Du monoïde des endomorphismes d'une extension intérieure filtrée

Bruno DESCHAMPS

LMNO - Le Mans Université

Résumé.— Dans la perspective de construire une théorie de Galois infinie pour les extensions non extérieures, nous montrons dans ce texte que le monoïde des endomorphismes d'une Z-extension intérieure filtrée s'identifie à la complétion procentrale du groupe de ses automorphismes intérieurs. En particulier, ce monoïde a une structure topologique naturelle qui fait de lui un espace complet et totalement discontinu.

Abstract.— In order to build an infinite Galois theory for non-outer extensions, we show that the monoïd of endomorphisms of a filtered inner Z-extension identifies with the procentral completion of the group of its inner automorphisms. In particular, this monoid has a natural topological structure for which it is a complete and totally discontinuous space.

1.— Introduction.

En théorie des corps, le théorème le plus général dont on dispose sur la structure du groupe des automorphismes d'une extension est du à Krull (pour le cas commutatif) et Jacobson (pour le cas général). Il affirme, entre autre, que si une extension de corps H/K est à la fois

• galoisienne (i.e. le corps des invariants de H, sous l'action du groupe $\mathrm{Aut}(H/K)$ des K-automorphismes de H, est égal à K),

• algébrique (i.e. pour tout $\alpha \in H$, les dimensions droite et gauche de $K(\alpha)$ sur K sont finies),

• extérieure (i.e. le groupe $\mathrm{Int}(H/K)$ des K-automorphisme intérieur de H est trivial, ce qui équivaut encore à dire que le centralisateur $\mathscr{C}_K(H)$ de K dans H est égal au centre $Z(H)$ de H),

alors le groupe $\mathrm{Gal}(H/K) = \mathrm{Aut}(H/K)$ s'identifie à la limite projective $\varprojlim \mathrm{Gal}(L/K)$ où L/K parcourt l'ensemble des sous-extensions galoisiennes finies de H/K. En particulier, le groupe $\mathrm{Gal}(H/K)$ est donc profini (et sa topologie afférente permet alors de caractériser les fameuses correspondances galoisiennes entre extensions intermédiaires et sous-groupes fermés). La condition d'extériorité de l'extension H/K est absolument nécessaire dans ce théorème, car la présence d'automorphismes intérieurs perturbe fortement les choses dans une extension de corps.

Dans l'article [Des] on s'est intéressé à l'arithmétique des extensions galoisiennes intérieures finies, c'est-à-dire aux extensions galoisiennes finies H/K pour lesquelles $\mathrm{Gal}(H/K) = \mathrm{Int}(H/K)$. Dans cet article, l'auteur a introduit la notion de *Z-extensions intérieures filtrées* qui sont, par définition, les corps H obtenus comme réunion croissante d'extensions galoisiennes intérieures finies et centrales H_n/K d'un même corps K. Ces extensions sont elles aussi algébriques et galoisiennes. Si, pour les extensions H_n/K, on remplace la condition "intérieure et centrale" par la condition "extérieure", on retombe sur Krull-Jacobson et l'on peut donc se demander si l'on dispose d'un théorème analogue pour les Z-extensions intérieures filtrées ?

Le présent article vise à unifier la partie structurelle du théorème de Krull-Jacobson pour les deux cas, intérieur et extérieur. Dans le cas extérieur, le groupe de Galois $\mathrm{Gal}(H/K)$ est égal au monoïde $\mathrm{End}_K(H)$ des K-endomorphismes de H (voir Exemples 6 et Proposition 7) et c'est la structure de ce monoïde que nous allons étudier plus généralement pour unifier les deux situations. Pour effectuer cette

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

unification, nous nous plaçons dans un cadre plus général : celui des extensions steiniziennes filtrées (voir §2). Pour une telle extension H/K, nous montrons aux §3&4 que le monoïde $\mathrm{End}_K(H)$ peut être décrit à la fois comme une complétion projective abstraite et comme la complétion d'un certain groupe topologique ultramétrique (théorèmes 13 et 15). Il en ressort notamment qu'il existe sur $\mathrm{End}_K(H)$ une topologie tout à fait naturelle qui fait de cet ensemble un espace complet et totalement discontinu. Dans le cas extérieur, on retombe exactement sur la structure compacte (et donc profinie) de $\mathrm{Gal}(K/H)$ du théorème de Krull-Jacobson et l'on voit ainsi que la structure dans le cas extérieur s'affaiblit au cas général par un passage compact⟶complet. Pour le cas d'application aux Z-extensions intérieures filtrées, on obtient quelque chose de plus précis que dans le cas général : le résultat principal de ce texte (théorème 19) est que, si H/K désigne une Z-extension intérieure filtrée, alors le monoïde $\mathrm{End}_K(H)$ est la complétion procentrale (voir §2.3. pour la définition) du groupe $\mathrm{Int}(H/K)$. Ces résultats se veulent être une première pierre à l'édification d'une théorie de Galois des extensions algébriques non nécessairement extérieures.

Dans ce texte, les corps considérés ne seront pas nécessairement commutatifs. Lorsque l'on parlera d'une *extension finie* de corps H/K ce sera pour indiquer que le K-espace vectoriel à gauche H est de dimension finie. Pour toute notion relative à la théorie de Galois sur les corps gauches que l'on utilise ici nous renvoyons à [Des], [Coh, Chapter 3] et [Jac, Chapters 6&7] pour de plus amples précisions.

2.— Complétion procentrale d'un groupe.

Dans ce § on considère un groupe abstrait G filtré par une suite décroissante $(G_n)_n$ de sous-groupes de G vérifiant $\bigcap_n G_n = 1$.

2.1.— Complétion topologique filtrée. Si la condition

$$(\mathcal{C}_0)\ \forall\sigma\in G,\ \forall n\geq 0, \exists m\geq n,\ G_m\subset \sigma G_n\sigma^{-1}$$

est vérifiée alors on sait (voir [Bou]) qu'il existe une et une seule topologie sur G qui confère à ce groupe la structure de groupe topologique et pour laquelle $(G_n)_n$ est une base de filtre de voisinages de l'unité. La condition $\bigcap_n G_n = 1$ assure alors que cette topologie est séparée. Elle est en fait (ultra)métrisable, une distance compatible étant donnée par l'application

$$d(\sigma,\tau) = \exp(-\max(n\geq 0/\ \sigma^{-1}\tau\in G_n))$$

La structure uniforme sous-jacente de G est donnée par d et l'on peut considérer le complété $(\widehat{G},\widehat{d})$ de G pour cette topologie, que l'on regardera comme l'ensemble des suites de Cauchy à valeurs dans G quotienté par la relation d'équivalence

$$(\sigma_n)_n \sim (\tau_n)_n \Longleftrightarrow \lim_n d(\sigma_n,\tau_n) = 0$$

La composition dans G se prolonge naturellement à $\widehat{G}$, par la loi de composition interne

$$(\sigma_n)_n \bmod(\sim).(\tau_n)_n \bmod(\sim) = (\sigma_n\tau_n) \bmod(\sim)$$

lui conférant ainsi une structure de monoïde. La seule difficulté pour établir cette dernière propriété réside dans le fait de montrer que la loi de composition interne sur $\widehat{G}$ est bien définie : si $(\sigma_n)_n$ et $(\tau_n)_n$ désignent deux suites de Cauchy, alors pour $n,m,h\geq 0$ donnés, on peut écrire

$$(\sigma_n\tau_n)^{-1}(\sigma_m\tau_m) = (\tau_n^{-1}\tau_h)(\tau_h^{-1}[\sigma_n^{-1}\sigma_m]\tau_h)(\tau_h^{-1}\tau_m)$$

Pour N fixé, il existe un indice h tel que pour tout $n,m\geq h$, $\tau_n^{-1}\tau_m\in G_N$ et, en particulier, $\tau_n^{-1}\tau_h, \tau_h^{-1}\tau_m\in G_N$. La propriété $(\mathcal{C}_0)$ assure l'existe d'un indice $N'\geq N$ tel que $\tau_h^{-1}G_{N'}\tau_h\subset G_N$. Or, il existe un indice $h' \geq h$, tel que $n, m \geq h'$, $\sigma_n^{-1}\sigma_m \in G_{N'}$ et l'on a donc finalement $(\sigma_n\tau_n)^{-1}(\sigma_m\tau_m) \in G_N$. La suite $(\sigma_n\tau_n)_n$ est bien de Cauchy. On montre avec le même type d'argument que si $(\sigma_n)_n \equiv (\sigma_n')_n \bmod(\sim)$ et $(\tau_n)_n \equiv (\tau_n')_n \bmod(\sim)$ alors $(\sigma_n\tau_n)_n \equiv (\sigma_n'\tau_n')_n \bmod(\sim)$.

