PHILIPPE RAMBOUR

Éléments fixes du complété d'une clôture séparable sous l'action de son groupe de Galois

Astérisque, tome 198-199-200 (1991), p. 285-294

<http://www.numdam.org/item?id=AST_1991__198-199-200__285_0>

ÉLÉMENTS FIXES DU COMPLÉTÉ D'UNE CLÔTURE SÉPARABLE SOUS L'ACTION DE SON GROUPE DE GALOIS

par Philippe RAMBOUR

Soit R un anneau, nœthérien, normal, intègre de corps des fractions K, et soit I un idéal de R qui ne soit pas confondu avec R tout entier.

On désigne par :

- R_s l'anneau des entiers sur R d'une clôture séparable K_s de K ;
- G le groupe $\mathrm{Gal}(K_s/K)$;
- $\hat{R}_s$ le complété de R_s pour la topologie définie par IR_s.

Le problème est de déterminer $\hat{R}_s^G$ qui est l'ensemble des éléments fixes du complété de R_s sous l'action de G.

J. Ax a répondu à la question dans le cas où le corps K est un corps local de caractéristique 0 ou p, c'est-à-dire un corps muni d'une valuation à valeur dans un groupe abélien et par laquelle K est hensélien [1]. Dans ce travail nous allons établir le théorème suivant :

THÉORÈME. — *L'anneau R_s est séparé pour la topologie I-adique et s'injecte donc dans $\hat{R}_s$. En caractéristique p, l'anneau $\hat{R}_s$ contient une clôture radicielle de R, notée $\sqrt{R}$, et $\hat{R}_s^G$ l'ensemble des points fixes de $\hat{R}_s$ sous l'action de G n'est autre que l'adhérence de $\sqrt{R}$ dans $\hat{R}_s$.*

Pour obtenir la dernière assertion nous utiliserons des approximations d'un élément de R_s qui dépendront du diamètre des conjugués, méthode mise au point par J. Ax [1].

I. — Séparation de R_s pour la topologie I-adique

PROPOSITION 1. — *Si $I \neq R$ alors $\bigcap_n I^n R_s$ est réduite à* 0 *et R_s est donc séparé pour la topologie définie par IR_s.*

Démonstration : supposons d'abord que I est un idéal principal. Il existe alors un élément x de R qui est un générateur de I. Puisque R est normal et nœthérien et $I \neq R$ il existe une valuation v vérifiant $v(x) > 0$ et cette valuation se prolonge à R_s. D'où si a appartient à $\bigcap_n I^n R_s$, alors $v(a) = +\infty$ et donc $a = 0$.

Démontrons maintenant la propriété dans le cas où I n'est pas forcément un idéal principal.

Notons S le schéma affine $\operatorname{Spec} R$ et soit $\tilde{S}$ le normalisé de l'éclaté $\hat{S}$ par rapport au sous-schéma fermé $Y = \operatorname{Spec}(R/I)$. Montrons tout d'abord que l'application canonique $\pi : \tilde{S} \to S$ est une application surjective. Pour cela remarquons que l'on peut écrire π comme la composée $\pi_2 \circ \pi_1$ où π_1 est l'application canonique de $\tilde{S}$ dans $\hat{S}$, π_2 l'application canonique de $\hat{S}$ dans S. π_1 et π_2 étant deux applications surjectives, il en est de même pour π.

π_1 est surjective : c'est le *going down* théorème (voir MATSUMURA : Commutative Algebra [2]).

π_2 est surjective : si $V = S - Y$, alors π_2 est un isomorphisme de $\pi_2^{-1}(V)$ sur V. Comme π_2 est propre, π_2 est fermé donc $\pi_2(\hat{S})$ est un fermé de S contenant V. Comme S est intègre S est aussi irréductible donc on a forcément $\pi_2(\hat{S}) = S$.

Soit maintenant $U = \operatorname{Spec} A$ un ouvert affine de $\tilde{S}$. On sait que A est un anneau nœthérien normal et si U est choisi assez petit parmi les ouverts affines vérifiant : $\pi^{-1}(Y) \cap U \neq \emptyset$ alors IA est un idéal principal de A, distinct de A. D'après ce qui a été démontré dans le cas principal on sait que $\bigcap_n I^n A_s = \{0\}$ avec A_s clôture intégrale de A contenue dans K_s. Puisque R est contenu dans A, alors R_s est contenu dans A_s et $\bigcap\limits_n I^n R_s$ est réduite à 0.

