Arithmétique des extensions intérieures

Bruno DESCHAMPS

LMNO - Le Mans Université

Résumé.— Dans cet article, nous étudions l'arithmétique des extensions galoisiennes intérieures finies de corps gauches et nous généralisons plusieurs des propriétés bien connues des algèbres à division telles que le célèbre théorème de Skolem-Noether ou encore la caractérisation d'être un produit croisé. Nous décrivons aussi, pour un corps K quelconque, l'analogue du groupe de Brauer pour K : il s'agit d'un certain sous-ensemble du groupe de Brauer du centre de K, $\mathrm{Br}(Z(K))$, qui décrit biunivoquement l'ensemble des extensions galoisiennes intérieures finies et centrales de K.

Abstract.— In this article, we study the structure of finite inner Galois extensions and generalize several well-known properties of division algebras such as the Skolem-Noether theorem or the characterization to be a crossed product. We also describe, for any field K, the analoguous of the Brauer group for K: it is a certain subset of the Brauer group of the center of K, $\mathrm{Br}(Z(K))$, which gives a one-to-one correspondance with the set of finite innner Galois and central extensions of K.

1.— Introduction.

(La lecture préalable des notations et conventions prescrites dans le §2.1 de ce texte peut être utile à la bonne compréhension de cette introduction.)

Dans l'océan des corps gauches, la première et la plus calme des mers à avoir été parcourue, fut celle des algèbres à division (i.e. des corps de dimension finie sur leurs centres). Ces corps présentent d'importantes propriétés arithmétiques, ils vérifient notamment le célèbre théorème de Skolem-Noether sur le relèvement des isomorphismes. Une conséquence capitale de ce théorème est que, si H désigne une k-algèbre à division alors, l'extension H/k est galoisienne, finie et l'on a $\mathrm{Gal}(H/k) = \mathrm{Int}(H)$ (i.e. l'extension H/k est intérieure). L'objet de ce texte est de voguer un peu plus loin que la mer des algèbres à division et de tenter d'explorer celle des extensions galoisiennes intérieures finies sans l'hypothèse de finitude sur leurs centres. On cherche en particulier à comprendre si l'on peut étendre à cette situation, plus générale, plusieurs des principales propriétés arithmétiques connues pour les k-algèbres à division. Pour une k-algèbre à division H donnée, citons parmi ces propriétés :

1/ La bicommutation (i.e. l'application $L \longmapsto \overline{L} = \mathscr{C}_H(L)$ qui à un corps intermédiaire $H/L/k$ associe son commutant dans H) est une involution. Autrement dit, le bicommutant de L dans H est égal à L (on dit que L bicommute).

2/ Le degré $[H : k]$ est un carré parfait.

3/ L'extension H/k satisfait au théorème de Skolem-Noether : si $\sigma : L \longrightarrow H$ désigne un k-plongement d'une extension intermédiaire $H/L/k$, alors σ se relève en un k-automorphisme (intérieur) de H.

4/ Si L/k est une extension centrale incluse dans H, alors L et son commutant $\overline{L}$ décomposent H de la manière suivante : $H \simeq L \otimes_k \overline{L}$.

5/ Les extensions commutatives maximales sont de degré $\sqrt{[H : k]}$ sur k.

6/ Le corps H est une extension croisée de k si et seulement si il existe une sous-extension commutative maximale de H/k qui est galoisienne sur k.

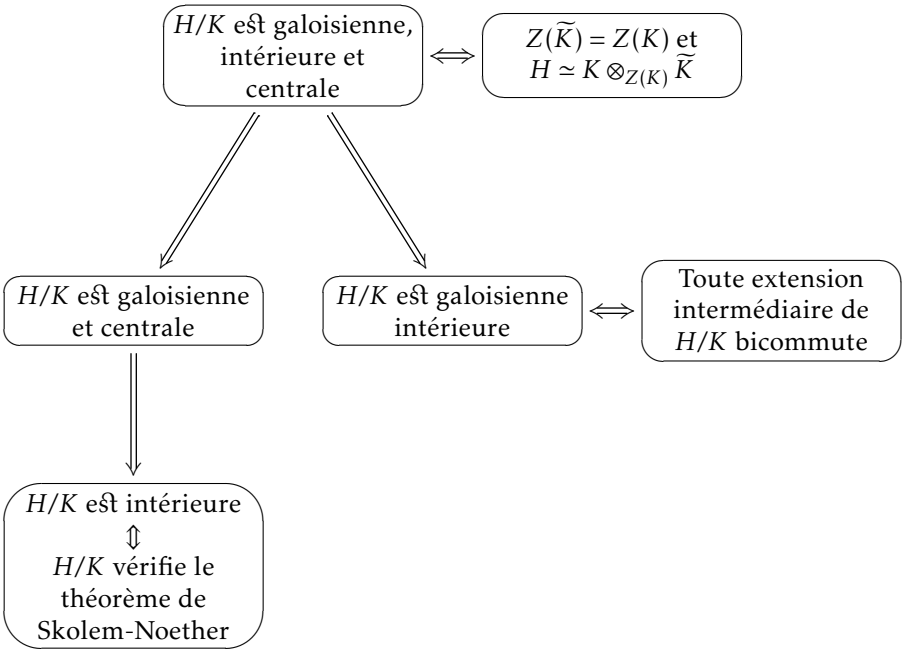
[0]Classification AMS 2020 : 12E15, 12E30, 16K40, 16K50.

7/ L'ensemble des k-algèbres à division (à k-isomorphisme près) est biunivoquement décrit par le groupe de Brauer, $\mathrm{Br}(k) = H^2(\mathrm{Gal}(k^{sep}/k), k^{sep*})$, du corps k[1].

La propriété 1/ se généralise telle quelle à notre situation (proposition 7). En fait, cette propriété est caractéristique : une extension finie est galoisienne intérieure si et seulement si toutes ses extensions intermédiaires bicommutent (corollaire 8).

Pour l'étude des autres propriétés, nous allons voir dans ce texte qu'une extension galoisienne intérieure finie H/K peut être découpée de manière unique par un corps $H/\Omega/K$ tel que Ω/K est une extension centrale (i.e. $Z(\Omega) = Z(K)$) et H/Ω est une extension purement intérieure (i.e. il n'existe aucune extension intermédiaire non triviale de H/Ω qui soit extérieure) (proposition 14). L'extension Ω/K est elle aussi galoisienne intérieure et on peut lui associer une certaine $Z(K)$-algèbre à division dont l'arithmétique galoisienne est la même que celle de Ω/K (théorème 10). C'est en fait pour l'extension Ω/K que nous allons généraliser les propriétés 2,3,4,5,6,7/ et comme $\Omega = H$ si et seulement si H/K est centrale, c'est donc finalement dans la situation où H/K est une extension galoisienne intérieure finie et centrale que nous les étudierons. Dans cette situation :

La propriété 2/ se généralise telle quelle (proposition 7). La propriété 3/ aussi et il est remarquable que le théorème de Skolem-Noether caractérise, pour les extensions galoisiennes, finies et centrales, le fait d'être intérieure (théorème 16 et corollaire 17). La propriété 4/ se généralise aussi telle quelle, mais nous montrons en plus que cette notion de "décomposition" caractérise presque la situation : pour une extension finie H/K donnée, H/K est galoisienne intérieure finie et centrale si et seulement si K et $\widetilde{K}$ ont même centre et $H \simeq K \otimes_{Z(K)} \widetilde{K}$ (corollaire 19). On peut alors résumer ces propriétés caractéristiques par le schéma implicatif suivant : si H/K désigne une extension finie de corps, alors



Pour la propriété 5/, il faut une généralisation de la notion de "sous-extension commutative maximale". Elle est tenue par celle de "sous-extension extérieure maximale". La propriété se généralise alors en remplaçant la première notion par la deuxième (corollaire 13).

Pour la propriété 6/, nous généralisons préalablement la notion de produit croisé : on part d'une ex-

[1] Les éléments du groupe de Brauer de k sont en fait les classes de similitude de k-algèbres simples centrales. La théorie montre que dans chacune de ces classes il existe une unique classe d'isomorphisme de k-algèbres à division et réciproquement.

tension galoisienne L/K de corps non nécessairement commutatifs, mais tels que l'extension L/K soit extérieure et l'on se donne un système de facteurs à valeurs dans le centre de L. On définit alors le produit croisé de L/K par f, comme dans le cas commutatif (début du §6), et l'on s'intéresse au cas où l'anneau H obtenu est un corps. Au contraire du cas restreint des algèbres à division sur leurs centres, certaines pathologies peuvent se produire. La principale est que l'extension H/K n'est pas forcément intérieure (un exemple explicite d'une telle situation est donné dans ce §). Le théorème 27 montre comment on peut mesurer le défaut d'intériorité de l'extension H/K en regardant la trivialité de certains 1-cocyles, déduits de f, dans un module de cohomologie non abélienne. Dans cet article, c'est probablement en examinant cette question que l'on mesure combien l'océan des corps gauches est bien plus délicat à naviguer dans sa globalité que sa tranquille mer des algèbres à division. Nonobstant cette pathologie, on obtient tout de même la généralisation attendue pour notre propriété : une extension galoisienne extérieure finie et centrale H/K est croisée si et seulement si il existe une sous-extension extérieure maximale dans H/K qui est galoisienne sur K (corollaire 30).

Pour la propriété 7/, à un corps K quelconque, nous montrons dans le §5 que l'ensemble des extensions galoisiennes intérieures finies et centrales de K (à K-isomorphisme près) est biunivoquement décrit par une certaine partie du groupe de Brauer $\mathrm{Br}(Z(K))$ du centre de K, cette description étant explicite par extension des scalaires à K. Nous montrons aussi, par un exemple, que cette partie n'est pas toujours un sous-groupe (exemple 21.b).

Ce travail s'inscrit dans le projet RIN "TIGaNoCo" (Théorie Inverse de Galois Non Commutative), financé par l'Union Européenne dans le cadre du programme opérationnel FEDER/FSE. Il est dans la continuité des travaux [Beh], [BDL], [Des1] et [DL] où l'on étudiait des propriétés galoisiennes d'extensions extérieures, en lien avec la théorie inverse de Galois pour les corps gauches. Plusieurs idées présentées ici se préfiguraient déjà dans ces articles.

2.— Notations, conventions et propriétés générales d'arithmétique des corps gauches.

2.1.— Notations et conventions. Au contraire du cas commutatif, la terminologie utilisée en théorie générale des corps varie souvent d'un auteur à l'autre et d'une langue à l'autre. Cet article s'inscrivant dans le cadre des précédents travaux de l'auteur *et alii* sur l'arithmétique des corps gauches, il est nécessaire que la terminologie soit cohérente avec celle introduite, au fur et à mesure, dans ces travaux. Pour éviter toute ambiguité, nous consacrons le début de ce § à préciser celles que nous allons utiliser, ainsi que les notations génériques s'y rapportant. De manière générale, dans tout cet article, lorsqu'elle sera utilisée comme objet mathématique, la lettre k désignera toujours un corps commutatif.

Corps et algèbre à division. Quand on parlera de corps, ce sera au sens large : un corps est un ensemble H muni de deux lois de composition internes, addition et produit, notées $+$ et $.$ telles que $(H,+)$ et $(H-\{0\},.)$ soient des groupes et telles que $.$ soit distributive à gauche et à droite par rapport à $+$.

On montre que l'addition est alors nécessairement commutative. Lorsque le produit est aussi une loi commutative on précise que H est un *corps commutatif* et dans le cas contraire on dit que H est un *corps gauche*.

On appelle *algèbre à division* tout corps de dimension finie sur son centre. On précisera parfois *k-algèbre à division* ou *algèbre à division sur k* pour indiquer que k est le centre de l'algèbre à division considérée. La théorie des algèbres simples montre qu'une k-algèbre à division n'est rien d'autre qu'une k-algèbre simple centrale sans diviseur de zéro. C'est cette caractérisation qui nous pousse à limiter la terminologie d'*algèbre à division* au cas des corps de dimension finie sur leur centre.[2]

[2] Un certain usage anglo-saxon réserve la terminologie de "corps" (field) au cas commutatif et celle "d'algèbre à division" (division algebra) au cas non commutatif, mais cet usage n'est pas systématique chez tous les auteurs de langue anglaise. Ainsi, chez certains d'entre eux, le mot "field" correspond bien à la notion de corps au sens large et ces gens appellent alors "skew field" les corps non commutatifs (corps gauches en bon français). Dans cette situation, la terminologie "division algebra" n'apporte aucune précision supplémentaire. C'est aussi pour cette raison que, dans ce texte, nous fixons cette restriction à la définition d'algèbre à division.

Commutant. Pour un anneau A et une partie E de A, on notera

$$\mathscr{C}_A(E) = \{a \in A/\ \forall x \in E,\ xa = ax\}$$

le centralisateur de E dans A. On notera $Z(A) = \mathscr{C}_A(A)$ le centre de l'anneau A.

Lorsque pour A nous utiliserons la lettre H pour désigner un corps, on notera $\widetilde{E}$ à la place de $\mathscr{C}_H(E)$ et l'on appellera parfois ce centralisateur le *commutant de E (dans H)*.

Groupe de Brauer. Pour une k-algèbre simple centrale $\mathscr{A}$, on notera $[\mathscr{A}]$ sa classe dans le groupe de Brauer $\mathrm{Br}(k)$ de k, $\exp(\mathscr{A})$ son exposant (c'est-à-dire l'ordre de $[\mathscr{A}]$ dans $\mathrm{Br}(k)$) et $\mathrm{ind}(\mathscr{A})$ son indice (c'est-à-dire l'entier $\sqrt{[H_{\mathscr{A}} : k]}$ où $H_{\mathscr{A}}$ désigne l'unique corps élément de $[\mathscr{A}]$).

Pour un nombre premier p, on notera $\mathrm{Br}(k)\{p\}$, la p-partie du groupe de Brauer du corps commutatif k, c'est-à-dire l'ensemble des éléments de $\mathrm{Br}(k)$ d'ordre une puissance de p.

Automorphisme intérieur. Pour un anneau A et un élément inversible $a \in A^*$ donnés, on notera $I_A(a)$ l'automorphisme intérieur de A associé à l'élément $a : x \longmapsto axa^{-1}$.

Extension intérieure, extérieure. Pour une extension de corps H/K, on notera $\mathrm{Aut}(H/K)$ (resp. $\mathrm{Int}(H/K)$) le groupe des K-automorphismes (resp. des K-automorphismes intérieurs) de H. On dira de l'extension H/K qu'elle est *intérieure* si $\mathrm{Aut}(H/K) = \mathrm{Int}(H/K)$ et qu'elle est *extérieure* si $\mathrm{Int}(H/K) = 1$.

Il convient de remarquer que, si H/K est extérieure, alors pour toute extension intermédiaire $H/L/K$, les extensions H/L et L/K sont aussi extérieures. La réciproque de cette propriété n'est pas vraie en général.

De même, si H/K est intérieure, alors pour toute extension intermédiaire $H/L/K$, l'extension H/L est aussi intérieure mais L/K ne l'est pas nécessairement.

Extension centrale. On dira d'une extension de corps H/K qu'elle est *centrale* ou que c'est une *Z-extension* si $Z(H) = Z(K)$.

Extension galoisienne. On dira d'une extension de corps H/K qu'elle est *galoisienne* si le corps $H^{\mathrm{Aut}(H/K)}$ des invariants de H par l'action de $\mathrm{Aut}(H/K)$ est égal à K. Par exemple, tout corps K est galoisien sur son centre $Z(K)$, car $Z(K)$ est le corps des invariants du sous-groupe $\mathrm{Int}(K)$ de $\mathrm{Aut}(K/Z(K))$.

Degré. Pour la majorité des extensions H/K que nous allons rencontrer dans ce texte (notamment lorsqu'il s'agira d'extensions galoisiennes finies) les dimensions de H en tant que K-espace vectoriel droite ou gauche coïncident. Quand ce ne sera pas le cas, on considérera toujours la structure à gauche et l'on notera $[H : K]$ la dimension associée. Ce sera le degré (gauche) de l'extension H/K.

N-groupe et théorie de Galois finie. Etant donné un corps H et un groupe G d'automorphismes de H, on note

$$\mathfrak{A}_H(G) = \{a \in H^*/\ I_H(a) \in G\} \cup \{0\}$$

C'est *l'ensemble associé au groupe G* (relativement à H). On dit alors du groupe G que c'est un *N-groupe* si $\mathfrak{A}_H(G)$ est un corps. On rappelle que le groupe de Galois G d'une extension galoisienne H/K est toujours un N-groupe (puisque $\mathfrak{A}_H(G) = \widetilde{K}$) et réciproquement que, si G est un N-groupe tel que H/K (avec $K = H^G$) soit finie, alors H/K est galoisienne de groupe G (généralisation du lemme d'Artin) et que

$$[H : K] = o(G/\mathrm{Int}(H/K)).[\mathfrak{A}_H(G) : Z(H)]$$

Cet entier est appelé l'*ordre réduit* de G. Dans cette situation de finitude de l'extension H/K, les correspondances galoisiennes s'établissent entre les corps intermédiaires de l'extension et les sous-N-groupes de G. Pour tout $H/L/K$, l'extension H/L est galoisienne et le groupe $\mathrm{Aut}(L/K)$ s'identifie au quotient du normalisateur $\mathscr{N}_{\mathrm{Gal}(H/K)}(\mathrm{Gal}(H/L))$ par le sous-groupe $\mathrm{Gal}(H/L)$. L'extension L/K est galoisienne si et seulement si $\mathrm{Gal}(H/L)$ est N-invariant, c'est-à-dire si le plus petit sous-N-groupe de $\mathrm{Gal}(H/K)$ qui contient $\mathscr{N}_{\mathrm{Gal}(H/K)}(\mathrm{Gal}(H/L))$ est égal à $\mathrm{Gal}(H/L)$ tout entier. On remarquera que si $\mathrm{Gal}(H/L)$ est distingué dans $\mathrm{Gal}(H/K)$ il s'agit bien sur d'un sous-groupe N-invariant, mais la réciproque de cette propriété

n'est pas vraie en général (au contraire du cas commutatif) : on peut tout à fait avoir une extension galoisienne L/K qui n'est pas laissée globalement invariante par certains éléments de $\mathrm{Gal}(H/K)$.