De manière générale, les sous-groupes G_n n'étant pas forcément normaux dans G, si $(\sigma_n)_n$ est de Cauchy rien n'assure que $(\sigma_n^{-1})_n$ le soit : la composition ne confère pas forcément à $\widehat{G}$ une structure de groupe (voir [Bou] pour un contre-exemple). Dans la suite, on notera

$$\begin{array}{rccc} \pi_1 : & G & \longrightarrow & \widehat{G} \\ & \sigma & \longmapsto & (\sigma)_n \bmod(\sim) \end{array}$$

le plongement canonique de G dans son complété.

2.2.— Complétion projective. Les applications sur les ensembles de classes à gauches

$$\begin{array}{ccc} (G/G_{n+1})_g & \longrightarrow & (G/G_n)_g \\ x \bmod_g(G_{n+1}) & \longmapsto & x \bmod_g(G_n) \end{array}$$

sont surjectives et définissent un système projectif d'ensembles dont on peut considérer la limite inverse

$$\Pi(G) = \varprojlim_n (G/G_n)_g$$

Sur l'ensemble $\Pi(G)$ on cherche à définir une structure de monoïde. Pour cela, on considère la condition suivante

$(\mathcal{C}_1)$ Pour tout $\sigma \in G$, il existe une infinité d'indices $n \geq 0$ tel que $\sigma \in \mathcal{N}_G(G_n)$

où $\mathcal{N}_G(G_n)$ désigne le normalisateur de G_n dans G. Cette condition est par exemple vérifiée lorsque la suite (croissante) des centralisateurs $(\mathcal{C}_G(G_n))_n$ des G_n dans G vérifie $\bigcup_n \mathcal{C}_G(G_n) = G$. Il convient de remarquer que la condition $(\mathcal{C}_1)$ est plus forte que $(\mathcal{C}_0)$: en effet, si l'on fixe G_n et $\sigma \in G$, par $(\mathcal{C}_1)$ il existe $m \geq n$ tel que $\sigma \in \mathcal{N}_G(G_m)$ et l'on peut donc écrire $\sigma^{-1}G_m\sigma = G_m \subset G_n$, ce qui donne bien $(\mathcal{C}_0)$.

On suppose désormais que $(\mathcal{C}_1)$ est vérifiée et l'on définit une loi de composition interne $*$ sur $\Pi(G)$ de la manière suivante : pour $\lambda = (\lambda_n \bmod_g(G_n))_n$ et $\mu = (\mu_n \bmod_g(G_n))_n$ deux éléments de $\Pi(G)$, on pose

$$\lambda * \mu = \rho = (\rho_n \bmod_g(G_n))_n$$

où, pour $n \geq 0$ et $m_0 = m_0(\mu_n) \geq n$ tel que $\mu_n \in \mathcal{N}_G(G_{m_0})$, l'on a posé $\rho_n = \lambda_m\mu_n$ pour un indice arbitraire $m \geq m_0$.

1/ La loi $*$ est définie de manière non équivoque.

• Fixons un indice $n \geq 0$ et prenons un indice m_0 tel que $\mu_n \in \mathcal{N}_G(G_{m_0})$. Pour tout $m \geq m_0$, la classe de $\lambda_m\mu_n$ modulo gauche G_n ne dépend pas de m. En effet, si $m' \geq m \geq m_0 \geq n$, alors $\lambda_{m'}^{-1}\lambda_m \in G_m \subset G_{m_0}$ et donc $(\lambda_{m'}\mu_n)^{-1}(\lambda_m\mu_n) = \mu_n^{-1}(\lambda_{m'}^{-1}\lambda_m)\mu_n \in G_{m_0} \subset G_n$ et l'on a donc bien $\lambda_m\mu_n \equiv \lambda_{m'}\mu_n \bmod_g(G_n)$.

On voit donc que, pour les suites $(\lambda_n)_n$ et $(\mu_n)_n$ fixées, l'élément $\rho_n \bmod_g(G_n)$ ne dépend pas du choix de m et donc *de facto* du choix de m_0 vérifiant $\mu_n \in \mathcal{N}_G(G_{m_0})$.

• On se donne deux autres suites $(\lambda_n')_n$ et $(\mu_n')_n$ telles que $\lambda = (\lambda_n' \bmod_g(G_n))_n$ et $\mu = (\mu_n' \bmod_g(G_n))_n$ et l'on considère la suite $(\rho_n' \bmod_g(G_n))_n$ où $\rho_n' = \lambda_m\mu_n'$ pour $m \geq m_0(\mu_n')$. D'après ce qui précède et la condition $(\mathcal{C}_1)$, pour tout $n \geq 0$, il existe un indice $m \geq n$ assez grand tel que $\lambda_m\mu_n \equiv \rho_n \bmod_g(G_n)$ et $\lambda_m'\mu_n' \equiv \rho_n' \bmod_g(G_n)$ et $\mu_n \in \mathcal{N}_G(G_m)$. On a alors

$$(\lambda_m\mu_n)^{-1}(\lambda_m'\mu_n') = (\mu_n^{-1}[\lambda_m^{-1}\lambda_m']\mu_n)(\mu_n^{-1}\mu_n') \in (\mu_n^{-1}G_m\mu_n).G_n = G_m.G_n = G_n$$

Ainsi, $\rho_n \equiv \rho_n' \bmod_g(G_n)$ et la définition de $\lambda * \mu$ ne dépend donc pas du choix des suites $(\lambda_n)_n$ et $(\mu_n)_n$.

2/ L'élément ρ est bien élément de $\Pi(G)$. Posons

$$\begin{array}{ll} \rho_n = \lambda_{m_1}\mu_n & \text{avec } \mu_n \in \mathcal{N}_G(G_{m_1}) \\ \rho_{n+1} = \lambda_{m_2}\mu_{n+1} & \text{avec } \mu_{n+1} \in \mathcal{N}_G(G_{m_2}) \end{array}$$

en ayant choisi $m_2 \geq m_1$ (ce qui est possible d'après ce qui précède). On a $\lambda_{m_2}^{-1}\lambda_{m_1} \in G_{m_1}$ et donc

$$\rho_{n+1}^{-1}\rho_n = \mu_{n+1}^{-1}(\lambda_{m_2}^{-1}\lambda_{m_1})\mu_n = (\mu_{n+1}^{-1}\mu_n)(\mu_n^{-1}(\lambda_{m_2}^{-1}\lambda_{m_1})\mu_n) \in G_n G_{m_1} = G_n$$

3/ La loi $*$ est associative. Soient $\lambda, \mu, \nu \in \Pi(G)$. Ce qui précède montre que, pour tout $n \geq 0$, il existe des indices l et m assez grands et tels que

$$[(\lambda * \mu) * \nu]_n \bmod_g(G_n) = \lambda_l \mu_m \nu_n \bmod_g(G_n) = [\lambda * (\mu * \nu)]_n \bmod_g(G_n)$$

4/ La suite $(1 \bmod_g(G_n))_n \in \Pi(G)$ est visiblement un neutre bilatère pour $*$.