II. — $\hat{R}_s$ contient une clôture radicielle de R

PROPOSITION 2. — *Si R est de caractéristique p, l'anneau $\hat{R}_s$ contient une clôture radicielle de R, on la note $\sqrt{R}$.*

Démonstration : soit β un élément de R et N un entier naturel. On va montrer que $\hat{R}_s$ contient une solution de $X^{p^N} = \beta$. Pour cela fixons un élément non nul de I, appelé a. Pour tout entier naturel m supérieur à N on définit X_m comme étant une racine de l'équation :

$$X^{p^N} - a^{p^m} X = \beta(1).$$

Puisque cette équation est séparable X_m est bien un élément de R_s. Nous allons montrer que la suite $(X_m)_{m>N}$ ainsi définie est une suite de Cauchy dans R_s. Elle sera alors convergente dans $\hat{R}_s$, avec une limite X_0 qui vérifiera, en faisant tendre m vers l'infini dans (1), $X_0^{p^N} = \beta$. Donc X_0 sera donc une racine p^N-ième de β, ce qui démontrera le théorème cherché.

Si m et m' vérifient :$m' > m > N$, on a :

$$X_m^{p^N} - X_{m'}^{p^N} = a^{p^m} X_m - a^{p^{m'}} X_{m'}$$

$$\left(\frac{X_m - X_{m'}}{a^{p^{m-N}}}\right)^{p^N} = X_m - a^{p^{m'}-p^m} X_m.$$

Cette dernière égalité prouve que $(X_m - X_{m'})/a^{p^{m-N}}$ est un élément entier sur R_s, et puisque R_s est un anneau normal $(X_m - X_{m'})/a^{p^{m-N}}$ est un élément de R_s. Si α cet élément, l'égalité $X_m - X_{m'} = a^{p^{m-N}} \alpha$ permet de savoir que $X_m - X_{m'}$ est un élément de $I^{p^{m-N}}$ ce qui prouve que la suite $(X_m)_{m>N}$ est bien une suite de Cauchy, ce qui achève la démonstration.

III. — Diamètre des conjugués

Dans tout le paragraphe on supposera la caractéristique de K égale à p.

DÉFINITION 1. — *Pour α élément de R_s, avec $\alpha \neq 0$, on pose :*

$$\delta(\alpha) = \max\{n/\alpha \in I^n\}.$$

DÉFINITION 2. — *Si K' est une extension finie de K on pose, si α est un élément de R_s :*

$$\Delta_{K'} = \min\{n/\delta(\sigma(\alpha) - \alpha) \in I^n,\ \ \sigma \in \mathrm{Gal}(K_s/K')\}.$$

Remarque : si α est un élément de K', on pose :

$$\Delta_{K'}(\alpha) = +\infty.$$

On remarque : $\Delta_{K'}(\alpha) \geq \delta(\alpha)$ pour toute extension finie K' de K.

PROPOSITION 3.. — *Il existe deux réels a et b tels que pour tout α de R_s il existe β de $\sqrt{R}$ vérifiant $\alpha - \beta \in I^{[a\Delta_K(\alpha)]+b}$, et si $[K(\alpha) : K]$ premier à p, alors $\alpha - \beta \in I^{\Delta_K(\alpha)}$.*

Démonstration :

(a) Démontrons tout d'abord la proposition dans le cas où $[K(\alpha) : K]$ premier à p. On remarque alors que $\mathrm{Tr}_{\mathrm{K}(\alpha)/\mathrm{K}}(\alpha)$ appartient à R puisque R est normal et donc $\mathrm{Tr}_{\mathrm{K}(\alpha)/\mathrm{K}}(\alpha)\Big/[\mathrm{K}(\alpha) : \mathrm{K}]$ est également un élément de R et de plus :

$$\Big((\mathrm{Tr}_{\mathrm{K}(\alpha)/\mathrm{K}})(\alpha)\Big/[\mathrm{K}(\alpha) : \mathrm{K}]\Big) - \alpha = \sum \frac{\alpha' - \alpha}{[\mathrm{K}(\alpha) : \mathrm{K}]}$$

α' parcourant les K conjugués de α. Ce dernier terme est un élément de $I^{\Delta_K}(\alpha)$.