Pour un exposé complet de la théorie de Galois des corps gauches, à laquelle nous ne cessons de faire référence dans ce texte, nous renvoyons le lecteur à [Coh] et [Jac].

***K*-anneau.** Etant donné un corps K, on appelle K-anneau, tout anneau A muni d'un plongement de K dans A. On peut donc considérer A comme K-espace vectoriel à gauche *via* la multiplication (à gauche) dans A. Il est remarquable que lorsque qu'un K-anneau A est de dimension finie sur K, alors A est un corps si et seulement si A est intègre. En effet, la multiplication à droite par un élément non nul $a \in A$ est visiblement un K-endomorphisme de A et comme A est intègre, c'est un monomorphisme. Puisque A est un K-espace vectoriel de dimension finie, c'est finalement un isomorphisme, ce qui implique que a est inversible à droite. Ceci étant valable pour tout $a \neq 0$ et, puisque $1 \in K$ est un neutre bilatère, on en déduit finalement que A est bien un corps.

Après ces quelques points de terminologie, la suite du §2 est consacrée à l'établissement de résultats plus ou moins élémentaires et qui seront utiles dans toute la suite du texte. Pour les résultats classiques relatifs aux produits tensoriels d'algèbres que nous utilisons, notamment pour les questions de centralité et de commutant, nous renvoyons le lecteur à [Bou].

2.2.— Multi-commutants.

Lemme 1.— *Soient H un corps et K, L deux sous-corps de H.*

a) $K \subset L \Longrightarrow \widetilde{L} \subset \widetilde{K}$.

b) $K \subset \widetilde{\widetilde{K}}$.

c) Pour tout $n \geq 0$, les itérées successives du commutant vérifient $\widetilde{K}^{[2n+2]} = \widetilde{\widetilde{K}}$ et $\widetilde{K}^{[2n+3]} = \widetilde{K}$. En particulier, $\widetilde{\widetilde{\widetilde{K}}} = \widetilde{K}$.

Preuve : a) et b) sont immédiats.

c) En appliquant les propriétés a) et b), on a $\widetilde{K} \subset \widetilde{\widetilde{\widetilde{K}}} = \widetilde{\widetilde{\widetilde{K}}} = \widetilde{\left(\widetilde{\widetilde{K}}\right)} \subset \widetilde{K}$ et donc $\widetilde{\widetilde{K}} = \widetilde{K}$. Ceci implique, par récurrence, que $\widetilde{K}^{[2n+3]} = \widetilde{K}$ pour tout $n \geq 0$ et, par suite, que $\widetilde{K}^{[2n+2]} = \widetilde{\widetilde{K}^{[2n+1]}} = \widetilde{\widetilde{K}}$

□

2.3.— Morphismes de restriction aux commutants.

Lemme 2.— *Soit $\sigma : H_1 \longrightarrow H_2$ un isomorphisme de corps. Pour tout sous-corps $L \subset H_1$, on a*

$$\sigma(\mathscr{C}_{H_1}(L)) = \mathscr{C}_{H_2}(\sigma(L))$$

En conséquence de quoi, si H/L désigne une extension, alors pour tout automorphisme $\sigma \in \mathrm{Aut}(H)$ on a $\sigma(\widetilde{L}) = \widetilde{\sigma(L)}$.

Preuve : Soit $a \in H_2$, on a

$$\begin{array}{rcl} a \in \mathscr{C}_{H_2}(\sigma(L)) & \Longleftrightarrow & \forall x \in L,\ a\sigma(x) = \sigma(x)a \Longleftrightarrow \forall x \in L,\ \sigma^{-1}(a)x = x\sigma^{-1}(a) \Longleftrightarrow \sigma^{-1}(a) \in \mathscr{C}_{H_1}(L) \\ & \Longleftrightarrow & a \in \sigma(\mathscr{C}_{H_1}(L)) \end{array}$$

Si l'on prend $H_1 = H$ et $H_2 = H$ on obtient $\sigma(\widetilde{L}) = \widetilde{\sigma(L)}$.

□

Pour une extension quelconque H/L, on déduit de ce lemme l'existence d'une application

$$\begin{array}{rccc} \Lambda^r_{H/L} : & \mathrm{Aut}(H/L) & \longrightarrow & \mathrm{Aut}(\widetilde{L}/Z(L)) \\ & \sigma & \longmapsto & \sigma_{|\widetilde{L}} \end{array}$$

qui est visiblement un morphisme de groupes. Dans la suite de ce texte, on la notera génériquement $\Lambda^r_{H/L}$ et on l'appellera le *morphisme de restriction au commutant* (pour l'extension H/L).

2.4.— Questions de centralité.

Lemme 3.— *Soit H un corps.*

a) Si A et B sont des sous-corps de H, alors $\widetilde{A} \cap \widetilde{B} = \widetilde{A \cup B} = \widetilde{A.B}$.

b) Pour tout sous-corps L de H on a $Z(H).Z(L) \subset Z(\widetilde{L}) = \widetilde{L.\widetilde{L}}$.

Preuve : a) L'égalité $\widetilde{A} \cap \widetilde{B} = \widetilde{A \cup B}$ est immédiate. Maintenant, comme $A \cup B \subset A.B$, par le lemme 1, on a $\widetilde{A.B} \subset \widetilde{A \cup B}$. Pour l'inclusion réciproque, commençons par décrire récursivement le compositum $A.B$. De manière générale, étant donnés un sous-anneau Ω de H et une partie $E \subset H$, on note $\Omega[E]$ le sous-anneau engendré sur Ω par E. Cet anneau se décrit de la manière suivante :

$$\Omega[E] = \left\{ \sum_{finie} \prod_{i=1}^{n} \omega_1 \varepsilon_1 \cdots \omega_n \varepsilon_n \omega_{n+1} / \; n \geq 1, \; \omega_i \in \Omega, \; \varepsilon_i \in E \right\}$$

On constate au passage que si $x \in \widetilde{\Omega \cup E}$ alors $x \in \widetilde{\Omega[E]}$. Introduisons la suite croissante d'anneaux : $R_1 = A[B]$, et pour tout $k \geq 1$, $R_{k+1} = R_k[R_k^{*-1}]$ où R_k^{*-1} désigne l'ensemble des inverses des éléments de $R_k - \{0\}$. Il est clair que chaque anneaux R_k est inclus dans $A.B$ et, comme tout élément non nul de R_k est inversible dans R_{k+1}, on voit que $\bigcup_k R_k$ est un corps contenant A et B. On en déduit que $\bigcup_k R_k = A.B$. Si $x \in \widetilde{A \cup B}$, alors x commute avec tout élément de R_1 et donc tout élément de R_1^{*-1}. Il commute donc avec tout élément de R_2 et, par récurrence immédiate, avec tout élément de R_k et donc finalement avec tout élément de $A.B$, ainsi $x \in \widetilde{A.B}$.

b) Puisque $Z(H) \subset \widetilde{L}$, il est immédiat que $Z(H) \subset Z(\widetilde{L})$. Par ailleurs, par le lemme 1, on a $Z(L) = L \cap \widetilde{L} \subset \widetilde{\widetilde{L}} \cap \widetilde{L} = Z(\widetilde{L})$ et donc $Z(H).Z(L) \subset Z(\widetilde{L})$. Enfin, d'après le a), on a $\widetilde{L.\widetilde{L}} = \widetilde{L} \cap \widetilde{\widetilde{L}} = Z(\widetilde{L})$.

□

2.5.— Extensions décomposables. Etant donnés trois k-algèbres A_1, A_2, B et $\varphi_i : A_i \longrightarrow B$ deux morphismes de k-algèbres, pour que l'application k-linéaire $\varphi : A_1 \otimes_k A_2 \longrightarrow B$ déduite des applications φ_i par propriété universelle du produit tensoriel soit un morphisme de k-algèbre, il faut et il suffit que chaque image $\varphi_i(A_i)$ soit dans le commutant dans B de l'autre image. En particulier, si K désigne un sous-corps d'un corps H tel que $Z(K) \subset Z(H)$, alors il existe un morphisme naturel de $Z(K)$-algèbres entre $K \otimes_{Z(K)} \widetilde{K}$ et H.

Définition 4.— *Etant donnée une extension de corps H/K, on dira que "K décompose H" si $Z(K) \subset Z(H)$ et si le morphisme naturel $K \otimes_{Z(K)} \widetilde{K} \longrightarrow H$ est un isomorphisme.*

Lemme 5.— *On considère une extension H/K telle que K décompose H.*

a) On a $Z(K) \subset Z(\widetilde{K}) = Z(H)$ et si K bicommute (i.e. $\widetilde{\widetilde{K}} = K$) alors $Z(K) = Z(\widetilde{K}) = Z(H)$.

b) Si H/K est de degré fini alors $\widetilde{K}$ est une $Z(\widetilde{K})$-algèbre à division de dimension $\dfrac{[H:K]}{[Z(\widetilde{K}):Z(K)]}$.

Preuve : a) Le lemme 3 assure que $Z(K) \subset Z(\widetilde{K}) \subset Z(\widetilde{\widetilde{K}})$ et donc, si K bicommute il y a bien égalité. Maintenant les propriétés générales sur les algèbres tensorielles assurent que

$$Z(K \otimes_{Z(K)} \widetilde{K}) = Z(K) \otimes_{Z(K)} Z(\widetilde{K})$$

et donc, par $Z(K)$-isomorphisme, $Z(H) = Z(\widetilde{K})$.

b) En tant que K-espaces vectoriels à gauche, on a

$$[H : K] = \dim_K(H) = \dim_K(K \otimes_{Z(K)} \widetilde{K}) = [\widetilde{K} : Z(K)] = [\widetilde{K} : Z(\widetilde{K})].[Z(\widetilde{K}) : Z(K)]$$

Il s'ensuit que $\widetilde{K}$ est un corps de dimension finie sur son centre. Le calcul de la dimension $[\widetilde{K} : Z(\widetilde{K})]$ découle alors de l'égalité.

□

2.6.— Extensions extérieures. Comme nous le verrons dans la proposition 7 à venir, lorsque H/K est une extension galoisienne intérieure finie, on dispose d'une extension $Z(K)/Z(H)$. Lorsque l'extension est extérieure, c'est le phénomène inverse qui se produit :

Proposition 6.— *Une extension L/K est extérieure si et seulement si $\mathscr{C}_L(K) = Z(L)$. En particulier, si L/K désigne une extension extérieure alors*

1/ On a une extension $Z(L)/Z(K)$ et, en particulier, $K \cap Z(L) = Z(K)$.

2/ Si, de plus, l'extension L/K est galoisienne alors

a) L'extension $Z(L)/Z(K)$ est galoisienne et la restriction des automorphismes au corps $Z(L)$ induit un morphisme naturel $\pi : \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(Z(L)/Z(K))$.

b) Si $[L : K] < +\infty$ alors π est un épimorphisme et, dans ces conditions, π est un isomorphisme si et seulement si $[Z(L) : Z(K)] = [L : K]$. Par ailleurs, on a $Z(L^{ker(\pi)}) = Z(L)$.

Preuve : Puisque $\mathrm{Int}(L/K)$ s'identifie au groupe quotient $\mathscr{C}_L(K)/Z(L)$, l'équivalence est immédiate.

1/ On a $Z(K) = \mathscr{C}_K(K) \subset \mathscr{C}_L(K) = Z(L)$, d'où l'extension. Puisque $K \subset L$, il est clair que $K \cap Z(L) \subset Z(K)$ et, comme $Z(K) \subset Z(L)$, on a aussi $Z(K) \subset K \cap Z(L)$.

2.a) Puisque le centre d'un corps est globalement invariant par les automorphismes du corps, il existe, par restriction, un morphisme $\pi : \mathrm{Gal}(L/K) \longrightarrow \mathrm{Aut}(Z(L)/Z(K))$. On a $Z(L)^{\pi(\mathrm{Gal}(L/K))} \subset L^{\mathrm{Gal}(L/K)} = K$ et $Z(L)^{\pi(\mathrm{Gal}(L/K))} \subset Z(L)$, et ainsi,

$$Z(K) \subset Z(L)^{\pi(\mathrm{Gal}(L/K))} \subset K \cap Z(L) = Z(K)$$

On en déduit que $Z(L)^{\pi(\mathrm{Gal}(L/K))} = Z(K)$: l'extension $Z(L)/Z(K)$ est bien galoisienne.

2.b) Si $[L : K] < +\infty$, comme L/K est galoisienne extérieure, on a $\sharp\mathrm{Gal}(L/K) = [L : K]$ et, en particulier, $\pi(\mathrm{Gal}(L/K))$ est un groupe fini. D'après ce qui précède, $Z(L)^{\pi(\mathrm{Gal}(L/K))} = Z(K)$ et le lemme d'Artin (dans le cas commutatif) prouve alors que $\mathrm{Gal}(Z(L)/Z(K)) = \pi(\mathrm{Gal}(L/K))$. L'épimorphisme π est alors bijectif si et seulement si $[Z(L) : Z(K)] = \sharp\pi(\mathrm{Gal}(L/K)) = \sharp\mathrm{Gal}(L/K) = [L : K]$.

L'extension $L/L^{\ker(\pi)}$ est galoisienne extérieure de groupe $\ker(\pi)$ (lemme d'Artin dans le cas non commutatif) et, par application de ce qui précède à cette extension, on déduit que $Z(L)/Z(L^{\ker(\pi)})$ est galoisienne de groupe trivial. On a donc $Z(L) = Z(L^{\ker(\pi)})$.

□

3.— Structure.

3.1.— Algèbre à division associée à une extension intérieure. Nous commençons par établir quelques propriétés structurelles, généralisant celles des algèbres à division, pour les extensions galoisiennes intérieures finies :

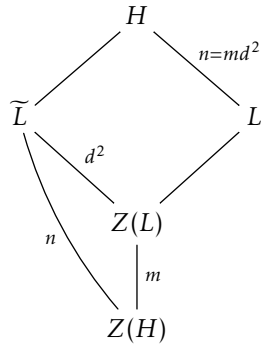
Proposition 7.— *Si H/K est une extension galoisienne intérieure finie alors pour toute extension intermédiaire $H/L/K$, H/L est une extension galoisienne intérieure finie et l'on a :*

a) $L = \widetilde{\widetilde{L}}$ (L bicommute).

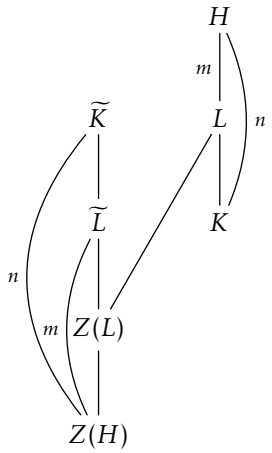
b) $Z(L) = L \cap \widetilde{L} = Z(\widetilde{L})$.

c) $Z(H) \subset Z(L)$.

d) $[\widetilde{L} : Z(H)] = [H : L]$, *en particulier,* $[H : L]$ *est divisible par* $[Z(L) : Z(H)]$ *et* $\dfrac{[H : L]}{[Z(L) : Z(H)]} = [\widetilde{L} : Z(L)]$ *est un carré parfait.*



e) $[\widetilde{K} : \widetilde{L}] = [L : K]$



Preuve : Puisque H/K est galoisienne finie, la théorie de Galois assure que H/L est galoisienne (finie) et comme $\mathrm{Gal}(H/L) \subset \mathrm{Gal}(H/K) = \mathrm{Int}(H/K)$, on a $\mathrm{Gal}(H/L) = \mathrm{Int}(H/L)$.

a) On a $K \subset L \subset \widetilde{\widetilde{L}} \subset H$ et comme l'extension H/K est supposée galoisienne intérieure finie, on a grâce au lemme 1.c) :

$$\mathrm{Gal}(H/\widetilde{\widetilde{L}}) = \left\{ I_H(a)/\ a \in \widetilde{\widetilde{L}}^* \right\} = \left\{ I_H(a)/\ a \in \widetilde{L}^* \right\} = \mathrm{Gal}(H/L)$$

ce qui prouve que $L = \widetilde{\widetilde{L}}$.

b) L'égalité $Z(L) = L \cap \widetilde{L}$ est immédiate et est en fait valable pour tout sous-corps L de H (indépendamment du fait que L soit une extension de K). On a donc $Z(\widetilde{L}) = \widetilde{L} \cap \widetilde{\widetilde{L}} = \widetilde{L} \cap L$ (d'après le lemme 1.a)) et donc $Z(L) = Z(\widetilde{L})$

c) On a $Z(H) \subset \widetilde{L} \subset H$ et donc $Z(H) \subset Z(\widetilde{L}) = Z(L)$ d'après le b).

d) On a $\mathfrak{A}_H(\mathrm{Gal}(H/L)) = \widetilde{L}$ et, puisque $\mathrm{Gal}(H/L) = \mathrm{Int}(H/L)$, l'ordre réduit de $\mathrm{Gal}(H/L)$ vaut donc

$$[H : L] = o(\mathrm{Gal}(H/L)/\mathrm{Gal}(H/L)).[\mathfrak{A}_H(\mathrm{Gal}(H/L)) : Z(H)] = [\widetilde{L} : Z(H)]$$

Puisque $\widetilde{L}$ est de dimension finie sur $Z(H)$, il l'est aussi sur $Z(\widetilde{L}) = Z(L)$ (d'après c)). Ainsi $\widetilde{L}$ est une $Z(L)$-algèbre à division et $[\widetilde{L} : Z(\widetilde{L})]$ est donc un carré parfait (propriété générale des algèbres simples centrales). Le reste de l'énoncé découle alors de la transitivité des degrés.

e) D'après le d), on a $[\widetilde{K} : \widetilde{L}] = \dfrac{[\widetilde{K} : Z(H)]}{[\widetilde{L} : Z(H)]} = \dfrac{[H : K]}{[H : L]} = [L : K]$.