Le magma $(\Pi(G), *)$ est donc un monoïde que l'on appellera par la suite *la complétion projective du groupe G relativement à la filtration* $(G_n)_n$.

L'application naturel $G \longrightarrow \Pi(G)$ qui à $a \in G$ associe $(a \bmod_g(G_n))_n$ est visiblement un morphisme de monoïdes, donc de groupes si on le considère à valeurs dans son image. Le noyau de ce morphisme est égal à $\bigcap_n G_n = 1$. On dispose ainsi d'un plongement canonique du groupe G dans $\Pi(G)$:

$$\begin{array}{rccc} \pi_2 : & G & \longrightarrow & \Pi(G) \\ & x & \longmapsto & (x \bmod_g(G_n))_n \end{array}$$

Du point de vue topologique, si l'on muni chaque ensemble $(G/G_n)_g$ de la topologie discrète alors $\Pi(G)$ est un sous-espace fermé de $\prod_n (G/G_n)_g$ muni de la topologie produit. Pour cette topologie, l'ensemble $\Pi(G)$ est en fait métrisable[1], par exemple pour la distance δ définie pour $\lambda = (\lambda_n \bmod_g(G_n))_n$ et $\mu = (\mu_n \bmod_g(G_n))_n$ par

$$\delta(\lambda, \mu) = \exp(-\max\{n / \ \lambda_n \equiv \mu_n \bmod_g(G_n)\})$$

Théorème 1.— *L'application*

$$\begin{array}{rccc} \Psi : & \Pi(G) & \longrightarrow & \widehat{G} \\ & (\lambda_n \bmod_g(G_n))_n & \longmapsto & (\lambda_n)_n \bmod(\sim) \end{array}$$

est un isomorphisme de monoïdes qui est, par ailleurs, une isométrie d'espaces métriques et qui fait commuter le diagramme

$$\begin{tikzcd} & G \arrow[dl, "\pi_2"'] \arrow[dr, "\pi_1"] & \\ \Pi(G) \arrow[rr, "\Psi"] & & \widehat{G} \end{tikzcd}$$

Preuve : Considérons un élément $\lambda = (\lambda_n \bmod_g(G_n))_n \in \Pi(G)$. Puisque, par définition, pour tout $n \geq 1$ et tout $m \geq n$, on a $\lambda_n^{-1}\lambda_m \in G_n$, on voit que

$$d(\lambda_n, \lambda_m) \leq \exp(-n)$$

[1] De manière générale, si l'on considère un système projectif $(E_n, \varphi_n)_{n\in\mathbb{N}}$ d'espaces topologiques discrets avec des applications φ_n surjectives, alors E_n étant séparé et φ_n continue pour tout $n \geq 0$, la limite projective $E = \varprojlim_n E_n$ est alors un sous-espace fermé non vide de l'espace $\prod_n E_n$ muni de la topologie produit. La topologie induite sur E est alors métrisable, par l'application $d((a_n)_n, (b_n)_n) = \exp(-\max\{n / \ a_n = b_n\})$. En effet, la boule ouverte $B((a_n)_n, e^{-n})$ est égale à l'ouvert fondamental $\{a_0\} \times \cdots \times \{a_n\} \times \prod_{m>n} E_m \cap E$ et, réciproquement, si $U = U_0 \times \cdots \times U_n \times \prod_{m>n} E_m \cap E$ désigne un ouvert fondamental alors U est la réunion des boules $B((a_n)_n, e^{-n})$ où $(a_n)_n \in E$ vérifie $a_i \in U_i$ pour tout $i = 0, \cdots, n$.

et donc que la suite $(\lambda_n)_n$ est de Cauchy. Si l'on écrit maintenant $\lambda = (\lambda_n^{'} \bmod_g(G_n))_n$, on a alors $\lambda_n^{-1}\lambda_n^{'} \in G_n$ pour tout $n \geq 1$, si bien que $d(\lambda_n, \lambda_n^{'})$ ($\leq \exp(-n)$) tend vers 0 avec n et donc $(\lambda_n)_n \equiv (\lambda_n^{'})_n \bmod(\sim)$. L'application

$$\begin{array}{rccc} \Psi : & \Pi(G) & \longrightarrow & \widehat{G} \\ & (\lambda_n \bmod_g(G_n))_n & \longmapsto & (\lambda_n)_n \bmod(\sim) \end{array}$$

est donc définie de manière non équivoque. Montrons qu'elle est bijective :

Injectivité de Ψ : soient $(\lambda_n \bmod_g(G_n))_n, (\mu_n \bmod_g(G_n))_n \in \Pi(G)$ telles que les suites $(\lambda_n)_n$ et $(\mu_n)_n$ soient équivalentes dans G (i.e. $\lim_n d(\lambda_n, \mu_n) = 0$). Pour tout $n \geq 1$, il existe un indice $m_n \geq n$ tel que $d(\lambda_{m_n}, \mu_{m_n}) \leq \exp(-n)$ et l'on a donc $\lambda_{m_n}^{-1}\mu_{m_n} \in G_n$. Puisque l'on a pris le soin de prendre $m_n \geq n$, ceci implique que $\lambda_n^{-1}\mu_n = (\lambda_n^{-1}\lambda_{m_n})(\lambda_{m_n}^{-1}\mu_{m_n})(\mu_{m_n}^{-1}\mu_n) \in G_n$ pour tout $n \geq 1$ et ainsi, $(\lambda_n \bmod_g(G_n))_n = (\mu_n \bmod_g(G_n))_n$.

Surjectivité de Ψ : Considérons un élément $(\lambda_n)_n \bmod(\sim) \in \widehat{G}$. Puisque la suite $(\lambda_n)_n$ est de Cauchy, on peut construire une suite d'indices $n_1 < n_2 < \cdots < n_k < \cdots$ telle que, pour tout $k \geq 1$ et tout $n, m \geq n_k$ on ait $d(\lambda_n, \lambda_m) \leq \exp(-k)$. La suite $(\lambda_{n_k})_k$ est alors suite extraite de la suite de Cauchy $(\lambda_n)_n$. Elle est donc elle aussi Cauchy et vérifie $(\lambda_n)_n \bmod(\sim) = (\lambda_{n_k})_k \bmod(\sim)$. Puisque, pour tout $p \geq k$, on a $d(\lambda_{n_k}, \lambda_{n_p}) \leq \exp(-k)$, on a $\lambda_{n_k}^{-1}\lambda_{n_p} \in G_k$ et donc on a $(\lambda_{n_k} \bmod_g(G_k))_k \in \Pi(G)$. L'image par Ψ de cette dernière suite étant égale à $(\lambda_{n_k})_k \bmod(\sim) = (\lambda_n)_n \bmod(\sim)$, on en déduit que ψ est surjective.

Montrons maintenant que Ψ est bien un morphisme de monoïdes. Si $a = (a_n \bmod_g(G_n))_n$ et $b = (b_n \bmod_g(G_n))_n$ sont deux éléments de $\Pi(G)$ alors, par définition de la loi de composition interne $*$, il existe une suite extraite $(a_{m_n})_n$ telle que $a * b = (a_{m_n} b_n \bmod_g(G_n))_n$. Comme la suite $(a_n)_n$ est de Cauchy, la suite extraite $(a_{m_n})_n$ lui est équivalente et l'on a donc

$$\Psi(a * b) = (a_{m_n} b_n)_n \bmod(\sim) = (a_{m_n})_n \bmod(\sim)(b_n)_n \bmod(\sim) = (a_n)_n \bmod(\sim)(b_n)_n \bmod(\sim) = \Psi(a)\Psi(b)$$

Le fait que le diagramme du théorème soit commutatif découle immédiatement des définitions de π_1, π_2 et Ψ.

