De l'instabilité des extensions galoisiennes intermédiaires

Bruno DESCHAMPS & Paul RODRIGUEZ

Résumé.— Grâce à une généralisation du théorème de Brauer-Cartan-Hua, nous montrons qu'à l'exacte contraire du cas extérieur, quand on dispose d'une extension galoisienne, finie, intérieure et concentrique alors aucune extension galoisienne intermédiaire stricte n'est stable par l'action du groupe de Galois.

Abstract.— Thanks to a generalization of the Brauer-Cartan-Hua theorem, we show that, to the exact opposite of the outer case, when we take a concentric finite inner Galois extension there exists no strict intermediate Galois extension invariant under the action of the Galois group.

Notations : Si H désigne un corps, et $a \in H^*$, on notera $I(a) : x \longmapsto axa^{-1}$ l'automorphisme intérieur associé à l'élément a. Si $\Omega \subset H^*$, on notera $\mathrm{Int}(\Omega) = \{I(a)/\ a \in \Omega\}$. Pour toute extension de corps H/K, on notera $\mathrm{Int}(H/K)$ l'ensemble des K-automorphismes intérieurs de H et $\widetilde{K} = \{x \in H/\ \forall y \in K,\ xy = yx\}$ le commutant (ou centralisateur) de K dans H. On remarquera alors que $\mathrm{Int}(H/K) = \mathrm{Int}(\widetilde{K}^*)$.

*
* *

La théorie de Galois généralisée aux corps gauches[1] n'est pas bien plus compliquée que celle du cas des corps commutatifs. Il faut juste prêter attention aux automorphismes intérieurs. Essentiellement, pour une extension galoisienne H/K finie, les correspondances galoisiennes s'opèrent entre l'ensemble des extensions intermédiaires de H/K et l'ensemble des sous-N-groupes de $\mathrm{Gal}(H/K)$. Rappelons qu'un sous-groupe $G < \mathrm{Gal}(H/K)$ est appelé N-groupe, si l'ensemble

$$\mathscr{A}_G = \{x \in H^*,\ I(x) \in G\} \cup \{0\}$$

forme un sous-corps de H. La qualité, pour une extension intermédiaire $H/M/K$, d'être galoisienne sur K se caractérise alors par le fait que le plus petit sous-N-groupe qui contient le normalisateur $\mathscr{N}_{\mathrm{Gal}(H/K)}(\mathrm{Gal}(H/M)$ est égal à $\mathrm{Gal}(H/K)$ tout entier (on dit que $\mathrm{Gal}(H/M)$ est N-invariant). On voit que cette condition d'être N-invariant est, *a priori*, plus faible que celle d'être distingué. En fait, la distinction d'un sous-groupe caractérise la stabilité de l'extension associée :

Proposition 1.— *Soient H/K une extension galoisienne finie. Pour qu'une extension intermédiaire $H/M/K$ soit stable (i.e. l'orbite de M sous l'action de $\mathrm{Gal}(H/K)$ est ponctuelle), il faut et il suffit que $\mathrm{Gal}(H/M)$ soit distingué dans $\mathrm{Gal}(H/K)$. En particulier, une extension intermédiaire stable est galoisienne sur K et l'on a donc, en toute généralité,*

$$M/K \text{ galoisienne} \Longleftarrow M \text{ est stable} \Longleftrightarrow \mathrm{Gal}(H/M) \triangleleft \mathrm{Gal}(H/K)$$

[1] Nous renvoyons le lecteur à [Coh] et [Jac] pour un exposé complet de cette théorie.