□

Cette proposition permet de caractériser les extensions intérieures en termes de bicommutation :

Corollaire 8.— *Si H/K désigne une extension finie, alors les propositions suivantes*

i) l'extension H/K est galoisienne intérieure,

ii) toute extension intermédiaire $H/L/K$ bicommute (i.e. $\widetilde{\widetilde{L}} = L$),

iii) K bicommute (i.e. $\widetilde{\widetilde{K}} = K$),

sont équivalentes.

Preuve : $i) \Rightarrow ii)$: c'est la proposition 7.a).

$ii) \Rightarrow iii)$: évident.

$iii) \Rightarrow i)$: le groupe d'automorphismes $G = \mathrm{Int}(H/K) = \left\{I_H(a)/\ a \in \widetilde{K}^*\right\}$ est visiblement un sous-groupe de $\mathrm{Aut}(H/K)$ et le corps des invariants de H par l'action de G vaut $\widetilde{\widetilde{K}} = K$. Ainsi, l'extension H/K est galoisienne. Pour tout $\alpha \in H^*$, on a

$$I_H(\alpha) \in G \Longleftrightarrow \exists a \in \widetilde{K}^*,\ I_H(\alpha) = I_H(a) \Longleftrightarrow \exists a \in \widetilde{K}^*, \lambda \in Z(H),\ \alpha = \lambda a \Longleftrightarrow \alpha \in \widetilde{K}^*$$

et donc $\mathfrak{A}_H(G) = \widetilde{K}$ est un corps, c'est-à-dire que G est un N-groupe. La théorie de Galois assure alors que $\mathrm{Gal}(H/K) = G = \mathrm{Int}(H/K)$.

□

Il découle aussi de la proposition 7 que, lorsque H/K désigne une extension galoisienne intérieure finie, le corps $\widetilde{K}$ est une $Z(K)$-algèbre à division.

Définition-Notation 9.— *Si H/K désigne une extension galoisienne intérieure finie, le corps $\widetilde{K}$ est appelé "l'algèbre à division associée à l'extension H/K".*

Pour toute extension intermédiaire $\widetilde{K}/L_0/Z(K)$, on notera $\overline{L_0}$ le commutant de L_0 dans $\widetilde{K}$, c'est-à-dire $\overline{L_0} = \mathscr{C}_{\widetilde{K}}(L_0) = \widetilde{K} \cap \widetilde{L_0}$.

Théorème 10.— *Soit H/K une extension galoisienne intérieure finie.*

1/ La sous-extension $\widetilde{Z(K)}/K$ est galoisienne intérieure finie et le morphisme $\Lambda = \Lambda^r_{\widetilde{Z(K)}/K}$ de restriction au commutant,

$$\Lambda : \mathrm{Gal}(\widetilde{Z(K)}/K) \longrightarrow \mathrm{Gal}(\widetilde{K}/Z(K))$$

est un isomorphisme, pour lequel la bijection induite entre les ensembles de sous-groupes préserve les qualités d'être un N-groupe et d'être N-invariant (i.e. pour tout $G_0 \leq \mathrm{Gal}(\widetilde{Z(K)}/K)$, G_0 est un N-groupe (resp. est N-invariant) si et seulement si $\Lambda(G_0)$ l'est aussi).

2/ a) L'application

$$\begin{array}{rccc} \Phi : & \left\{\widetilde{Z(K)}/L/K\right\} & \longrightarrow & \left\{\widetilde{K}/L_0/Z(K)\right\} \\ & L & \longmapsto & L_0 = \widetilde{K}^{\Lambda(\mathrm{Gal}(\widetilde{Z(K)}/L))} \end{array}$$

est bijective et respecte les qualités galoisiennes, i.e. L/K est galoisienne si et seulement si $L_0/Z(K)$ l'est aussi, et dans ces conditions $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(L_0/Z(K))$.

b) Pour tout $\widetilde{Z(K)}/L/K$, on a $\Phi(L) = \widetilde{\widetilde{L}} = L \cap \widetilde{K}$.

c) La commutation induit des applications

$$\begin{array}{rccc} \Psi, \Psi^{-1} : & \left\{\widetilde{Z(K)}/L/K\right\} & \longleftrightarrow & \left\{\widetilde{K}/L_0/Z(K)\right\} \\ & L & \longmapsto & L_0 = \widetilde{L} \\ & L = \widetilde{L_0} & \longleftarrow & L_0 \end{array}$$

qui sont bijective et réciproques l'une de l'autre.

d) Pour tout $\widetilde{K}/L_0/Z(K)$, on a $\widetilde{\widetilde{L_0}} = L_0$. En particulier, pour tout $\widetilde{Z(K)}/L/K$, on a $[\widetilde{Z(K)} : L] = [\widetilde{L} : Z(K)]$.

Preuve : 1/ Par hypothèse, on a $\mathrm{Gal}(H/K) = \left\{I_H(a)/\ a \in \widetilde{K}^*\right\}$ et, puisque $\widetilde{K} \subset \widetilde{Z(K)}$, on a, par restriction, un morphisme

$$\begin{array}{rccc} \mathrm{res} : & \mathrm{Gal}(H/K) & \longrightarrow & \mathrm{Int}(\widetilde{Z(K)}/K) \\ & I_H(a) & \longmapsto & I_{\widetilde{Z(K)}}(a) \end{array}$$

Comme $K \subset \widetilde{Z(K)}^{\mathrm{Int}(\widetilde{Z(K)}/K)} \subset \widetilde{Z(K)}^{\mathrm{res}(\mathrm{Gal}(H/K))} \subset H^{\mathrm{Gal}(H/K)} = K$, on en déduit que $\widetilde{Z(K)}/K$ est galoisienne de groupe $\mathrm{Int}(\widetilde{Z(K)}/K)$ et donc intérieure. On remarque que le morphisme res est en fait un épimorphisme, ce qui prouve au passage que $\mathrm{Gal}(H/\widetilde{Z(K)})$ n'est pas seulement N-invariant mais bien distingué dans $\mathrm{Gal}(H/K)$.

Toujours parce que $\widetilde{K} \subset \widetilde{Z(K)}$, le morphisme de restriction au commutant

$$\begin{array}{rccc} \Lambda : & \mathrm{Gal}(\widetilde{Z(K)}/K) = \left\{I_{\widetilde{Z(K)}}(a)/\ a \in \widetilde{K}^*\right\} & \longrightarrow & \mathrm{Gal}(\widetilde{K}/Z(K)) = \left\{I_{\widetilde{K}}(a)/\ a \in \widetilde{K}^*\right\} \\ & I_{\widetilde{Z(K)}}(a) & \longmapsto & I_{\widetilde{K}}(a) \end{array}$$

est un épimorphisme. Si $a \in \widetilde{K}^*$ est tel que $I_{\widetilde{K}}(a) = \mathrm{Id}_{\widetilde{K}}$ alors $a \in Z(\widetilde{K}) = Z(K)$ et donc $I_{\widetilde{Z(K)}}(a) = \mathrm{Id}_{\widetilde{Z(K)}}$. L'épimorphisme Λ est donc aussi injectif.

Considérons un sous-groupe $G_0 \leq \mathrm{Gal}(\widetilde{Z(K)}/K)$. On a les égalités d'ensembles

$$\begin{array}{rcl} \mathfrak{A}_{\widetilde{Z(K)}}(G_0) & = & \left\{a \in \widetilde{Z(K)}^*/\ I_{\widetilde{Z(K)}}(a) \in G_0\right\} = \left\{a \in \widetilde{K}^*/\ I_{\widetilde{Z(K)}}(a) \in G_0\right\} \\ & = & \left\{a \in \widetilde{K}^*/\ I_{\widetilde{K}}(a) \in \Lambda(G_0)\right\} = \mathfrak{A}_{\widetilde{K}}(\Lambda(G_0)) \end{array}$$

et ainsi, $\mathfrak{A}_{\widetilde{Z(K)}}(G_0)$ est un corps si et seulement si $\mathfrak{A}_{\widetilde{K}}(\Lambda(G_0))$ en est un, c'est-à-dire que G_0 est un N-groupe si et seulement si $\Lambda(G_0)$ en est un aussi.

De manière générale, un isomorphisme de groupes envoie le normalisateur d'un sous-groupe sur le normalisateur de l'image de ce sous-groupe. Pour un N-sous groupe $G_0 \leq \mathrm{Gal}(\widetilde{Z(K)}/K)$, la bijection induite par Λ sur les ensembles de sous-groupes est visiblement croissante. On vient de voir que cette bijection respectait la qualité d'être un N-groupe. Dire que G_0 est N-invariant veut dire que le plus petit sous-N-groupe de $\mathrm{Gal}(\widetilde{Z(K)}/K)$ contenant $\mathscr{N}_{\mathrm{Gal}(\widetilde{Z(K)}/K)}(G_0)$ vaut $\mathrm{Gal}(\widetilde{Z(K)}/K)$. Ceci équivaut donc à dire que le plus petit sous-N-groupe de $\mathrm{Gal}(\widetilde{K}/Z(K))$ contenant $\Lambda\left(\mathscr{N}_{\mathrm{Gal}(\widetilde{Z(K)}/K)}(G_0)\right) = \mathscr{N}_{\mathrm{Gal}(\widetilde{K}/Z(K))}(\Lambda(G_0))$ vaut $\Lambda(\mathrm{Gal}(\widetilde{Z(K)}/K)) = \mathrm{Gal}(\widetilde{K}/Z(K))$, c'est-à-dire que $\Lambda(G_0)$ est N-invariant dans $\mathrm{Gal}(\widetilde{K}/Z(K))$.

2/ a) Il s'agit d'une conséquence immédiate du 1/ et de la théorie des correspondances galoisiennes en dimension finie rappelée au début de cet article.

b) Puisque $\widetilde{L} \subset \widetilde{Z(K)}$, on a $\mathrm{Gal}(\widetilde{Z(K)}/L) = \left\{I_{\widetilde{Z(K)}}(a)/\ a \in \widetilde{L}^*\right\}$. Ainsi, $\Phi(L)$ est le sous-corps de $\widetilde{K}$ laissé fixe par tous les $I_{\widetilde{K}}(a)$ avec $a \in \widetilde{L}^*$, c'est-donc le commutant de $\widetilde{L}$ dans $\widetilde{K}$ et ainsi, $\Phi(L) = \widetilde{\widetilde{L}} = L \cap \widetilde{K}$.

c) L'application Ψ est la composée de la commutation $L_0 \longmapsto \overline{L_0}$ dans $\widetilde{K}$, qui est bijective, avec Φ qui est bijective, c'est donc une application bijective. Puisque $\widetilde{\widetilde{L}} = L$ (proposition 7.a)) on en déduit que $\Psi^{-1} : L_0 \longmapsto \widetilde{L_0}$ est son application réciproque.

d) L'égalité $\widetilde{\widetilde{L_0}} = L_0$ est une conséquence immédiate du c) et comme H/L est une extension galoisienne intérieure finie, la proposition 7.e) assure que $[\widetilde{Z(K)} : L] = [\widetilde{L} : \widetilde{\widetilde{Z(K)}}] = [\widetilde{L} : Z(K)]$.

□

3.2.— Extensions extérieures maximales. Dans la suite de ce § on considérera une extension galoisienne intérieure finie H/K et son algèbre à division associée $\widetilde{K}$.

Lemme-Définition 11.— *Pour tout corps intermédiaire $H/L/K$, les propositions suivantes*

i) $\widetilde{L} = Z(L)$ *(i.e. l'algèbre à division associée à H/L est triviale),*

ii) $\widetilde{L} \subset L$,

iii) $\widetilde{L}$ *est commutatif,*

iv) $[Z(L) : Z(H)] = [H : L]$,

v) $[\widetilde{K} : Z(L)] = [L : K]$,

vi) il n'existe aucune extension intermédiaire non triviale $H/M/L$ telle que M/L soit extérieure,

sont équivalentes.

Lorsque le corps L satisfera l'une de ces conditions, on dira de l'extension H/L qu'elle est "purement intérieure".

Preuve : *i)* $\Longleftrightarrow$ *ii)* On a $Z(L) = L \cap \widetilde{L}$, d'où l'équivalence.

i) $\Longleftrightarrow$ *iii)* On a $\widetilde{L}$ commutatif $\Longleftrightarrow \widetilde{L} = Z(\widetilde{L})$ $(= Z(L)$ d'après la proposition 7.b).

i) $\Longleftrightarrow$ *iv)* D'après la proposition 7.c,d), on a $[H : L] = [\widetilde{L} : Z(H)] = [\widetilde{L} : Z(L)].[Z(L) : Z(H)]$, et l'équivalence en découle.

i) $\Longleftrightarrow$ *v)* D'après la proposition 7.c,e), on a $[\widetilde{K} : Z(L)] = [\widetilde{K} : \widetilde{L}].[\widetilde{L} : Z(L)] = [L : K].[\widetilde{L} : Z(L)]$, et l'équivalence en découle.

i) $\Longrightarrow$ *vi)* On considère une extension extérieure M/L incluse dans H. La proposition 6 montre que $Z(L) \subset Z(M)$. On a donc une tour d'extensions $\widetilde{L}/\widetilde{M}/Z(M)/Z(L)$ et l'hypothèse i) fournit alors l'égalité $\widetilde{L} = \widetilde{M} = Z(M) = Z(L)$. En utilisant la proposition 7.a., on trouve $M = \widetilde{\widetilde{M}} = \widetilde{Z(L)}$ et le théorème 10.1. dit alors que M/L est galoisienne intérieure. Ainsi, M/L est une extension galoisienne qui est à la fois intérieure et extérieure, on a donc nécessairement $\mathrm{Gal}(M/L) = 1$ et, par suite, $M = L$.

non i) $\Longrightarrow$ *non vi)* La $Z(L)$-algèbre à division $\widetilde{L}$ étant non triviale, il existe une extension commutative maximale et non triviale $L_0/Z(L)$ incluse dans $\widetilde{L}$. La proposition 12 ci-dessous montre (indépendamment de l'équivalence *i)* $\Longleftrightarrow$ *vi)* de ce lemme) que $\widetilde{L_0}/L$ est une extension extérieure non triviale.

□

On considère maintenant les ensembles d'extensions intermédiaires suivants :

$$\begin{aligned}
\mathscr{S}(H/K) &= \left\{\widetilde{Z(K)}/L/K \text{ tel que } \widetilde{L} = Z(L)\right\} \\
\mathscr{E}(H/K) &= \left\{\widetilde{Z(K)}/L/K \text{ tel que } L/K \text{ extérieure}\right\} \\
\mathscr{S}_0(H/K) &= \left\{\widetilde{K}/L_0/Z(K) \text{ tel que } L_0 \text{ commutatif}\right\} \\
\mathscr{E}_0(H/K) &= \left\{\widetilde{K}/L_0/Z(K) \text{ tel que } \overline{L_0} \text{ commutatif}\right\}
\end{aligned}$$

que l'on notera plus simplement $\mathscr{I}$,$\mathscr{E}$,$\mathscr{I}_0$,$\mathscr{E}_0$ et que l'on considérera comme ensemble ordonnés pour l'inclusion.

Proposition 12.— *La bijection décroissante de la proposition 10.c),* $\Psi : \left\{\widetilde{Z(K)}/L/K\right\} \longrightarrow \left\{\widetilde{K}/L_0/Z(K)\right\}$, *donnée par* $\Psi(L) = \widetilde{L}$, *induit, par restriction aux ensembles, une bijection entre* $\mathscr{I}$ *et* $\mathscr{I}_0$ *et une bijection entre* $\mathscr{E}$ *et* $\mathscr{E}_0$.