Reste finalement à montrer que Ψ est une isométrie. Si $\lambda = (\lambda_n \bmod_g(G_n))_n$ et $\mu = (\mu_n \bmod_g(G_n))_n$ alors

$$\delta(\lambda, \mu) = \exp(-\max\{n/\ \lambda_n \equiv \mu_n \bmod_g(G_n)\}) = \exp(-\max\{n/\ \mu_n^{-1}\lambda_n \in G_n\}) = d(\Psi(\lambda), \Psi(\mu))$$

□

Corollaire 2.— *Les espaces métriques isomètres $(\widehat{G}, \widehat{d})$ et $(\Pi(G), \delta)$ sont totalement discontinus et complets et l'on a l'équivalence*

$$\Pi(G) \text{ et } \widehat{G} \text{ sont compacts} \iff (G/G_n)_g \text{ est fini pour tout } n$$

Preuve : L'ensemble $\Pi(G)$ est un fermé de l'espace topologique produit $\prod_n (G/G_n)_g$. Si chaque $(G/G_n)_g$ est fini, en tant qu'espaces discrets ils sont donc tous compacts. Il en est donc de même du produit cartésien (théorème de Tykhonov) et finalement de $\Pi(G)$.

Réciproquement, chaque projection canonique $\Pi(G) \longrightarrow (G/G_n)_g$ étant surjective (ceci vient du fait que $x \bmod_g(G_{n+1}) \longmapsto x \bmod_g(G_n)$ est surjective pour tout n) et continue (conséquence de la propriété caractéristique de la topologie produit), si $\Pi(G)$ est compact alors $(G/G_n)_g$ est un espace topologique à la fois discret et compact, il est donc fini.

□

Remarque 3.— Il n'y a aucune raison *a priori* que la condition $(\mathcal{C}_0)$ entraine la condition $(\mathcal{C}_1)$. Pour autant, juste sous la condition $(\mathcal{C}_0)$, l'application Ψ continue d'exister entre les structures d'ensembles de $\Pi(G)$ et $\widehat{G}$, ce qui veut dire que l'on peut, dans tous les cas, conférer à $\Pi(G)$ une structure de monoïde même si de manière générale la loi de composition interne obtenue est moins évidente à décrire.

2.3.— Complétion procentrale. Lorsque le groupe G est de centre trivial et qu'on le filtre par une suite croissante $(P_n)_n$ de sous-groupes vérifiant $G = \bigcup_n P_n$, on peut alors considérer la suite $(G_n)_n$ définie pour $n \geq 0$ par $G_n = \mathscr{C}_G(P_n)$. Puisque $Z(G)$ est supposé trivial, on a bien $\bigcap_n G_n = 1$. Par ailleurs, la condition $G = \bigcup_n P_n$ montre que la condition $(\mathcal{C}_1)$ est vérifiée. On peut donc considérer la complétion projective du groupe G relativement à la filtration $(G_n)_n$. Le monoïde $(\Pi(G), *)$ ainsi obtenu est appelé la *complétion procentrale* de G relativement à la filtration croissante de sous-groupes $(P_n)_n$.

Remarque 4.— Dans ce §2, la condition initiale $\bigcap_n G_n = 1$ est imposée pour des raisons topologiques : cette hypothèse permet de conférer aux objets algébriques une structure d'espace métrique. Pour autant, la définition de complétion projective a bien un sens lorsque $I = \bigcap_n G_n \neq 1$, ainsi que la structure de monoïde que l'on y définit. Dans cette situation plus générale, le noyau de l'application naturelle $G \longrightarrow \Pi(G)$ vaut précisément I et l'on voit donc que c'est G/I qui se plonge canoniquement dans $\Pi(G)$. On remarque qu'alors I est nécessairement normal dans G, ce qui montre que la condition $(\mathcal{C}_0)$ ne peut pas à elle seule entrainer $(\mathcal{C}_1)$. Dans ce cadre plus général, la notion de complétion procentrale existe bien et l'on voit que $I = Z(G)$. Ceci explique le choix de cette terminologie.

3.— Extensions steiniziennes filtrées.

3.1.— Généralités.

Définition 5.— *On dira d'une extension de corps H/K qu'elle possède la "propriété de relèvement des isomorphismes", ou "propriété de Steiniz", ou encore qu'elle est "steinizienne" si pour tout corps intermédiaire $H/L/K$ et tout K-isomorphisme $\sigma \in \mathrm{Isom}_K(L,H)$ il existe un relevé $\widetilde{\sigma} \in \mathrm{End}_K(H)$ de σ à H.*

Exemples 6.— a) Pour tout corps commutatif k, l'extension $\overline{k}/k$ est steinizienne. Ce résultat n'est rien d'autre que le théorème éponyme de Steiniz.

b) Si H désigne une k-algèbre à division[2], alors l'extension H/k est steinizienne. C'est une conséquence du théorème de Skolem-Noether.

c) Les extensions extérieures, algébriques et galoisiennes de corps sont steiniziennes. C'est un des points clés de la théorie de Galois et du théorème de Krull-Jacobson.

d) Une extension galoisienne (au sens général d'Artin), même dans le cas commutatif, n'est pas toujours steinizienne. Par exemple, l'extension $k(t)/k$ avec k commutatif infini, bien que galoisienne, ne vérifie pas la propriété de Steiniz en vertu de la proposition qui suit.

Proposition 7.— *Si une extension H/K est steinizienne alors* $\mathrm{End}_K(H) = \mathrm{Aut}(H/K)$.

Preuve : Soit $\sigma \in \mathrm{End}_K(H)$ et $L = \sigma(H)$. La réciproque $\sigma^{-1} : L \longrightarrow H$ est un K-isomorphisme et se relève donc à H tout entier en un élément $\tau \in \mathrm{End}_K(H)$. Puisque $\sigma^{-1}(L) = H$, on en déduit que $\tau(H) = H = \tau(L)$ et si $L \neq H$ alors τ ne peut plus être injectif. Ainsi, $L = H$ et $\sigma \in \mathrm{Aut}(H/K)$.

□

e) Une extension steinizienne, même finie, n'est pas nécessairement galoisienne. C'est, par exemple, le cas de l'extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Définition 8.— *On appellera "extension steinizienne filtrée" toute extension H/K telle qu'il existe une suite*

[2] En accord avec la terminologie introduite dans [Des], on rappelle qu'une k-algèbre à division est un corps de dimension finie sur son centre k. Autrement dit, les k-algèbres à division sont les k-algèbres simples centrales qui sont des corps.

croissante $(H_n)_n$ d'extensions intermédiaires vérifiant les hypothèses suivantes :

$(\mathcal{P}_0)$ *$H = \bigcup_n H_n$.*

$(\mathcal{P}_1)$ *H_n/K est de type fini.*

$(\mathcal{P}_2)$ *H_n/K vérifie la propriété de Steiniz.*

$(\mathcal{P}_3)$ *Il existe un sous-groupe Γ du groupe $\mathrm{Aut}(H/K)$ relevant les groupes $\Gamma_n = \mathrm{Aut}(H_n/K)$ de la manière suivante :*

a) Pour tout $n \geq 0$ et tout $\sigma_n \in \Gamma_n$ il existe $\sigma \in \Gamma$ tel que $\sigma_{|H_n} = \sigma_n$.

b) Pour tout $\sigma \in \Gamma$, il existe une infinité d'indices $n \geq 0$ tels $\sigma_{|H_n} \in \Gamma_n$.

On pourra préciser que H/K est l'extension steinizienne filtrée par la suite $(H_n)_n$ et le sous-groupe Γ.

