$ et $(\sigma-Id)(v) = w$, autrement dit $\sigma(w) = w$ et $\sigma(v) = v+w$. Soit alors $x = w^{-1}v$, on a $\sigma(x) = w^{-1}(v+w) = x+1$. Les éléments x et $x+1$ sont donc deux éléments distincts et conjugués du corps $k(x)$, ainsi x ne peut être radiciel. On en déduit que $k(x)$ contient des éléments séparables qui ne sont pas dans K.

Montrons maintenant la proposition par récurrence sur le degré $n = [K : k]$. Pour $n = 1$ la propriété est évidente. Pour $n \geq 2$, supposons la vraie pour les extensions de degré $< n$. D'après ce qui précède, il existe $x \in K-k$ séparable. Le

corps $L_0 = k(x)$ est donc une extension stricte et séparable de k. Si $\widetilde{L_0}$ désigne le commutant de L_0 dans K, on a $L_0 \subset \widetilde{L_0}$ et comme $\widetilde{\widetilde{L_0}} = L_0$ (théorème 47), on en déduit que le centre de $\widetilde{L_0}$ est L_0. Par ailleurs, puisque nous sommes dans un corps K, $\widetilde{L_0}$ est aussi un corps (si $z \in \widetilde{L_0}$ alors $z^{-1} \in \widetilde{L_0}$). Puisque $[\widetilde{L_0} : L_0] < [K : k] = n$, l'hypothèse de récurrence assure qu'il existe un sous-corps commutatif maximal L de $\widetilde{L_0}$ qui est une extension séparable de L_0. Par tansitivité, L est une extension séparable de k. Par ailleurs, d'après le théorème 14, on a

$$[\widetilde{L_0} : k][L_0 : k] = [K : k]$$

et, puisque L est un sous-corps commutatif maximal de $\widetilde{L_0}$, par le corollaire 51 on a aussi

$$[L : L_0]^2 = [\widetilde{L_0} : L_0]$$

On en déduit que

$$[L : k]^2 = [L : L_0]^2[L_0 : k]^2 = [\widetilde{L_0} : L_0][L_0 : k][L_0 : k] = [\widetilde{L_0} : k][L_0 : k] = [K : k]$$

et, en application du corollaire 51, on conclue finalement que L est bien un sous-corps commutatif maximal de K.

Supposons maintenant que k soit séparablement clos. Si K un corps de dimension finie sur son centre k, alors comme l'unique extension séparable de k étant k, on déduit de ce qui précède et du corollaire 51 que $[K : k] = [k : k]^2 = 1$ et donc $K = k$. Ainsi, $\mathrm{Br}(k) = 0$.

Corollaire 69.— *Toute k-algèbre simple centrale A possède un corps neutralisant qui est une extension galoisienne de k.*

Preuve : Si K désigne le corps (unique à isomorphisme prés) élément de $[A]$, d'après la proposition précédente il existe un sous-corps commutatif maximal L de K qui est une extension séparable de k. D'après le théorème 64, L est un corps neutralisant de $\mathcal{A}$. La cloture galoisienne $\overline{L}$ de L sur k est une extension finie de L et est, par conséquent, un corps neutralisant de K donc de A.

Ces résultats sur l'existence de corps neutralisant permettent de donner une nouvelle caractérisation des algèbres simples centrales :

Théorème 70.— *Soit A une algèbre de dimension finie sur son centre k. Les propositions suivantes*

i) A est simple,

ii) il existe une extension commutative finie L/k telle que $A \otimes_k L \simeq \mathscr{M}_n(L)$ *pour un certain entier n,*

ii′) il existe une extension commutative finie L/k, séparable, telle que $A \otimes_k L \simeq \mathscr{M}_n(L)$ *pour un certain entier n,*

iii) $A \otimes_k k^{sep} \simeq \mathscr{M}_n(k^{sep})$ *pour un certain entier* n,

sont équivalentes.

Preuve : $i) \Rightarrow ii')$ C'est la traduction du le corollaire 65.

$ii') \Rightarrow iii)$ Si $A \otimes_k L \simeq \mathscr{M}_n(L)$ pour un certain entier n, alors puisque k^{sep} est une extension de L, on a d'après la proposition 38-2

$$A \otimes_k k^{sep} \simeq (A \otimes_k L) \otimes_L k^{sep} \simeq \mathscr{M}_n(L) \otimes_L k^{sep} \simeq \mathscr{M}_n(k^{sep})$$

$iii) \Rightarrow i)$ Soit J est un idéal bilatère non nul de A, c'est en particulier un sous-espace vectoriel de A. L'espace vectoriel $J \otimes_k k^{sep}$ est un idéal bilatère de $A \otimes_k k^{sep} \simeq \mathscr{M}_n(k^{sep})$. Comme $\mathscr{M}_n(k^{sep})$ est simple, on en déduit que $J \otimes_k k^{sep} = A \otimes_k k^{sep}$ et, par application du corollaire 28, que $J = A$. Ainsi, A est simple.

$ii') \Rightarrow i)$ se montre exactement comme $iii) \Rightarrow i)$, en remplacant k^{sep} par L.

———

Ces propriétés permettent de donner une nouvelle caractérisation de l'indice. En appliquant les résultats du corollaire 65 et de la proposition 68, on voit que si A désigne une k-algèbre simple centrale A alors :

$$\begin{array}{rcl} \mathrm{Ind}(A) & = & \min\{[L:k]/\ L \text{ corps neutralisant de } A\} \\ & = & \min\{[L:k]/\ L \text{ corps neutralisant de } A,\ L/k \text{ séparable}\} \end{array}$$

Notons que cette notion de minimum vaut aussi bien pour l'ordre usuel $\leq$ sur $\mathbb{N}$ que pour l'ordre "divise" $.|.$ sur $\mathbb{N}^*$. Ainsi, on a

$$\begin{array}{rcl} \mathrm{Ind}(A) & = & \mathrm{pgcd}\{[L:k]/\ L \text{ corps neutralisant de } A\} \\ & = & \mathrm{pgcd}\{[L:k]/\ L \text{ corps neutralisant de } A,\ L/k \text{ séparable}\} \end{array}$$

Finissons ce paragraphe par des propriétés relatives à la neutralisation d'un produit tensoriel :

Proposition 71.— *Soient* k *un corps commutatif et* A *et* B *deux* k*-algèbres simples centrales.*

a) Si A *et* B *possède un corps neutralisant* L *en commun, alors* L *est aussi neutralisant de* $A \otimes_k B$. *En particulier, si* L *est neutralisant de* A, *alors il l'est aussi de* $A^{\otimes i} = A \otimes_k \cdots \otimes_k A$ *(*i *fois) pour tout* $i \geq 1$.

b) Si L *est neutralisant de* A *et* M *est neutralisant de* B *et si* L *et* M *sont linéairement disjoints sur* k, *alors* $L \otimes_k M$ *est un corps neutralisant de* $A \otimes_k B$.

Preuve : a) On a

$$\begin{array}{rcl} (A \otimes_k B) \otimes_k L & \simeq & A \otimes_k (B \otimes_k L) \simeq A \otimes_k \mathscr{M}_n(L) \simeq A \otimes_k (L \otimes_k \mathscr{M}_n(k)) \\ & \simeq & (A \otimes_k L) \otimes_k \mathscr{M}_n(k) \simeq \mathscr{M}_m(L) \otimes_k \mathscr{M}_n(k) \simeq \mathscr{M}_{nm}(L) \end{array}$$

et donc L neutralise $A \otimes_k B$. La suite de l'énoncé s'obtient par récurrence immédiate.

b) L'algèbre $L \otimes_k M$ est un corps commutatif (proposition41), extension finie de k. On a

$$\begin{aligned}(A \otimes_k B) \otimes_k (L \otimes_k M) &\simeq (A \otimes_k L) \otimes_k (B \otimes_k M) \simeq \mathscr{M}_n(L) \otimes_k \mathscr{M}_n(M) \\ &\simeq (\mathscr{M}_n(k) \otimes_k L) \otimes_k (\mathscr{M}_m(k) \otimes_k M) \\ &\simeq (\mathscr{M}_n(k) \otimes_k \mathscr{M}_m(k)) \otimes_k (L \otimes_k M) \\ &\simeq \mathscr{M}_{nm}(k) \otimes_k (L \otimes_k M) \simeq \mathscr{M}_{nm}(L \otimes_k M)\end{aligned}$$

et donc $L \otimes_k M$ neutralise de $A \otimes_k B$.

Corollaire 72.— *Soient k un corps commutatif et $\alpha, \beta \in \mathrm{Br}(k)$. Si α et β engendrent le même sous-groupe de* $\mathrm{Br}(k)$ *alors* $\mathrm{Ind}(\alpha) = \mathrm{Ind}(\beta)$.

Preuve : Par hypothèse, il existe deux entiers $i, j > 0$ tel que $\beta = i\alpha$ et $\alpha = j\beta$. Le lemme 71-a montre que si L neutralise α alors L neutralise β et réciproquement. Les éléments α et β ont donc même ensemble de corps neutralisants, leurs indices respectifs sont donc égaux.

2.1.4 Norme réduite.

On considère une k-algèbre simple centrale A et l'on se donne un corps neutralisant D de A. Il existe donc un entier $n \geq 1$ et un D-isomorphisme $\varphi : A \otimes_k D \longrightarrow \mathscr{M}_n(D)$. On définit alors l'application $\mathrm{Nrd}_{A/k}$ comme étant la composée

$$\mathrm{Nrd}_{A/k} : A \xrightarrow{a \mapsto a \otimes 1} A \otimes_k D \xrightarrow{\varphi} \mathscr{M}_n(D) \xrightarrow{\det} D$$

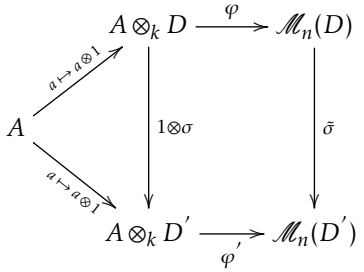
Proposition-Définition 73.— *L'application* $\mathrm{Nrd}_{A/k}$ *précédemment définie ne dépend ni du corps neutralisant D ni de l'isomorphisme φ. Elle est à valeur dans k et on l'appelle "la norme réduite" de la k-algèbre simple centrale A.*

Preuve : Commençons par montrer que pour le corps D fixé, la norme réduite ne dépend effectivement pas de φ. Considérons un autre isomorphisme $\varphi' : A \otimes_k D \longrightarrow \mathscr{M}_n(D)$. L'application $\varphi^{-1} \circ \varphi$ est alors un k-automorphisme de A et le théorème de Skolem-Noether (théorème 53) assure alors que c'est un automorphisme intérieur. Puisque le déterminant est invariant par conjugaison, on en déduit bien que $\mathrm{Nrd}_{A/k}$ ne dépend pas du choix du k-isomorphisme φ.

Etablissons maintenant une propriété relative à la norme réduite considérée sur une extension. Considérons une extension D'/D et notons $\sigma : D \longrightarrow D'$ le k-monomorphisme associé. Le corps D' est alors lui aussi un corps neutralisant de A. Le plongement σ se prolonge en un plongement $1 \otimes \sigma : A \otimes_k D \longrightarrow A \otimes_k D'$ en posant

$$1 \otimes \sigma(a \otimes \lambda) = a \otimes \sigma(\lambda)$$

Par ailleurs, σ définit, par identification des coefficients, un plongement $\tilde{\sigma} : \mathscr{M}_n(D) \longrightarrow \mathscr{M}_n(D')$. Cela permet de définir un k-isomorphisme $\varphi' : A \otimes_k D' \longrightarrow \mathscr{M}_n(D')$ qui fait commuter le diagramme suivant



(i.e. $\varphi'(a \otimes \sigma(\lambda)) = \tilde{\sigma}(\varphi(a \otimes \lambda))$). Le déterminant étant une application polynomiale en les coefficients d'une matrice, on en déduit que, pour tout $a \in A$, $\det(\varphi'(a \otimes 1)) = \sigma(\det(\varphi(a \otimes 1)))$.

D'après le corollaire 69, on sait que A possède un corps neutralisant D_0 galoisien sur k. On applique ce qui précède à $D = D' = D_0$ et il vient donc que $\det(\varphi(a \otimes 1)) \in D_0$ est invariant par tout élément $\sigma \in \mathrm{Gal}(D_0/k)$, ce qui montre que $\det(\varphi(a \otimes 1)) \in k$ pour le choix $D = D_0$.

Soit maintenant n'importe quel corps neutralisant D de A. Puisque D et D_0 sont extensions de k, on peut plonger D et D_0 dans leur compositum au moyen de k-monomorphismes $\sigma : D_0 \longrightarrow D_0.D$ et $\rho : D_0 \longrightarrow D_0.D$. On se donne des isomorphismes $\varphi : A \otimes_k D_0 \longrightarrow \mathscr{M}_n(D_0)$, $\varphi' : A \otimes_k D \longrightarrow \mathscr{M}_n(D)$ et $\varphi'' : A \otimes_k D_0.D \longrightarrow \mathscr{M}_n(D_0 D)$. Le propriété ci-dessus assure que pour tout $a \in A$, on a

$$\sigma(\det(\varphi(a \otimes 1))) = \det(\varphi''(a \otimes 1)) = \tau(\det(\varphi'(a \otimes 1)))$$

mais puisque $\det(\varphi(a \otimes 1))$ est élément de k d'après ce qui précède, on en déduit finalement que $\det(\varphi'(a \otimes 1)) = \det(\varphi(a \otimes 1))$ et la norme réduite ne dépend donc pas du choix de D.

Remarque : Lorsque $A = \mathscr{M}_n(k)$, en prenant $D = k$, on voit que $\mathrm{Nrd}_{A/k} = \det$.

Proposition 74.— *Soient A une k-algèbre simple centrale et $n^2 = [A : k]$.*

1/ Un élément $a \in A$ est inversible si et seulement si $\mathrm{Nrd}_{A/k}(a) \neq 0$.

2/ Si k est un corps infini et si $(e_1, \cdots, e_{n^2})$ désigne une k-base de A, alors le polynôme $P \in k[x_1, \cdots, x_{n^2}]$ défini, pour $(t_1, \cdots, t_{n^2}) \in k^{n^2}$, par

$$P(t_1, \cdots, t_{n^2}) = \mathrm{Nrd}_{A/k}(t_1 e_1 + \cdots + t_{n^2} e_{n^2})$$

est homogène de degré n.