En conséquence de quoi, les chaines maximales des ensembles $\mathscr{I}$ *et* $\mathscr{E}$ *sont des intervalles fermés (i.e. possèdent chacune un plus petit et un plus grand élément) et l'on a*

$$\mathscr{I} \cap \mathscr{E} = \min \mathscr{I} = \max \mathscr{E}$$

où $\min \mathscr{I}$ *(resp.* $\max \mathscr{E}$*) désigne l'ensemble des éléments minimaux de* $\mathscr{I}$ *(resp. des éléments maximaux de* $\mathscr{E}$*). Cet ensemble, que nous noterons* $\mathscr{M}(H/K)$, *est en bijection par* Ψ *avec l'ensemble*

$$\mathscr{M}_0(H/K) = \left\{\widetilde{K}/L_0/Z(K) \text{ tel que } L_0 \text{ soit commutatif maximal}\right\}$$

En particulier, $\mathscr{M}(H/K) \neq \emptyset$.

Preuve : Il est clair que Ψ envoie $\mathscr{I}$ dans $\mathscr{I}_0$. Si l'on prend maintenant $L_0 \in \mathscr{I}_0$ alors, d'après la proposition 10.d), on a

$$Z(\widetilde{L_0}) = \widetilde{L_0} \cap \widetilde{\widetilde{L_0}} = \widetilde{L_0} \cap L_0 = Z(L_0) = L_0 = \widetilde{\widetilde{L_0}}$$

et donc $\Psi^{-1}(L_0) = \widetilde{L_0} \in \mathscr{I}$.

Pour un corps intermédiaire $\widetilde{K}/L_0/Z(K)$ et $L = \Psi^{-1}(L_0) = \widetilde{L_0}$, on a

$$Z(L) = Z(\widetilde{L_0}) = Z(L_0) = Z(\overline{L_0}) \subset \overline{L_0} = \widetilde{L_0} \cap \widetilde{K} = L \cap \widetilde{K}$$

et, comme par ailleurs, on a

$$\mathrm{Int}(L/K) \simeq \mathscr{C}_L(K)^*/Z(L)^* = (\widetilde{K} \cap L)^*/Z(L)^*$$

on en déduit que

$$L \in \mathscr{E} \Longleftrightarrow \mathrm{Int}(L/K) = 1 \Longleftrightarrow \widetilde{K} \cap L = Z(L) \Longleftrightarrow Z(\overline{L_0}) = \overline{L_0} \Longleftrightarrow L_0 \in \mathscr{E}_0$$

Puisque l'extension $\widetilde{K}/Z(K)$ est finie, les chaines maximales de $\mathscr{I}_0$ et $\mathscr{E}_0$ sont des intervalles fermés et comme Ψ est monotone, il en est de même des chaines maximales de $\mathscr{I}$ et $\mathscr{E}$. Puisque l'on a l'équivalence

$$L_0 \text{ commutative maximale } \Longleftrightarrow L_0 = \overline{L_0}$$

on voit immédiatement que $\mathscr{I}_0 \cap \mathscr{E}_0 = \mathscr{M}_0 = \max \mathscr{I}_0$. Pour voir que $\mathscr{M}_0 = \min \mathscr{E}_0$, il suffit de constater que la commutation $L_0 \longrightarrow \overline{L_0}$ est une bijection décroissante de l'ensemble $\left\{\widetilde{K}/L_0/Z(K)\right\}$ dans lui-même et qu'elle applique $\mathscr{I}_0$ sur $\mathscr{E}_0$.

La bijectivité de Ψ prouve alors que

$$\Psi(\mathscr{M}_0) = \Psi(\mathscr{I}_0 \cap \mathscr{E}_0) = \Psi(\mathscr{I}_0) \cap \Psi(\mathscr{E}_0) = \mathscr{I} \cap \mathscr{E}$$

et sa décroissance que $\mathscr{I} \cap \mathscr{E} = \min \mathscr{I} = \max \mathscr{E}$.

□

Le rôle analogue des sous-extensions commutative maximale de l'algèbre à division associée est donc rempli par celui des sous-extensions extérieures maximales de $\widetilde{Z(K)}/K$. On en déduit, en particulier,

Corollaire 13.— *Pour tout* $L \in \mathscr{M}(H/K)$, *on a*

$$[\widetilde{Z(K)} : K] = [L : K]^2 = [\widetilde{Z(K)} : L]^2 = [Z(L) : Z(K)]^2 = [\widetilde{K} : Z(L)]^2 = [\widetilde{K} : Z(K)]$$

Preuve : D'après la proposition 10.d), on a $\widetilde{\widetilde{Z(K)}} = Z(K)$ et comme $\widetilde{L} \in \mathscr{M}_0$, on a

$$[L : K]^2 = [\widetilde{K} : \widetilde{L}]^2 = [\widetilde{K} : Z(K)] = [\widetilde{K} : \widetilde{\widetilde{Z(K)}}] = [\widetilde{Z(K)} : L]$$

□

3.3.— Décomposition pure/centrale d'une extension intérieure. Nous finissons le §3. en caractérisant de deux manières le corps intermédiaire $\widetilde{Z(K)}$ d'une extension galoisienne intérieure finie H/K :

Proposition 14.— *Si H/K désigne une extension galoisienne intérieure finie alors le corps $\widetilde{Z(K)}$ est la plus grande Z-extension de K incluse dans H.*

En conséquence de quoi, le corps $L = \widetilde{Z(K)}$ est l'unique extension intermédiaire $H/L/K$ qui vérifie les deux conditions suivantes :

a) L/K est centrale,

b) H/L est purement intérieure.

Preuve : On a $Z(\widetilde{Z(K)}) = Z(Z(K)) = Z(K)$ (Proposition 7.a)) et donc $\widetilde{Z(K)}$ est bien une Z-extension de K. On a

$$\mathrm{Gal}(H/\widetilde{Z(K)}) = \mathrm{Int}(H/\widetilde{Z(K)}) = \left\{ I_H(a)/\ a \in \widetilde{\widetilde{Z(K)}}^* \right\} = \{ I_H(a)/\ a \in Z(K)^* \}$$

et ainsi, si $H/L/K$ vérifie $Z(L) = Z(K)$, alors pour tout $a \in Z(K)^*$ et tout $x \in L$, $I_H(a)(x) = x$. Ceci montre que $L \subset H^{\mathrm{Gal}(H/\widetilde{Z(K)})} = \widetilde{Z(K)}$.

Si L/K est centrale, on a donc $L \subset \widetilde{Z(K)}$. Si l'on suppose, de plus, que H/L est purement intérieure alors on a $[Z(L) : Z(H)] = [H : L]$ (lemme 11) et donc

$$[H : \widetilde{Z(K)}] = [\widetilde{Z(H)} : \widetilde{Z(K)}] = [Z(K) : Z(H)] = [Z(L) : Z(H)] = [H : L]$$

(la deuxième égalité provenant de la proposition 7.e.) ce qui prouve que $L = \widetilde{Z(K)}$.

□

Remarques.— 1/ La première caractérisation de $\widetilde{Z(K)}/K$ concerne sa maximalité dans l'ensemble des Z-extensions intermédiaires de H/K. Une caractérisation duale en terme de minimalité dans l'ensemble des sous-extensions purement intérieures n'est pas possible : si H désigne une k-algèbre à division, alors pour toute extension commutative maximale $H/L/k$ on a H/L purement intérieure alors que $H = \widetilde{k} \not\subset L$.

2/ Pour une extension galoisienne intérieure finie H/K les notions "être centrale" et "être purement intérieure" sont aux antipodes : la première équivaut à $[Z(K) : Z(H)] = 1$ et la deuxième à $[Z(K) : Z(H)] = [H : K]$. La deuxième caractérisation de $\widetilde{Z(K)}$ montre que ce corps mesure les degrés d'éloignement de l'extension H/K par rapport aux deux notions considérées : $\widetilde{Z(K)}$ est le pivot central/pur de l'extension H/K.

4.— Extension des scalaires.

Une conséquence tout à fait significative du théorème 10 est le

Corollaire 15.— *Si H/K désigne une extension galoisienne intérieure finie alors :*

a) Pour tout $\widetilde{Z(K)}/L/K$, on a

$$L = K.\widetilde{\widetilde{L}} \simeq K \otimes_{Z(K)} \widetilde{\widetilde{L}}$$

b) Pour toute Z-extension M/K incluse dans H, on a $\widetilde{Z(K)} = M.\widetilde{M} \simeq M \otimes_{Z(K)} \widetilde{M}$. En particulier, M décompose $\widetilde{Z(K)}$.

Preuve : a) Comme rappelé en fin de §2, les $Z(K)$-plongements $K \hookrightarrow \widetilde{Z(K)}$ et $\overline{\widetilde{L}} \hookrightarrow \widetilde{K} \hookrightarrow \widetilde{Z(K)}$ fournissent un morphisme naturel de $Z(K)$-algèbres $\varphi : K \otimes_{Z(K)} \overline{\widetilde{L}} \longrightarrow \widetilde{Z(K)}$. L'image de φ est visiblement incluse dans le compositum $K.\overline{\widetilde{L}}$ et, comme $\overline{\widetilde{L}} = \widetilde{\overline{L}} \cap \widetilde{K} = L \cap \widetilde{K}$, on a donc

$$\mathrm{Im}(\varphi) \subset K.\overline{\widetilde{L}} \subset L$$

En tant que K-espace vectoriel à gauche, on a $\dim_K K \otimes_{Z(K)} \overline{\widetilde{L}} = [\overline{\widetilde{L}} : Z(K)]$. Maintenant, comme $\widetilde{K}$ est une $Z(K)$-algèbre à division, on a $[\widetilde{K} : Z(K)] = [\Omega : Z(K)].[\overline{\Omega} : Z(K)]$ pour tout corps intermédiaire $\widetilde{K}/\Omega/Z(K)$. En prenant $\Omega = \widetilde{L}$ et en appliquant la proposition 7.e), on trouve alors

$$\dim_K K \otimes_{Z(K)} \overline{\widetilde{L}} = [\overline{\widetilde{L}} : Z(K)] = [\widetilde{K} : \widetilde{L}] = [L : K]$$

Ainsi, pour montrer que φ est un isomorphisme, il suffit de prouver que $\mathrm{Im}(\varphi) = L$. Montrons ce dernier point :

Notons $M = \mathrm{Im}(\varphi) \subset L$. L'anneau M est un K-anneau par le plongement $\varphi_{|K \otimes_{Z(K)} Z(K)}$. Puisqu'il est inclus dans un corps, il est intègre et comme il est de dimension finie en tant que K-espace vectoriel, c'est un corps. Le corps M contient les corps K et $\overline{\widetilde{L}}$ et, en vertu de ce que l'on vient de voir, on a donc $M = K.\overline{\widetilde{L}}$. Par application du lemme 3, on a

$$\widetilde{M} = \widetilde{K.\overline{\widetilde{L}}} = \widetilde{K} \cap \overline{\widetilde{L}} = \overline{\widetilde{L}} = \widetilde{L}$$

et, en appliquant la proposition 7.a), on en déduit que $M = L$.

b) En appliquant le a) à $L = \widetilde{Z(K)}$, on a donc

$$\widetilde{Z(K)} = K.\overline{\widetilde{Z(K)}} = K.\overline{Z(K)} = K.\widetilde{K} \simeq K \otimes_{Z(K)} \widetilde{K}$$

Si M désigne une Z-extension de K alors elle est incluse dans $\widetilde{Z(K)}$ (proposition 14) et l'extension H/M est galoisienne intérieure finie (théorème 10.1). En appliquant ce qui précède à H/M, on obtient $\widetilde{Z(K)} = \widetilde{Z(M)} = M.\widetilde{M} \simeq M \otimes_{Z(K)} \widetilde{M}$. Pour voir que M décompose bien $\widetilde{Z(K)}$ il suffit de constater qu'en utilisant le lemme 3, on a

$$\mathscr{C}_{\widetilde{Z(K)}}(M) = \widetilde{Z(K)} \cap \widetilde{M} = \widetilde{Z(K)}.M = \widetilde{Z(M)}.M = \widetilde{M}$$

et donc que $\widetilde{Z(K)} = M.\mathscr{C}_{\widetilde{Z(K)}}(M) \simeq M \otimes_{Z(K)} \mathscr{C}_{\widetilde{Z(K)}}(M)$.

□

Lorsque H/K est une Z-extension galoisienne intérieure finie, on a alors $H = \widetilde{Z(K)}$ et tout ce qui a été démontré jusqu'ici s'applique donc directement à H. Une première conséquence de taille du corollaire 15 est le

Théorème 16.— (Généralisation de Skolem-Noether) *Soit H/K une Z-extension galoisienne intérieure finie. Si $\sigma : L_1 \longrightarrow L_2$ désigne un K-isomorphisme entre deux extensions intermédiaires de H/K, alors σ se relève en un K-automorphisme intérieur de H.*

Preuve : Par application du corollaire 15 on peut écrire $L_i = K.\widetilde{L_i} \simeq K \otimes_{Z(K)} \widetilde{L_i}$ pour $i = 1, 2$. Il s'ensuit que l'on a $\mathscr{C}_{L_i}(K) = \widetilde{L_i}$ et, par application du lemme 2, on en déduit que la restriction de σ à $\widetilde{L_1}$ est un $Z(K)$-isomorphisme à valeurs dans $\widetilde{L_2}$. Le théorème de Skolem-Noether assure alors qu'il existe $a \in \overline{K}^*$ tel que $I_{\overline{K}}(a)_{|\widetilde{L_1}} = \sigma_{|\widetilde{L_1}}$. Puisque $a \in \widetilde{K}$, on a $I_H(a)_{|K} = \mathrm{Id}$ et donc $I_H(a) \in \mathrm{Int}(H/K)$ relève σ.

□

On en déduit la caractérisation suivante :

Corollaire 17.— *Si H/K désigne une Z-extension galoisienne finie, alors les proposition suivantes*

i) H/K est intérieure,

ii) H/K vérifie le théorème de Skolem-Noether,

sont équivalentes.

Le corollaire 15.b) montre que toute Z-extension galoisienne intérieure finie H/K provient d'une extension des scalaires de K par une algèbre à division sur $Z(K)$. Réciproquement :

Proposition 18.— *Soient K un corps de centre k, H_0 une k-algèbre à division et $H = K \otimes_k H_0$.*

a) Le centre de la k-algèbre H est k.

b) On a $\widetilde{K} = H_0$.

c) Si H est un corps, alors H/K est une Z-extension galoisienne intérieure finie de groupe de Galois isomorphe au groupe $\mathrm{Gal}(H_0/k)$.

Preuve : a) On a $Z(H) = Z(K) \otimes_k Z(H_0) = k \otimes_k k = k$.

b) On a $\widetilde{K} = \widetilde{K \otimes_k k} = \mathscr{C}_K(K) \otimes_k \mathscr{C}_{H_0}(k) = k \otimes_k H_0 = H_0$.

c) L'action sur le facteur droite des tenseurs $\sigma(x \otimes h) = x \otimes \sigma(h)$ fournit un monomorphisme $\mathrm{Gal}(H_0/k) \longrightarrow \mathrm{Gal}(H/K)$ dont on note Γ l'image. On a donc

$$\Gamma = \{I_H(1 \otimes \alpha) / \ \alpha \in H_0^*\}$$

Il est clair que $H^\Gamma = K$, ce qui montre déjà que l'extension H/K est galoisienne. Puisque $[H : K] = [H_0 : k] < +\infty$, cela prouve aussi qu'il s'agit d'une extension intérieure (car $\mathrm{Int}(H/K)$ est un N-groupe).

Considérons un élément $x \in H^*$ tel que $I_H(x) \in \Gamma$. Par définition de Γ, il existe $\alpha \in H_0$ tel que $I_H(x) = I_H(1 \otimes \alpha)$. On a alors $(1 \otimes \alpha)x^{-1} \in Z(H) = k$ et donc $x \in H_0$. Ceci prouve que $\mathfrak{A}_H(\Gamma) = H$ et donc que Γ est un N-groupe. Puisque H/K est finie, cela prouve finalement que $\mathrm{Gal}(H/K) = \Gamma$.

□

La conjonction du corollaire 15.b), de la proposition 18 et du lemme 5 donne alors le

Corollaire 19.— *Si H/K désigne une extension finie, alors les propositions suivantes*

i) H/K est une Z-extension galoisienne intérieure finie,

ii) $Z(\widetilde{K}) = Z(K)$ et K décompose H,

sont équivalentes.

Remarque : Si l'on considère une extension de corps commutatifs H/K, alors $K \otimes_{Z(K)} \widetilde{K} = K \otimes_K H = H$ et l'on voit donc que la condition $Z(\widetilde{K}) = Z(K)$ du ii) est indispensable à notre caratérisation.

5.— Ensemble de Brauer d'un corps gauche.