Preuve : Posons $G = \mathrm{Gal}(H/M)$, de sorte que $M = H^G$. On a alors

$$M = H^G \text{ est stable} \iff \forall \sigma \in \mathrm{Gal}(H/K), H^G = \sigma(H^G) = H^{\sigma G \sigma^{-1}}$$

Si $\sigma G \sigma^{-1}$ est lui aussi un N-groupe, on pourra affirmer, grâce aux correspondances galoisiennes, que $H^G = H^{\sigma G \sigma^{-1}} \Longrightarrow \sigma G \sigma^{-1} = G$. Montrons que c'est bien toujours le cas :

$$\begin{aligned} \mathscr{A}^*_{\sigma G \sigma^{-1}} &= \{x \in H^*,\ I(x) \in \sigma G \sigma^{-1}\} = \{x \in H^*,\ \sigma^{-1} \circ I(x) \circ \sigma \in G\} \\ &= \{x \in H^*,\ I(\sigma^{-1}(x)) \in G\} = \{x \in H^*,\ \sigma^{-1}(x) \in \mathscr{A}^*_G\} = \sigma(\mathscr{A}^*_G) \end{aligned}$$

Puisque G est un N-groupe l'ensemble $\mathscr{A}_G$ est un corps et il en est donc de même de $\sigma(\mathscr{A}_G) = \mathscr{A}_{\sigma G \sigma^{-1}}$, c'est-à-dire que $\sigma G \sigma^{-1}$ est bien un N-groupe.

□

Lorsque l'extension H/K est extérieure (e.g. lorsque H est commutatif), c'est-à-dire lorsque $\mathrm{Gal}(H/K)$ ne contient aucun automorphisme intérieur, tous les sous-groupes sont des N-groupes et l'on a donc l'équivalence

$$M/K \text{ galoisienne} \iff M \text{ est stable}$$

L'objet de cette note est de montrer qu'en toute généralité, cette équivalence n'est pas valable : quand on introduit des automorphismes intérieurs un phénomène d'instabilité peut apparaitre. Introduisons quelques éléments de terminologie : si H/K désigne une extension galoisienne finie, on dira qu'elle est *stable* (resp. *totalement stable*) si toute extension intermédaire $H/M/K$ galoisienne sur K (resp. *a priori* quelconque) est stable sous l'action de $\mathrm{Gal}(H/K)$. Une extension non stable sera qualifiée *d'instable* et l'on réservera la terminologie de *totalement instable* lorsque, à part les cas $M = K$ et $M = H$, aucune extension intermédiaire $H/M/K$ n'est stable sous l'action de $\mathrm{Gal}(H/K)$.

Comme on vient de le rappeler, on voit qu'une extension galoisienne finie extérieure H/K est toujours stable, mais on notera qu'elle n'est que rarement totalement stable, cette dernière condition équivalent en fait à dire que tout sous-groupe de $\mathrm{Gal}(H/K)$ est distingué. Dans une extension totalement stable, tout sous-corps intermédiaire est en fait galoisien sur K, la réciproque étant fausse (voir exemple en fin de texte). Enfin, on notera que pour être à la fois totalement stable et totalement instable il faut et il suffit d'être simple (i.e. sans extension intermédiaire, e.g. d'ordre premier).

Dans ce texte, on commence par étudier le cas des extensions qui sont galoisiennes, intérieures (i.e. $\mathrm{Gal}(H/K) = \mathrm{Int}(H/K)$) et finies. On montre (corollaire 4) qu'à l'exact contraire du cas extérieur, quand H/K est supposée en plus concentrique (i.e. $Z(H) = Z(K)$) alors elle est totalement instable. Pour autant, il existe des situations dans le cas intérieur non concentrique où l'équivalence reste vraie et où l'on peut même assurer du caractère totalement stable (voir corollaire 5). Finalement, en application de ces résultats nous proposons dans le § 2, un découpage systématique pour une extension galoisienne finie donnée en trois parties "totalement stable/totalement instable/stable".

1.— Cas des extensions intérieures.