(b) Pour montrer la proposition dans ce cas nous allons avoir besoin des lemmes suivants :

LEMME 1. — *On se donne K' et K" deux extensions finies séparables de K avec K' contenu dans K" et vérifiant $[K" : K'] = p$. Alors si α est un élément de R_s appartenant à K" on a :*

(i) on peut trouver β un élément de R', où R' est l'anneau des entiers de K', qui soit tel que :

$$\alpha^p - \beta \in I^{\Delta_{K'}(\alpha)+\delta(\alpha)(p-1)}$$

(ii) pour tout entier naturel n non nul on peut trouver un élément β_n de R' avec :

$$\alpha^{p^n} - \beta_n \in I^{\Delta_{K'}(\alpha)p^n(1-a^n)} \qquad \text{où} \qquad a = (p-1)/p.$$

Démonstration du Lemme 1 :

Si α est un élément de K' il n'y a rien à démontrer. Sinon $[K'(\alpha) : K']$ vaut p et on peut faire la démonstration ci-dessous.

(i) Si $\alpha_1 \cdots \alpha_p$ désigne les racines du polynôme minimal de α sur K', on pose $\eta_i = \alpha_i - \alpha$. Alors

$$\begin{aligned} N_{K'(\alpha)/K'}(\alpha) &= \prod_{i=1}^{p} \alpha_i = \prod_{i=1}^{p}(\alpha + \eta_i) \\ &= \alpha^p + b_1\alpha^{p-1} + \cdots + b_p. \end{aligned}$$

En remarquant que le b_j sont, au signe près, les j-ième fonctions symétriques élémentaires de η_j pour $1 \leq j \leq p$, et que les η_j sont des éléments de $I^{\Delta_{K'}(\alpha)}$ on obtient facilement que : $N_{K'(\alpha)/K'}(\alpha) - \alpha^p$ est un élément d'un I^N avec :

$$N \geq \min_{1 \leq j \leq p}((p-j)\delta(\alpha) + j\Delta_{K'}(\alpha)) = \Delta_{K'}(\alpha) + \delta(\alpha)(p-1)$$

en utilisant que $\Delta_{K'}(\alpha) \geq \delta(\alpha)$.

Comme R' est normal, on a $N_{K'(\alpha)/K'}(\alpha)$ élément de R d'où le résultat.

(ii) Démontrons d'abord par récurrence sur n que l'on peut trouver un élément β_n de R' vérifiant :

$$\alpha^{p^n} - \beta_n \in I^{\Delta_{K'}(\alpha)p^n(1-a^n/p)^n)+(p-1)^n\delta(\alpha)}$$

La formule annoncée sera alors une conséquence immédiate de ce résultat.

Si $n = 1$ c'est ce que l'on a obtenu au (i).

Montrons maintenant la formule pour n quelconque. D'après l'hypothèse de récurrence il existe un élément β_{n-1} de R' vérifiant :

$$\alpha^{p^{n-1}} - \beta_{n-1} \in I^{\Delta_{K'}(\alpha)p^{n-1}(1-a^{n-1})+(p-1)^{n-1}\delta(\alpha)}$$

posons $x_{n-1} = \alpha^{p^{n-1}} - \beta_{n-1}$.

$$\delta(x_{n-1}) \geq \Delta_{K'}(\alpha)p^{n-1}(1-a^{n-1}) + (p-1)^{n-1}\delta(\alpha).$$

et

$$\Delta_{K'}(x_{n-1}) = \Delta_{K'}(\alpha)p^{n-1}$$

grâce au (i) on sait qu'il existe β un élément de R' vérifiant

$$x_{n-1}^p - \beta \in I^{\Delta_{K'}(x_{n-1})+\delta(x_{n-1})(p-1)}$$

ce qui implique, d'après les remarques ci-dessus :

$$\begin{aligned}\delta(\alpha^{p^n} - \beta_{n-1}^p - \beta) &\geq \Delta_{K'}(\alpha)p^{n-1} \\ &+(p-1)(\Delta_{K'}(\alpha)(1-a^{n-1})p^{n-1} + (p-1)^{n-1}\delta(\alpha)).\end{aligned}$$

C'est-à-dire que si l'on pose $\beta_{n-1}^p + \beta = \beta_n$ et que si l'on fait un petit calcul pour transformer $p^{n-1} + p^{n-1}(1-(p-1/p)^{n-1})(p-1)$ en $p^n(1-(p-1/p)^n)$ on obtient

$$\delta(\alpha^{p^n} - \beta) \geq \Delta_{K'}(\alpha)p^n(1-a^n) + (p-1)^n\delta(\alpha)$$

qui est le résultat annoncé.