Remarque 9.— La propriété $(\mathcal{P}_2)$ permet de construire des applications $\varphi_n : \mathrm{Aut}(H_n/K) \longrightarrow \mathrm{Aut}(H_{n+1}/K)$ telles que $\mathrm{res}_n \circ \varphi_n = \mathrm{Id}$, où $\mathrm{res}_n : \mathrm{Aut}(H_{n+1}/K) \longrightarrow \mathrm{Isom}_K(H_n, H)$ désigne la restriction des applications à H_n. Le système inductif $(\Gamma_n, \varphi_n)_n$ produit, par passage à la limite directe, un ensemble $\Gamma = \varinjlim_n \Gamma_n$ qui s'injecte dans le groupe $\mathrm{Aut}(H/K)$ de la manière suivante : un élément de $\sigma \in \varinjlim_n \Gamma_n = \bigsqcup_n \Gamma_n \big/ \sim$ est représenté par un certain élément de Γ_n pour un certain indice $n \geq 0$. On note abusivement σ ce représentant. Pour tout $x \in H$, il existe $m \geq n$ tel que $x \in H_m$ et l'on pose alors $\widetilde{\sigma}(x) = \varphi_{n,m}(\sigma)(x)$ où $\varphi_{n,m} = \varphi_{m-1} \circ \varphi_{m-2} \circ \cdots \circ \varphi_n$. On voit que la définition de $\widetilde{\sigma}(x)$ ne dépend que de x (et non de m ou du représentant de σ) et que $\widetilde{\sigma}$ est bien un élément de $\mathrm{Aut}(H/K)$. Cette correspondance est bien injective, car si $\sigma \in \Gamma_n$ et $\tau \in \Gamma_m$ (avec $m \geq n$) sont tels que $\widetilde{\sigma} = \widetilde{\tau}$ alors, en particulier, pour tout $x \in H_m$, on a $\tau(x) = \varphi_{n,m}(\sigma)(x)$, c'est-à-dire $\varphi_{n,m}(\sigma) = \tau$ et donc $\sigma \sim \tau$.

L'ensemble Γ vérifie visiblement les conditions $(\mathcal{P}_3.a, b)$. Nonobstant, rien n'assure que Γ soit un sous-groupe. Une manière de palier à cela consiste à considérer la propriété

Pour tout $n \geq 0$, il existe un monomorphisme de groupes $\varphi_n : \Gamma_n \longrightarrow \Gamma_{n+1}$ tel que $\mathrm{res}_n \circ \varphi_n = \mathrm{Id}$.

propriété qui implique bien la propriété $(\mathcal{P}_3)$ puisqu'alors $\varinjlim_n \Gamma_n$ devient naturellement un sous-groupe de $\mathrm{Aut}(H/K)$. Pour autant, le caractère morphique des applications φ_n n'est pas forcément nécessaire au fait que Γ soit un sous-groupe[3].

Exemples 10.— a) On considère une extension algébrique galoisienne extérieure H/K de corps telle que H soit filtrée par une suite croissante d'extensions galoisiennes finies H_n/K. L'extension H/K est alors une extension steinizienne filtrée par la suite $(H_n)_n$ et n'importe quel sous-groupe $\Gamma \subset \mathrm{Gal}(H/K)$ qui soit dense pour la topologie de Krull-Jacobson. En effet, dans cette situation, la théorie de Galois est exactement la même que lorsque les corps sont supposés commutatifs. On sait donc que $\mathrm{Gal}(H/K)$ est un groupe profini qui s'identifie à la limite inverse $\varprojlim_n \mathrm{Gal}(H_n/K)$ et l'hypothèse de densité faite sur Γ assure alors que la projection $\Gamma \longrightarrow \mathrm{Gal}(H_n/K)$ est un épimorphisme de groupes pour tout $n \geq 0$.

b) (Z-extensions intérieures filtrées) On fixe un corps commutatif k et l'on considère une suite croissante $(H_n)_n$ de k-algèbres à division. Si l'on pose $H = \bigcup_n H_n$ alors, l'extension H/k a une structure naturelle d'extension steinizienne filtrée en considérant le sous-groupe $\Gamma = \mathrm{Int}(H/k) \leq \mathrm{Aut}(H/k)$. En effet, comme nous l'avons rappelé, l'extension H_n/k est bien steinizienne. Par ailleurs, d'après le théorème de Skolem-Noether, pour tout $n \geq 0$ on a $\mathrm{Aut}(H_n/K) = \mathrm{Gal}(H_n/K) = \mathrm{Int}(H_n/K)$ et ce groupe se plonge tout à fait naturellement dans $\mathrm{Aut}(H/K)$ et l'on voit alors que le groupe $\Gamma = \mathrm{Int}(H/K) = \bigcup_n \mathrm{Int}(H_n/K)$

[3]Par exemple, on considère pour un nombre premier $p \geq 3$ fixé, la $\mathbb{Z}_p$-extension $H/\mathbb{Q}$ que l'on filtre par la suite $H_n = H^{p^n \mathbb{Z}_p}$. On a $\Gamma_n = \mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$ et $\mathrm{Gal}(H/\mathbb{Q}) = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. Pour $n \geq 0$, on considère l'application de relèvement $\varphi_n : \mathrm{Gal}(H_n/\mathbb{Q}) = \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathrm{Gal}(H_{n+1}/\mathbb{Q}) = \mathbb{Z}/p^{n+1}\mathbb{Z}$ définie, pour $a = 0, \cdots, (p^n - 1)/2$, par $\varphi_n(a \bmod (p^n)) = a \bmod (p^{n+1})$ et $\varphi_n((p^n - a) \bmod (p^n)) = (p^{n+1} - a) \bmod (p^{n+1})$. On constate que la limite directe, $\Gamma = \varinjlim_n \mathbb{Z}/p^n\mathbb{Z}$, du système inductif $(\Gamma_n, \varphi_n)_n$, s'injecte dans $\mathrm{Gal}(H/\mathbb{Q}) = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ et que l'image de cette injection est un sous-groupe (dense) isomorphe à $\mathbb{Z}$. (On pourra consulter [DS] pour plus de détails sur les systèmes inductifs extraits de systèmes projectifs.)

joue le rôle attendu dans la définition d'extension steinizienne filtrée. Plus généralement, il a été démontré dans [Des] la généralisation du théorème de Skolem-Noether au cas des extensions galoisiennes, intérieures, finies et centrales. Ainsi, si K désigne un corps commutatif ou non et $(H_n)_n$ une suite croissante d'extensions galoisiennes, intérieures, finies et centrales de K, alors l'extension H/K a une structure naturelle d'extension steinizienne filtrée en considérant le sous-groupe $\Gamma = \mathrm{Int}(H/K) \leq \mathrm{Aut}(H/K)$.

3.2.— Monoïde des endomorphismes. Dans toute la suite de ce texte, on reprend les notations des § précédents et l'on considère H/K une extension steinizienne filtrée par une suite $(H_n)_n$ et un sous-groupe $\Gamma \subset \mathrm{Aut}(H/K)$. Pour tout indice $n \geq 0$, on considère le sous-groupe $\widetilde{\Gamma_n} = \Gamma \cap \mathrm{Aut}(H/H_n)$. On a alors

Lemme 11.— *La suite $(\widetilde{\Gamma_n})_n$ est décroissante et vérifie $\bigcap_n \widetilde{\Gamma_n} = 1$ et l'on a, en outre, la propriété suivante*

$$\forall \sigma \in \Gamma,\ \forall n \geq 0, \exists m \geq n,\ \widetilde{\Gamma_m} \subset \sigma \widetilde{\Gamma_n} \sigma^{-1}$$

Preuve : La propriété $(\mathcal{P}_3.b)$ assure qu'il existe $m \geq n$ tel que $\sigma_{|H_m} \in \Gamma_m$. On a alors $\sigma^{-1}\widetilde{\Gamma_m}\sigma \subset \widetilde{\Gamma_m} \subset \widetilde{\Gamma_n}$.