5.1.— Définition. Soient H_1 et H_2 deux extensions galoisiennes intérieures finies d'un même corps K. Si H_1 et H_2 sont K-isomorphes, alors on voit que les commutants respectifs $\mathscr{C}_{H_1}(K)$ et $\mathscr{C}_{H_2}(K)$ sont des $Z(K)$-algèbres à division isomorphes. Ainsi, étant donnée un corps K fixé, à partir de l'ensemble $\mathscr{E}xt(K)$ des extensions galoisiennes intérieures et finies de K, on peut définir l'application

$$\mathscr{E}xt(K)\Big/K\text{-isom.} \quad \longrightarrow \quad \mathrm{Br}(Z(K))$$

$$H \bmod(K\text{-isom.}) \quad \longmapsto \quad [\mathscr{C}_H(K)]$$

entre l'ensemble des extensions galoisiennes intérieures finies de K, modulo la relation d'équivalence "être K-isomorphes à", et le groupe de Brauer du centre $Z(K)$ de K. Une conséquence du corollaire 15 et de la proposition 18 est que la restriction C_K de cette application à l'ensemble $\mathscr{Z}\text{-}\mathscr{E}xt(K)$ des Z-extensions galoisiennes intérieures finies fournit des bijections

$$\begin{array}{rccc} C_K : & \mathscr{Z}\text{-}\mathscr{E}xt(K)\Big/K\text{-isom.} & \longleftrightarrow & \mathrm{Im}(C_K) \subset \mathrm{Br}(Z(K)) \\ & H \bmod(K\text{-isom.}) & \longmapsto & [\mathscr{C}_H(K)] \\ & K \otimes_{Z(K)} H_0 \bmod(K\text{-isom.}) & \longleftarrow & [H_0] \end{array}$$

réciproque l'une de l'autre. Lorsque K et commutatif, la théorie du groupe de Brauer montre que l'application C_K est bijective sur $\mathrm{Br}(Z(K))$ tout entier. Pour cette raison, on définit de manière générale :

Définition 20.— *Etant donné un corps K, on appelle "ensemble de Brauer" ou plus simplement "Brauer" de K, l'image de C_K dans* $\mathrm{Br}(Z(K))$ *et l'on note cet ensemble* $\mathrm{Br}(K)$.

Cette image, $\mathrm{Br}(K)$, étant *a priori* juste un ensemble, on se gardera de parler du "groupe de Brauer" de K. Nous allons d'ailleurs donner, un peu plus loin, un exemple explicite où $\mathrm{Br}(K)$ n'est pas un sous-groupe de $\mathrm{Br}(k)$ (exemple21.b). Le Brauer d'un corps gauche joue alors le parfait analogue du groupe de Brauer d'un corps commutatif : il paramètre biunivoquement les extensions galoisiennes intérieures finies et centrale de ce corps, à isomorphisme près.

5.2.— Cas des algèbres à division. Fixons une k-algèbre à division K. Pour tout $\alpha \in \mathrm{Br}(k)$, on note K_α l'unique k-algèbre à division dans α. La k-algèbre simple centrale $K \otimes_k K_\alpha$ est un corps si et seulement si $[K \otimes_k K_\alpha : k] = \mathrm{Ind}(K \otimes_k K_\alpha)^2$ et comme, $[K \otimes_k K_\alpha : k] = [K : k].[K_\alpha : k] = \mathrm{Ind}([K])^2.\mathrm{Ind}(\alpha)^2$, on en déduit donc que

$$\mathrm{Br}(K) = \Big\{\alpha \in \mathrm{Br}(k)/\ \mathrm{Ind}([K] + \alpha) = \mathrm{Ind}([K]).\mathrm{Ind}(\alpha)\Big\}$$

Exemples 21.— a) Comme nous l'avons déjà remarqué, pour un corps commutatif K, $\mathrm{Br}(K)$ est bien le groupe de Brauer de K.

b) On considère le corps de séries de Laurent en cascade à deux variables $k = \mathbb{R}((x))((y))$. Un petit calcul arithmético-cohomologique (dont on pourra trouver le détail dans [Des3]) montre que

- le groupe $\mathrm{Br}(k)$ est isomorphe à $(\mathbb{Z}/2)^4$,
- il existe un sous-groupe $\Omega \leq \mathrm{Br}(k)$ d'ordre 8 et tel que tout élément de Ω soit d'indice ≤ 2,
- l'ensemble $\mathrm{Br}(k) - \Omega$ est composé de quatre éléments d'indice 2 et de quatre autres d'indice 4.

Considérons alors un élément $\alpha \notin \Omega$ d'indice 2 et notons K la k-algèbre à division telle que $[K] = \alpha$. L'ensemble $\{\alpha + \beta/\ \beta \in \Omega\}$ compte exactement huit éléments dont aucun n'est dans Ω. Il existe donc exactement quatre éléments $\beta_1, \cdots, \beta_4 \in \Omega$ non nuls tels que $\alpha + \beta_1, \cdots, \alpha + \beta_4$ soient les quatre éléments d'indice 4 de $\mathrm{Br}(k)$. Puisque que, pour tout $\gamma \in \mathrm{Br}(k) - \{\beta_1, \cdots, \beta_4\}$, l'indice de $\alpha + \gamma$ vaut au plus 2, on déduit finalement que

$$\mathrm{Br}(K) = \{[k], \beta_1, \cdots, \beta_4\}$$

Puisque $\sharp\mathrm{Br}(K) = 5$, l'ensemble $\mathrm{Br}(K)$ ne saurait être un sous-groupe de $\mathrm{Br}(k)$.

c) On considère un corps H de quaternion sur un corps réel clos R. Puisque $\mathrm{Br}(R) = \{[R], [H]\}$ et que $H \otimes_k H \simeq \mathscr{M}_4(R)$ n'est pas un corps, on voit que $\mathrm{Br}(H) = 1$ et que $\mathscr{Z}\text{-}\mathscr{E}xt(H) = \{H \bmod(H\text{-isom.})\}$. Dans cette situation, on a aussi $\mathscr{E}xt(H) = \{H \bmod(H\text{-isom.})\}$. En effet, d'après [Des2,corollaire 2.4.], tout corps gauche de degré fini sur R est un corps de quaternion sur un sous corps réel clos R' et $\overline{R}$ et, en particulier, un tel corps est de degré 4 sur R.

Plus généralement, on a la proposition suivante :

Proposition 22.— *Si k désigne un corps commutatif, alors pour toute k-algèbre à division K, on a*

$$\bigoplus_{p \nmid exp(K)} \mathrm{Br}(k)\{p\} \subset \mathrm{Br}(K)$$

où $\mathrm{Br}(k)\{p\}$ *désigne la composante p-primaire du groupe de Brauer de k.*

Si l'on suppose, en outre, que le groupe de Brauer de k possède la propriété suivante : pour tout entier $n \geq 1$, $\mathrm{Br}(k)$ possède au plus un sous-groupe d'ordre n *(e.g.* $\mathrm{Br}(k) = \mathbb{Z}/2, \mathbb{Q}/\mathbb{Z}$*), alors on a*

$$\bigoplus_{p \nmid exp(K)} \mathrm{Br}(k)\{p\} = \mathrm{Br}(K)$$

Preuve : Rappelons que si K et H sont deux k-algèbres à division d'indices premiers entre eux, alors $K \otimes_k H$ est une k-algèbre à division. En particulier, toute k-algèbre à division H se décompose de manière unique sous la forme $H = \bigotimes_p H_p$ où H_p est l'unique k-algèbre à division représentant la composante p-primaire de $[H]$ dans $\mathrm{Br}(k)$ (ce que nous appellerons la décomposition p-primaire de H).

Si H est une k-algèbre à division qui représente un élément de $\bigoplus_{p \nmid \exp(K)} \mathrm{Br}(k)\{p\}$ alors son indice est premier à $\mathrm{ind}(K)$ (car l'indice et l'exposant sont des entiers ayant même radicaux). Il s'ensuit que $K \otimes_k H$ est un corps et la proposition 18 prouve alors que $[H] \in \mathrm{Br}(K)$.

Plaçons nous sous l'hypothèse faite sur $\mathrm{Br}(k)$. Soit $K = \bigotimes_p K_p$ la décomposition p-primaire de K et $H = \bigotimes_p H_p$ celle d'une k-algèbre à division quelconque. Si l'on suppose que $K \otimes_k H$ est un corps, alors $K_q \otimes_k H_p$ en est aussi un pour tout premiers p et q. En effet, $K_q \otimes_k H_p$ s'injecte dans $K \otimes_k H$ et est donc une k-algèbre intègre de dimension finie, c'est donc un corps. Fixons un premier p et notons $M = K_p \otimes_k H_p$ qui est donc une k-algèbre à division. Dans $\mathrm{Br}(k)$, on a $[M] = [K_p] + [H_p]$, mais puisqu'il s'agit d'éléments d'ordres une puissance de p, on en déduit que $\exp(M) | \max(\exp(K_p), \exp(H_p))$.

Si $\max(\exp(K_p), \exp(H_p)) = \exp(H_p)$ alors comme $\mathrm{Br}(k)$ ne compte qu'un seul sous-groupe d'ordre $\exp(H_p)$, il existe un entier $d \geq 1$ tel que $[M] = d[H_p]$ et, en examinant les indices, on a $\mathrm{ind}(M) = \mathrm{ind}(H_p^{\otimes d}) \leq \mathrm{ind}(H_p)$. Ceci implique que $[H_p : k] \leq [M : k] = \mathrm{ind}(M)^2 \leq \mathrm{ind}(H_p)^2 = [H_p : k]$ et donc $M = H_p$, c'est-à-dire $K_p = k$.

Si $\max(\exp(K_p), \exp(H_p)) = \exp(K_p)$ alors, le même raisonnement que précédemment prouve que $H_p = k$.

En conclusion, si $[H] \in \mathrm{Br}(K)$, alors pour tout $p | \exp(K)$ on a $H_p = k$ et par conséquent, $[H] \in \bigoplus_{p \nmid \exp(K)} \mathrm{Br}(k)\{p\}$.

□

Le corps K de l'exemple b) montre que l'égalité $\bigoplus_{p \nmid \exp(K)} \mathrm{Br}(k)\{p\} = \mathrm{Br}(K)$ est fausse en général.

5.3.— Cas des Z-extensions intérieures filtrées. Une *Z-extension intérieure filtrée* d'un corps K est un corps H obtenu par réunion d'une suite croissante $(H_n)_n$ de Z-extensions galoisiennes intérieures finies de K. Pour une telle extension, on a $Z(H) = Z(K)$ et

$$\mathrm{Br}(H) = \bigcap_n \mathrm{Br}(H_n)$$

En effet, si $x \in Z(H)$, il existe $n \geq 0$ tel que $x \in H_n$ et donc, $x \in Z(H_n) = Z(K)$. Réciproquement, si $x \in Z(K)$ alors x commute avec tous les éléments de H_n pour tout $n \geq 0$ et donc $x \in Z(H)$. Par ailleurs, si Ω désigne une $Z(K)$-algèbre à division, on voit que la $Z(K)$-algèbre $\Omega \otimes_{Z(K)} H$ s'identifie à la réunion croissante des

$Z(K)$-algèbres $\Omega \otimes_{Z(K)} H_n$. Puisque $\Omega \otimes_{Z(K)} H_n$ est un H_n-anneau de dimension finie, c'est un corps si et seulement si il est intègre. On a ainsi

$$\Omega \otimes_{Z(K)} H \text{ est un corps} \Longleftrightarrow \forall n \geq 0,\ \Omega \otimes_{Z(K)} H_n \text{ est un corps}$$

ce qui permet de voir que

$$\begin{array}{rcl} [\Omega] \in \mathrm{Br}(H) & \Longleftrightarrow & \Omega \otimes_{Z(K)} H \text{ est un corps} \\ & \Longleftrightarrow & \forall n \geq 0,\ \Omega \otimes_{Z(K)} H_n \text{ est un corps} \\ & \Longleftrightarrow & \forall n \geq 0,\ [\Omega] \in \mathrm{Br}(H_n) \end{array}$$

Exemple.— Considérons un corps commutatif k dont le groupe de Brauer possède au plus un sous-groupe d'ordre n pour tout $n \geq 1$ et, pour tout premier p, un élément $[K_p] \in \mathrm{Br}(k)\{p\}$. Comme nous l'avons vu précédemment, la k-algèbre $H_n = \bigotimes_{p \leq n} K_p$ est un corps et l'on peut donc considérer la Z-extension intérieure filtrée $H = \bigcup_n H_n$. Par application de la proposition 22 et de ce qui précède, on voit que

$$\mathrm{Br}(H) = \bigcap_n \mathrm{Br}(H_n) = \bigcap_n \bigoplus_{p>n} \mathrm{Br}(k)\{p\} = 0$$

6.— Produit croisé.

6.1.— Généralités. On considère une extension galoisienne extérieure L/K de groupe fini G (de neutre noté e) et un système de facteurs $f : G \times G \longrightarrow Z(L)^*$ à valeurs dans le centre de L. On se donne un L-espace vectoriel à gauche A de dimension $\sharp G$ que l'on rapporte à une base $\{a_\sigma\}_{\sigma \in G}$. Sur A, on définit une loi de composition interne (dite *produit croisé*), par la formule suivante :

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

Il s'agit de la même définition que dans le cas commutatif et le fait que l'on prenne un système de facteurs à valeurs dans le centre de L va permettre de conférer à A une structure de L-anneau (à gauche). En effet, il est déjà clair que cette multiplication est distributive à gauche et à droite par rapport à $+$. Montrons qu'elle est associative. Il suffit de vérifier la relation d'associativité 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

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

Cet anneau est unitaire, son neutre étant ωa_e où $\omega = f(e,e)^{-1}$. L'application $x \longmapsto \omega x$ plonge alors L dans cet anneau et lui confère ainsi sa structure de L-anneau.

Définition 23.— *Le L-anneau A ainsi construit s'appelle le "produit croisé de L par G relativement au système de facteurs f". On le note $\mathscr{A}(L/K, f)$.*

On dira d'une extension finie de corps H/K qu'elle est "croisée" s'il existe une extension intermédiaire L/K galoisienne extérieure telle que $H \simeq \mathscr{A}(L/K, f)$ pour un certain système de facteurs f à valeurs dans $Z(L)^*$.

Proposition 24.— *Avec les notations précédentes,*

a) Si f et f' sont deux systèmes de facteurs différant d'un cobord alors $\mathscr{A}(L/K, f) \simeq \mathscr{A}(L/K, f')$ en tant que L-anneaux.

b) Le L-anneau $\mathscr{A}(L/K, f)$ est un K-espace vectoriel à gauche de dimension n^2 où $n = \sharp G$.

c) Le commutant $\widetilde{L}$ de L dans $\mathscr{A}(L/K,f)$ vaut $\widetilde{L}=Z(L)$ et celui de K vaut $\widetilde{K}=\bigoplus_{\sigma\in G}Z(L)a_\sigma$.

d) On a $Z(\mathscr{A}(L/K,f))=Z(K)$.

Preuve : a) Soit $h:G\longrightarrow Z(L)^*$ une application telle que pour tout $\sigma,\tau\in G$, on ait

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

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

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

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

$$\begin{array}{rcl}\theta(x_\sigma a_\sigma y_\tau a_\tau) &=& f(\sigma,\tau)h(\sigma\tau)x_\sigma y_\tau^\sigma a_{\sigma\tau}=f^{'}(\sigma,\tau)h(\tau)^\sigma h(\sigma)x_\sigma y_\tau^\sigma a_{\sigma\tau}\\ &=& f^{'}(\sigma,\tau)x_\sigma h(\sigma)(y_\tau h(\tau))^\sigma a_{\sigma\tau}=(x_\sigma h(\sigma)a_\sigma)(y_\tau h(\tau)a_\tau)\\ &=& \theta(x_\sigma a_\sigma)\theta(y_\tau a_\tau)\end{array}$$

et ainsi, θ est un isomorphisme de L-anneaux. Quitte à multiplier par un cobord bien choisi, on peut donc supposer dans la suite que f est unitaire (i.e. $f(e,e)=1$). Dans cette situation, on a $a_e=1$ et, pour tout $\sigma\in G$, $f(e,\sigma)=f(\sigma,e)=1$.

b) $\dim_K(\mathscr{A}(L/k,f))=\dim_L(\mathscr{A}(L/k,f))[L:K]=n^2$.

c) On a $x=\sum_{\tau\in G}x_\tau a_\tau\in\widetilde{L}$ si et seulement si

$$\forall\lambda\in L,\ \sum_{\tau\in G}\lambda x_\tau a_\tau=\sum_{\tau\in G}x_\tau\lambda^\tau a_\tau\Longleftrightarrow\forall\tau\in G,\forall\lambda\in L,\lambda x_\tau=x_\tau\lambda^\tau$$

Si $x_\tau\neq 0$ alors, pour tout $\lambda\in L$, $\lambda^\tau=I_L(x_\tau)(\lambda)=\mathrm{Id}_L(\lambda)=\lambda$ (car L/K est extérieur) et donc $\tau=e$. Ainsi $x=x_e$ mais comme $\lambda x=x\lambda$ pour tout $\lambda\in L$, on a finalement $x\in Z(L)$.

De même, on a $x=\sum_{\tau\in G}x_\tau a_\tau\in\widetilde{K}$ si et seulement si

$$\forall\lambda\in K,\ \sum_{\tau\in G}\lambda x_\tau a_\tau=\sum_{\tau\in G}x_\tau\lambda a_\tau\Longleftrightarrow\forall\tau\in G,\ \forall\lambda\in K,\lambda x_\tau=x_\tau\lambda\Longleftrightarrow\forall\tau\in G,\ x_\tau\in\mathscr{C}_L(K)=Z(L)$$

(la dernière égalité venant à nouveau du fait que L/K est extérieur, cf. proposition 8).

d) D'après le c), on a $Z(\mathscr{A}(L/K,f))=\mathscr{A}(\widetilde{L/K},f)\subset\widetilde{L}=Z(L)$. Soit $x\in Z(\mathscr{A}(L/K,f))\subset Z(L)$, pour tout $\tau\in G$, on a $xa_\tau=a_\tau x=x^\tau a_\tau$ et donc x est laissé stable par G, c'est-à-dire $x\in K$. Ainsi, $x\in K\cap Z(L)=Z(K)$ (cette égalité venant du fait que, puisque L/K est extérieure, $Z(K)\subset Z(L)$, cf. proposition 8.1.).