Pour étudier cette question d'instabilité, nous commençons par donner une généralisation d'un théorème du à Cartan, Brauer et Hua :

Théorème 2.— *Soient H un corps, $H_0 \subset H$ un sous-corps et $G = \mathrm{Int}(H_0^*)$. Si $M \subset H$ est un sous-corps stable par G, alors, ou bien $M \subset \widetilde{H_0}$, ou bien $H_0 \subset M$.*

Preuve : Un petit calcul élémentaire montre que, pour tout $a, b \in H$, on a

$$([b,a]-[b,a-1])a = 1-[b,a-1]$$

où $[.,.]$ désigne le commutateur. Par hypothèse, pour tout $b \in M$ et tout $a \in H_0^*$, on a $[b,a] = b.(ab^{-1}a^{-1}) \in M$, si bien que si $[b,a-1]$ (qui est lui aussi élément de M) est différent de 1 alors, $a = ([b,a]-[b,a-1])^{-1}(1-[b,a-1]) \in M$. Puisque $[b,a-1] \neq 1 \Longleftrightarrow [b,a] \neq 1$, on voit donc que, dés que $a \in H_0^*$ et $b \in M$ ne commutent pas, on a nécessairement $a \in M$.

Supposons que $M \not\subset \widetilde{H_0}$ et fixons alors un élément $b_0 \in M - \widetilde{H_0}$ et un élément $a_0 \in H_0$ tel que $[b_0, a_0] \neq 1$. D'après ce qui précède, on a $a_0 \in M$. Pour tout $a \in H_0$, on a alors :

• si $[b_0, a] \neq 1$ alors $a \in M$, d'après ce qui précède.

• si $[b_0, a] = 1$ alors $[b_0, a+a_0] \neq 1$ (car $b_0(a+a_0)-(a+a_0)b_0 = b_0a_0 - a_0b_0 \neq 0$) et donc, toujours d'après ce qui précède, $a + a_0 \in M$. Comme $a_0 \in M$, finalement $a \in M$.

On vient bien de prouver que, si $M \not\subset \widetilde{H_0}$ alors $H_0 \subset M$.

□

Si l'on choisit $H_0 = H$, alors $\widetilde{H_0} = Z(H)$ et l'on retrouve le

Théorème de Cartan-Brauer-Hua.— [Coh, Th 3.9.2] *Si H un corps et $M \subset H$ est un sous-corps de H stable par tout automorphisme intérieur de H alors, ou bien $M \subset Z(H)$, ou bien $M = H$.*

Le théorème 2 est donc une généralisation du théorème de Cartan-Brauer-Hua. Sa preuve est inspirée de celle du théorème de Cartan-Brauer-Hua présentée dans [Coh]. Nous allons maintenant l'appliquer au cas d'une extension intérieure.

Théorème 3.— *Si H/K désigne une extension galoisienne, intérieure et finie alors, pour toute extension intermédiaire $H/M/K$ différente de K, on a*

$$M \text{ est stable} \Longleftrightarrow \widetilde{Z(K)} \subset M$$

Preuve : Les extensions galoisiennes, intérieures et finies ont été étudiées dans [Des]. Dans cet article, il est montré les propriétés suivantes :

a) $\widetilde{\widetilde{K}} = K$ [Des,Prop.7.a],

b) $\widetilde{Z(K)} = K.\widetilde{K} \simeq K \otimes_{Z(K)} \widetilde{K}$ [Des,Coro.15.b],

c) $Z(K) = Z(\widetilde{K})$ [Des,Prop 7.b],

d) $\widetilde{\widetilde{Z(K)}} = Z(K)$ [Des,Th.10.b],

que nous allons utiliser pour montrer l'équivalence.

$\Longrightarrow$: si M est stable, alors comme $\mathrm{Gal}(H/K) = \mathrm{Int}(H/K) = \mathrm{Int}(\widetilde{K}^*)$, on peut appliquer le théorème 2 avec $H_0 = \widetilde{K}$ et l'on trouve que :

• soit $\widetilde{K} \subset M$, mais comme $K \subset M$, on a alors en utilisant la propriété b) que $\widetilde{Z(K)} = K.\widetilde{K} \subset M$,

• soit $M \subset \widetilde{\widetilde{K}} = K$ (d'après la propriété a)) et l'on a $M = K$, ce qui est exclu.