□

Le choix $G = \Gamma$ dans le §2.1 assure qu'il existe une et une seule topologie sur Γ qui confère à ce groupe la structure de groupe topologique et pour laquelle $(\widetilde{\Gamma_n})_n$ est une base de filtre de voisinages de l'unité. Cette topologie est (ultra)métrisable, par l'application

$$d(\sigma, \tau) = \exp(-\max(n \geq 0 / \ \sigma^{-1}\tau \in \widetilde{\Gamma_n}))$$

pour laquelle on peut donc considérer le complété $(\widehat{\Gamma}, \widehat{d})$ de Γ pour d.

Lemme 12.— *On considère un élément $\sigma \in \mathrm{End}_K(H)$.*

a) Pour tout $n \geq 0$, il existe $\sigma_n \in \Gamma$ tel que $\sigma_{|H_n} = \sigma_{n|H_n}$.

b) Si $(\sigma_n)_n$ désigne une suite d'éléments de Γ vérifiant $\sigma_{|H_n} = \sigma_{n|H_n}$ pour tout n, alors cette suite est de Cauchy.

c) Si $(\sigma_n)_n$ et $(\sigma_n^{'})_n$ désignent deux suites vérifiant $\sigma_{|H_n} = \sigma_{n|H_n} = \sigma^{'}_{n|H_n}$ pour tout n, alors $(\sigma_n)_n \sim (\sigma_n^{'})_n$.

Preuve : a) Par l'hypothèse $\mathcal{P}_1$ l'extension H_n/K est de type fini, il en est donc de même de $\sigma(H_n)/K$. Puisque H est la réunion des H_n, il existe donc $m \geq n$ tel que $H_n \cup \sigma(H_n) \subset H_m$. La propriété de Steiniz montre alors qu'il existe $\sigma_n \in \Gamma_m$ tel que $\sigma_{|H_n} = \sigma_{n|H_n}$. La propriété $(\mathcal{P}_3.a)$ fournit alors un relevé à Γ de σ_n.

b) Puisque $\sigma_{n+1|H_n} = \sigma_{n|H_n}$ on a $\sigma_n^{-1}\sigma_{n+1} \in \widetilde{\Gamma_n}$ et donc $d(\sigma_n, \sigma_{n+1}) \leq e^{-n}$. La suite $(d(\sigma_n, \sigma_{n+1}))_n$ converge donc vers 0 ce qui assure que $(\sigma_n)_n$ est de Cauchy (puisque d est ultramétrique).

c) De même, si l'on a $\sigma_{n|H_n} = \sigma^{'}_{n|H_n}$ alors $\sigma_n^{-1}\sigma_n^{'} \in \widetilde{\Gamma_n}$ et donc $d(\sigma_n, \sigma_n^{'}) \leq e^{-n} \longrightarrow 0$ ce qui justifie bien que $(\sigma_n)_n \sim (\sigma_n^{'})_n$.

□

Le lemme 12 permet alors de définir de manière non équivoque une application

$$\begin{array}{cccc} \Theta : & \mathrm{End}_K(H) & \longrightarrow & \widehat{\Gamma} \\ & \sigma & \longmapsto & (\sigma_n)_n \bmod(\sim) \end{array}$$

où $(\sigma_n)_n$ est un représentant de la classe $(\sigma_n)_n \bmod(\sim)$ qui vérifie que $\sigma_{n|H_n} = \sigma_{|H_n}$ pour tout $n \geq 0$.

Théorème 13.— *L'application Θ est un isomorphisme de monoïdes.*

Preuve : Injectivité. Considérons $\sigma, \tau \in \mathrm{End}_K(H)$ tels que $\Theta(\sigma) = \Theta(\tau)$ et fixons un indice $m_0 \geq 0$. Puisque $(\sigma_n)_n$ mod($\sim$) = $(\tau_n)_n$ mod($\sim$) il existe un indice $m \geq m_0$ tel que $d(\sigma_m, \tau_m) \leq e^{-m_0}$ et l'on a alors $\sigma_{|H_{m_0}} = \sigma_{m|H_{m_0}} = \tau_{m|H_{m_0}} = \tau_{|H_{m_0}}$. Puisque m_0 est quelconque et que $H = \bigcup_{m_0} H_{m_0}$, on en déduit finalement que $\sigma = \tau$.

Surjectivité. Etant donné $(\sigma_n)_n$ mod($\sim$) $\in \widehat{\Gamma}$, la propriété de Cauchy permet d'affirmer que, pour tout entier k, il existe un rang n_k tel que, pour tout $n \geq n_k$, $d(\sigma_n, \sigma_{n_k}) \leq e^{-k}$, c'est-à-dire que $\sigma_{n|H_k} = \sigma_{n_k|H_k}$. On peut bien sur choisir une suite d'indice $(n_k)_k$ qui soit strictement croissante quand k varie. Etant donné un élément $x \in H$, il existe k tel que $x \in H_k$ et l'on pose alors

$$\sigma(x) = \sigma_{n_k}(x)$$

Cette définition est non équivoque car si $x \in H_{k'}$ avec $k' > k$ alors, puisque $n_{k'} > n_k$, on a $\sigma_{n_{k'}}(x) = \sigma_{n_k}(x)$. Puisque chaque σ_{n_k} est un K-automorphisme, on voit sans mal que σ est un K-endomorphisme. On a alors $\Theta(\sigma) = (\sigma_{n_k})_k$ mod($\sim$) et, comme $(\sigma_{n_k})_k$ est une suite extraite de $(\sigma_n)_n$ et que cette suite est de Cauchy, on a $(\sigma_{n_k})_k \sim (\sigma_n)_n$, c'est-à-dire que $\Theta(\sigma) = (\sigma_n)_n$ mod($\sim$).

Caractère morphique : posons $\Theta(\sigma) = (\sigma_n)_n$ mod($\sim$), $\Theta(\tau) = (\tau_n)_n$ mod($\sim$) et $\Theta(\sigma\tau) = ((\sigma\tau)_n)_n$ mod($\sim$). Pour un indice $h \geq 0$ quelconque fixé, la propriété $(\mathcal{P}_3.b)$ assure qu'il existe $N \geq h$ tel que $\tau_{h|H_N} \in \Gamma_N$. Pour $n \geq N$ et $x \in H_h$, puisque $x \in H_h \subset H_N \subset H_n$, on a $\tau(x) \in H_N$ et l'on peut donc écrire

$$\sigma_n(\tau_n(x)) = \sigma_n(\tau_h(x)) = \sigma_n(\tau(x)) = \sigma(\tau(x)) = (\sigma\tau)_n(x)$$

Ainsi, pour tout $h \geq 0$, il existe un rang N tel que pour tout $n \geq N$, $d(\sigma_n\tau_n, (\sigma\tau)_n) \leq e^{-h}$. On a donc $(\sigma_n\tau_n)_n \equiv ((\sigma\tau)_n)_n$ mod($\sim$), c'est-à-dire $\Theta(\sigma\tau) = \Theta(\sigma)\Theta(\tau)$.

□

L'isomorphisme Θ confère donc à $\mathrm{End}_K(H)$ une structure d'espace (ultra)métrique complet pour la distance $\vartriangle$ obtenue par Θ-isométrie à la distance $\widehat{d}$ induite par complétion sur $\widehat{\Gamma}$. La distance $\vartriangle$ est en fait définie, pour $\sigma, \tau \in \mathrm{End}_K(H)$, par

$$\vartriangle(\sigma, \tau) = \exp(-\max\{n \geq 0 / \ \sigma_{|H_n} = \tau_{|H_n}\})$$

Proposition 14.— *Si les extensions H_n/K sont finies et si le monoïde* $\mathrm{End}_K(H)$ *est compact, alors l'extension H/K a la propriété de Steiniz. En particulier, dans cette situation, on a* $\mathrm{End}_K(H) = \mathrm{Aut}(H/K)$.