□

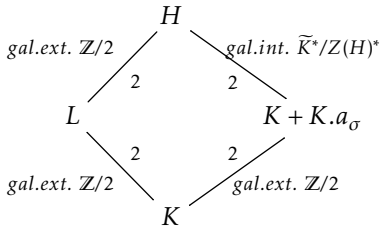
6.2.— Intériorité. Examinons à présent la question de l'intériorité de l'extension $\mathscr{A}(L/K,f)/K$ lorsque $\mathscr{A}(L/K,f)$ est un corps. Toute extension croisée $H/Z(H)$ est évidemment galoisienne intérieure (d'après le théorème de Skolem-Noether), mais quand $K\neq Z(H)$ des pathologies peuvent apparaitre :

Exemple 25.— (Une extension croisée qui n'est pas galoisienne intérieure) Examinons le cas où $\mathrm{Gal}(L/K)=\{1,\sigma\}=\mathbb{Z}/2$ et f est le système de facteurs défini par $f(1,1)=f(1,\sigma)=f(\sigma,1)=1$ et $f(\sigma,\sigma)=-1$. Dans cette situation, un petit calcul classique montre que l'anneau $H=L+L.a_\sigma=\mathscr{A}(L/K,f)$ est un corps si et seulement si

$$\forall\lambda\in L,\ \lambda\lambda^\sigma\neq-1$$

Plaçons-nous dans cette situation et supposons que $Z(L)=Z(K)$. Pour $\lambda,\mu\in L$, en étudiant la commutation avec les éléments de K, on voit que $I_H(\lambda+\mu a_\sigma)\in\mathrm{Int}(H/K)$ si et seulement si $\lambda,\mu\in\mathscr{C}_L(K)=Z(L)=$

$Z(K) \subset K$. Il s'ensuit que $a_\sigma \in H^{\mathrm{Int}(H/K)}$ et par suite, pour des raison de dimension, que $H^{\mathrm{Int}(H/K)} = K + Ka_\sigma \neq K$. L'extension H/K n'est donc pas intérieure. Pourtant, elle est bien galoisienne et l'on a le diagramme suivant :



En effet, remarquons pour commencer que l'application $\tau : a + b.a_\sigma \longmapsto a - b.a_\sigma$ est un élément de $\mathrm{Aut}(H/L)$ d'ordre 2 et que τ n'est pas un automorphisme intérieur (sinon il fixerait $H^{\mathrm{Int}(H/K)} = K + K\sigma$, ce qui n'est visiblement pas le cas).

Puisque τ n'est pas intérieur, le groupe $G =< \tau >= \{1, \tau\}$ est visiblement un N-groupe (son algèbre associée étant tout simplement $Z(H)$). La théorie de Galois assure alors que H/H^G est galoisienne extérieure de groupe G, et comme visiblement $H^G = L$, on a bien H/L galoisienne extérieure de groupe de Galois $\mathbb{Z}/2$.

La restriction de τ à $K+K\sigma = H^{\mathrm{Int}(H/K)}$ est visiblement un K-automorphisme qui vérifie $(K+Ka_\sigma)^{<\tau>} = K$. Ainsi, $H^{<\tau,\mathrm{Int}(H/K)>} = K$ et donc H/K est galoisienne. Il est alors clair que $H/H^{\mathrm{Int}(H/K)}$ est galoisienne intérieure et que $H^{\mathrm{Int}(H/K)}/K$ est galoisienne extérieure (puisque $\mathrm{Int}(H/K)$ est un sous-N-groupe distingué de $\mathrm{Gal}(H/K)$, donc N-invariant). Comme visiblement $K \neq K + K.a_\sigma \neq H$ et que $[H : K] = 4$, l'extension $K + K.\sigma/K$ est galoisienne extérieure de groupe $\mathbb{Z}/2$ (engendré par la restriction de τ).

On voit en passant que, bien que H/L et L/K soient extérieures, ce n'est pas le cas de H/K. Par ailleurs, puisque $\mathrm{Int}(H/K) = \widetilde{K}^*/Z(H)^*$ est distingué dans $\mathrm{Gal}(H/K)$, on a une suite exacte scindée

$$1 \longrightarrow \mathrm{Int}(H/K) \longrightarrow \mathrm{Gal}(H/K) \underset{\tau \mapsto \tau}{\longleftarrow} \mathrm{Gal}(K + K.a_\sigma/K) \longrightarrow 1$$

(puisque le générateur de $\mathrm{Gal}(K + K.a_\sigma/K)$ se relève sur τ) et donc

$$\mathrm{Gal}(H/K) = \widetilde{K}^*/Z(H)^* \rtimes \mathbb{Z}/2$$

Pour construire un exemple se plaçant dans cette situation, on considère Ω_p, la $\mathbb{Z}_p$-extension de $\mathbb{Q}$ (avec $p \neq 2$), α un générateur de $\mathrm{Gal}(\Omega_p/\mathbb{Q})$ et les corps de fractions tordus (voir [GW], [Ore] ou [Coh]) $K = \Omega_p(t^2, \alpha^2)$ et $L = \Omega_p(t, \alpha)$. Un petit calcul montre que $Z(L) = \Omega_p^{<\alpha>} = \mathbb{Q} = \Omega_p^{<\alpha^2>} = Z(K)$ (car $p \neq 2$ et donc α^2 est aussi générateur de $\mathbb{Z}_p$) et que L/K est galoisienne extérieure de groupe de Galois $\mathbb{Z}/2$ (engendré par l'automorphisme σ induit par la correspondance $t \longmapsto -t$).

En plongeant le corps L dans le corps des séries de Laurent tordu $\Omega_p((t, \alpha))$, on voit que si un élément $\lambda \in L$ vérifiait $\lambda\lambda^\sigma = -1$ alors, *via* le plongement, λ s'écrirait $\lambda = a_0 + a_1 t + \cdots$ avec $a_0 \in \Omega_p$ vérifiant $a_0^2 = -1$. Compte-tenue du fait que $\Omega_p \subset \mathbb{Q}^{\mathrm{tr}} \subset \mathbb{R}$, ceci est impossible et donc $H = \mathscr{A}(L/K, f)$ est bien un corps.

Venons-en maintenant à l'étude du corps des invariants par les automorphismes intérieurs d'une extension croisée en toute généralité. Pour mener à bien cette étude, nous allons avoir besoin d'une généralisation du théorème 90 d'Hilbert

Proposition 26.— *Soit L/K une extension extérieure.*

1/ (Généralisation du lemme de Dedekind) *L'ensemble* $\mathrm{Aut}(L/K)$ *forme une famille libre du L-espace vectoriel (droite ou gauche) des fonctions de L dans L.*

2/ (Généralisation du théorème 90 d'Hilbert) *Pour tout sous-groupe fini $G \subset \mathrm{Aut}(L/K)$, l'ensemble de cohomologie (non abélienne si L est un corps gauche)* $\mathrm{H}^1(G, L^*)$ *est trivial.*

Preuve : 1/ Supposons le contraire et considérons une famille L-liée $\{f_1, \cdots, f_n\} \subset \mathrm{Aut}(L/K)$ de cardinal n minimal. On a $n \geq 2$ et par hypothèse de minimalité de n, il existe $a_1, \cdots, a_n \in L^*$ tel que, pour tout $x \in L$,

$$\sum_{i=1}^{n} a_i f_i(x) = 0$$

Pour tout $z \in L$, on a donc

$$\begin{array}{rcccl} \displaystyle\sum_{i=1}^{n} a_i f_i(zx) = \sum_{i=1}^{n} a_i f_i(z) f_i(x) & = & \displaystyle\sum_{i=1}^{n-1} a_i f_i(z) f_i(x) + a_n f_n(z) f_n(x) & = & 0 \\ a_n f_n(z) a_n^{-1} \left(\displaystyle\sum_{i=1}^{n} a_i f_i(x) \right) = \displaystyle\sum_{i=1}^{n} a_n f_n(z) a_n^{-1} a_i f_i(x) & = & \displaystyle\sum_{i=1}^{n-1} a_n f_n(z) a_n^{-1} a_i f_i(x) + a_n f_n(z) f_n(x) & = & 0 \end{array}$$

En effectuant la différence, on trouve que

$$\sum_{i=1}^{n-1} \left(a_n f_n(z) a_n^{-1} a_i - a_i f_i(z) \right) f_i(x)$$

pour tout $x \in L$ et donc, par minimalité de n, on a pour tout $i = 1, \cdots, n-1$ et tout $z \in L$,

$$a_n f_n(z) a_n^{-1} = a_i f_i(z) a_i^{-1}$$

ce qui implique que $f_n \circ f_i^{-1} = I_L(a_n^{-1} a_i) \in \mathrm{Aut}(L/K)$. Puisque L/K est supposée extérieure, on en déduit finalement que $f_n = f_i$, ce qui est absurde. Pour la structure d'espace vectoriel à droite, le preuve s'obtient de la même façon.

2/ La preuve s'obtient grâce au lemme de Dedekind, exactement comme dans le cas abélien : on considère un 1-cocyle f, c'est-à-dire une application $f : G \longrightarrow L^*$ qui vérifie pour tout $\sigma, \rho \in G$, $f(\sigma\rho) = f(\sigma) f(\rho)^\sigma$, et l'on veut montrer que f est cohomologue au cocycle trivial, c'est-à-dire qu'il existe $a \in L^*$ tel que $f(\sigma) = a^{-1} a^\sigma$. Pour ce faire, on utilise le lemme de Dedekind généralisé qui assure l'existence d'un élément $c \in L^*$ tel que

$$b = \sum_{\rho \in G} f(\rho) c^\rho \neq 0$$

On a alors

$$b^\sigma = \sum_{\rho \in G} f(\rho)^\sigma c^{\sigma\rho} = \sum_{\rho \in G} f(\sigma)^{-1} f(\sigma\rho) c^{\sigma\rho} = f(\sigma)^{-1} \left(\sum_{\rho \in G} f(\sigma\rho) c^{\sigma\rho} \right) = f(\sigma)^{-1}.b$$

et l'on en déduit que $f(\sigma) = a^{-1} a^\sigma$ pour le choix $a = b^{-1}$.

□

(Il existe une version encore plus générale du lemme de Dedekind, 1/ de cet énoncé, dans le cas où L/K est quelconque. Voir [Coh, Th.3.3.2.]).

Théorème 27.— *Soient L/K une extension galoisienne extérieure finie de groupe G et f un système de facteurs à valeurs dans $Z(L)^*$ (supposé unitaire) tel que $H = \mathscr{A}(L/K, f)$ soit un corps. On note N le noyau de l'épimorphisme $G = \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(Z(L)/Z(K))$ de la proposition 6 sur lequel on fait agir G par conjugaison. On note $\widetilde{N}$ l'ensemble des G-orbites de N sous cette action.*

1/ Pour tout $\tau \in N$,

a) L'application

$$r_\tau : \begin{array}{ccc} \mathscr{C}_G(\tau) & \longrightarrow & L^* \\ \mu & \longmapsto & f(\tau,\mu)f(\mu,\tau)^{-1} \end{array}$$

est un 1*-cocycle.*

b) L'ensemble

$$J_\tau = \left\{ x_\tau \in L^* / \ \forall \mu \in \mathscr{C}_G(\tau),\ r_\tau(\mu) = x_\tau^{-1}.x_\tau^\mu \right\} \cup \{0\}$$

est un K-espace vectoriel isomorphe au K-espace vectoriel $L^{\mathscr{C}_G(\tau)}$*. Sa dimension sur K est donc égale à* $[L^{\mathscr{C}_G(\tau)} : K] = \sharp G/\sharp\mathscr{C}_G(\tau)$*.*

c) Pour tout $\sigma \in G$ *l'application*

$$\omega_{\tau,\sigma} : \begin{array}{ccc} J_\tau & \longrightarrow & J_{\sigma\tau\sigma^{-1}} \\ x_\tau & \longmapsto & x_{\sigma\tau\sigma^{-1}} \end{array}$$

où

$$x_{\sigma\tau\sigma^{-1}} = \omega_{\tau,\sigma}(x_\tau) = x_\tau^\sigma f(\sigma,\tau)f(\sigma\tau\sigma^{-1},\sigma)^{-1}$$

est un isomorphisme de K-espaces vectoriels.

d) Pour tout $x_\tau \in J_\tau$ *et tout* $\mu \in \mathscr{C}_G(\tau)$ *on a*

$$x_\tau^\sigma f(\sigma,\tau)f(\sigma\tau\sigma^{-1},\sigma)^{-1} = x_\tau^{\sigma\mu} f(\sigma\mu,\tau)f((\sigma\mu)\tau(\sigma\mu)^{-1},\sigma\mu)^{-1}$$

En conséquence de quoi, la somme

$$\sum_{\widehat{\sigma}\in G/\mathscr{C}_G(\tau)} x_\tau^\sigma f(\sigma,\tau)f(\sigma\tau\sigma^{-1},\sigma)^{-1}a_{\sigma\tau\sigma^{-1}} \in H$$

est définie de manière non équivoque.

e) L'ensemble

$$E_\tau = \left\{ \sum_{\widehat{\sigma}\in G/\mathscr{C}_G(\tau)} x_\tau^\sigma f(\sigma,\tau)f(\sigma\tau\sigma^{-1},\sigma)^{-1}a_{\sigma\tau\sigma^{-1}} /\ x_\tau \in J_\tau \right\}$$

est un K-espace vectoriel isomorphe au K-espace vectoriel J_τ *et si* $\tau' \in N$ *est tel que* $\widetilde{\tau} = \widetilde{\tau'}$ *alors* $E_\tau = E_{\tau'}$*. En conséquence de quoi, on peut considérer le K-espace vectoriel* $E_{\widetilde{\tau}} = E_\tau$ *dont la définition ne dépend que de la classe de* τ*.*

2/ Le corps des invariants de H par l'action de $\mathrm{Int}(H/K)$ *vaut alors*

$$H^{\mathrm{Int}(H/K)} = \bigoplus_{\widetilde{\tau}\in\widetilde{N}} E_{\widetilde{\tau}}$$

et l'on a $[H^{\mathrm{Int}(H/K)} : K] = \sharp N$*. En conséquence de quoi, on a l'équivalence*

$$H/K \text{ est galoisienne intérieure} \Longleftrightarrow N = \{\mathrm{Id}\} \Longleftrightarrow [Z(L) : Z(K)] = [L : K]$$

Preuve : 1.a) Pour tous $\mu, \mu' \in \mathscr{C}_G(\tau)$, on a par cocyclicité

$$\begin{array}{rll} r_\tau(\mu')^\mu r_\tau(\mu) = & f(\tau,\mu')^\mu f(\mu',\tau)^{-\mu} f(\tau,\mu)f(\mu,\tau)^{-1} = [f(\tau,\mu')^\mu f(\mu,\tau)^{-1}].[f(\mu',\tau)^{-\mu}].f(\tau,\mu) & \\ = & [f(\mu\tau,\mu')f(\mu,\tau\mu')^{-1}].[f(\mu,\mu'\tau)f(\mu\mu',\tau)^{-1}f(\mu,\mu')^{-1}].f(\tau,\mu) & \\ = & f(\mu\tau,\mu')f(\mu\mu',\tau)^{-1}f(\mu,\mu')^{-1}f(\tau,\mu) & \\ & (\text{car } \tau\mu' = \mu'\tau) & \\ = & f(\mu\tau,\mu')f(\mu\mu',\tau)^{-1}f(\mu,\mu')^{-\tau}f(\tau,\mu) = [f(\tau\mu,\mu')f(\mu,\mu')^{-\tau}f(\tau,\mu)].f(\mu\mu',\tau)^{-1} & \\ & (\text{car } \tau \in N \text{ et } f(\mu,\mu') \in Z(L)) \qquad (\text{car } \tau\mu = \mu\tau) & \\ = & f(\tau,\mu\mu')f(\mu\mu',\tau)^{-1} & \\ = & r_\tau(\mu\mu') & \end{array}$$

1.b) La généralisation du théorème 90 d'Hilbert, vue dans la proposition 26, montre qu'il existe un élément $x_\tau \in J_\tau$ non nul. Pour $y_\tau \in L^*$, on a

$$y_\tau \in J_\tau \iff \forall \mu \in \mathscr{C}_G(\tau),\ y_\tau^{-1}.y_\tau^\mu = r_\tau(\mu) = x_\tau^{-1}.x_\tau^\mu \iff \forall \mu \in \mathscr{C}_G(\tau),\ x_\tau y_\tau^{-1} = (x_\tau y_\tau^{-1})^\mu \iff y_\tau \in L^{\mathscr{C}_G(\tau)}.x_\tau$$

L'application $\lambda \longmapsto \lambda.x_\tau$ est donc un isomorphisme de K-espaces vectoriels.