Preuve : 1/ On reprend les notations du début de paragraphe. Si $a \in A$ est inversible dans A alors $a \otimes 1$ est inversible dans $A \otimes_k D$ et donc $\varphi(a \otimes 1)$ est une matrice inversible, ce qui assure que $\mathrm{Nrd}_{A/k}(a) = \det(\varphi(a \otimes 1)) \neq 0$.

Réciproquement, puisque A est une k-algèbre simple centrale, elle est isomorphe à $\mathcal{M}_n(K)$ pour un certain entier $n \geq 1$ et un certain corps K de centre k. Une matrice de $\mathcal{M}_n(K)$ est non inversible si et seulement si elle est pas diviseur de zéro dans $\mathcal{M}_n(K)$. Ainsi, si $a \in A$ est non inversible alors a est diviseur de zéro dans A et donc $a \otimes 1$ est diviseur de zéro dans $A \otimes_k D$ et donc la matrice $\varphi(a \otimes 1)$ est diviseur de zéro dans $\mathscr{M}_n(D)$. Ainsi, on a $\mathrm{Nrd}_{A/k}(a) = \det(\varphi(a \otimes 1)) = 0$.

2/ Le caractère polynomial du déterminant vu comme application ayant les coefficients d'une matrice comme variables, montre que P est bien un polynôme. Puisque k est infini et que P ne prend que des valeurs dans k sur k^n, on en déduit que P est bien élément de $k[x_1, \cdots, x_{n^2}]$.

Soient $t_1, \cdots, t_{n^2} \in k^{n^2}$ et $\lambda \in k$. Si l'on pose $a = t_1 e_1 + \cdots + t_{n^2} e_{n^2} \in A$, par propriété du déterminant on a alors

$$\begin{aligned} P(\lambda t_1, \cdots, \lambda t_{n^2}) &= \mathrm{Nrd}_{A/k}(\lambda a) = \det(\varphi(\lambda a \otimes 1)) = \det(\lambda \varphi(a \otimes 1)) = \lambda^n \det(\varphi(a \otimes 1)) \\ &= \lambda^n \mathrm{Nrd}_{A/k}(a) = \lambda^n P(\lambda t_1, \cdots, \lambda t_{n^2}) \end{aligned}$$

et comme k est infini, on en déduit bien que P est un polynôme homogène de degré n.

Exemple : On considère le corps $\mathbb{H}$ des quaternions d'Hamilton. On considère la $\mathbb{R}$-base $\{1, i, j, k\}$ de $\mathbb{H}$ où $i^2 = j^2 = k^2 = ijk = -1$. Le corps $\mathbb{C}$ des complexes est un corps neutralisant de $\mathbb{H}$ de sorte que $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}$ est $\mathbb{C}$-isomorphe à $\mathscr{M}_2(\mathbb{C})$. Pour calculer explicitement la norme réduite, il faut être en mesure d'exhiber un $\mathbb{C}$-isomorphe entre $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}$ et $\mathscr{M}_2(\mathbb{C})$. Puisque $\{1 \otimes 1, i \otimes 1, j \otimes 1, k \otimes 1\}$ est une $\mathbb{C}$-base de $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}$ et que les relations $(i \otimes 1)^2 = (j \otimes 1)^2 = (k \otimes 1)^2 = (i \otimes 1).(j \otimes 1).(k \otimes 1) = -1$ définissent à elles seules les constantes de structure de $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}$, il suffit de trouver trois matrice $A, B, C \in \mathscr{M}_2(\mathbb{C})$ telles que $A^2 = B^2 = C^2 = ABC = -I$ et telles que $\{I, A, B, C\}$ forment une $\mathbb{C}$-base de $\mathscr{M}_2(\mathbb{C})$. La correspondance $1 \longleftrightarrow I$, $(i \otimes 1) \longleftrightarrow A$, $(j \otimes 1) \longleftrightarrow B$, $(k \otimes 1) \longleftrightarrow C$ définira, par linéarité, un $\mathbb{C}$-isomorphe explicite entre $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}$ et $\mathscr{M}_2(\mathbb{C})$. On vérifie sans mal que le choix

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad C = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

convient. Ainsi, pour tout $a, b, c, d \in \mathbb{R}$, on a

$$\mathrm{Nrd}_{\mathbb{H}/\mathbb{R}}(a + bi + cj + dk) = \begin{vmatrix} a + ic & -b + id \\ b + id & a - ic \end{vmatrix} = a^2 + b^2 + c^2 + d^2$$

Il s'ensuit que le polynôme homogènes associé à la norme réduite de $\mathbb{H}$ relativement à la base pour le choix de la base $\{1, i, j, k\}$, tel que défini dans la proposition 74-2 est la forme quadratique

$$P(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

Extension des scalaires : On se donne une k-algèbre simple centrale A et une extension K/k de corps commutatifs. On a montré que l'algèbre $\Omega = A \otimes_k K$ obtenue à partir de A par extension des scalaires de k à K était une K-algèbre simple centrale (proposition 37). Si $n^2 = [\Omega : K] = [A : k]$ et $\underline{e} = (e_1, \cdots, e_{n^2})$ désigne une k-base de A alors $\underline{\tilde{e}} = (\tilde{e_1}, \cdots, \tilde{e_{n^2}})$ est une K-base de Ω. On note P_A (resp. P_Ω) le polynôme homogènes associé à la norme réduite de A (resp. Ω) relativement à la base $\underline{e}$ (resp. $\underline{\tilde{e}}$) tel que défini dans la proposition 74-2.

Proposition 75.— *Avec les notations précédentes, si le corps k est infini alors les polynômes P_A et P_Ω sont égaux.*

Preuve : On considère la clôture algébrique $\overline{K}$ de K. Il existe un k-isomorphisme

$$\varphi : \Omega \otimes_K \overline{K} = (A \otimes_k K) \otimes_K \overline{K} \longrightarrow A \otimes_k \overline{K}$$

que l'on peut choisir avec la propriété que $\varphi((a \otimes 1) \otimes 1) = a \otimes 1$. Le corps $\overline{K}$ est un corps neutralisant de la k-algèbre $\mathscr{A}$ et de la K-algèbre Ω, si bien qu'il existe un isomorphisme $\psi : A \otimes_k \overline{K} \longrightarrow \mathscr{M}_n(\overline{K})$. Le diagramme suivant

$$\begin{array}{ccccccc} A & \xrightarrow[a\mapsto a\otimes 1]{f} & A \otimes_k \overline{K} & \xrightarrow{\psi} & \mathscr{M}_n(\overline{K}) & \xrightarrow{\det} & \overline{K} \\ {\scriptstyle a\mapsto a\otimes 1}\downarrow & & \uparrow{\scriptstyle \varphi} & \nearrow{\scriptstyle \psi\circ\varphi} & & & \\ A \otimes_k K & \xrightarrow[x\mapsto x\otimes 1]{g} & (A \otimes_k K) \otimes_K \overline{K} & & & & \end{array}$$

est alors commutatif. Comme $\mathrm{Nrd}_{A/k} = \det \circ \psi \circ f$ et $\mathrm{Nrd}_{\Omega/K} = \det \circ (\psi \circ \varphi) \circ g$, on en déduit que

$$\mathrm{Nrd}_{A/k} = \mathrm{Nrd}_{\Omega/K} \circ \theta$$

Pour tout $(x_1, \cdots, x_{n^2}) \in k^{n^2}$, on a $\theta(x_1 e_1 + \cdots + x_{n^2} e_{n^2}) = x_1 \tilde{e_1} + \cdots + x_{n^2} \tilde{e_{n^2}}$ et donc $P_A(x_1, \cdots, x_{n^2})) = P_\Omega(x_1, \cdots, x_{n^2})$. Puisque le corps k est infini, on en conclut que $P_A = P_\Omega$.

———

On peut appliquer cette propriété pour étudier la question du produit tensoriel de deux corps, question que nous avons abordée dans le paragraphe 1.3.3 dans le cas des corps commutatifs. On se donne un corps non commutatif H de dimension finie sur son centre k. On note $n^2 = [H : k]$ et l'on se donne une k-base $\underline{e} = (e_1, \cdots, e_{n^2})$ de A. On considère alors le polynôme homogène P_H associé à la norme réduite de H relativement à cette base.

Corollaire 76.— *Avec les notations précédentes, pour toute extension de corps commutatifs L/k, l'algèbre $H \otimes_k L$ est un corps si et seulement si le polynôme homogène P_H ne possède que le zéro trivial sur L^{n^2}.*

Preuve : Il résulte du théorème de Wedderburn que k est nécessairement infini, on peut donc appliquer la proposition 75 pour affirmer que $P_{H\otimes_k L} = P_H$. Le fait que $H \otimes_k L$ soit un corps équivaut à dire que la norme réduite de tout élément

non nul de $H \otimes_k L$ est non nulle (proposition 74-1) ce qui équivaut visiblement à dire que $P_{H\otimes_k L}$ ne possède que le zéro trivial sur L^{n^2}.

Corollaire 77.— *Avec les notations précédentes, l'algèbre $H(t) = H \otimes_k k(t)$ (resp. $H((t)) = H \otimes_k k((t))$) est un corps de dimension $[H : k]$ sur son centre $k(t)$ (resp. $k((t))$).*

Preuve : Supposons donné $(r_1(t), \cdots, r_{n^2}(t))$ un zéro non trivial de P_H dans $k((t))^{n^2}$. On considérant ν la valuation minimale des séries $r_i(t)$, on peut écrire pour tout $i = 1, \cdots, n^2$, $r_i(t) = t^\nu r_i^{'}(t)/r(t)$ avec $r_i^{'}(t) \in k[[t]]$. L'une des séries entière $r_{i_0}^{'}(t)$ étant alors de valuation nulle. Puisque P_H est homogène de degré n, on voit que $P_H(r_1(t), \cdots, r_{n^2}(t)) = t^{n\nu}(r_1^{'}(t), \cdots, r_{n^2}^{'}(t))$ et donc $(r_1^{'}(t), \cdots, r_{n^2}^{'}(t))$ est un zéro non trivial de P_H dans $k[[t]]^{n^2}$. Il s'ensuit que $(r_1^{'}(0), \cdots, r_{n^2}^{'}(0))$ est un zéro de P_H dans k^{n^2}. Ce zéro est nécessairement non trivial puisque $r_{i_0}^{'}(0) \neq 0$. On vient donc de prouver que P_H ne possède aucun zéro non trivial dans $k((t))^{n^2}$ et ainsi le corollaire 76 assure bien que $H((t))$ est un corps. Puisque $k(t)$ se plonge dans $k((t))$, le polynôme P_H ne possède aucun zéro non trivial dans $k(t)^{n^2}$ et donc $H(t)$ est donc lui aussi un corps.

Le corps $H(t)$ (resp. $H((t))$) s'appelle le corps des fractions rationnelles (resp. des séries formelles) à coefficients dans H et à indéterminée centrale.

2.2 Interprétation cohomologique

2.2.1 Le produit croisé

Dans cette section on se fixe une extension galoisienne L/k de degré n fini et on note $G = \mathrm{Gal}(L/k)$ le groupe de Galois de cette extension. On considère un L-espace vectoriel à gauche A de dimension $n = [L : k] = o(G)$ et on note $\{a_\sigma\}_{\sigma\in G}$ une L-base de A. Etant donné $f : G \times G \longrightarrow L^*$ un système de facteurs, on considère sur A la multiplication définie par la formule

$$\left(\sum_{\sigma\in G} x_\sigma a_\sigma\right).\left(\sum_{\tau\in G} y_\tau a_\tau\right) = \sum_{\sigma,\tau\in G} f(\sigma,\tau) x_\sigma y_\tau^\sigma a_{\sigma\tau}$$

Il est clair que cette multiplication est k-bilinéaire. Elle est aussi associative. Pour montrer ceci, il suffit de le vérifier pour les éléments de A de la forme

$x_\sigma a_\sigma$. Soient donc $\sigma, \tau, \rho \in G$ et $x_\sigma, y_\tau, z_\rho \in L$, on a

$$\begin{aligned}
(x_\sigma a_\sigma . y_\tau a_\tau).z_\rho a_\rho &= (f(\sigma,\tau)x_\sigma y_\tau^\sigma a_{\sigma\tau}).z_\rho a_\rho \\
&= f(\sigma\tau,\rho)f(\sigma,\tau)x_\sigma y_\tau^\sigma z_\rho^{\sigma\tau} a_{\sigma\tau\rho} \\
&= f(\sigma,\tau\rho)f(\tau,\rho)^\sigma x_\sigma y_\tau^\sigma z_\rho^{\sigma\tau} a_{\sigma\tau\rho} \\
&= f(\sigma,\tau\rho)x_\sigma \left(f(\tau,\rho)y_\tau z_\rho^\tau\right)^\sigma a_{\sigma\tau\rho} \\
&= x_\sigma a_\sigma .(f(\tau,\rho)y_\tau z_\rho^\tau a_{\tau\rho}) \\
&= a_\sigma x_\sigma .(a_\tau y_\tau . a_\rho z_\rho)
\end{aligned}$$

L'associativité découle donc du fait que f est un système de facteurs. Ainsi, muni de ce produit, A est une k-algèbre de dimension n^2.

Définition 78.— *La k-algèbre A ainsi construite s'appelle le produit croisé de L par G relativement au système de facteurs f. On la note $\mathscr{A}(L/k, f)$.*

Théorème 79.— *Soit L/k une extension galoisienne finie et f un système de facteurs. La k-algèbre $\mathscr{A}(L/k, f)$ est unitaire, simple et de centre k, de plus elle admet une sous-algèbre commutative maximale qui est un corps isomorphe à L.*

Preuve : Notons e le neutre de $G = \mathrm{Gal}(L/k)$ et posons $\omega = f(e,e)$. Pour tout $\sigma \in G$ on a, d'après ???, $f(e,\sigma) = \omega$ et $f(\sigma,e) = \omega^\sigma$. Ainsi, pour tout $\sigma \in G$ et tout $x_\sigma \in L$ on a

$$\begin{aligned}
(x_\sigma a_\sigma).(\omega^{-1}a_e) &= x_\sigma f(\sigma,e)(\omega^{-1})^\sigma a_\sigma = x_\sigma a_\sigma \\
(\omega^{-1}a_e).(x_\sigma a_\sigma) &= f(e,\sigma)\omega^{-1}x_\sigma a_\sigma = x_\sigma a_\sigma
\end{aligned}$$

on en déduit que $\omega^{-1}a_e$ est neutre bilatère de $\mathscr{A}(L/k, f)$.