LEMME 2. — *Soit $H_m \supset H_{m-1} \supset \cdots \supset H_1 \supset H_0$ une tour d'extensions finies séparables de K avec $[H_i : H_{i-1}] = p$ pour $1 \leq i \leq m$. On appelle R_0 l'anneau des entiers de H_0 par rapport à R, et R_i l'anneau des entiers de H_i sur R_0. Si α est un élément de H_m et si n est un entier naturel donné on peut trouver un élément β_{m-i} de R_{m-i} vérifiant :*

$$\alpha^{p^{ni}} - \beta_{m-i} \in I^{\Delta_{H_0}(\alpha)p^{ni}(1-a^n)^i} \qquad 1 \leq i \leq m.$$

Démonstration : Démontrons ce lemme par récurrence.

Pour $i = 1$ c'est une application immédiate du point (ii) du lemme 1 avec $K' = H_{m-1}$ en remarquant que puisque H_0 est contenu dans H_{m-1}, $\Delta_{H_0}(\alpha) \leq \Delta_{H_{m-1}}(\alpha)$.

Démontrons maintenant le lemme pour un i quelconque $1 \leq i \leq m$.

D'après l'hypothèse de récurrence il existe β_{i-1} élément de R'_{m-i+1} avec

$$\alpha^{p^{(n-i)}} - \beta_{m-i+1} \in I^{\Delta_{H_0}(\alpha)p^{n(i-1)}(1-a^n)^{(i-1)}}. \tag{I}$$

on a

$$\Delta_{H_0}(\beta_{m-i+1}) \geq \Delta_{H_0}(\alpha)p^{n(i-1)}(1-a^n)^{(i-1)}(1)$$

en effet si σ un élément de $Gal(K_s/H_0)$, et si $\alpha' = \sigma(\alpha)$, et si $\beta'_{m-i+1} = \sigma(\beta_{m-i+1})$, alors :

$$\begin{aligned}\beta'_{m-i+1} - \beta_{m-i+1} = \beta'_{m-i+1} &- \alpha'^{p^{n(i-1)}} + \alpha'^{p^{n(i-1)}} \\ &+ \alpha^{p^{n(i-1)}} - \alpha^{p^{n(i-1)}} - \beta_{m-i+1}\end{aligned}$$

en remarquant que :$\beta'_{m-i+1} - \alpha'^{p^{n(i-1)}}$ et $\beta_{m-i+1} - \alpha^{p^{n(i-1)}}$ sont des éléments de $I^{\Delta_{H_0}(\alpha)p^{n(i-1)}(1-a^n)^{(i-1)}}$ et comme $\alpha^{p^{n(i-1)}} - \alpha'^{p^{n(i-1)}}$ dans $I^{\Delta_{H0}(\alpha)p^n(i-1)}$ on obtient l'inégalité (1).

Si l'on applique maintenant le résultat (ii) du lemme 1 avec $K' = H_{m-i}$ on peut trouver un élément de R_{m-i} avec :

$$\beta^{p^n}_{m-i+1} - \beta_{m-i} \in I^{\Delta_{H_{m-i}}(\beta_{m-i+1}).p^n(1-a^n)} \tag{II}$$

et remarquant que $\Delta_{H_{m-i}}(\beta_{m-i+1}) \geq \Delta_{H_0}(\beta_{m-i+1})$

$$\beta^{p^n}_{m-i+1} - \beta_{m-i} \in I^{\Delta_{H_0}(\beta_{m-i+1})p^n(1-a^n)}.$$

Soit d'aprés l'inégalité (1) :

$$\beta^{p^n}_{m-i+1} - \beta_{m-i} \in I^{\Delta_{H_0}(\alpha)p^{ni}(1-a^n)^i} \tag{II'}$$

D'autre part en élevant $\alpha^{p^{n(i-1)}} - \beta_{m-i+1}$ à la puissance p^n la relation (I) donne :

$$\delta(\alpha^{p^{ni}} - \beta^{p^n}_{m-i+1}) \geq \Delta_{H_0}(\alpha)p^{ni}(1-a^n)^i \qquad \text{(I')}.$$

d'où en combinant (II') et (I') :

$$\delta(\alpha^{p^{ni}} - \beta_{m-i}) \geq \Delta_{H_0}(\alpha)p^{ni}(1-a^n)^i.$$

ce qui est le résultat annoncé.

(c) Démonstration de la proposition 3 dans le cas $[\tilde{K} : K] = p^m$.