Preuve : On considère un corps intermédiaire $H/L/K$ et, pour tout $n \geq 0$, on pose $L_n = L \cap H_n$. Puisque H_n/K est supposée finie, il en est de même[4] de L_n/K et, par suite, si l'on se donne un $\sigma \in \mathrm{Isom}_K(L, H)$ alors il existe $m \geq n$ tel que $\sigma(L_n) \subset H_m$. Puisque H_m/K a la propriété de Steiniz, le K-isomorphisme $\sigma_{|L_n} \in \mathrm{Isom}_K(L_n, H)$ se relève dans $\mathrm{Aut}(H_m/K)$ et donc finalement dans $\Gamma \subset \mathrm{End}_K(H)$. Ainsi, pour tout $n \geq 0$, l'ensemble

$$F_n = \{\tau \in \mathrm{End}_K(H) / \ \tau_{|L_n} = \sigma_{|L_n}\}$$

est non vide. Il s'agit d'un ensemble fermé : si $\tau_0 \notin F_n$ alors $\tau \notin F_n$ pour tout $\tau \in \mathrm{End}_K(H)$ tel que $\tau_{|H_n} = \tau_{0|H_n}$. On a donc $F_n \cap B(\tau_0, e^{-n}) = \emptyset$ et le complémentaire de F_n voisine donc tous ses points. Si l'on suppose $\mathrm{End}_K(H)$ compact alors le théorème des fermés emboités montre que $\bigcap_n F_n$ est un ensemble non vide. Tout élément de cette intersection est alors un relevé de σ à H tout entier.

□

Pour pouvoir utiliser les théorèmes 1 et 13 et confondre $(\mathrm{End}_K(H), \circ, \vartriangle)$ et $(\widehat{\Gamma}, ., d)$ à la complétion projective $(\Pi(\Gamma), *, \delta)$ relative à la filtration $(\widetilde{\Gamma_n})_n$, il faut vérifier que la condition $(\mathcal{C}_1)$ est satisfaite. C'est bien le cas : si, pour $n \geq 0$, on considère le sous-groupe

$$\Omega_n = \{\sigma \in \Gamma / \ \sigma_{|H_n} \in \Gamma_n\}$$

[4]Cet argument ne fonctionne *a priori* pas si l'on suppose juste H_n/K de type fini.

et, d'après ($\mathcal{P}_{3.b}$), tout élément $\sigma \in \Gamma$ appartient à une infinité de $\Omega_n \subset \mathcal{N}_\Gamma(\widetilde{\Gamma_n})$. En conclusion, nous venons de montrer que

Théorème 15.— *Le monoïde* $\mathrm{End}_K(H)$ *des* K*-endomorphismes d'une extension* H/K *steinizienne filtrée par une suite* $(H_n)_n$ *et un sous-groupe* Γ *s'identifie à la complétion projective de* Γ *relativement à la filtration* $(\Gamma \cap \mathrm{Aut}(H/H_n))_n$.

3.3.— Le théorème de Krull-Jacobson. On considère une extension algébrique galoisienne extérieure H/K qui est filtrée par une suite croissante d'extensions galoisiennes finies H_n/K (le fait d'être dénombrablement filtré est équivalent à dire que le groupe profini $\mathrm{Gal}(H/K)$ est de rang topologique dénombrable). Si Γ désigne n'importe quel sous-groupe de $\mathrm{Gal}(H/K)$ dense pour la topologie Krull-Jacobson alors la théorie de Galois assure que l'extension H/K est steinizienne filtrée. La topologie induite sur Γ par le §2.1 est exactement la topologie de Krull-Jacobson et ce qui précède montre que $\mathrm{End}_K(H)$ s'identifie au complété de Γ. La proposition 7 assure que l'on a l'égalité $\mathrm{End}_K(H) = \mathrm{Gal}(H/K)$ puisque l'extension H/K est elle aussi steinizienne. On retrouve ainsi la partie structurelle du théorème de Krull-Jacobson : le groupe topologique $\mathrm{Gal}(H/K)$ s'identifie au complété de Γ qui s'identifie à la limite projective $\varprojlim_n \mathrm{Gal}(H_n/K)$. On remarquera que le corollaire 2 prédisait déjà que le groupe $\mathrm{Gal}(H/K)$ était profini.

La conclusion de ce § est que la théorie des extensions steiniziennes filtrées appliquée aux classiques extensions algébriques galoisiennes extérieures permet de redonner la structure du groupe de Galois établie dans le théorème de Krull-Jacobson.

3.4.— Application aux Z-extensions intérieures filtrées. Nous allons maintenant mettre à profit les travaux présentés dans [Des] à la situation suivante :

Définition 16.— *On dira d'une extension de corps* H/K *que c'est une "*Z*-extension intérieure filtrée" si* H *est la réunion d'une suite croissante de sous-extensions* H_n *telles que* H_n/K *soit une extension galoisienne intérieure finie et centrale pour tout* $n \geq 0$.

Comme esquissé dans l'introduction, ces extensions jouent un rôle analogue, dans le cas intérieur, au rôle tenu par les extensions algébriques galoisiennes extérieures du théorème de Krull-Jacobson. Du point de vue arithmétique, on a en effet

Proposition 17.— *Toute* Z*-extension intérieure filtrée* H/K *est algébrique, galoisienne et centrale (i.e.* $Z(H) = Z(K)$*). Le sous-groupe* $\mathrm{Int}(H/K)$ *est "dense" dans* $\mathrm{Gal}(H/K)$ *(i.e.* $H^{\mathrm{Int}(H/K)} = K$*).*

Preuve : Si $x \in H$, alors il existe un indice $n \geq 0$ tel que $x \in H_n$. Puisque $[H_n : K]$ est finie, il en est de même de $[K(x) : K]$ (les dimensions droite et gauche coïncident ici car l'extension H_n/K est supposée galoisienne). Ceci montre que H/K est algébrique.

Le caractère galoisien de H/K découle du fait (plus fort) que $H^{\mathrm{Int}(H/K)} = K$: si $x \in H$ est invariant par $\mathrm{Int}(H/K)$ il l'est par $\mathrm{Int}(H_n/K)$ pour tout $n \geq 0$. Comme $x \in H_n$ pour un certain indice n et que H_n/K est galoisienne intérieure, on a donc $x \in K$.

Si $x \in Z(H)$ alors, comme $x \in H_n$ pour un certain indice n, on a $x \in Z(H_n) = Z(K)$ et donc $Z(H) \subset Z(K)$. Réciproquement, comme tout élément de $Z(K)$ commute avec tout élément de H_n pour tout $n \geq 0$ et que $H = \bigcup_n H_n$ on en déduit que $Z(K) \subset Z(H)$.

□

Les Z-extension intérieure filtrée peuvent se décomposer grâce à une suite de $Z(K)$-algèbres à division :

Proposition 18.— (Décomposition en produit d'algèbres à division) *Soit* H/K *une* Z*-extension intérieure filtrée par une suite* $(H_n)_n$. *Il existe une suite* $(K_n)_n$ *de* $Z(K)$*-algèbres à division et, pour tout* $n \geq 1$, *des* K*-isomorphismes* $\varphi_n : H_n \longrightarrow K \otimes_{Z(K)} K_1 \otimes_{Z(K)} \cdots \otimes_{Z(K)} K_n$ *faisant commuter les diagrammes*

$$\begin{array}{ccc} H_{n+1} & \xrightarrow{\varphi_{n+1}} & K \otimes_{Z(K)} K_1 \otimes_{Z(K)} \cdots \otimes_{Z(K)} K_{n+1} \\ \uparrow \subset & & \uparrow x_1\otimes\cdots\otimes x_n \mapsto x_1\otimes\cdots\otimes x_n\otimes 1 \\ H_n & \xrightarrow{\varphi_n} & K \otimes_{Z(K)} K_1 \otimes_{Z(K)} \cdots \otimes_{Z(K)} K_n \end{array}$$

de sorte que, pour tout $m \geq 0$, H est K-isomorphe au corps $\varinjlim_{n\geq m} H_m \otimes_{Z(K)} K_m \otimes_{Z(K)} \cdots \otimes_{Z(K)} K_n$.