On définit maintenant une application $\varphi : L \longrightarrow \mathscr{A}(L/k, f)$, pour $z \in L$, par

$$\varphi(z) = \omega^{-1} z a_e$$

L'application φ est visiblement k-linéaire, mais comme pour $x, y \in L$ on a

$$\varphi(x)\varphi(y) = (\omega^{-1}xa_e).(\omega^{-1}ya_e) = \omega\omega^{-1}x\omega^{-1}ya_e = \omega^{-1}xya_e = \varphi(xy)$$

on en déduit que f est un isomorphisme de L sur une sous-algèbre de $\mathscr{A}(L/k, f)$. Si $\sigma \in G$, $x_\sigma \in L$ et $z \in L$ on a

$$\varphi(z).(x_\sigma a_\sigma) = (\omega^{-1}za_e).(x_\sigma a_\sigma) = f(e,\sigma)zx_\sigma\omega^{-1}a_\sigma = zx_\sigma a_\sigma$$

On pourra donc identifier L à son image par φ dans $\mathscr{A}(L/k, f)$, les produits à gauche coincidant. Etant donné $\sigma \in G$, puisque

$$f(\sigma^{-1},\sigma)^\sigma f(\sigma,e) = f(e,\sigma)f(\sigma,\sigma^{-1})$$

on a

$$\begin{aligned}
a_\sigma.(\omega f(\sigma^{-1},\sigma))^{-1}a_{\sigma^{-1}} &= f(\sigma,\sigma^{-1})(\omega^{-1})^\sigma (f(\sigma^{-1},\sigma)^{-1})^\sigma a_e \\
&= f(\sigma,\sigma^{-1})f(\sigma,e)^{-1}(f(\sigma^{-1},\sigma)^{-1})^\sigma a_e \\
&= f(e,\sigma)^{-1}a_e \\
&= \omega^{-1}a_e
\end{aligned}$$

Par ailleurs, comme

$$(\omega f(\sigma^{-1},\sigma))^{-1}a_{\sigma^{-1}}.a_\sigma = f(\sigma^{-1},\sigma)(\omega f(\sigma^{-1},\sigma))^{-1}a_e = \omega^{-1}a_e$$

on en déduit que a_σ est inversible et que $a_\sigma^{-1} = (\omega f(\sigma^{-1},\sigma))^{-1}a_{\sigma^{-1}}$.

Maintenant, si $z \in L$ on a

$$\begin{array}{rcl} a_\sigma.\varphi(z).a_\sigma^{-1} & = & \left(a_\sigma.\omega^{-1}za_e\right).a_\sigma^{-1} \\ & = & \left(f(\sigma,e)(\omega^{-1})^\sigma z^\sigma a_\sigma\right).a_\sigma^{-1} \\ & = & (z^\sigma a_\sigma).a_\sigma^{-1} \\ & = & (z^\sigma a_\sigma).(\omega f(\sigma^{-1},\sigma))^{-1}a_{\sigma^{-1}} \\ & = & z^\sigma f(\sigma,\sigma^{-1})(\omega^{-1})^\sigma(f(\sigma^{-1},\sigma)^{-1})^\sigma a_e \\ & = & z^\sigma f(\sigma,\sigma^{-1})(f(\sigma,e))^{-1}(f(\sigma^{-1},\sigma)^\sigma)^{-1}a_e \\ & = & z^\sigma f(e,\sigma)^{-1}a_e = \omega^{-1}z^\sigma a_e = \varphi(z^\sigma) \end{array}$$

et donc en identifiant L à son image dans $\mathscr{A}(L/k,f)$ par φ, on constate que l'action de $\sigma \in G$ sur $z \in L$ correspond à l'image de $\varphi(z)$ sous l'action de l'automorphisme intérieur défini par a_σ.

Considérons un élément $\lambda = \sum_{\sigma\in G} x_\sigma a_\sigma$ dans le centre de $\mathscr{A}(L/k,f)$. Pour tout $z \in L$ on a

$$\begin{array}{rcl} 0 & = & \varphi(z).\left(\sum_{\sigma\in G} x_\sigma a_\sigma\right) - \left(\sum_{\sigma\in G} x_\sigma a_\sigma\right).\varphi(z) = \sum_{\sigma\in G}\varphi(z).(x_\sigma a_\sigma) - (x_\sigma a_\sigma).\varphi(z) \\ & = & \sum_{\sigma\in G} zx_\sigma a_\sigma - \varphi(x_\sigma)a_\sigma\varphi(z)a_\sigma^{-1}.a_\sigma = \sum_{\sigma\in G} zx_\sigma a_\sigma - \varphi(x_\sigma).\varphi(z^\sigma).a_\sigma \\ & = & \sum_{\sigma\in G} zx_\sigma a_\sigma - x_\sigma z^\sigma.a_\sigma = \sum_{\sigma\in G}(z-z^\sigma)x_\sigma a_\sigma \end{array}$$

Pour tout $\sigma \neq e$, il existe $z \in L$ tel que $z^\sigma \neq z$. On en déduit donc que $x_\sigma = 0$ et par suite que $\lambda = x_e a_e$ (les éléments du centre sont donc dans L). Pour tout $\sigma \in G$ on a

$$(\omega x_e)a_\sigma = f(e,\sigma)x_e a_\sigma = (x_e a_e).a_\sigma = a_\sigma.(x_e a_e) = f(\sigma,e)x_e^\sigma a_\sigma = (\omega x_e)^\sigma a_\sigma$$

et donc $\omega x_e = (\omega x_e)^\sigma$. Ainsi, $\omega x_e \in k$ et par suite $\lambda = \varphi(\omega x_e) \in \varphi(k)$. Le centre de $\mathscr{A}(L/k,f)$ est bien k (après identification par φ).

Venons-en à la simplicité de $\mathscr{A}(L/k,f)$: considérons un idéal bilatère $J \neq (0)$ et considérons un élément $\lambda = \sum_{\sigma\in G} x_\sigma a_\sigma \neq 0$ de J possédant un nombre minimal de coefficients $x_\sigma \neq 0$. Ecrivons pour simplifier $\lambda = \sum_{i=1}^{k} x_{\sigma_i} a_{\sigma_i}$ avec les σ_i dans G distincts deux à deux et les x_{σ_i} tous non nul. Supposons que $k > 1$. Comme $\sigma_1 \neq \sigma_2$ il existe $z \in L$ tel que $z^{\sigma_1} \neq z^{\sigma_2}$, on a alors

$$\sum_{i=1}^{k}(z^{\sigma_i} - z^{\sigma_1})x_{\sigma_i}a_{\sigma_i} = \left(\sum_{i=1}^{k} x_{\sigma_i}a_{\sigma_i}\right).z - z^{\sigma_1}.\left(\sum_{i=1}^{k} x_{\sigma_i}a_{\sigma_i}\right) = \lambda.z - z^{\sigma_1}.\lambda \in J$$

(on a identifié z à $\varphi(z)$). Comme $z^{\sigma_i} - z^{\sigma_1} \neq 0$ la somme est non nulle et elle compte au plus $k-1$ coefficients non nulle, ce qui est contraire au hypothèdes. Ainsi $k = 1$ et il existe un élément non nul dans J de la forme $x_\sigma a_\sigma$. On en déduit que $a_\sigma \in J$, mais comme a_σ est inversible, on trouve finalement que $J = \mathscr{A}(L/k, f)$. L'algèbre $\mathscr{A}(L/k, f)$ est simple.

Pour finir, puisque $\mathscr{A}(L/k, f)$ est une k-algèbre simple centrale, $\varphi(L)$ est bien une sous-algèbre commutative maximale puisque $[A : k] = [L : k]^2$ (corollaire 50).

Exemples 80.— 1/ Pour une extension galoisienne L/k de degré n et de groupe de Galois G, on considère le système de facteurs trivial f (i.e. pour tout $\sigma, \tau \in G$, $f(\sigma, \tau) = 1$).

Pour $\lambda = \sum_{\sigma \in G} x_\sigma a_\sigma \in \mathscr{A}(L/k, f)$, on considère l'application

$$\begin{array}{rccc} u_\lambda : & L & \longrightarrow & L \\ & z & \longmapsto & \displaystyle\sum_{\sigma \in G} z^\sigma x_\sigma \end{array}$$

qui visiblement un élément de $\mathscr{L}_k(L)$. On peut donc définir une application

$$\begin{array}{rccc} \Theta : & \mathscr{A}(L/k, f) & \longrightarrow & \mathscr{L}_k(L) \\ & \lambda & \longmapsto & u_\lambda \end{array}$$

Il est clair que Θ est une application k-linéaire et, si l'on prend deux éléments $\lambda = \sum_{\sigma \in G} x_\sigma a_\sigma$ et $\mu = \sum_{\tau \in G} x_\tau a_\tau$ dans $\mathscr{A}(L/k, f)$, on a

$$\begin{aligned} \lambda.\mu &= \sum_{\sigma, \tau \in G} x_\sigma x_\tau^\sigma a_{\sigma\tau} \\ \forall z \in L,\ u_\lambda \circ u_\mu(z) &= \sum_{\sigma \in G} \left(\sum_{\tau \in G} z^\tau x_\tau \right)^\sigma x_\sigma = \sum_{\sigma, \tau \in G} z^{\sigma\tau} x_\sigma x_\tau^\sigma \end{aligned}$$

On a donc $\Theta(\lambda.\mu) = \Theta(\lambda) \circ \Theta(\mu)$, et ainsi Θ est un morphisme non trivial de k-algèbres de $\mathscr{A}(L/k, f)$ vers $\mathscr{L}_k(L)$. Comme $\mathscr{A}(L/k, f)$ est simple, Θ est injective et comme les dimensions de $\mathscr{A}(L/k, f)$ et $\mathscr{L}_k(L) \simeq \mathscr{M}_n(k)$ sur k coincident, on en déduit qu'elles sont isomorphes en tant que k-algèbres.

Ainsi, dans le cas du système de facteurs trivial, on a $\mathscr{A}(L/k, f) \simeq \mathscr{M}_n(k)$.

2/ On considère l'extension $\mathbb{C}/\mathbb{R}$, on note c la conjugaison complexe (de sorte que $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{Id, c\}$). On considère le système de facteurs f suivant :

	Id	c
Id	1	1
c	1	-1

L'algèbre $A = \mathscr{A}(\mathbb{C}/\mathbb{R}, f)$ a donc comme multiplication explicite :

$$(xa_{Id} + ya_c).(ua_{Id} + va_c) = (xu - y\overline{v})a_{Id} + (xv + y\overline{u})a_c$$

ce qui prouve, d'après la définition que l'on en a donné dans l'exemple 60-2, que A est isomorphe au corps $\mathbb{H}$ des quaternions d'Hamilton.

La notion de produit croisé décrit en fait complétement les algèbres satisfaisant aux hypothèses du théorème 79. On a en effet la réciproque suivante :

Proposition 81.— *Soit A une k-algèbre simple centrale admettant un corps L comme sous-algèbre commutative maximale tel que L/k soit galoisienne. Il existe alors un système de facteurs f tel que $A \simeq \mathscr{A}(L/k, f)$.*

Preuve : Nous noterons G le groupe de Galois de L/k et pour $\sigma \in G$ et $x \in L$, $x^\sigma = \sigma(x)$ l'action à gauche de σ sur x.

Comme L est une sous-algèbre simple de A, si σ est un élément de G, alors d'après le théorème de Skolem-Nœther (théorème 53) il existe un élément $a_\sigma \in A$ inversible tel que pour tout $x \in L$, $x^\sigma = a_\sigma x a_\sigma^{-1}$. On suppose maintenant s'être donné pour tout $\sigma \in G$ un élément a_σ satisfaisant la condition précédente. Si σ, τ sont des éléments de G, on a

$$a_{\sigma\tau} x a_{\sigma\tau}^{-1} = x^{\sigma\tau} = (x^\tau)^\sigma = a_\sigma a_\tau x a_\sigma^{-1} a_\tau^{-1} = (a_\sigma a_\tau) x (a_\sigma a_\tau)^{-1}$$

on en déduit que l'élément $(a_\sigma a_\tau)a_{\sigma\tau}^{-1}$ commute avec tous les éléments $x \in L$. Maintenant, comme L est un corps qui est une sous-algèbre commutative maximale de A, il est égal à son commutant. Ainsi, il existe $f(\sigma, \tau) \in L$ tel que

$$a_\sigma a_\tau = f(\sigma, \tau) a_{\sigma\tau}$$

Puisque la multiplication est associative, pour tout $\sigma, \tau, \rho \in G$, on a

$$\begin{array}{rcl} (a_\sigma a_\tau)a_\rho & = & f(\sigma,\tau)a_{\sigma\tau}a_\rho = f(\sigma,\tau)f(\sigma\tau,\rho)a_{\sigma\tau\rho} = \\ a_\sigma(a_\tau a_\rho) & = & a_\sigma f(\tau,\rho)a_{\tau\rho} = a_\sigma f(\tau,\rho)a_\sigma^{-1}a_\sigma a_{\tau\rho} = f(\tau,\rho)^\sigma f(\sigma,\tau\rho)a_{\sigma\tau\rho} \end{array}$$

Ainsi on a

$$f(\tau,\rho)^\sigma f(\sigma,\tau\rho) = f(\sigma,\tau)f(\sigma\tau,\rho)$$

et donc f est un système de facteurs.

Montrons maintenant que la famille $\{a_\sigma\}_{\sigma\in G}$ est une famille libre de A considéré comme L-espace vectoriel à gauche (structure induite par la multiplication). A cet effet, considérons une équation de dépendance linéaire non triviale $\sum_\sigma x_\sigma a_\sigma = 0$ et supposons l'avoir choisie pour qu'elle possède le moins possible de coefficients non nuls. Il est clair qu'au moins deux coefficients $x_{\sigma_1}, x_{\sigma_2}$ sont non nuls. Considérons un élément $z \in L$ tel que $z^{\sigma_1} \neq z^{\sigma_2}$ et posons $\omega = f(e,e)$, on a alors

$$0 = (\omega z)^{\sigma_1}\left(\sum_\sigma x_\sigma a_\sigma\right) = \sum_\sigma (\omega z^{\sigma_1}) x_\sigma a_\sigma$$

et

$$0 = \left(\sum_\sigma x_\sigma a_\sigma\right) z = \sum_\sigma x_\sigma a_\sigma z = \sum_\sigma f(\sigma, e) z^\sigma x_\sigma a_\sigma$$

On sait que ??? pour tout $\sigma \in G$, on a $f(\sigma, e) = \omega^\sigma$. Ainsi, en soustrayant,

$$\sum_\sigma ((\omega z)^{\sigma_1} - (\omega z)^\sigma) x_\sigma a_\sigma = 0$$

Cette équation de dépendance linéaire est non triviale (car le coefficient de a_{σ_2} est non nul) et elle possède au moins un coefficient nul de plus que celle dont on est partie (celui de a_{σ_1}). Ceci étant absurde, on en déduit bien que la famille est libre.