Le calcul de la dimension découle de la théorie de Galois : puisque L/K est galoisienne extérieure et finie, on a $[L:K] = \sharp G$ et $[L:L^{\mathscr{C}_G(\tau)}] = \sharp\mathscr{C}_G(\tau)$, ce qui montre bien que

$$\dim_K J_\tau = [L^{\mathscr{C}_G(\tau)}:K] = [L:K]/[L:L^{\mathscr{C}_G(\tau)}] = \sharp G/\sharp\mathscr{C}_G(\tau)$$

1.c) Il s'agit, en premier lieu, de montrer que l'application $\omega_{\tau,\sigma}$ est bien à valeurs dans $J_{\sigma\tau\sigma^{-1}}$, c'est-à-dire de montrer que, si $x_\tau^\mu f(\mu,\tau) = x_\tau f(\tau,\mu)$ pour tout $\mu \in \mathscr{C}_G(\tau)$, alors $x_{\sigma\tau\sigma^{-1}}^\nu f(\nu,\sigma\tau\sigma^{-1}) = x_{\sigma\tau\sigma^{-1}} f(\sigma\tau\sigma^{-1},\nu)$ pour tout $\nu \in \mathscr{C}_G(\sigma\tau\sigma^{-1}) = \sigma\mathscr{C}_G(\tau)\sigma^{-1}$, autrement dit,

$$x_{\sigma\tau\sigma^{-1}}^{\sigma\mu\sigma^{-1}} f(\sigma\mu\sigma^{-1},\sigma\tau\sigma^{-1}) = x_{\sigma\tau\sigma^{-1}} f(\sigma\tau\sigma^{-1},\sigma\mu\sigma^{-1})$$

pour tout $\mu \in \mathscr{C}_G(\tau)$. Ceci est vrai puisque, par cocyclicité, on a

$$\begin{aligned}
x_{\sigma\tau\sigma^{-1}}^{\sigma\mu\sigma^{-1}} f(\sigma\mu\sigma^{-1},\sigma\tau\sigma^{-1}) = {} & [x_\tau^{\sigma\mu}].f(\sigma,\tau)^{\sigma\mu\sigma^{-1}}.[f(\sigma\tau\sigma^{-1},\sigma)^{-\sigma\mu\sigma^{-1}} f(\sigma\mu\sigma^{-1},\sigma\tau\sigma^{-1})] \\
= {} & x_\tau^\sigma.[f(\tau,\mu)^\sigma].[f(\mu,\tau)^{-\sigma}].[f(\sigma,\tau)^{\sigma\mu\sigma^{-1}}].[f(\sigma\mu\sigma^{-1},\sigma\tau)f(\sigma\mu\tau\sigma^{-1},\sigma)^{-1}] \\
= {} & x_\tau^\sigma.[f(\sigma\tau,\mu)f(\sigma,\tau)f(\sigma,\tau\mu)^{-1}].[f(\sigma\mu,\tau)^{-1}f(\sigma,\mu)^{-1}f(\sigma,\mu\tau)] \\
& .[f(\sigma\mu,\tau)f(\sigma\mu\sigma^{-1},\sigma)f(\sigma\mu\sigma^{-1},\sigma\tau)^{-1}].[f(\sigma\mu\sigma^{-1},\sigma\tau)f(\sigma\mu\tau\sigma^{-1},\sigma)^{-1}] \\
= {} & x_\tau^\sigma f(\sigma\tau,\mu)f(\sigma,\tau)f(\sigma,\mu)^{-1}f(\sigma\mu\sigma^{-1},\sigma)f(\sigma\mu\tau\sigma^{-1},\sigma)^{-1} \\
& (\text{car } \tau\mu = \mu\tau) \\
= {} & x_\tau^\sigma f(\sigma\tau,\mu)f(\sigma,\tau)f(\sigma,\mu)^{-\sigma\tau\sigma^{-1}}f(\sigma\mu\sigma^{-1},\sigma)f(\sigma\mu\tau\sigma^{-1},\sigma)^{-1} \\
& (\text{car } \sigma\tau\sigma^{-1} \in N \text{ et } f(\sigma,\mu) \in Z(L)) \\
= {} & x_\tau^\sigma f(\sigma,\tau).[f(\sigma\tau,\mu)f(\sigma,\mu)^{-\sigma\tau\sigma^{-1}}].f(\sigma\mu\sigma^{-1},\sigma)f(\sigma\mu\tau\sigma^{-1},\sigma)^{-1} \\
= {} & x_\tau^\sigma f(\sigma,\tau).[f(\sigma\tau\sigma^{-1},\sigma\mu)f(\sigma\tau\sigma^{-1},\sigma)^{-1}].f(\sigma\mu\sigma^{-1},\sigma)f(\sigma\mu\tau\sigma^{-1},\sigma)^{-1} \\
= {} & x_\tau^\sigma[f(\sigma,\tau)f(\sigma\tau\sigma^{-1},\sigma)^{-1}f(\sigma\tau\sigma^{-1},\sigma\mu\sigma^{-1})] \\
& .[f(\sigma\tau\sigma^{-1},\sigma\mu\sigma^{-1})^{-1}f(\sigma\tau\sigma^{-1},\sigma\mu).f(\sigma\mu\sigma^{-1},\sigma)f(\sigma\mu\tau\sigma^{-1},\sigma)^{-1}] \\
= {} & x_\tau^\sigma[f(\sigma,\tau)f(\sigma\tau\sigma^{-1},\sigma)^{-1}f(\sigma\tau\sigma^{-1},\sigma\mu\sigma^{-1})] \\
& .[f(\sigma\tau\sigma^{-1},\sigma\mu\sigma^{-1})^{-1}f(\sigma\tau\sigma^{-1},\sigma\mu).f(\sigma\mu\sigma^{-1},\sigma)^{\sigma\tau\sigma^{-1}}f(\sigma\tau\mu\sigma^{-1},\sigma)^{-1}] \\
& (\text{car } \tau\mu = \mu\tau \text{ et}, \sigma\tau\sigma^{-1} \in N \text{ et } f(\sigma\mu\sigma^{-1},\sigma) \in Z(L)) \\
= {} & x_\tau^\sigma f(\sigma,\tau)f(\sigma\tau\sigma^{-1},\sigma)^{-1}f(\sigma\tau\sigma^{-1},\sigma\mu\sigma^{-1}) \\
= {} & x_{\sigma\tau\sigma^{-1}} f(\sigma\tau\sigma^{-1},\sigma\mu\sigma^{-1})
\end{aligned}$$

Comme on peut s'y attendre, $\omega_{\tau,\sigma}$ est bijective et admet $\omega_{\sigma\tau\sigma^{-1},\sigma^{-1}}$ pour réciproque :

$$\begin{aligned}
\omega_{\sigma\tau\sigma^{-1},\sigma^{-1}} \circ \omega_{\tau,\sigma}(x_\tau) = {} & \omega_{\sigma\tau\sigma^{-1},\sigma^{-1}}(x_{\sigma\tau\sigma^{-1}}) = x_{\sigma\tau\sigma^{-1}}^{\sigma^{-1}} f(\sigma^{-1},\sigma\tau\sigma^{-1})f(\tau,\sigma^{-1})^{-1} \\
= {} & x_\tau.[f(\sigma,\tau)^{\sigma^{-1}}].[f(\sigma\tau\sigma^{-1},\sigma)^{-\sigma^{-1}}f(\sigma^{-1},\sigma\tau\sigma^{-1})]f(\tau,\sigma^{-1})^{-1} \\
= {} & x_\tau.[f(\sigma^{-1},\sigma)f(\sigma^{-1},\sigma\tau)^{-1}].[f(\sigma^{-1},\sigma\tau)f(\tau\sigma^{-1},\sigma)^{-1}].f(\tau,\sigma^{-1})^{-1} \\
= {} & x_\tau.f(\sigma^{-1},\sigma)^\tau f(\tau,1)f(\tau\sigma^{-1},\sigma)^{-1}.f(\tau,\sigma^{-1})^{-1} \\
& (\text{car } \tau \in N \text{ et } f(\sigma^{-1},\sigma) \in Z(L)) \\
= {} & x_\tau
\end{aligned}$$

L'application $\omega_{\tau,\sigma}$ est visiblement K-linéaire et son noyau est certainement réduit à $\{0\}$. Puisque les espaces considérés sont de dimensions finies, on en déduit bien que $\omega_{\tau,\sigma}$ est un isomorphisme.

1.d) Il s'agit de montrer que

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

pour tout $\sigma \in G$ et tout $\mu \in \mathscr{C}_G(\tau)$. A cet effet, on a

$$\begin{aligned}
[f(\tau,\mu)^{\sigma}].[f(\mu,\tau)^{-\sigma}].f(\sigma\mu,\tau)f(\sigma\tau\sigma^{-1},\sigma\mu)^{-1} &= [f(\sigma\tau,\mu)f(\sigma,\tau)f(\sigma,\tau\mu)^{-1}].[f(\sigma\mu,\tau)^{-1}f(\sigma,\mu)^{-1}f(\sigma,\mu\tau)] \\
&\quad .f(\sigma\mu,\tau)f(\sigma\tau\sigma^{-1},\sigma\mu)^{-1} \\
&= f(\sigma\tau,\mu)f(\sigma,\tau)f(\sigma,\mu)^{-1}f(\sigma\tau\sigma^{-1},\sigma\mu)^{-1} \\
&\quad (\text{car } \tau\mu=\mu\tau) \\
&= f(\sigma\tau,\mu)f(\sigma,\tau)f(\sigma,\mu)^{-1}f(\sigma\tau\sigma^{-1},\sigma\mu)^{-1} \\
&\quad (\text{car } \tau\mu=\mu\tau) \\
&= f(\sigma,\tau).[f(\sigma\tau,\mu)f(\sigma,\mu)^{-\sigma\tau\sigma^{-1}}f(\sigma\tau\sigma^{-1},\sigma\mu)^{-1}] \\
&\quad (\text{car } \sigma\tau\sigma^{-1}\in N \text{ et } f(\sigma,\mu)\in Z(L)) \\
&= f(\sigma,\tau)f(\sigma\tau\sigma^{-1},\sigma)^{-1}
\end{aligned}$$

1.e) L'application

$$\begin{array}{ccc} J_\tau & \longrightarrow & H \\ x_\tau & \longmapsto & \displaystyle\sum_{\widehat{\sigma}\in G/\mathscr{C}_G(\tau)} x_\tau^{\sigma} f(\sigma,\tau)f(\sigma\tau\sigma^{-1},\sigma)^{-1}a_{\sigma\tau\sigma^{-1}} \end{array}$$

est visiblement K-linéaire et comme son image vaut E_τ, ceci assure que ce dernier ensemble est bien un K-espace vectoriel. Par ailleurs, les éléments $a_{\sigma\tau\sigma^{-1}}$ formant une famille L-libre, notre application a donc un noyau trivial, ce qui montre qu'il s'agit d'un K-isomorphisme entre J_τ et E_τ.

Pour tout $\rho \in G$, puisque $\omega_{\tau,\rho}$ est une bijection entre les ensembles J_τ et $J_{\rho\tau\rho^{-1}}$, on a

$$E_{\rho\tau\rho^{-1}} = \left\{ \sum_{\widehat{\sigma}\in G/\mathscr{C}_G(\rho\tau\rho^{-1})} x^{\sigma}_{\rho\tau\rho^{-1}} f(\sigma,\rho\tau\rho^{-1})f(\sigma\rho\tau\rho^{-1}\sigma^{-1},\sigma)^{-1}a_{\sigma\rho\tau\rho^{-1}\sigma^{-1}} / \; x_{\rho\tau\rho^{-1}} = \omega_{\tau,\rho}(x_\tau),\; x_\tau \in J_\tau \right\}$$

Maintenant, pour $x_{\rho\tau\rho^{-1}} = \omega_{\tau,\rho}(x_\tau) = x_\tau^{\sigma} f(\sigma,\tau)f(\sigma\tau\sigma^{-1},\sigma)^{-1}$, on a pour tout $\sigma \in G$,

$$\begin{aligned}
&\sum_{\widehat{\sigma}\in G/\mathscr{C}_G(\rho\tau\rho^{-1})} x^{\sigma}_{\rho\tau\rho^{-1}} f(\sigma,\rho\tau\rho^{-1})f(\sigma\rho\tau\rho^{-1}\sigma^{-1},\sigma)^{-1}a_{\sigma\rho\tau\rho^{-1}\sigma^{-1}} \\
= &\sum_{\widehat{\sigma}\in G/\mathscr{C}_G(\tau)} x^{\rho\sigma\rho^{-1}}_{\rho\tau\rho^{-1}} f(\rho\sigma\rho^{-1},\rho\tau\rho^{-1})f(\rho\sigma\tau\sigma^{-1}\rho^{-1},\rho\sigma\rho^{-1})^{-1}a_{\rho\sigma\tau\sigma^{-1}\rho^{-1}} \\
= &\sum_{\widehat{\sigma}\in G/\mathscr{C}_G(\tau)} x^{\rho\sigma}_{\tau} f(\rho,\tau)^{\rho\sigma\rho^{-1}} f(\rho\tau\rho^{-1},\rho)^{-\rho\sigma\rho^{-1}} f(\rho\sigma\rho^{-1},\rho\tau\rho^{-1})f(\rho\sigma\tau\sigma^{-1}\rho^{-1},\rho\sigma\rho^{-1})^{-1}a_{\rho\sigma\tau\sigma^{-1}\rho^{-1}} \\
= &\sum_{\widehat{\sigma}\in G/\mathscr{C}_G(\tau)} x^{\sigma}_{\tau} f(\rho,\tau)^{\sigma\rho^{-1}} f(\rho\tau\rho^{-1},\rho)^{-\sigma\rho^{-1}} f(\sigma\rho^{-1},\rho\tau\rho^{-1})f(\sigma\tau\sigma^{-1},\sigma\rho^{-1})^{-1}a_{\sigma\tau\sigma^{-1}} \\
= &\sum_{\widehat{\sigma}\in G/\mathscr{C}_G(\tau)} x^{\sigma}_{\tau} f(\sigma,\tau)f(\sigma\tau\sigma^{-1},\sigma)^{-1}a_{\sigma\tau\sigma^{-1}}
\end{aligned}$$

la dernière égalité étant assurée si l'on montre que

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

or

$$\begin{aligned}
f(\sigma,\tau).[f(\sigma\tau\sigma^{-1},\sigma)^{-1}] &= f(\sigma,\tau).[f(\sigma\rho^{-1},\rho)^{\sigma\tau\sigma^{-1}}f(\sigma\tau\rho^{-1},\rho)^{-1}f(\sigma\tau\sigma^{-1},\sigma\rho^{-1})^{-1}] \\
&= f(\sigma,\tau)f(\sigma\rho^{-1},\rho)f(\sigma\tau\rho^{-1},\rho)^{-1}f(\sigma\tau\sigma^{-1},\sigma\rho^{-1})^{-1} \\
&\quad (\text{car } \sigma\tau\sigma^{-1}\in N \text{ et } f(\sigma\rho^{-1},\rho)\in Z(L)) \\
&= f(\sigma,\tau)f(\sigma\rho^{-1},\rho)\Big(f(\sigma\rho^{-1},\rho\tau)^{-1}f(\sigma\rho^{-1},\rho\tau)\Big)f(\sigma\tau\rho^{-1},\rho)^{-1} \\
&\quad \Big(f(\sigma\rho^{-1},\rho\tau\rho^{-1})^{-1}f(\sigma\rho^{-1},\rho\tau\rho^{-1})\Big)f(\sigma\tau\sigma^{-1},\sigma\rho^{-1})^{-1} \\
&= [f(\sigma,\tau)f(\sigma\rho^{-1},\rho)f(\sigma\rho^{-1},\rho\tau)^{-1}].[f(\sigma\rho^{-1},\rho\tau)f(\sigma\tau\rho^{-1},\rho)^{-1}f(\sigma\rho^{-1},\rho\tau\rho^{-1})^{-1}] \\
&\quad .f(\sigma\rho^{-1},\rho\tau\rho^{-1})f(\sigma\tau\sigma^{-1},\sigma\rho^{-1})^{-1} \\
&= f(\rho,\tau)^{\sigma\rho^{-1}}f(\rho\tau\rho^{-1},\rho)^{-\sigma\rho^{-1}}f(\sigma\rho^{-1},\rho\tau\rho^{-1})f(\sigma\tau\sigma^{-1},\sigma\rho^{-1})^{-1}
\end{aligned}$$

On en déduit que

$$\begin{aligned} E_{\rho\tau\rho^{-1}} &= \left\{ \sum_{\widetilde{\sigma}\in G/\mathscr{C}_G(\rho\tau\rho^{-1})} x^{\sigma}_{\rho\tau\rho^{-1}} f(\sigma,\rho\tau\rho^{-1}) f(\sigma\rho\tau\rho^{-1}\sigma^{-1},\sigma)^{-1} a_{\sigma\rho\tau\rho^{-1}\sigma^{-1}} / \; x_{\rho\tau\rho^{-1}} \in J_{\rho\tau\rho^{-1}} \right\} \\ &= \left\{ \sum_{\widetilde{\sigma}\in G/\mathscr{C}_G(\tau)} x^{\sigma}_{\tau} f(\sigma,\tau) f(\sigma\tau\sigma^{-1},\sigma)^{-1} a_{\sigma\tau\sigma^{-1}} / \; x_{\tau} \in J_{\tau} \right\} = E_{\tau} \end{aligned}$$

2/ On a $x = \sum_{\tau\in G} x_\tau a_\tau \in H^{\mathrm{Int}}$ si et seulement si $x \in \widetilde{\widetilde{K}}$, c'est-à-dire d'après la proposition 24.c),

$$\begin{aligned} &(1) \quad \forall \lambda \in Z(L),\ \lambda x = x\lambda \iff \sum_{\tau\in G} \lambda x_\tau a_\tau = \sum_{\tau\in G} x_\tau \lambda^\tau a_\tau = \sum_{\tau\in G} \lambda^\tau x_\tau a_\tau \\ &(2) \quad \forall \sigma \in G,\ a_\sigma x = x a_\sigma \iff \sum_{\tau\in G} x^\sigma_\tau f(\sigma,\tau) a_{\sigma\tau} = \sum_{\tau\in G} x_{\sigma\tau\sigma^{-1}} f(\sigma\tau\sigma^{-1},\sigma) a_{\sigma\tau} \end{aligned}$$

Si $x_\tau \neq 0$, la condition (1) implique alors $\lambda^\tau = \lambda$ pour tout $\lambda \in Z(L)$, c'est-à-dire $\tau \in N$. On voit alors que $(1) \Longleftrightarrow x = \sum_{\tau\in N} x_\tau a_\tau$. Sous la condition (1), la condition (2) équivaut alors à

$$\forall \tau \in N\ \forall \sigma \in G,\ x^\sigma_\tau f(\sigma,\tau) = x_{\sigma\tau\sigma^{-1}} f(\sigma\tau\sigma^{-1},\sigma)$$

Ceci montre, en particulier, que $\bigoplus_{\widetilde{\tau}\in\widetilde{N}} E_{\widetilde{\tau}} \subset H^{\mathrm{Int}(H/K)}$.