Preuve : D'après [Des, corollaire 15.b] on sait que H_{n-1} décompose H_n et que l'on dispose d'un K-isomorphismes $\varphi_n : H_n \longrightarrow H_{n-1} \otimes_{Z(K)} \mathscr{C}_{H_n}(H_{n-1})$ naturel. Les corps $K_n = \mathscr{C}_{H_n}(H_{n-1})$, qui sont bien des $Z(K)$-algèbres à division (cf [Des, proposition 7 et définition-notation 9]), fournissent alors la suite recherchée.

□

Théorème 19.— *Si H/K désigne une Z-extension intérieure filtrée par une suite $(H_n)_n$ alors l'extension H/K est une extension steinizienne filtrée par la suite $(H_n)_n$ et le sous-groupe $\mathrm{Int}(H/K)$.*

En particulier, le monoïde $\mathrm{End}_K(H)$ est isomorphe à la complétion procentrale du groupe $\mathrm{Int}(H/K)$ relativement à la filtration $(\mathrm{Int}(H_n/K))_n$:

$$\mathrm{End}_K(H) \simeq \varprojlim_n (\mathrm{Int}(H/K)/\mathrm{Int}(H/H_n))_g$$

Preuve : Les propriétés $(\mathcal{P}_{0,1})$ sont immédiatement vérifiées. La propriété $(\mathcal{P}_2)$ découle de la généralisation du théorème de Skolem-Noether [Des, théorème 14] et enfin, $(\mathcal{P}_3)$ découle du fait que $\mathrm{Int}(H_n/K)$ s'injecte canoniquement dans $\mathrm{Int}(H/K)$. L'extension H/K est donc bien steinizienne filtrée par la suite $(H_n)_n$ et le sous-groupe $\mathrm{Int}(H/K)$.

Avec les notations des § précédents, on pose

- $G = \Gamma = \mathrm{Int}(H/K) = \{I(x)/\ x \in \mathscr{C}_H(K)^*\}$,
- $P_n = \Gamma_n = \mathrm{Int}(H_n/K) = \left\{I(\alpha)/\ \alpha \in \mathscr{C}_{H_n}(K)^*\right\}$ (on identifie canoniquement $\mathrm{Int}(H_n/K)$ dans $\mathrm{Int}(H/K)$ en regardant l'automorphisme intérieur $I(\alpha)$ de H_n comme automorphisme intérieur de H),
- $G_n = \widetilde{\Gamma_n} = \mathrm{Int}(H/K) \cap \mathrm{Aut}(H/H_n) = \mathrm{Int}(H/H_n) = \{I(x)/\ \beta \in \mathscr{C}_H(H_n)^*\}$,

Puisque la suite $(P_n)_n$ est croissante, que $\bigcup_n P_n = \Gamma$ et que $P_n \subset \mathscr{N}_\Gamma(\widetilde{\Gamma_n})$, on voit que la condition $(\mathcal{C}_1)$ est satisfaite. Le théorème 15 assure alors que $\mathrm{End}_K(H)$ est isomorphe à la complétion projective du groupe $\mathrm{Int}(H/K)$ relativement à la filtration $(\mathrm{Int}(H/H_n))_n$. Pour voir que cette complétion est la complétion procentrale de $\mathrm{Int}(H/K)$ relativement à la filtration $(\mathrm{Int}(H_n/K))_n$, il faut montrer en plus les deux points suivants :

- $\mathrm{Int}(H/H_n) = \mathscr{C}_{\mathrm{Int}(H/K)}(\mathrm{Int}(H_n/K))$: l'inclusion $\mathrm{Int}(H/H_n) \subset \mathscr{C}_{\mathrm{Int}(H/K)}(\mathrm{Int}(H_n/K))$ est claire : si $\alpha \in \mathscr{C}_{H_n}(K)^*$ et $\beta \in \mathscr{C}_H(H_n)^*$ alors $\alpha\beta = \beta\alpha$ et donc, pour tout $x \in H$, $I(\alpha) \circ I(\beta)(x) = \alpha\beta x\beta^{-1}\alpha^{-1} = \beta\alpha x\alpha^{-1}\beta^{-1} = I(\beta) \circ I(\alpha)(x)$.

Réciproquement, considérons un élément $\alpha \in \mathscr{C}_H(K)^*$ tel que $I(\alpha) \in \mathscr{C}_{\mathrm{Int}(H/K)}(\mathrm{Int}(H_n/K))$. Pour tout $a \in \mathscr{C}_{H_n}(K)^*$ on a donc $I(\alpha a\alpha^{-1}a^{-1}) = \mathrm{Id}$ et il existe ainsi $\lambda(a) \in Z(H)$ tel que $\alpha a\alpha^{-1} = \lambda(a)a$. Pour $a \neq -1$, on peut alors écrire

$$\lambda(a+1)a\alpha + \lambda(a+1)\alpha = \lambda(a+1)(a+1)\alpha = \alpha(a+1) = \alpha a + \alpha = \lambda(a)a\alpha + \alpha$$

ce qui assure que $(\lambda(a+1) - \lambda(a))a = (1 - \lambda(a+1))$. Si $a \notin Z(H)$, on a nécessairement $(\lambda(a+1) - \lambda(a)) = (1-\lambda(a+1)) = 0$ c'est-à-dire $\lambda(a) = \lambda(a+1) = 1$. Si $a \in Z(H)$ alors l'égalité $\alpha a\alpha^{-1} = \lambda(a)a$ implique que dans ce cas aussi $\lambda(a) = 1$. Ceci montre finalement que $\alpha a = a\alpha$, pour tout $a \in \mathscr{C}_{H_n}(K)^* \cup K$. Maintenant, comme rappelé dans la preuve de la proposition 18, K décompose H_n c'est-à-dire que $H_n = K \otimes_{Z(K)} \mathscr{C}_{H_n}(K)$ et l'on en déduit finalement que $\alpha a = a\alpha$, pour tout $a \in H_n$: $I(\alpha) \in \mathrm{Int}(H/H_n)$.

• $Z(\mathrm{Int}(H/K)) = 1$: ce point découle immédiatement du précédent car $\mathrm{Int}(H/K) = \bigcup_n \mathrm{Int}(H_n/K)$ et donc

$$Z(\mathrm{Int}(H/K)) = \mathscr{C}_{\mathrm{Int}(H/K)}\left(\bigcup_n \mathrm{Int}(H_n/K)\right) = \bigcap_n \mathscr{C}_{\mathrm{Int}(H/K)}(\mathrm{Int}(H_n/K)) = \bigcap_n \mathrm{Int}(H/H_n) = \mathrm{Int}(H/H) = 1$$

Bibliographie

[Bou] Nicolas Bourbaki, *Éléments de mathématique. Topologie générale. Chapitres 5 à 10.*, Hermann, Paris, 1974.

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

[DS] Bruno Deschamps et Ivan Suarez Atias, *Prographes sylvestres et groupes profinis presque libres*, Math. Ann. 350, no. 2, 475-495 (2011).

[Des] Bruno Deschamps, *Arithmétique des extensions intérieures*, à paraître dans Journal of Algebra.

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

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