Maintenant, comme L est commutative maximale on a, d'après le corollaire 50, $[A : L] = [L : k] = o(G)$. Ainsi, la famille $\{a_\sigma\}_{\sigma \in G}$ est une L-base de A. Ainsi, le produit de A est entièrement défini par la formule

$$\left(\sum_\sigma x_\sigma a_\sigma\right)\left(\sum_\sigma y_\tau a_\tau\right) = \sum_{\sigma,\tau} x_\sigma y_\tau^\sigma f(\sigma, \tau) a_{\sigma\tau}$$

Ceci assure bien que $A \simeq \mathscr{A}(L/k, f)$.

Pour finir, intéressons-nous aux classes d'isomorphismes de produits croisés.

Proposition 82.— *Soit L/k une extension galoisienne finie et f_1, f_2 deux systèmes de facteurs. Les propositions suivantes*

i) $\mathscr{A}(L/k, f_1) \simeq \mathscr{A}(L/k, f_2)$,

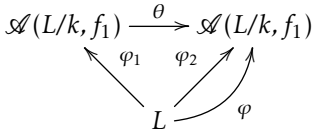
ii) f_1 et f_2 diffèrent d'un 2-cobord,

sont équivalentes.

Preuve : Considérons les algèbres $\mathscr{A}(L/k, f_1)$ et $\mathscr{A}(L/k, f_2)$ comme L-espaces vectoriels gauches rapportés à une même base $\{a_\sigma\}_{\sigma \in G}$ et notons $*_1$ et $*_2$ les multiplications respectives de $\mathscr{A}(L/k, f_1)$ et $\mathscr{A}(L/k, f_2)$.

$i) \Rightarrow ii)$: Nous reprenons les notations et propriétés établies dans le théorème 79 et sa preuve.

Notons φ_1 et φ_2 les plongements de L dans $\mathscr{A}(L/k, f_1)$ et $\mathscr{A}(L/k, f_2)$. Soit $\theta : \mathscr{A}(L/k, f_1) \longrightarrow \mathscr{A}(L/k, f_2)$ un isomorphisme d'algèbre. Posons $\varphi = \theta \circ \varphi_1 : L \longrightarrow \mathscr{A}(L/k, f_2)$, on a donc le diagramme (non commutatif) suivant :



Comme $\varphi(L)$ et $\varphi_1(L)$ sont isomorphes (à L) dans $\mathscr{A}(L/k, f_2)$, d'après le théorème de Skolem-Noether, il existe $a \in \mathscr{A}(L/k, f_2)$ tel que pour tout $x \in L$,

$$\varphi(x) = a *_2 \varphi_2(x) *_2 a^{-1}$$

Par ailleurs, dans la preuve du théorème 79 nous avons établi que pour tout $\sigma \in G$ et tout $x \in L$,

$$\left\{ \begin{array}{lcl} \varphi_1(x^\sigma) & = & a_\sigma *_1 \varphi_1(x) *_1 a_\sigma^{-1} \\ \varphi_2(x^\sigma) & = & a_\sigma *_2 \varphi_2(x) *_2 a_\sigma^{-1} \end{array} \right.$$

On a, par ailleurs,

$$\begin{array}{rcl} a *_2 a_\sigma *_2 \varphi_2(x) *_2 a_\sigma^{-1} *_2 a^{-1} & = & a *_2 \varphi_2(x^\sigma) *_2 a^{-1} \\ & = & \varphi(x^\sigma) = \theta \circ \varphi_1(x^\sigma) \\ & = & \theta(a_\sigma) *_2 \theta \circ \varphi_1(x) *_2 \theta(a_\sigma)^{-1} \\ & = & \theta(a_\sigma) *_2 \varphi(x) *_2 \theta(a_\sigma)^{-1} \\ & = & \theta(a_\sigma) *_2 a *_2 \varphi_2(x) *_2 a^{-1} *_2 \theta(a_\sigma)^{-1} \end{array}$$

Ainsi, pour tout $x \in L$, on a

$$(a_\sigma^{-1} *_2 a^{-1} *_2 \theta(a_\sigma) *_2 a) *_2 \varphi_2(x) *_2 (a_\sigma^{-1} *_2 a^{-1} *_2 \theta(a_\sigma) *_2 a)^{-1} = \varphi_2(x)$$

et donc $(a_\sigma^{-1} *_2 a^{-1} *_2 \theta(a_\sigma) *_2 a)$ est un élément du commutant de $\varphi_2(L)$, mais comme ce corps est une sous-algèbre maximale, il est égal à son propre commutant. Il existe donc $g(\sigma) \in L$ tel que

$$a^{-1} *_2 \theta(a_\sigma) *_2 a = a_\sigma *_2 \varphi_2(g(\sigma))$$

Considérons $\sigma, \tau \in G$, on a

$$\begin{array}{rcl} \theta(a_\sigma *_1 a_\tau) & = & \theta(\varphi_1(f_1(\sigma,\tau)) *_1 a_{\sigma\tau}) \\ & = & \varphi(f_1(\sigma,\tau)) *_2 a *_2 a_{\sigma\tau} *_2 \varphi_2(g(\sigma\tau)) *_2 a^{-1} \\ & = & a *_2 \varphi_2(f_1(\sigma,\tau)) *_2 a_{\sigma\tau} *_2 \varphi_2(g(\sigma\tau)) *_2 a^{-1} \\ & = & a *_2 \varphi_2(f_1(\sigma,\tau) g(\sigma\tau)^{\sigma\tau}) *_2 a_{\sigma\tau} *_2 a^{-1} \\ \theta(a_\sigma) *_2 \theta(a_\tau) & = & a *_2 a_\sigma *_2 \varphi_2(g(\sigma)) *_2 a_\tau *_2 \varphi_2(g(\tau)) *_2 a^{-1} \\ & = & a *_2 a_\sigma *_2 \varphi_2(g(\sigma)) *_2 a_\tau *_2 \varphi_2(g(\tau)) *_2 a^{-1} \\ & = & a *_2 \varphi_2(g(\sigma)^\sigma) *_2 a_\sigma *_2 a_\tau *_2 \varphi_2(g(\tau)) *_2 a^{-1} \\ & = & a *_2 \varphi_2(g(\sigma)^\sigma) *_2 \varphi_2(f_2(\sigma,\tau)) *_2 a_{\sigma\tau} *_2 \varphi_2(g(\tau)) *_2 a^{-1} \\ & = & a *_2 \varphi_2(g(\sigma)^\sigma) *_2 \varphi_2(f_2(\sigma,\tau)) *_2 \varphi_2(g(\tau)^{\sigma\tau}) *_2 a_{\sigma\tau} *_2 a^{-1} \\ & = & a *_2 \varphi_2(g(\sigma)^\sigma f_2(\sigma,\tau) g(\tau)^{\sigma\tau}) *_2 a_{\sigma\tau} *_2 a^{-1} \end{array}$$

On en déduit que

$$f_1(\sigma,\tau) g(\sigma\tau)^{\sigma\tau} = g(\sigma)^\sigma f_2(\sigma,\tau) g(\tau)^{\sigma\tau}$$

et ainsi les 2-cocycles f_1 et f_2 diffèrent du 2-cobord défini par l'application $h(\sigma) = g(\sigma)^\sigma$.

$ii) \Rightarrow i)$: soit $h : G \longrightarrow L^*$ une application telle que pour tout $\sigma, \tau \in G$, on ait

$$f_1(\sigma,\tau)h(\sigma\tau) = f_2(\sigma,\tau)h(\tau)^\sigma h(\sigma)$$

Considérons l'application L-linéaire $\theta : \mathscr{A}(L/k, f_1) \longrightarrow \mathscr{A}(L/k, f_2)$ définie pour tout $\sigma \in G$, par

$$f(a_\sigma) = h(\sigma)a_\sigma$$

Pour tout $\sigma, \tau \in G$ et tout $x_\sigma, y_\tau \in L$, on a

$$\begin{array}{rcl} \theta(x_\sigma a_\sigma *_1 y_\tau a_\tau) & = & f_1(\sigma,\tau)h(\sigma\tau)x_\sigma y_\tau^\sigma a_{\sigma\tau} \\ & = & f_2(\sigma,\tau)h(\tau)^\sigma h(\sigma)x_\sigma y_\tau^\sigma a_{\sigma\tau} \\ & = & f_2(\sigma,\tau)x_\sigma h(\sigma)(y_\tau h(\tau))^\sigma a_{\sigma\tau} \\ & = & (x_\sigma h(\sigma)a_\sigma) *_2 (y_\tau h(\tau)a_\tau) \\ & = & \theta(x_\sigma a_\sigma) *_2 \theta(y_\tau a_\tau) \end{array}$$

On en déduit que θ est un isomorphisme de k-algèbres.

Plongement explicite d'un produit croisé. Soient L/k une extension galoisienne de groupe $G = \{\sigma_1, \cdots, \sigma_n\}$, f un système de facteurs et $A = \mathscr{A}(L/k, f)$ le produit croisé de L par G relativement au système de facteurs f rapporté à la L-base formelle $\{a_{\sigma_1}, \cdots, a_{\sigma_n}\}$. Puisque L est une sous-algèbre commutative maximale de A, c'est aussi un corps neutralisant. Ainsi, l'algèbre $A \otimes_k L$ est une algèbres de matrices à coefficients dans L. Pour des raisons évidentes de dimension, on a en fait $A \otimes_k L \simeq \mathscr{M}_n(L)$ et, par suite, puisque A se plonge canoniquement dans $A \otimes_k L$, il existe un plongement de A dans $\mathscr{M}_n(L)$ (en tant que k-algèbres). On peut décrire explicitement un tel plongement en considérant l'application

$$\begin{array}{rccl} \Theta : & \mathscr{A}(L/k, f) & \longrightarrow & \mathscr{M}_n(L) \\ & x = \displaystyle\sum_{i=1}^n x_{\sigma_i} a_{\sigma_i} & \longmapsto & M_x = \left(f(\sigma_i, \sigma_i^{-1}\sigma_j) x^{\sigma_i}_{\sigma_i^{-1}\sigma_j} \right)_{i,j} \end{array}$$

L'application Θ est visiblement k-linéaire et injective. Il s'agit donc de montrer que si $x = \displaystyle\sum_{i=1}^n x_{\sigma_i} a_{\sigma_i}$ et $y = \displaystyle\sum_{i=1}^n y_{\sigma_i} a_{\sigma_i}$ sont deux éléments de $\mathscr{A}(L/k, f)$, alors $\Theta(xy) = M_{xy} = M_x M_y = \Theta(x)\Theta(y)$. On a, d'une part

$$xy = \sum_{i=1}^n z_{\sigma_i} a_{\sigma_i} = \sum_{i=1}^n \left(\sum_{k=1}^n x_{\sigma_k} y^{\sigma_k}_{\sigma_k^{-1}\sigma_i} f(\sigma_k, \sigma_k^{-1}\sigma_i) \right) a_{\sigma_i}$$

et donc

$$M_{xy} = \left(\sum_{k=1}^n x^{\sigma_i}_{\sigma_k} y^{\sigma_i\sigma_k}_{\sigma_k^{-1}\sigma_i^{-1}\sigma_j} f(\sigma_k, \sigma_k^{-1}\sigma_i^{-1}\sigma_j)^{\sigma_i} f(\sigma_i, \sigma_i^{-1}\sigma_j) \right)_{i,j}$$

et d'autre part

$$\begin{aligned} M_x M_y &= \left(f(\sigma_i, \sigma_i^{-1}\sigma_j) x^{\sigma_i}_{\sigma_i^{-1}\sigma_j} \right)_{i,j} \left(f(\sigma_i, \sigma_i^{-1}\sigma_j) y^{\sigma_i}_{\sigma_i^{-1}\sigma_j} \right)_{i,j} \\ &= \left(\sum_{h=1}^{n} f(\sigma_i, \sigma_i^{-1}\sigma_h) x^{\sigma_i}_{\sigma_i^{-1}\sigma_h} f(\sigma_h, \sigma_h^{-1}\sigma_j) y^{\sigma_h}_{\sigma_h^{-1}\sigma_j} \right)_{i,j} \end{aligned}$$

Fixons le couple d'indice (i,j) et effectuons le changement d'indice $\sigma_k = \sigma_i^{-1}\sigma_h$, on a alors, en utilisant la relation de cocyclicité

$$\begin{aligned} & \sum_{h=1}^{n} f(\sigma_i, \sigma_i^{-1}\sigma_h) x^{\sigma_i}_{\sigma_i^{-1}\sigma_h} f(\sigma_h, \sigma_h^{-1}\sigma_j) y^{\sigma_h}_{\sigma_h^{-1}\sigma_j} \\ = & \sum_{k=1}^{n} f(\sigma_i\sigma_k, \sigma_k^{-1}\sigma_i^{-1}\sigma_j) f(\sigma_i, \sigma_k) x^{\sigma_i}_{\sigma_k} y^{\sigma_i\sigma_k}_{\sigma_k^{-1}\sigma_i^{-1}\sigma_j} \\ = & \sum_{k=1}^{n} f(\sigma_k, \sigma_k^{-1}\sigma_i^{-1}\sigma_j)^{\sigma_i} f(\sigma_i, \sigma_i^{-1}\sigma_j) x^{\sigma_i}_{\sigma_k} y^{\sigma_i\sigma_k}_{\sigma_k^{-1}\sigma_i^{-1}\sigma_j} \end{aligned}$$

ce qui achève la vérification.

En prenant en particulier $k = \mathbb{R}$, $L = \mathbb{C}$ ($G = \{Id, c\}$ où c désigne la conjugaison complexe) et le système de facteurs $f(Id,Id) = f(Id,c) = f(c,Id) = 1$ et $f(c,c) = -1$, alors le corps des quaternions d'Hamilton $\mathbb{H} \simeq \mathscr{A}(\mathbb{C}/\mathbb{R}, f)$ s'identifie à la sous-algèbre de $\mathscr{M}_2(\mathbb{C})$ constituée des matrices de la forme

$$\begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix}$$

où u et v parcourent $\mathbb{C}$.