Réciproquement, considérons $x = \sum_{\tau\in N} x_\tau a_\tau \in H^{\mathrm{Int}}$ et fixons un élément $\tau \in N$ pour lequel $x_\tau \neq 0$. Pour tout $\mu \in \mathscr{C}_G(\tau)$, on a donc

$$x^\mu_\tau f(\mu,\tau) = x_\tau f(\tau,\mu)$$

ce qui assure que $x_\tau \in J_\tau$. On en déduit que

$$x = \sum_{\widetilde{\tau}\in\widetilde{N}} \sum_{\widetilde{\sigma}\in G/\mathscr{C}_G(\tau)} x_{\sigma\tau\sigma^{-1}} a_{\sigma\tau\sigma^{-1}} = \sum_{\widetilde{\tau}\in\widetilde{N}} \sum_{\widetilde{\sigma}\in G/\mathscr{C}_G(\tau)} x^\sigma_\tau f(\sigma,\tau) f(\sigma\tau\sigma^{-1},\sigma)^{-1} a_{\sigma\tau\sigma^{-1}} \in \bigoplus_{\widetilde{\tau}\in\widetilde{N}} E_{\widetilde{\tau}}$$

Les énoncés 1.b,e) et l'équation des classes permettent alors d'écrire

$$[H^{\mathrm{Int}(H/K)} : K] = \dim_K \bigoplus_{\widetilde{\tau}\in\widetilde{N}} E_{\widetilde{\tau}} = \sum_{\widetilde{\tau}\in\widetilde{N}} \dim_K E_{\widetilde{\tau}} = \sum_{\widetilde{\tau}\in\widetilde{N}} \dim_K J_\tau = \sum_{\widetilde{\tau}\in\widetilde{N}} \sharp G/\sharp\mathscr{C}_G(\tau) = \sharp N$$

L'équivalence finale découle alors immédiatement de cette dernière égalité.

□

Une question légitime est celle de la qualité galoisienne de l'extension $H^{\mathrm{Int}(H/K)}/K$ (et plus généralement de l'extension H/K) et du lien qui pourrait exister entre N et le groupe $\mathrm{Gal}(H^{\mathrm{Int}(H/K)}/K)$ lorsque l'extension est effectivement galoisienne. A moindres frais, on peut répondre à cette question lorsque N est central dans G :

Proposition 28.— *On garde les notations du théorème 27 et l'on note $n = \sharp N$ et μ_n le groupe des racines n-ième de l'unité. Si $N \subset Z(G)$ et que le corps $Z(K)$ est de caractéristique première à n et vérifie $\mu_n \subset Z(K)$, alors l'extension $H^{\mathrm{Int}(H/K)}/K$ est galoisienne extérieure de groupe de Galois isomorphe à N.*

Preuve : Avec l'hypothèse $N \subset Z(G)$, le théorème 27 montre qu'il existe une famille $\{x_\tau\}_{\tau\in N}$ d'élément de L^* telle que

$$H^{\mathrm{Int}(H/K)} = \bigoplus_{\tau\in N} K.x_\tau a_\tau$$

Avec les hypothèses, on peut faire agir $\mathrm{Hom}(N,\mu_n)$, le dual de N, sur le corps $H^{\mathrm{Int}(H/K)}$ en posant, pour tout $\varphi \in \mathrm{Hom}(N,\mu_n)$,

$$\left(\sum_{\tau\in N} \lambda_\tau.x_\tau a_\tau\right)^\varphi = \sum_{\tau\in N} \varphi(\tau)\lambda_\tau.x_\tau a_\tau$$

Cette action est visiblement fidèle et chaque élément de $\mathrm{Hom}(N,\mu_n)$ fixe les éléments de K. On en déduit que $\mathrm{Aut}(H^{\mathrm{Int}(H/K)}/K)$ contient un sous-groupe isomorphe à $\mathrm{Hom}(N,\mu_n)$. Comme N est abélien, il est isomorphe à son dual et donc $\mathrm{Aut}(H^{\mathrm{Int}(H/K)}/K)$ contient un sous-groupe isomorphe à N. Puisque l'extension $H^{\mathrm{Int}(H/K)}/K$ est extérieure de degré $n = \sharp N$, la théorie de Galois assure alors qu'elle est galoisienne et que $\mathrm{Gal}(H^{\mathrm{Int}(H/K)}/K) \simeq N$.

□

Remarque : Sous les hypothèses de l'énoncé précédent, on remarque que le dual de G agit aussi, de la même manière, sur H tout entier (si l'on rajoute l'hypothèse que $\mu_m \subset Z(K)$ avec $m = \sharp G$). Le morphisme de restriction est alors compatible avec les actions de $\mathrm{Hom}(G,\mu_m)$ sur H et de $\mathrm{Hom}(N,\mu_n)$ sur $H^{\mathrm{Int}(H/K)}$, c'est-à-dire que le diagramme suivant

$$\begin{array}{ccc} \mathrm{Hom}(G,\mu_m) & \xrightarrow{res} & \mathrm{Hom}(N,\mu_n) \\ \downarrow & & \downarrow \\ \mathrm{Aut}(H/K) & \xrightarrow{res} & \mathrm{Isom}_K(H^{\mathrm{Int}(H/K)},H) \end{array}$$

est commutatif. Ainsi, dés que le morphisme de restriction $\mathrm{Hom}(G,\mu_m) \xrightarrow{res} \mathrm{Hom}(N,\mu_n)$ est surjective, le groupe $\mathrm{Gal}(H^{\mathrm{Int}(H/K)}/K)$ se relève à $\mathrm{Aut}(H/K)$ et donc l'extension H/K est galoisienne. La classique suite exacte de cohomologie montre que cette condition de surjectivité est équivalente à dire que le morphisme de transgression $\mathrm{Hom}(N,\mu_n) \longrightarrow \mathrm{H}^2(G/N,\mu_m)$ est trivial.

6.3.— Caractérisation des produits croisés. On considère à présent une extension galoisienne intérieure finie H/K et l'on considère les deux ensembles

$$\begin{array}{rcl} \mathscr{M}_0^{\mathrm{gal}}(H/K) & = & \{L_0 \in \mathscr{M}_0(H/K) \text{ tel que } L_0/Z(K) \text{ soit galoisienne}\} \\ \mathscr{M}^{\mathrm{gal}}(H/K) & = & \{L \in \mathscr{M}(H/K) \text{ tel que } L/K \text{ soit galoisienne}\} \end{array}$$

Par application du théorème 10 et de la proposition 12, on voit que la commutation définit une bijection entre les ensembles $\mathscr{M}_0^{\mathrm{gal}}$ et $\mathscr{M}^{\mathrm{gal}}$. La théorie du groupe de Brauer assure que $\widetilde{K}/Z(K)$ est une extension croisée si et seulement si $\mathscr{M}_0^{\mathrm{gal}} \neq \emptyset$. Plus précisément, pour tout $L_0 \in \mathscr{M}_0^{\mathrm{gal}}$, il existe un 2-cocyle $f \in H^2(L_0/Z(K))$ tel que $\widetilde{K} \simeq \mathscr{A}(L_0/Z(K),f)$. L'extension $\widetilde{Z(K)}/K$ hérite de cette propriété relativement à $\mathscr{M}^{\mathrm{gal}}$:

Théorème 29.— *Pour tout $L \in \mathscr{M}^{gal}$, il existe un 2-cocyle $f \in H^2(\mathrm{Gal}(L/K),Z(L)^*)$ tel que*

$$\widetilde{Z(K)} \simeq \mathscr{A}(L/K,f)$$

et l'on a en outre $\widetilde{K} \simeq \mathscr{A}(Z(L)/Z(K),f)$.

Réciproquement, pour tout $L_0 \in \mathscr{M}_0^{gal}$, si l'on pose $L = \widetilde{L_0}$, alors

$$\widetilde{Z(K)} \simeq \mathscr{A}(L/K,f)$$

pour tout 2-cocyle $f \in H^2(L_0/Z(K))$ vérifiant $\widetilde{K} \simeq \mathscr{A}(L_0/Z(K), f)$.

Preuve : Considérons un corps $L \in \mathscr{M}^{\text{gal}}$. Puisque $\widetilde{Z(K)}/K$ est une Z-extension galoisienne intérieure (propositions 10 et 14), d'après la généralisation du théorème de Skolem-Noether (théorème 16) tout élément $\sigma \in G = \mathrm{Gal}(L/K)$ se relève en un automorphisme intérieur $I_{\widetilde{Z(K)}}(a_\sigma)$ de $\widetilde{Z(K)}$. Puisque $I_{\widetilde{Z(K)}}(a_\sigma)$ laisse fixe K, on a $a_\sigma \in \widetilde{K} \subset \widetilde{Z(K)}$. On suppose maintenant s'être donné, pour tout $\sigma \in G$, un élément a_σ tel que précédemment. Si σ, τ sont des éléments de G, alors pour tout $x \in L$,

$$I_{\widetilde{Z(K)}}(a_{\sigma\tau})(x) = \sigma \circ \tau(x) = I_{\widetilde{Z(K)}}(a_\sigma) \circ I_{\widetilde{Z(K)}}(a_\tau)(x) = I_{\widetilde{Z(K)}}(a_\sigma a_\tau)(x)$$

on en déduit que l'élément $a_\sigma a_\tau a_{\sigma\tau}^{-1}$ est dans $\widetilde{L} = Z(L)$. Ainsi, il existe $f(\sigma, \tau) \in Z(L)^*$ tel que

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

Pour tout $\sigma, \tau, \rho \in G$, on a

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

et comme la multiplication est associative, on en déduit que f est un système de facteurs à valeurs dans $Z(L)^*$.

Montrons maintenant que la famille $\{a_\sigma\}_{\sigma\in G}$ est une famille libre de $\widetilde{Z(K)}$ considéré comme L-espace vectoriel à gauche. A cet effet, supposons qu'il existe une équation de dépendance linéaire $\sum_{\sigma\in G} x_\sigma a_\sigma = 0$ et supposons l'avoir choisie pour qu'elle possède le moins possible de coefficients non nuls. Deux au moins de ces coefficients, $x_{\sigma_1}, x_{\sigma_2}$ sont non nuls. Considérons alors un élément $z \in Z(L)$ tel que $z^{\sigma_1} \neq z^{\sigma_2}$. Une telle chose est possible car, d'après le corollaire 13, on a $[Z(L) : Z(K)] = [L : K]$ et l'épimorphisme canonique $\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(Z(L)/Z(K))$ est alors un isomorphisme (proposition 6). On a alors

$$0 = z^{\sigma_1}\left(\sum_{\sigma\in G} x_\sigma a_\sigma\right) = \sum_{\sigma\in G} z^{\sigma_1} x_\sigma a_\sigma \text{ et } \left(\sum_{\sigma\in G} x_\sigma a_\sigma\right) z = \sum_{\sigma\in G} z^\sigma x_\sigma a_\sigma$$

et, en soustrayant, on obtient

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

et il s'agit là d'une équation de dépendance linéaire non triviale (car le coefficient en a_{σ_2} est non nul) qui compte moins de coefficients non nuls que celle dont on est partis. Ceci étant absurde, on en déduit bien que la famille est libre.

Le L-espace vectoriel gauche A engendré par les a_σ est donc un sous-anneau de $\widetilde{Z(K)}$ isomorphe à $\mathscr{A}(L/K, f)$. On a $\dim_K(A) = \dim_L(A).[L : K] = \sharp G.[L : K] = [L : K]^2 = [\widetilde{Z(K)} : K]$ (corollaire 13) et donc $A = \widetilde{Z(K)}$.

Comme on l'a remarqué, les éléments a_σ sont dans $\widetilde{K}$ et les groupes de Galois, $\mathrm{Gal}(L/K)$ et $\mathrm{Gal}(Z(L)/Z(K))$, sont canoniquement isomorphes. Les mêmes arguments montrent alors que $\widetilde{K} \simeq \mathscr{A}(Z(L)/Z(K), f)$.

La réciproque se montre de la même manière.

□

Corollaire 30.— *Pour qu'une extension galoisienne intérieure finie H/K soit croisée, il faut et il suffit qu'elle soit centrale et qu'elle vérifie l'une des conditions équivalentes suivantes :*

i) son algèbre à division associée est croisée,

ii) $\mathscr{M}_0^{gal}(H/K) \neq \emptyset$ *(i.e. il existe une extension commutative maximale de* $Z(K)$ *dans* $\widetilde{K}$ *qui est galoisienne),*

iii) $\mathscr{M}^{gal}(H/K) \neq \emptyset$ *(i.e. il existe une extension extérieure maximale de* K *dans* H *qui est galoisienne).*

Preuve : Les conditions sont clairement suffisantes par le théorème 29 car si $Z(H) = Z(K)$ alors $H = \widetilde{Z(K)}$. Elles sont aussi suffisantes à cause de la proposition 24.d) et du théorème 29.

□

L'énoncé dual de ce corollaire est déjà formulé dans le théorème 27 :

Corollaire 31.— *Pour qu'une extension croisée* $\mathscr{A}(L/K, f)/K$ *soit galoisienne intérieure, il faut et il suffit que* $[Z(L) : Z(K)] = [L : K]$.

Bibliographie

[Beh] Angelot Behajaina, *Théorie inverse de Galois sur les corps des fractions rationnelles tordus*, J. Pure Appl. Algebra 225-4 (2021).

[Bou] Nicolas Bourbaki, *Éléments de mathématique. Algèbre. Chapitre 1 à 3.*, Springer-Verlag, Berlin, xxiv+709 pp (1998).

[BDL] Angelot Behajaina, Bruno Deschamps et François Legrand, *Problèmes de plongement finis sur les corps non commutatifs*, Israel J. Math. (2021), 249, no. 2, 617-650 (2022).

[Coh] Paul Moritz Cohn, *Skew fields. Theory of general division rings*, Encyclopedia of Mathematics and its Applications, 57. Cambridge University Press, Cambridge, xvi + 500 pp (1995).

[Des1] Bruno Deschamps, *La méthode Behajaina appliquée aux corps de fractions tordus par une dérivation*, Res. Number Theory 7-2 (2021).

[Des2] Bruno Deschamps, *A propos d'un théorème de Frobenius*, Ann. Math. Blaise Pascal 8-2, 61-66 (2001).

[Des3] Bruno Deschamps, *Indices dans* $\mathrm{Br}(\mathbb{R}((x))((y)))$, note de travail non publiée, disponible à l'adresse web https://perso.univ-lemans.fr/~bdesch/Brauerdeg.pdf

[DL] Bruno Deschamps et François Legrand, *Le problème inverse de Galois sur les corps des fractions tordus à indéterminée centrale*, J. Pure Appl. Algebra 224-5 (2020).

[GW] Kenneth Goodearl and Robert Breckenridge Warfield, *An introduction to noncommutative Noetherian rings. Second edition*, London Mathematical Society Student Texts, 61. Cambridge University Press, Cambridge, xxiv+344 pp (2004).

[Jac] Nathan Jacobson, *Structure of rings*, American mathematical society colloquium publications (1956).

[Ore] Oystein Ore, *Theory of non-commutative polynomials*, Ann. of Math.(2), 34(3), 480-508 (1933).

Bruno Deschamps
Laboratoire de Mathématiques Nicolas Oresme, CNRS UMR 6139
Université de Caen - Normandie
BP 5186, 14032 Caen Cedex - France

Département de Mathématiques
Le Mans Université
Avenue Olivier Messiaen, 72085 Le Mans cedex 9 - France
E-mail : Bruno.Deschamps@univ-lemans.fr