$\Longleftarrow$: On a $\mathrm{Gal}(H/M) = \mathrm{Int}(H/M) = \mathrm{Int}(\widetilde{M}^*)$ et puisque $\widetilde{Z(K)} \subset M$, on voit que $\widetilde{M} \subset \widetilde{\widetilde{Z(K)}} = Z(K) = Z(\widetilde{K})$ (d'après les propriétés c) et d)). Si l'on prend $x \in \widetilde{M}^*$ et $y \in \widetilde{K}^*$ alors $yxy^{-1} = x$

(puisque $x \in Z(\widetilde{K})$), et donc $I(y)I(x)I(y)^{-1} = I(x)$: le groupe $\mathrm{Gal}(H/M) = \mathrm{Int}(\widetilde{M}^*)$ est (trivialement) distingué dans $\mathrm{Gal}(H/K) = \mathrm{Int}(\widetilde{K}^*)$ et la proposition 1 permet de conclure.

□

Si H/K est supposée, en plus, concentrique alors $Z(H) = Z(K)$ et donc $\widetilde{Z(K)} = H$: l'extension $H/\widetilde{Z(K)}$ est alors triviale et l'on en déduit le

Corollaire 4.— *Toute extension galoisienne, intérieure, finie et concentrique est totalement instable.*

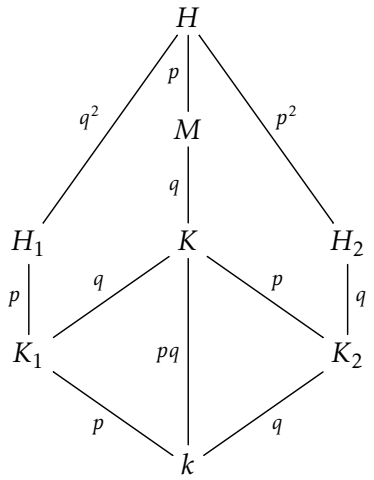
Le théorème 3 a aussi pour conséquence le

Corollaire 5.— *Toute extension galoisienne, intérieure et finie H/K telle que $K = \widetilde{Z(K)}$ est totalement stable*

Le cadre d'application le plus immédiat du corollaire 4 est celui des k-algèbres à division, c'est-à-dire des corps de dimension finie sur leur centre k. Si H désigne une k-algèbre à division, alors H/k est finie et concentrique par définition et elle est galoisienne et intérieure en vertu du théorème de Skolem-Noether. Très souvent, on dispose d'extensions intermédiaires strictes $H/M/k$ qui sont galoisiennes sur k et qui fournissent donc des exemples d'extensions galoisiennes instables. Par exemple, si l'on considère le corps $\mathbb{H}$ des quaternions d'Hamilton, il est de dimension 4 sur son centre $\mathbb{R}$. Les extensions intermédiaires strictes de $\mathbb{H}/\mathbb{R}$ sont donc toutes d'ordre 2 et, étant obtenues par l'adjonction à $\mathbb{R}$ d'un élément de $\mathbb{H} - \mathbb{R}$, il s'agit d'extensions galoisiennes de $\mathbb{R}$ (toutes isomorphes à $\mathbb{C}$)[2]. L'extension $\mathbb{H}/\mathbb{C}$ fournit aussi un exemple d'extension non simple qui est totalement instable bien que toutes ses extensions intermédiaires soient galoisiennes sur $\mathbb{R}$.