Le plongement Θ permet alors de définir un isomorphisme explicite entre $\mathscr{A}(L/k, f) \otimes_k L$ et $\mathscr{M}_n(L)$. En effet, on considère le plongement $\Pi : L \longrightarrow \mathscr{M}_n(L)$ défini par $\Pi(\lambda) = \lambda I_n$ et l'on voit que les éléments de $\Pi(L)$ commutent avec ceux de $\Theta(\mathscr{A}(L/k, f))$, si bien que, d'après la proposition 30, les morphismes Θ et Π définissent un morphisme de k-algèbres entre $\mathscr{A}(L/k, f) \otimes_k L$ et $\mathscr{M}_n(L)$. Ce morphisme est visiblement non nul, et comme $\mathscr{A}(L/k, f) \otimes_k L$ est une k-algèbre simple (théorème 34), il est injectif. Pour des raisons de dimensions, c'est finalement un k-isomorphisme d'algèbres.

En conclusion, on voit que la norme réduite se calcule explicitement par la formule

$$\mathrm{Nrd}_{\mathscr{A}(L/k,f)/k}\left(\sum_{i=1}^{n} x_{\sigma_i} a_{\sigma_i} \right) = \det\left(f(\sigma_i, \sigma_i^{-1}\sigma_j) x^{\sigma_i}_{\sigma_i^{-1}\sigma_j} \right)_{i,j}$$

Construction explicite de corps gauches. L'idée générale, pour cette application, est la suivante : on se donne une extension galoisienne L/k de degré

un nombre premier p dont on connait explicitement l'arithmétique et on considère un système de facteurs de $G = \mathrm{Gal}(L/k)$ à valeurs dans L^*. Le produit croisé $A = \mathscr{A}(L/k, f)$ est alors explicite. On sait qu'il existe un corps K de centre k et un entier n tels que $A \simeq \mathscr{M}_n(K)$. Si l'on note $[K : k] = r^2$, on a alors $[A : k] = [L : k]^2 = p^2 = n^2 r^2$ et comme p est premier on en déduit que $n = 1$ ou p. Si $n = 1$, l'algèbre A est donc un corps, sinon $n = p$ et $r = 1$ c'est-à-dire que $A \simeq \mathscr{M}_n(k)$ est un représentant de la classe neutre de $\mathrm{Br}(k)$.

En résumé, si l'on dispose d'une extension galoisienne L/k de degré premier et d'un système de facteurs f qui n'est pas un cobord, alors le produit croisé $A = \mathscr{A}(L/k, f)$ est un corps gauche de dimension p^2 sur son centre k.

On se place ici dans le cas où $p = 3$ et donc L/k est une extension cyclique de groupe $G = \mathrm{Gal}(L/k) = \{Id, c, c^2\}$. Un 2-cobord de G à valeurs dans L^* est une application $f : G \times G \longrightarrow L^*$ telle qu'il existe une application $g : G \longrightarrow L^*$ vérifiant pour tout $\sigma, \tau \in G$, $f(\sigma, \tau) = g(\sigma)^\tau g(\tau) g^{-1}(\sigma\tau)$. Ainsi, f est un 2-cobord si et seulement si il existe $u, v, w \in L^*$ tel que f soit de la forme

	Id	c	c^2
Id	u	u^c	u^{c^2}
c	u	$vv^c w^{-1}$	$u^{-1} v^{c^2} w$
c^2	u	$u^{-1} v w^c$	$v^{-1} w w^{c^2}$

On en déduit que si f est un 2-cobord alors

$$f(c, Id) f(c, c) f(c, c^2) = v v^c v^{c^2} = N_{L/k}(v) \in N_{L/k}(L^*)$$

Maintenant, si $x \in k^*$ alors l'application f_x définie par

	Id	c	c^2
Id	1	1	1
c	1	x	1
c^2	1	1	x^{-1}

est visiblement un 2-cocycle. Ainsi, si $x \notin N_{L/k}(L^*)$ alors f_x n'est pas un 2-cobord et donc $\mathscr{A}(L/k, f_x)$ est un corps.

Intéressons-nous au cas où $k = \mathbb{Q}$ et $L = \mathbb{Q}\left(\cos\left(\frac{2\pi}{9}\right)\right)$. L'extension $L/\mathbb{Q}$ est galoisienne de degré 3 et que $\alpha = 2\cos\left(\frac{2\pi}{9}\right)$ est un élément primitif de cette extension ayant $P(X) = X^3 - 3X + 1$ comme polynôme minimal. Si l'on note N la norme relative à cette extension, un petit calcul très simple montre que pour tout $t = A\alpha^2 + B\alpha + C$, $A, B, C \in \mathbb{Q}$, on a

$$N(A\alpha^2 + B\alpha + C) = A^3 - B^3 + C^3 + 9A^2C + 3A^2B - 3B^2C - 6C^2A + 3ABC$$

Si q désigne un dénominateur commun aux rationnels alors il existe $a, b, c \in \mathbb{Z}$ tels que

$$N(t) = \frac{a^3 - b^3 + c^3 + 9a^2c + 3a^2b - 3b^2c - 6c^2a + 3abc}{q^3}$$

La réduction modulo 2 du numérateur de cette dernière fraction vaut $a-b+c+ac+ab-bc+abc$ mod (2). Si l'on suppose qu'un des trois entiers a, b ou c soit congru à 1 modulo 2 alors ce numérateur est lui-même congru à 1 modulo 2. Ainsi, si a,b et c ne sont pas simultanément pair, alors $a^3-b^3+c^3+9a^2c+3a^2b-3b^2c-6c^2a+3abc$ est impair. Considérons alors $h=\min(v_2(a),v_2(b),v_2(c))$, $r=v_2(q)$ et posons $a^{'}=a/2^h$, $b^{'}=b/2^h$, $c^{'}=c/2^h$, et $q^{'}=q/2^r$. On a

$$N(t)=2^{3(h-r)}\frac{a^{'3}-b^{'3}+c^{'3}+9a^{'2}c^{'}+3a^{'2}b^{'}-3b^{'2}c^{'}-6c^{'2}a^{'}+3a^{'}b^{'}c^{'}}{q^{'3}}$$

Le numérateur de la fraction est impair d'après ce que l'on vient de dire, le dénominateur l'est aussi et donc $v_2(N(t))=3(h-r)$ est un multiple de 3. En conséquence de quoi, si $x\in\mathbb{Q}^*$ est tel que $v_2(x)\notin 3\mathbb{Z}$ (par exemple $x=2$), alors x n'est certainement pas la norme d'un élément de L.

On déduit finalement de tout cela que, pour $x\in\mathbb{Q}^*$ tel que $v_2(x)\notin 3\mathbb{Z}$, l'algèbre $\mathscr{A}\left(\mathbb{Q}\left(\cos\left(\frac{2\pi}{9}\right)\right)/\mathbb{Q},f_x\right)$ est un corps de dimension 9 sur son centre $\mathbb{Q}$.

On peut décrire explicitement son arithmétique : on a $\mathrm{Gal}(L/k)=\{Id,c,c^2\}$ où c est l'automorphisme qui envoie $\cos\left(\frac{2\pi}{9}\right)$ sur $\cos\left(\frac{4\pi}{9}\right)$ (c^2 envoie alors $\cos\left(\frac{2\pi}{9}\right)$ sur $\cos\left(\frac{8\pi}{9}\right)$). Si l'on identifie le groupe additif de $\mathscr{A}\left(\mathbb{Q}\left(\cos\left(\frac{2\pi}{9}\right)\right)/\mathbb{Q},f_x\right)$ à L^3 alors, la multiplication dans $\mathscr{A}\left(\mathbb{Q}\left(\cos\left(\frac{2\pi}{9}\right)\right)/\mathbb{Q},f_x\right)$ s'écrit :

$$(u,v,w).(u^{'},v^{'},w^{'})=\left(uu^{'}+vw^{'c}+ww^{'c^2},uv^{'}+vu^{'c}+x^{-1}ww^{'c^2},uw^{'}+xvv^{'c}+wu^{'c^2}\right)$$

En vertu du paragraphe précédent, ce corps s'identifie à la sous-algèbre de $\mathscr{M}_3\left(\mathbb{Q}\left(\cos\left(\frac{2\pi}{9}\right)\right)\right)$ consituée des matrices de la forme

$$\begin{pmatrix} u & v & w \\ w^c & u^c & xv^c \\ v^{c^2} & x^{-1}w^{c^2} & u^{c^2}\end{pmatrix}$$

où u, v et w parcourent $\mathbb{Q}\left(\cos\left(\frac{2\pi}{9}\right)\right)$. En examinant la première ligne du produit de deux telles matrices, on retrouve bien la multiplication de $\mathscr{A}(\mathbb{Q}(\cos\left(\frac{2\pi}{9}\right))/\mathbb{Q},f_x)$ décrite ci-dessus.

2.2.2 Le point de vue cohomologique

Dans la théorie du produit croisé apparait une donnée cohomologique. Cette dernière peut paraitre anecdotique puisque finalement juste liée à l'associativité du produit dans les algèbres. En fait, le lien entre cohomologie et groupe de Brauer est trés profond, comme nous allons le voir maintenant.

Théorème 83.— *Soit L/k une extension galoisienne finie et $\mathrm{Br}(k) \xrightarrow{\beta_{L/k}} \mathrm{Br}(L)$ l'homomorphisme naturel. Il existe un isomorphisme de groupe*

$$\theta_{L/k} : H^2(L/k) \longrightarrow \ker(\beta_{L/k})$$

induit par la théorie du produit croisé. Ainsi, on a la suite exacte

$$1 \longrightarrow H^2(L/k) \xrightarrow{\theta_{L/k}} \mathrm{Br}(k) \xrightarrow{\beta_{L/k}} \mathrm{Br}(L)$$

Preuve : Soit $\alpha \in H^2(L/k)$ et f un 2-cocycle représentant α. La proposition 82, montre que le produit croisé $\mathscr{A}(L/k, f)$ ne dépend pas (à isomorphisme près) du choix de f dans α. Maintenant, le théorème 79 assure que L est une sous-algèbre maximale de $\mathscr{A}(L/k, f)$, on en déduit (théorème 64) que L est un corps neutralisant de $\mathscr{A}(L/k, f)$. Ainsi, le produit croisé définit bien une application

$$\theta_{L/k} : H^2(L/k) \longrightarrow \ker(\beta_{L/k})$$

Surjectivité de $\theta_{L/k}$. Un élément de $\alpha \in \ker(\beta_{L/k})$ est une classe d'algèbres neutralisée par L. Etant donnée une telle classe, on sait d'après le théorème 64 qu'il existe une algèbre A dans cette classe telle que L soit une sous-algèbre commutative maximale. La proposition 81 assure alors que $A \simeq \mathscr{A}(L/k, f)$ pour un certain 2-cocycle f et donc l'image par $\theta_{L/k}$ de la classe de f est α.

Injectivité de $\theta_{L/k}$. Soit $\alpha_1, \alpha_2 \in H^2(L/k)$ tels que $\theta_{L/k}(\alpha_1) = \theta_{L/k}(\alpha_2)$. Notons f_1 et f_2 des 2-cocycles représentants respectifs de α_1 et α_2. Les algèbres $\mathscr{A}(L/k, f_1)$ et $\mathscr{A}(L/k, f_2)$ sont donc semblables, mais comme elles ont la même dimension sur k on en déduit qu'elles sont isomorphes. La proposition 82 assure alors que f_1 et f_2 diffèrent d'un 2-cobord, c'est-à-dire que $\alpha_1 = \alpha_2$.

Venons en maintenant au fait que $\theta_{L/k}$ est un morphisme : il s'agit de montrer que si f et g sont deux systèmes de facteurs et que si $A = \mathscr{A}(L/k, f)$, $B = \mathscr{A}(L/k, f)$ et $C = \mathscr{A}(L/k, fg)$, alors les algèbres $A \otimes_k B$ et C sont semblables.

Notons $(a_\sigma)_\sigma$ (resp. $(b_\sigma)_\sigma$, resp. $(c_\sigma)_\sigma$) une L-base formelle de A (resp. B, resp. C) sur laquelle le produit croisé est défini comme précédemment. L'algèbre $A \otimes_k B$ est de dimension n^4 sur k et est formée des sommes d'éléments de la forme $x_\sigma a_\sigma \otimes y_\lambda b_\lambda$. Le produit sur $A \otimes_k B$ est alors donné par

$$(x_\sigma a_\sigma \otimes y_\lambda b_\lambda)(x_\tau a_\tau \otimes y_\mu b_\mu) = f(\sigma, \tau) x_\sigma x_\tau^\sigma a_{\sigma\tau} \otimes g(\lambda, \mu) y_\lambda y_\mu^\lambda b_{\lambda\mu}$$

On considère maintenant V le sous-k-espace vectoriel de $A \otimes_k B$ engendré par les éléments

$$s^\sigma x_\sigma a_\sigma \otimes y_\lambda b_\lambda - x_\sigma a_\sigma \otimes s^\lambda y_\lambda b_\lambda$$

(s étant pris dans L). On définit une loi de composition externe à droite de C sur $A \otimes_k B$ en posant :

$$(x_\sigma a_\sigma \otimes y_\lambda b_\lambda).(z_\rho c_\rho) = f(\sigma, \rho) x_\sigma z_\rho^\sigma a_{\sigma\rho} \otimes g(\lambda, \rho) y_\lambda b_{\lambda\rho}$$

On a alors

$$\begin{aligned}(x_\sigma a_\sigma \otimes y_\lambda b_\lambda).[(z_\rho c_\rho)(z_{\rho'} c_{\rho'})] &= (x_\sigma a_\sigma \otimes y_\lambda b_\lambda).(z_\rho z_{\rho'}^{\rho} f(\rho,\rho')g(\rho,\rho')c_{\rho\rho'}) \\ &= f(\rho,\rho')^\sigma f(\sigma,\rho\rho')x_\sigma z_\rho^\sigma z_{\rho'}^{\sigma\rho} g(\rho,\rho')^\sigma a_{\sigma\rho\rho'} \otimes y_\lambda g(\lambda,\rho\rho')b_{\lambda\rho\rho'}\end{aligned}$$

et

$$\begin{aligned}[(x_\sigma a_\sigma \otimes y_\lambda b_\lambda).(z_\rho c_\rho)].(z_{\rho'} c_{\rho'}) &= (f(\sigma,\rho)x_\sigma z_\rho^\sigma a_{\sigma\rho} \otimes g(\lambda,\rho)y_\lambda b_{\lambda\rho}).(z_{\rho'} c_{\rho'}) \\ &= f(\sigma,\rho)f(\sigma\rho,\rho')x_\sigma z_\rho^\sigma z_{\rho'}^{\sigma\rho} a_{\sigma\rho\rho'} \otimes g(\lambda,\rho)g(\lambda\rho,\rho')y_\lambda b_{\lambda\rho\rho'} \\ &= f(\rho,\rho')^\sigma f(\sigma,\rho\rho')x_\sigma z_\rho^\sigma z_{\rho'}^{\sigma\rho} a_{\sigma\rho\rho'} \otimes g(\rho,\rho')^\lambda g(\lambda,\rho\rho')y_\lambda b_{\lambda\rho\rho'}\end{aligned}$$

En posant $s = g(\rho,\rho')^{(\rho\rho')^{-1}}$ et en utilisant la définition de V, on voit alors que

$$(x_\sigma a_\sigma \otimes y_\lambda b_\lambda).[(z_\rho c_\rho)(z_{\rho'} c_{\rho'})] - [(x_\sigma a_\sigma \otimes y_\lambda b_\lambda).(z_\rho c_\rho)].(z_{\rho'} c_{\rho'}) \in V$$

et ainsi, on peut considérer $M = A \otimes_k B/V$ comme un C-module à droite (les détails de cette dernière assertion ne posant pas de problème particulier, ils sont laissés à la discrétion du lecteur).

D'un autre coté, on a

$$\begin{aligned}&(x_\tau a_\tau \otimes y_\mu b_\mu)(s^\sigma x_\sigma a_\sigma \otimes y_\lambda b_\lambda - x_\sigma a_\sigma \otimes s^\lambda y_\lambda b_\lambda) \\ = \;& s^{\tau\sigma} x_\tau f(\tau,\sigma)x_\sigma^\tau a_{\tau\sigma} \otimes y_\mu g(\mu,\lambda)y_\lambda^\mu b_{\mu\lambda} - x_\tau f(\tau,\sigma)x_\sigma^\tau a_{\tau\sigma} \otimes s^{\mu\lambda} y_\mu g(\mu,\lambda)y_\lambda^\mu b_{\mu\lambda} \in V\end{aligned}$$

et donc V est un idéal à gauche de $A \otimes_k B$ si bien que, M a une structure naturelle de $A \otimes_k B$-module à gauche.

Enfin, on a

$$\begin{aligned}&\Big[(x_\sigma a_\sigma \otimes y_\lambda b_\lambda).(x_\tau a_\tau \otimes y_\mu b_\mu)\Big].(z_\rho c_\rho) \\ = \;& (f(\sigma,\tau)x_\sigma x_\tau^\sigma a_{\sigma\tau} \otimes g(\lambda,\mu)y_\lambda y_\mu^\lambda b_{\lambda\mu}).(z_\rho c_\rho) \\ = \;& f(\sigma\tau,\rho)f(\sigma,\rho)x_\sigma x_\tau^\sigma z_\rho^{\sigma\tau} a_{\sigma\tau\rho} \otimes g(\lambda\mu,\rho)g(\lambda,mu)y_\lambda y_\mu^\lambda b_{\lambda\mu\rho} \\ = \;& f(\tau,\rho)^\sigma f(\sigma,\tau\rho)x_\sigma x_\tau^\sigma z_\rho^{\sigma\tau} a_{\sigma\tau\rho} \otimes g(\mu,\rho)^\lambda g(\lambda,\mu\rho)y_\lambda y_\mu^\lambda b_{\lambda\mu\rho} \\ = \;& (x_\sigma a_\sigma \otimes y_\lambda b_\lambda)).(f(\tau,\rho)x_\tau z_\rho^\tau a_{\tau\rho} \otimes g(\mu,\rho)y_\mu b_{\mu\rho}) \\ = \;& (x_\sigma a_\sigma \otimes y_\lambda b_\lambda).\Big[(x_\tau a_\tau \otimes y_\mu b_\mu).(z_\rho c_\rho)\Big]\end{aligned}$$

et donc les actions considérées commutent entre elles, de sorte que M a une structure de $A \otimes_k B$-C-bimodule. On peut donc regarder M comme un $(A \otimes_k B) \otimes_k C^{\mathrm{op}}$-module à gauche et, l'algèbre $(A \otimes_k B) \otimes_k C^{\mathrm{op}}$ étant simple, le morphisme $(A \otimes_k B) \otimes_k C^{\mathrm{op}} \longrightarrow \mathscr{L}_k(M)$ est injectif.

On a, d'une part $[(A \otimes_k B) \otimes_k C^{\mathrm{op}} : k] = [A : k][B : k][C : k] = n^6$, et d'autre part $[\mathscr{L}_k(M) : k] = [M : k]^2$. Ainsi, si l'on prouve que $[M : k] = n^3$, alors $(A \otimes_k B) \otimes_k C^{\mathrm{op}}$ sera isomorphe à $\mathscr{L}_k(M) \simeq \mathscr{M}_{n^3}(k)$ et donc, dans le groupe de Brauer de k, on aura $[(A \otimes_k B) \otimes_k C^{\mathrm{op}}] = [A \otimes_k B] - [C] = [\mathscr{M}_{n^3}(k)] = 0$. Ainsi, on aura $[A \otimes_k B] = [C]$ dans $\mathrm{Br}(k)$ et donc les algèbres $A \otimes_k B$ et C seront semblables.

Examinons donc la dimension de M sur k. Soit $\{\varepsilon_1, \cdots, \varepsilon_n\}$ une k-base normale de L. La famille $\{\varepsilon_i a_\sigma \otimes \varepsilon_j b_\lambda\}_{i,j,\sigma,\lambda}$ est alors une k-base de $A \otimes_k B$, mais comme les éléments $\varepsilon_i a_\sigma \otimes b_\lambda$ et $a_\sigma \otimes \varepsilon_j b_\lambda$ où $\varepsilon_j = \varepsilon_i^{\lambda\sigma^{-1}}$ sont congrus modulo V, on en déduit que l'image dans M de la famille $\{a_\sigma \otimes \varepsilon_j b_\lambda\}_{j,\sigma,\lambda}$ est une famille génératrice de M.

Pour un couple $(\sigma, \lambda) \in G^2$ on considère la k-application linéaire $g_{\sigma,\lambda} : A \otimes_k B \longrightarrow L$ définie sur la base $\{\varepsilon_i a_\tau \otimes \varepsilon_j b_\mu\}_{i,j,\tau,\mu}$ par

$$g_{\sigma,\lambda}(\varepsilon_i a_\tau \otimes \varepsilon_j b_\mu) = \delta_{(\sigma,\lambda),(\tau,\mu)} \varepsilon_i^{\lambda\sigma^{-1}} \varepsilon_j$$

où $\delta_{(\sigma,\lambda),(\tau,\mu)}$ désigne le symbôle de Kronecker. Si $x, y \in L$, on a alors $g_{\sigma,\lambda}(x a_\tau \otimes y b_\mu) = \delta_{(\sigma,\lambda),(\tau,\mu)} x^{\lambda\sigma^{-1}} y$.

On considère une somme $S = \sum_{\sigma,\lambda} a_\sigma \otimes \alpha_{\sigma,\lambda} b_\lambda$. Si pour un couple donné $(\sigma, \lambda) \in G^2$ on a $\alpha_{\sigma,\lambda} \neq 0$, alors $g_{\sigma,\lambda}(S) = \alpha_{\sigma,\lambda} \neq 0$.

Maintenant, de part le définition de V, on voit que les applications $g_{\sigma,\lambda}$ sont toutes nulles sur V. En conclusion, si $\sum_{\sigma,\lambda} a_\sigma \otimes \alpha_{\sigma,\lambda} b_\lambda$ est une somme non triviale, elle ne peut appartenir à V. Ceci prouve en particulier que l'image de la famille $\{a_\sigma \otimes \varepsilon_j b_\lambda\}_{j,\sigma,\lambda}$ est une famille libre de M, et donc une k-base de M. Puisque cette famille contient n^3 éléments, on obtient bien finalement que $[M : k] = n^3$.

———

Considérons une extension galoisienne finie L/k de groupe G et un corps intermédiaire L_0. Notons H le groupe de Galois de L/L_0. Considérons un système de facteurs $f : G \times G \longrightarrow L^*$ et le produit croisé $A = \mathscr{A}(L/k, f)$ rapporté à une base $\{a_\sigma\}_{\sigma \in G}$. Dans A considérons l'ensemble

$$B = \left\{ \sum_{\sigma \in H} x_\sigma a_\sigma / \; x_\sigma \in L \text{ pour tout } \sigma \in H \right\}$$

C'est visiblement une sous-algèbre de A, c'est-même l'algèbre $\mathscr{A}(L/L_0, \mathrm{res}(f))$ (rapportée à la base $\{a_\sigma\}_{\sigma \in H}$) où $\mathrm{res}(f)$ désigne la restriction de f à H. Ainsi, B est une L_0-algèbre simple centrale.

Théorème 84.— *Sous les hypothèses précédentes, la L_0-algèbre simple centrale B est semblable à $A \otimes_k L_0$.*

Preuve : L'algèbre B étant une sous-algèbre de A, on peut donc conférer à A une structure de B^{op}-module à droite en considérant la multiplication à gauche : pour $x \in A$ et $y \in B$, $x *_1 y = yx$. On ainsi un monomorphisme de B^{op} dans $\mathscr{L}_{L_0}(A)$. De même, on définit sur A une structure de $A \otimes_k L_0$-module à droite en posant, pour $x_\sigma a_\sigma \in A$, $\lambda \in L_0$ et $y_\tau a_\tau \in A$,

$$y_\tau a_\tau *_2 (x_\sigma a_\sigma \otimes \lambda) *_2 = y_\tau x_\sigma^\tau f(\tau, \sigma) \lambda a_{\tau\sigma}$$

La loi externe $*_2$ confère bien une structure de module à droite puisque

$$\begin{aligned}(z_\rho a_\rho)*_2((y_\tau a_\tau\otimes\mu)(x_\sigma a_\sigma\otimes\lambda)) &= (z_\rho a_\rho)*_2(y_\tau x_\sigma^\tau f(\tau,\sigma)a_{\tau\sigma}\otimes\mu\lambda)\\ &= z_\rho y_\tau^\rho x_\sigma^{\rho\tau} f(\tau,\sigma)^\rho f(\rho,\tau\sigma)\mu\lambda a_{\rho\tau\sigma}\\ &= z_\rho y_\tau^\rho x_\sigma^{\rho\tau} f(\rho,\tau)f(\rho\tau,\sigma)\mu\lambda a_{\rho\tau\sigma}\\ &= (z_\rho y_\tau^\rho f(\rho,\tau)\mu a_{\rho\tau})*_2(x_\sigma a_\sigma\otimes\lambda)\\ &= \Big((z_\rho a_\rho)*_2(y_\tau a_\tau\otimes\mu)\Big)*_2(x_\sigma a_\sigma\otimes\lambda)\end{aligned}$$

Ainsi, on dispose d'un monomorphisme de $A\otimes_k L_0$ dans $\mathscr{L}_{L_0}(A)$. Maintenant, pour $x_\sigma a_\sigma\in A$, $\lambda\in L_0$, $y_\tau a_\tau\in B$ ($\tau\in H$ et donc $\lambda^\tau=\lambda$) et $z_\rho a_\rho\in A$, on a

$$\begin{aligned}\Big((z_\rho a_\rho)*_1(y_\tau a_\tau)\Big)*_2(x_\sigma a_\sigma\otimes\lambda) &= \Big(y_\tau a_\tau.z_\rho a_\rho\Big)*_2(x_\sigma a_\sigma\otimes\lambda)\\ &= \Big(y_\tau z_\rho^\tau f(\tau,\rho)a_{\tau\rho}\Big)*_2(x_\sigma a_\sigma\otimes\lambda)\\ &= y_\tau z_\rho^\tau x_\sigma^{\tau\rho} f(\tau,\rho)f(\tau\rho,\sigma)\lambda a_{\tau\rho\sigma}\\ &= y_\tau z_\rho^\tau x_\sigma^{\tau\rho} f(\rho,\sigma)^\tau f(\tau,\rho\sigma)\lambda a_{\tau\rho\sigma}\\ &= (y_\tau a_\tau).(z_\rho x_\sigma^\rho f(\rho,\sigma)\lambda a_{\rho\sigma})\\ &= (z_\rho x_\sigma^\rho f(\rho,\sigma)\lambda a_{\rho\sigma})*_1(y_\tau a_\tau)\\ &= \Big((z_\rho a_\rho)*_2(x_\sigma a_\sigma\otimes\lambda)\Big)*_1(y_\tau a_\tau)\end{aligned}$$

les opérations externes $*_1$ et $*_2$ commutent donc et par suite, dans $\mathscr{L}_{L_0}(A)$ il y a deux algèbres isomorphes respectivement à B^{op} et $A\otimes_k L_0$ qui commutent l'une avec l'autre. Nous allons montrer, par des considérations de dimensions, que chacune d'elle est en fait le commutant de l'autre dans $\mathscr{L}_{L_0}(A)$.

On a

$$[A\otimes_k L_0 : L_0] = [A:k] = [L:k]^2 \text{ et } [B:L_0] = [L:L_0]^2$$

par ailleurs, puisque $[L:L_0][L_0:k][L:k] = [L:k]^2 = [A:k] = [A:L_0][L_0:k]$ on en déduit que

$$[A:L_0] = [L:k][L:L_0]$$

et, par suite, que

$$[A\otimes_k L_0 : L_0][B:L_0] = [A:L_0]^2 = \dim_{L_0}\mathscr{L}_{L_0}(A)$$

Ainsi, B^{op} et $A\otimes_k L_0$ sont des L_0-algèbres simple centrales incluses l'une l'autre dans le commutant de l'autre. La dernière égalité de dimension assure alors, d'après le théorème 47, qu'elles sont le commutant l'une de l'autre dans $\mathscr{L}_{L_0}(A)$. La remarque 59 montre alors que les algèbres B^{op} et $A\otimes_k L_0$ appartiennent à des classes opposées dans $\mathrm{Br}(L_0)$, ce qui veut dire que B et $A\otimes_k L_0$ sont dans la même classe de $\mathrm{Br}(L_0)$ et ainsi que ces algèbres sont semblables.