Les k-algèbres à division fournissent aussi un moyen simple d'illustrer le corollaire 5 : si H désigne une k-algèbre à division, on sait que les extensions commutatives maximales $H/K/k$ sont caractérisées par la relation $K = \widetilde{K}$. Pour une telle extension, on a $K = Z(K)$ et donc $\widetilde{Z(K)} = \widetilde{K} = K$. Ainsi, par application du théorème 3, dans l'extension galoisienne intérieure finie H/K l'équivalence " galoisienne $\Longleftrightarrow$ stable " est bien valable pour toute extension intermédiaire. Dans cette situation, il n'y aucune raison pour que H/K soit sans extensions intermédiaires (et donc que la propriété soit triviale) comme le montre l'exemple suivant : on se donne un corps commutatif k et deux k-algèbres à division H_1, H_2 de dimensions respectives p^2 et q^2, où p et q sont des entiers premiers entre eux. Les indices $\mathrm{Ind}(H_1) = p$ et $\mathrm{Ind}(H_2) = q$, étant premiers entre eux, on a $\mathrm{Ind}(H_1 \otimes_k H_2) = \mathrm{Ind}(H_1).\mathrm{Ind}(H_2)$ et donc $H = H_1 \otimes_k H_2$ est une k-algèbre à division (de dimension p^2q^2) qui contient canoniquement H_1 et H_2. On se donne maintenant K_1 et K_2 deux sous-corps commutatifs maximaux de H_1 et H_2 respectivement et l'on considère $K = K_1 \otimes_k K_2$. C'est une k-algèbre incluse dans H, elle est donc intègre et étant de dimension finie, c'est un corps (commutatif). Puisque $[K : k] = [K_1 : k].[K_2 : k] = pq$, c'est une extension commutative maximale de k dans H et l'extension H/K vérifie donc les hypothèses du corollaire 5. Le compositum $M = K.H_2$ fournit alors un exemple d'extension intermédiaire stricte de H/K.

[2] Plus systématiquement, si l'on considère une k-algèbre H obtenue par produit croisée d'une extension galoisienne de corps commutatifs L/k et d'un élément de $H^2(L/k)$ alors L est une extension galoisienne intermédiaire instable.



En effet, il est d'abord clair que $K \neq M$ car sinon $H_2 \subset K$ et $q^2 = [H_2 : k]$ diviserait $pq = [K : k]$. Pour montrer que $M \neq H$ on raisonne par l'absurde. Au niveau des centralisateurs, on a

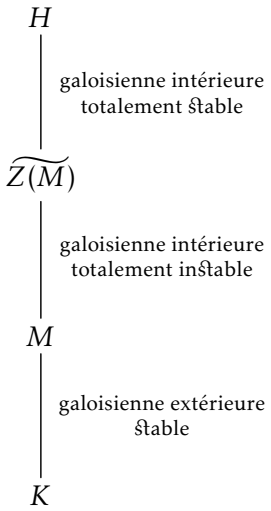
$$\widetilde{H_1} = \mathscr{C}_H(H_1) = \mathscr{C}_H(H_1 \otimes_k k) = \mathscr{C}_{H_1}(H_1) \otimes_k \mathscr{C}_{H_2}(k) = k \otimes_k H_2 = H_2$$

ainsi les corps H_1 et H_2 sont commutants l'un de l'autre dans H. On peut donc écrire

$$H = M \Longrightarrow \widetilde{H} = \widetilde{K.H_2} = \widetilde{K} \cap \widetilde{H_2} \Longrightarrow k = K \cap H_1$$ [3]

ce qui est visiblement impossible car $K_1 \subset K \cap H_1$.

2— Cas général Si l'on se donne une extension galoisienne finie H/K alors le sous-groupe $\mathrm{Int}(H/K)$ est visiblement distingué dans $\mathrm{Gal}(H/K)$ si bien que, si l'on pose $M = H^{\mathrm{Int}(H/K)}$ alors M/K est galoisienne extérieure et H/M est galoisienne intérieure. L'extension $\widetilde{Z(M)}/M$ est alors galoisienne intérieure [Des,Th.10] tout comme $H/\widetilde{Z(M)}$. Ce qui précède fournit alors un découpage systématique de H/K :



[3] La propriété $\widetilde{A.B} = \widetilde{A} \cap \widetilde{B}$ est valable pour toute paire $\{A, B\}$ de sous-corps d'un corps donné (voir [Des,Lemme 3])

Bibliographie

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

[Des] Bruno Deschamps, *Arithmétique des extensions intérieures*, J. of Algebra, 620, 50-88 (2023).

[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

Paul Rodriguez
Département de Mathématiques - École Normale Supérieure de Lyon
15 parvis René Descartes - BP 7000
69342 Lyon Cedex 07 - France
E-mail : paul.rodriguez@ens-lyon.fr