Corollaire 85.— *Sous les hypothèses précédentes, le noyau C de l'homorphisme $\mathrm{Br}(k)\xrightarrow{\beta_{L_0/k}}\mathrm{Br}(L_0)$ est l'image isomorphe par $\theta_{L/k}$ du noyau K de l'homomorphisme de restriction $H^2(L/k)\xrightarrow{\mathrm{res}}H^2(L/L_0)$.*

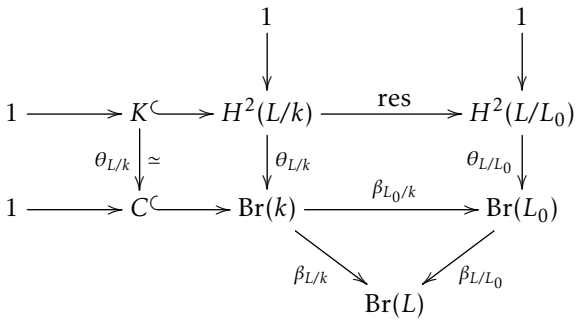
Preuve : On garde les notations précédentes et l'on considère une k-algèbre simple centrale A.

Si $[A] \in \theta_{L/k}(K)$, alors il existe un 2-cocyle f tel que $\mathrm{res}(\widehat{f}) = 0$ et tel que A soit semblable à l'algèbre $\mathscr{A}(L/k, f)$. D'après ce qui précède, les algèbres $A \otimes_k L_0$, $\mathscr{A}(L/k, f) \otimes_k L_0$ et $\mathscr{A}(L/L_0, \mathrm{res}(f))$ sont semblables, mais comme $\mathrm{res}(f) = 0$, on en déduit que $[A \otimes_k L_0] = 0$, c'est-à-dire $[A] \in C$. Ainsi, $\theta_{L/k}(K) \subset C$.

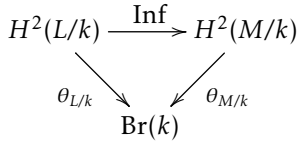
Maintenant, si $[A] \in C$ alors L neutralise A et donc, il existe un 2-cocycle f tel que $[A] = [\mathscr{A}(L/k, f)]$. D'après ce qui précède, les L_0 algèbres $A \otimes_k L_0$, $\mathscr{A}(L/k, f) \otimes_k L_0$ et $\mathscr{A}(L/L_0, \mathrm{res}(f))$ sont semblables. Puisque $[A \otimes_k L_0] = 0$, on a donc $[\mathscr{A}(L/L_0, \mathrm{res}(f))]$ et ainsi, $\theta_{L/L_0}(\mathrm{res}(\widehat{f})) = 0$. Comme θ_{L/L_0} est un isomorphisme, on en déduit finalement que $\mathrm{res}(\widehat{f}) = 0$. Ainsi, $C \subset \theta_{L/k}(K)$, mais comme $\theta_{L/k}$ est un isomorphisme, on en déduit finalement que C est l'image isomorphe par $\theta_{L/k}$ de K.

———

En résumé, on a le diagramme commutatif suivant :



Théorème 86.— *Soit $M/L/k$ une une tour d'extensions galoisiennes finies. Le diagramme suivant*



est commutatif.

Preuve : Considérons les groupes $G = \mathrm{Gal}(M/k)$ et $H = \mathrm{Gal}(M/L)$, le groupe $\mathrm{Gal}(L/k)$ s'identifie alors à G/H. Pour $\sigma \in G$, on note $\overline{\sigma}$ la classe de σ modulo H, qui est donc d'un point de vue arithmétique la restriction de l'automorphisme σ à L.

Considérons un 2-cocycle f de G/H à valeur dans L^*, l'image de $\widehat{f}$ par $\theta_{L/k}$ est la classe de l'algèbre $A = \mathscr{A}(L/k, f)$. Par ailleurs, un 2-cocycle $\widetilde{f}$ de G à valeurs dans M^* représentant l'inflation de la classe $\widehat{f}$ est donné pour $\sigma, \tau \in G$

et $h, h' \in H$, par

$$\widetilde{f}(\sigma h, \tau h') = f(\overline{\sigma}, \overline{\tau})$$

L'image de $\widehat{\widetilde{f}}$ par $\theta_{M/k}$ est la classe de l'algèbre $B = \mathscr{A}(M/k, \widetilde{f})$. Il s'agit donc de montrer que $\mathscr{A}(L/k, f)$ et $\mathscr{A}(M/k, \widetilde{f})$ sont semblables.

On rapporte l'algèbre A à la L-base $\{a_{\overline{\sigma}}\}_{\overline{\sigma} \in G/H}$ et l'algèbre B à la M-base $\{a_\sigma\}_{\sigma \in G}$. Notons que le lien qui lie $\widetilde{f}$ à f permet d'écrire le produit croisé dans B de la manière suivante :

$$\left(\sum_{\sigma \in G} \lambda_\sigma a_\sigma\right)\left(\sum_{\tau \in G} \mu_\tau a_\tau\right) = \sum_{\sigma, \tau \in G} \lambda_\sigma \mu_\tau^\sigma f(\overline{\sigma}, \overline{\tau}) a_{\sigma\tau}$$

On considère le k-espace vectoriel V des sommes formelles $\sum_{\overline{\sigma} \in G/H} \mu_{\overline{\sigma}} a_{\overline{\sigma}}$ où les $\mu_{\overline{\sigma}}$ sont des éléments de M.

On fait agir à droite l'algèbre A sur V : par linéarité il suffit de définir l'action de $\lambda a_{\overline{\tau}} \in A$ sur le monôme $\mu_{\overline{\sigma}} a_{\overline{\sigma}}$. On pose

$$(\mu_{\overline{\sigma}} a_{\overline{\sigma}}).(\lambda a_{\overline{\tau}}) = \mu_{\overline{\sigma}} \lambda^{\overline{\sigma}} f(\overline{\sigma}, \overline{\tau}) a_{\overline{\sigma\tau}}$$

Il s'agit bien d'une action puisque :

$$\begin{aligned}
(\mu_{\overline{\sigma}} a_{\overline{\sigma}}).\Big((\lambda a_{\overline{\tau}})(\nu a_{\overline{\rho}})\Big) &= (\mu_{\overline{\sigma}} a_{\overline{\sigma}}).\Big(\lambda \nu^{\overline{\tau}} f(\overline{\tau}, \overline{\rho}) a_{\overline{\sigma\tau\rho}}\Big) \\
&= \mu_{\overline{\sigma}} \lambda^{\overline{\sigma}} \nu^{\overline{\sigma\tau}} f(\overline{\tau}, \overline{\rho})^{\overline{\sigma}} f(\overline{\sigma}, \overline{\tau\rho}) a_{\overline{\sigma\tau\rho}} \\
&= \mu_{\overline{\sigma}} \lambda^{\overline{\sigma}} \nu^{\overline{\sigma\tau}} f(\overline{\sigma\tau}, \overline{\rho}) f(\overline{\sigma}, \overline{\tau}) a_{\overline{\sigma\tau\rho}} \\
&= \Big(\mu_{\overline{\sigma}} \lambda^{\overline{\sigma}} f(\overline{\sigma}, \overline{\tau}) a_{\overline{\sigma\tau}}\Big).(\nu a_{\overline{\rho}}) \\
&= ((\mu_{\overline{\sigma}} a_{\overline{\sigma}}).(\lambda a_{\overline{\tau}})).(\nu a_{\overline{\rho}})
\end{aligned}$$

On peut aussi faire agir, à gauche cette fois, l'algèbre B sur V en posant

$$(\lambda a_\tau).(\mu_{\overline{\sigma}} a_{\overline{\sigma}}) = \lambda \mu_{\overline{\sigma}}^\tau f(\overline{\tau}, \overline{\sigma}) a_{\overline{\tau\sigma}}$$

Il s'agit bien d'une action puisque :

$$\begin{aligned}
(\nu a_\rho).((\lambda a_\tau).(\mu_{\overline{\sigma}} a_{\overline{\sigma}})) &= (\nu a_\rho).(\lambda \mu_{\overline{\sigma}}^\tau f(\overline{\tau}, \overline{\sigma}) a_{\overline{\tau\sigma}}) \\
&= \nu \lambda^\rho \mu_{\overline{\sigma}}^{\rho\tau} f(\overline{\tau}, \overline{\sigma})^\rho f(\overline{\rho}, \overline{\tau\sigma}) a_{\overline{\rho\tau\sigma}} \\
&= \nu \lambda^\rho \mu_{\overline{\sigma}}^{\rho\tau} f(\overline{\tau}, \overline{\sigma})^{\overline{\rho}} f(\overline{\rho}, \overline{\tau\sigma}) a_{\overline{\rho\tau\sigma}} \\
&= \nu \lambda^\rho \mu_{\overline{\sigma}}^{\rho\tau} f(\overline{\rho\tau}, \overline{\sigma}) f(\overline{\rho}, \overline{\tau}) a_{\overline{\rho\tau\sigma}} \\
&= (\nu \lambda^\rho f(\overline{\rho}, \overline{\tau}) a_{\overline{\rho\tau}}).(\mu_{\overline{\sigma}} a_{\overline{\sigma}}) \\
&= \Big((\nu a_\rho).(\lambda a_\tau)\Big).(\mu_{\overline{\sigma}} a_{\overline{\sigma}})
\end{aligned}$$

Maintenant, pour $\nu a_\rho \in B$, $\lambda a_{\overline{\tau}} \in A$ et $\mu_{\overline{\sigma}} a_{\overline{\sigma}} \in V$, on a

$$\begin{aligned}
(\nu a_\rho).((\mu_{\overline{\sigma}} a_{\overline{\sigma}}).(\lambda a_{\overline{\tau}})) &= (\nu a_\rho).(\mu_{\overline{\sigma}} \lambda^{\overline{\sigma}} f(\overline{\sigma},\overline{\tau}) a_{\overline{\sigma\tau}}) \\
&= \nu \mu^{\rho}_{\overline{\sigma}} \lambda^{\rho\overline{\sigma}} f(\overline{\sigma},\overline{\tau})^{\rho} f(\overline{\rho},\overline{\sigma\tau}) a_{\overline{\rho\sigma\tau}} \\
&= \nu \mu^{\rho}_{\overline{\sigma}} \lambda^{\overline{\rho\sigma}} f(\overline{\sigma},\overline{\tau})^{\overline{\rho}} f(\overline{\rho},\overline{\sigma\tau}) a_{\overline{\rho\sigma\tau}} \\
&= \nu \mu^{\rho}_{\overline{\sigma}} \lambda^{\overline{\rho\sigma}} f(\overline{\rho\sigma},\overline{\tau}) f(\overline{\rho},\overline{\sigma}) a_{\overline{\rho\sigma\tau}} \\
&= \left(\nu \mu^{\rho}_{\overline{\sigma}} f(\overline{\rho},\overline{\sigma}) a_{\overline{\rho\sigma}}\right).(\lambda a_{\overline{\tau}}) \\
&= \left((\nu a_\rho).(\mu_{\overline{\sigma}} a_{\overline{\sigma}})\right).(\lambda a_{\overline{\tau}})
\end{aligned}$$

et donc, par linéarité, pour tout $a \in A$, pour tout $b \in B$ et tout $x \in V$ on a

$$(b.x).a = b.(x.a)$$

Ainsi, V est un B-A-bimodule et l'on peut donc regarder V comme un $B \otimes A^{\mathrm{op}}$-module gauche (remarque 31). Il existe alors un morphisme naturel de $B \otimes A^{\mathrm{op}}$ vers $\mathscr{L}_k(V)$, ce morphisme étant certainement injectif puisque $B \otimes A^{\mathrm{op}}$ est une algèbre simple. Par ailleurs, on a d'une part $[V : k] = [L : k].[M : k]$ et donc $[\mathscr{L}_k(V) : k] = ([L : k].[M : k])^2$, et d'autre part $[A : k] = [L : k]^2$ et $[B : k] = [M : k]^2$. Ainsi, les algèbres $B \otimes A^{\mathrm{op}}$ et $\mathscr{L}_k(V)$ ayant même dimension, sont isomorphes et donc $B \otimes A^{\mathrm{op}}$ est une algèbre de matrices à coefficients dans k. Ceci prouve que $[A^{\mathrm{op}}] = -[B]$ dans $\mathrm{Br}(k)$ et donc que $[A] = [B]$.

———

Corollaire 87.— *Le groupe de Brauer d'un corps k est isomorphe à la limite inductive $\varinjlim H^2(L/k)$ prise sur l'ensemble des extensions galoisiennes finies L/k relativement aux morphismes d'inflations.*

Preuve : La donnée des groupes $H^2(L/k)$ pour L/k galoisienne finie et des morphismes d'inflation définit un système inductif filtrant à droite. Le théorème 86 assure que la donnée des morphismes $\theta_{L/k}$ est compatible avec ce système inductif. Il existe donc un morphisme $\Phi : \varinjlim H^2(L/k) \longrightarrow \mathrm{Br}(k)$ tel que pour toute extension galoisienne finie L/k, le diagramme suivant

$$\begin{array}{ccc}
 & H^2(L/k) & \\
{\scriptstyle \theta_{L/k}}\swarrow & & \searrow{\scriptstyle \varphi_{L/k}} \\
\mathrm{Br}(k) & \xleftarrow[\Phi]{} & \varinjlim H^2(L/k)
\end{array}$$

($\varphi_{L/k}$ désignant le morphisme canonique de $H^2(L/k)$ sur $\varinjlim H^2(L/k)$) soit commutatif. Les morphismes $\theta_{L/k}$ sont injectifs, donc Φ l'est aussi. Par ailleurs, tout élément de $\mathrm{Br}(k)$ étant neutralisé par une extension galoisienne de k (corollaire 69), on en déduit que $\mathrm{Br}(k) = \bigcup_{L/k} \theta_{L/k}(H^2(L/k))$ et donc Φ est aussi surjective.

———

Nous allons voir dans la section suivante que cette limite inductive peut se considérer comme un groupe de cohomologie, mais pour une autre cohomologie : celle des groupes profinis.

Pour ce qui est de la structure du groupe de Brauer à proprement parler, une conséquence importante du théorème 83 est la suivante :

Théorème 88.— *Soient A une k-algèbre simple centrale et L/k une extension séparable neutralisante de A. L'exposant de A,* $\exp(A)$*, divise* $[L:k]$*, en particulier il est fini.*

Preuve : Notons $\widetilde{L}$ la clôture galoisienne de l'extension L/k. Le corollaire 85 montre que $[A]$ est l'image, par $\theta_{\widetilde{L}/k}$, d'un élément du noyau de la restriction $H^2(\widetilde{L}/k) \xrightarrow{\text{res}} H^2(\widetilde{L}/L)$. On sait (???) que tous les éléments de ce noyau sont d'exposant $\dfrac{o(\mathrm{Gal}(\widetilde{L}/k))}{o(\mathrm{Gal}(\widetilde{L}/L))} = \dfrac{[\widetilde{L}:k]}{[\widetilde{L}:L]} = [L:k]$. Ainsi, $[L:k].[A] = 0$ et donc $\exp(A)$ divise $[L:k]$.

———

Corollaire 89.— *Le groupe de Brauer d'un corps est un groupe abélien de torsion.*

Preuve : C'est une conséquence immédiate du théorème précédent et de la proposition 68.

———

Etant donnés un corps k et un nombre premier p, on notera $\mathrm{Br}(k)[p] = \{\alpha \in \mathrm{Br}(k)/\ p\alpha = 0\}$ (resp. $\mathrm{Br}(k)\{p\} = \{\alpha \in \mathrm{Br}(k)/\ \exists i \geq 0,\ p^i\alpha = 0\}$) le sous-groupe de p-torsion (resp. la composante p-primaire) de $\mathrm{Br}(k)$. Une conséquence du corollaire 89 est alors que

$$\mathrm{Br}(k) = \bigoplus_p \mathrm{Br}(k)\{p\}$$

2.3 Quelques propriétés de l'indice.

On établit dans ce paragraphe des résultats plus sophistiqués sur l'indice d'une algèbre.

Théorème 90.— *Soit A une k-algèbre simple centrale. On a*

$$\mathrm{rad}(\mathrm{Ind}(A)) \,\Big|\, \exp(A) \,\Big|\, \mathrm{Ind}(A)$$

où $\mathrm{rad}(d)$ *désigne le radical de l'entier d (i.e. le produit des nombres premiers qui le divisent).*

En particulier, $\mathrm{rad}(\exp(A)) = \mathrm{rad}(\mathrm{Ind}(A))$.

Preuve : Posons $n = \exp(A)$ et d'indice $d = \mathrm{Ind}(A)$ et montrons pour commencer que $n|d$. Soit K le corps représentant $[A]$ et L/k une extension commutative et séparable maximale de k dans K (qui existe d'après la proposition

68). On a $[L : k] = d$ (corollaire 51). On sait, d'après le théorème 64, que L est un corps neutralisant de α. Notons $\widetilde{L}$ la clôture galoisienne de L sur k, il s'agit aussi d'un corps neutralisant de A (proposition 62).

Puisque l'image de $[A]$ dans $\mathrm{Br}(L)$ et dans $\mathrm{Br}(\widetilde{L})$ est nulle, d'après le corollaire 85, on peut affirmer que l'image de $[A]$ dans $H^2(\widetilde{L}/k)$ est en fait dans le noyau du morphisme de restriction $H^2(\widetilde{L}/k) \longrightarrow H^2(\widetilde{L}/L)$. La proposition ??? sur la structure du noyau de la restriction montre alors que n divise $[\mathrm{Gal}(\widetilde{L}/k) : \mathrm{Gal}(\widetilde{L} : L)] = \dfrac{[\widetilde{L}/k]}{[\widetilde{L} : L]} = [L : k] = d$.

Considérons maintenant une extension galoisienne neutralisante de A quelconque L/k, de groupe G. On sait que $[L : k]$ est un multiple de d, d'après le corollaire 65. Soient alors un nombre premier p qui divise d, G_p un p-sous-groupe de Sylow de G et L_p le corps des invariants de L par G_p. Le corps L_p n'est certainement pas une extension neutralisante de A car si c'était le cas, $[L_p : k]$ serait multiple de d, or, par définition, $[L_p : k]$ est premier à p.

Considérons le morphisme naturel $\beta_{L_p/k} : \mathrm{Br}(k) \longrightarrow \mathrm{Br}(L_p)$ et notons n' l'ordre de $\beta_{L_p/k}([A])$. On vient de voir que $n' \neq 1$, mais maintenant comme L est neutralise A, elle neutralise aussi pour $\beta_{L_p/k}([A])$ et donc, comme n' est un diviseur de $\mathrm{Ind}(\beta_{L_p/k}([A]))$ et que cet entier est lui-même un diviseur de $[L : L_p]$, on en déduit que $n' = p^h$ (pour un certain entier $h \geq 1$). Maintenant, comme $\beta_{L_p/k}$ est un morphisme, on a $n'|n$ et, par suite, on a bien $p|n$. En appliquant cette propriété à tous les $p|d$, on trouve finalement que $\mathrm{rad}(d)|n$.

———

Comme conséquences immédiates de ce résulat on a :

Corollaire 91.— *a) Soient A une k-algèbre simple centrale et p un nombre premier. L'exposant de A est une puissance de p si et seulement si son indice l'est aussi.*

b) Soient A et B deux k-algèbres simples centrales. Les entiers $\exp(A)$ *et* $\exp(B)$ *sont premiers entre eux si et seulement si les entiers* $\mathrm{Ind}(A)$ *et* $\mathrm{Ind}(B)$ *le sont aussi.*

On peut alors apporter une précision à la proposition61-d) :

Proposition 92.— *Soient A et B deux k-algèbres simples centrales. Si les entiers* $\mathrm{Ind}(A)$ *et* $\mathrm{Ind}(B)$ *sont premiers entre eux, alors* $\mathrm{Ind}(A \otimes_k B) = \mathrm{Ind}(A).\mathrm{Ind}(B)$.

Preuve : Soit Ω/k une extension commutative finie et $\beta_{\Omega/k} : \mathrm{Br}(k) \longrightarrow \mathrm{Br}(\Omega)$ le morphisme canonique. Comme les groupes de Brauer sont abéliens de torsion, $\beta_{\Omega/k}$ envoie la composante p-primaire $\mathrm{Br}(k)\{p\}$ dans la composante p-primaire $\mathrm{Br}(\Omega)\{p\}$ pour chaque p premier.

Maintenant, puisque $\mathrm{Ind}(A)$ et $\mathrm{Ind}(B)$ sont premiers entre eux et que $\exp(A)$ (resp. $\exp(B)$) divise $\mathrm{Ind}(A)$ (resp. $\mathrm{Ind}(B)$), on en déduit que $(o([A]), o([B])) = 1$. Compte-tenu de la remarque précédente, on trouve finalement que $\beta_{\Omega/k}([A] + [B]) = 0$ si et seulement si $\beta_{\Omega/k}([A]) = \beta_{\Omega/k}([B]) = 0$. En d'autre termes, le corps

Ω neutralise $A \otimes_k B$ si et seulement si Ω neutralise A et B.

En prenant pour Ω un corps neutralisant tel que $[\Omega : k] = \mathrm{Ind}(A \otimes_k B)$, on en déduit que $\mathrm{Ind}(A)|\mathrm{Ind}(A \otimes_k B)$ et $\mathrm{Ind}(B)|\mathrm{Ind}(A \otimes_k B)$, ce qui implique puisque $(\mathrm{Ind}(A), \mathrm{Ind}(B)) = 1$, que $\mathrm{Ind}(A).\mathrm{Ind}(B)|\mathrm{Ind}(A \otimes_k B)$.

Réciproquement, soient L et M des corps neutralisants respectivement A et B et vérifiant $[L : k] = \mathrm{Ind}(A)$ et $[M : k] = \mathrm{Ind}(B)$. Puisque $[L : k]$ et $[M : k]$ sont premiers entre eux, les corps L et M sont donc linéairement disjoints sur k. Ainsi, $L \otimes_k M$ est un corps neutralisant de $A \otimes_k B$ et donc $\mathrm{Ind}(A \otimes_k B)|\mathrm{Ind}(A).\mathrm{Ind}(B)$.

Corollaire 93.— *Soient A et B deux corps de centre k. Si les entiers* $\mathrm{Ind}(A)$ *et* $\mathrm{Ind}(B)$ *sont premiers entre eux, alors $A \otimes_k B$ est un corps.*

Preuve : En utilisant les propositions 92 et 61, on peut écrire

$$\mathrm{Ind}(A \otimes_k B) = \mathrm{Ind}(A).\mathrm{Ind}(B) = \deg(A).\deg(B) = \deg(A \otimes_k B)$$

et, en appliquant à nouveau la proposition 61, on trouve finalement que $A \otimes_k B$ est bien un corps.

Considérons une k-algèbre simple centrale A et notons $\mathrm{Ind}(D) = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ la décomposition en facteur premier de l'entier $\mathrm{Ind}(A)$. Le théorème 90 permet d'affirmer que la décomposition en facteur premier de $\exp(D)$ est de la forme $\exp(D) = p_1^{\beta_1} \cdots p_n^{\beta_n}$ avec $1 \leq \beta_i \leq \alpha_i$ pour tout $i = 1, \cdots, n$.

Puisque $\mathrm{Br}(k) = \bigoplus_p \mathrm{Br}(k)\{p\}$ et que $o([A]) = p_1^{\beta_1} \cdots p_n^{\beta_n}$, on en déduit que $[A] \in \bigoplus_{i=1}^n \mathrm{Br}(k)\{p_i\}$. On en déduit que, pour tout $i = 1, \cdots, n$, il existe une k-algèbre centrale simple A_i telle que $[A_i] \in \mathrm{Br}(k)\{p_i\}$ la donnée de ces algèbres vérifiant $[A] = [A_{p_1}] + \cdots + [A_{p_n}]$. Les algèbres A et $A_1 \otimes_k \cdots \otimes_k A_n$ sont donc semblables. Puisque l'entier $o([A_i])$ est une puissance de p_i, on en déduit que $\exp(A_i) = p_i^{\beta_i}$. Maintenant, $\mathrm{Ind}(A_i)$ est aussi une puissance de p_i (corollaire91-a) et donc, en appliquant la proposition 92, on a

$$\mathrm{Ind}(A) = \prod_{i=1}^{n} \mathrm{Ind}(A_i)$$

et donc $\mathrm{Ind}(A_i) = p^{\alpha_i}$.

Notons qu'à similitude près, les algèbres A_i sont uniques pour la condition $[A_i] \in \mathrm{Br}(k)\{p_i\}$ et $[A] = [A_{p_1}] + \cdots + [A_{p_n}]$. Dans le cas des corps on obtient plus précisément :

Théorème 94.— *Soient D un corps de centre k,*

$$\mathrm{Ind}(D) = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$$

la décomposition en facteur premier de l'entier $\mathrm{Ind}(D)$ *et*

$$\exp(D) = p_1^{\beta_1} \cdots p_n^{\beta_n}$$

la décomposition en facteur premier de l'entier $\exp(D)$.

Il existe une famille de corps $\{D_1, \cdots, D_n\}$ *de centre* k, *chaque* D_i *étant unique à isomorphisme près, telle que*

- *Pour tout* $i = 1, \cdots, n$, $\mathrm{rad}(\mathrm{Ind}(D_i)) = \mathrm{rad}(\exp(D_i)) = p_i$ *(i.e.* $[D_i] \in \mathrm{Br}(k)\{p_i\}$*).*
- $D \simeq D_1 \otimes_k \cdots \otimes_k D_n$.

Sous ces conditions, pour tout $i = 1, \cdots, n$ *on a* $\mathrm{Ind}(D_i) = p_i^{\alpha_i}$ *et* $\exp(D_i) = p_i^{\beta_i}$.

Preuve : En reprenant les notations et en posant $A = D$ et $A_i = D_i$ le corps représentant $[A_i]$, on voit qu'il ne reste que deux choses à démontrer : l'unicité à isomorphisme près de D_i et l'isomorphisme entre D et $D_1 \otimes_k \cdots \otimes_k D_n$. L'unicité de D_i vient du fait qu'il n'y a qu'un seul corps dans $[D_i]$. Pour le second isomorphisme, remarquons qu'en appliquant la proposition 92, on trouve

$$\deg(D) = \mathrm{Ind}(D) = \prod_{i=1}^{n} \mathrm{Ind}(D_i) = \prod_{i=1}^{n} \deg(D_i) = \deg(D_1 \otimes_k \cdots \otimes_k D_n)$$

Ainsi, d'après la proposition61-e, $D \simeq D_1 \otimes_k \cdots \otimes_k D_n$.

En revenant au cas général, on voit que l'on peut choisir les A_i pour que $A \simeq A_1 \otimes_k \cdots \otimes_k A_n$, mais on constate que si A n'est pas un corps, alors les A_i ne sont pas uniques. En effet, écrivons $A \simeq \mathscr{M}_n(D)$ pour un certain corps D de centre k. Appliquons le théorème 94 et posons $D \simeq D_1 \otimes_k \cdots \otimes_k D_n$. On a alors pour tout $i = 1, \cdots, n$,

$$A \simeq D_1 \otimes_k \cdots \otimes_k D_{i-1} \otimes_k \mathscr{M}_n(D_i) \otimes_k D_{i+1} \otimes_k \cdots \otimes_k D_n$$

Pour finir ce paragraphe, examinons comment se comporte l'indice par extension des scalaires :

Proposition 95.— *Soit* A *une* k*-algèbre simple centrale et* L/k *une extension finie. On a*

$$\mathrm{Ind}(A \otimes_k L) \,\Big|\, \mathrm{Ind}(A) \,\Big|\, [L : k].\mathrm{Ind}(A \otimes_k L)$$

Si, en particulier, $\mathrm{Ind}(A)$ *est étranger à* $[L : k]$, *alors* $\mathrm{Ind}(A) = \mathrm{Ind}(A \otimes_k L)$. *Dans cette situation, si* A *est un corps, alors* $A \otimes_k L$ *en est aussi un.*

Preuve : Si M/L est une extension neutralisante de la L-algèbre simple centrale $A \otimes_k L$, alors M est un corps neutralisant de A, puisque $\beta_{M/k}([A]) = \beta_{M/L} \circ \beta_{L/k}([A]) = \beta_{M/L}([A \otimes_k L]) = 0$. Si l'on choisit M de sorte que $[M : L] = \mathrm{Ind}(A \otimes_k L)$, alors puisque M neutralise A, on a

$$\mathrm{Ind}(A) | [M : k] = [M : L][L : k] = [L : k].\mathrm{Ind}(A \otimes_k L)$$

Puisque la propriété porte sur l'indice, on peut supposer que A est un corps et on a donc $\deg(A) = \mathrm{Ind}(A)$. On a $\deg(A \otimes_k L)^2 = [A \otimes_k L : L] = [A : k] = \deg(A)^2 = \mathrm{Ind}(A)^2$ et comme $\mathrm{Ind}(A \otimes_k L)$ divise $\deg(A \otimes_k L)$, on en déduit que $\mathrm{Ind}(A \otimes_k L)$ divise $\mathrm{Ind}(A)$.

———

3 Illustrations, exemples, applications.

3.1 Construction de corps gauches.

3.2 Algèbres cycliques.