Où $\tilde{K}$ désigne une extension galoisienne de degré minimale de K contenant α. En utilisant que Gal($\tilde{\mathrm{K}}(\alpha)$: K) est résoluble on peut obtenir une tour d'extensions séparables :

$$\tilde{K} = K_m \supset K_{m-1} \supset \cdots \supset K_1 \supset K_0 = K.$$

On appelle R_i l'anneau des entiers de K_i sur R. Soit n un entier naturel. Si on applique le lemme 2 avec $i = m$ et $H_m = \tilde{K}$, $H_0 = K$, on obtient l'existence d'un élément β_0 de R vérifiant :

$$\alpha^{p^{nm}} - \beta_0 \in I^{\Delta_K(\alpha)p^{nm}}(1-a^n)^m.$$

Si l'on choisit maintenant n tel que :

$$1 - (p - 1/p)^n \geq 1/2,$$

on obtient :

$$\alpha^{p^{nm}} - \beta_0 \in I^{\Delta_K(\alpha)[p^{nm}/2]}.$$

Si l'on admet pour l'instant que $x^{p^j} \in I^N$ implique :

$$x \in I^{[N/p^j]-r+1}$$

avec r désignant le nombre de générateurs de I, on obtient que si β vaut $\beta_0^{1/p^{nm}}$ alors :

$$\alpha - \beta \in I^{[\Delta_K(\alpha)[p^{nm}/2]/p^{nm}]-r+1}.$$

En remarquant que l'on peut choisir encore n pour que :

$$[\Delta_K(\alpha)[p^{nm}/2]/p^{nm}] \geq \left[\frac{\Delta_K(\alpha)}{2}\right] - 1.$$

On obtient : $\alpha - \beta \in I^{[\Delta(\alpha)/2]-r}$ ce qui est le résultat voulu. Reste à démontrer le lemme suivant :

LEMME 3. — *Si A est un anneau de caractéristique p pour lequel $x \longmapsto x^p$ est bijectif, si J un idéal de A engendré par r éléments de A, alors si n et N sont deux entiers naturels $x^{p^n} \in J^N$ implique $x \in J^{[N/p^n]-r+1}$.*

Démonstration : démontrons ce lemme grâce à une récurrence sur r, où r désigne le nombre des générateurs.

Si $r = 1$. Alors I est un idéal principal et la propriété $x \longmapsto x^p$ bijectif donne le résultat.

Montrons maintenant la propriété pour r quelconque. Posons $J = (y_1, \cdots, y_r)$ et $H = (y_2, \cdots, y_r)$. Si x est tel que $x^{p^n} \in J^N$ on peut écrire :

$$x^{p^n} = X_0 y_1^N + X_1 y_1^{N-1} + \cdots + X_i y_1^{N-i} + \cdots + X_N$$

avec X_i élément de H^i pour i vérifiant $0 \leq i \leq N$. On obtient ainsi que :

$$x = X_0^{1/p^n} y_1^{N/p^n} + X_1^{1/p^n} y_1^{N-1/p^n} + \cdots + X_i^{1/p^n} y_1^{(N-i)/p^n} + \cdots + X_N^{1/p^n} (1).$$

Comme

$$\left[\frac{N-i}{p^n}\right] \geq \left[\frac{N}{p^n}\right] - \left[\frac{i}{p^n}\right] - 1.$$

y_1^{N-i/p^n} est donc un élément de $J^{[N/p^n]-[i/p^n]-1}$ et d'après l'hypothèse de récurrence appliquée à H on sait que X_i^{1/p^n} est un élément de $H^{[i/p^n]-r+2}$. Donc chaque terme de la sommation (1) appartient à : $J^{[N/p^n]-[i/p^n]-1+[i/p^n]-r+2}$ c'est-à-dire à : $J^{[N/p^n]-r+1}$ ce qui démontre le lemme.

(d) Démonstration de la proposition 3 dans le cas général.

Soit donc α un élément de R_s tel que $[K(\alpha) : K]$ n'est pas un entier premier à p. Si $\tilde{K}$ désigne encore une extension galoisienne de K de degré minimal contenant α, on a : $[\tilde{K} : K] = qp^m$ avec q premier à p.

Si G' est un p-groupe de Sylow de Gal(K(α)/K). Soit H l'ensemble des points fixes de G' dans $\tilde{K}$. On sait qu'alors H est une extension finie de K contenue dans $\tilde{K}$ et telle que :

- $\tilde{K}$ est une extension galoisienne de H.
- $[\tilde{K}(\alpha) : H] = p^n$.

On appelle R' l'anneau des entiers de H. Si n désigne un entier naturel on peut appliquer à $\tilde{K}(\alpha)$ et H ce qui a été fait au (b) avec H dans le rôle de K. On peut donc obtenir γ avec γ élément de R' et :

$$\alpha - \gamma \in I^{[\Delta_H(\alpha)/2]-r}.$$

D'après a) on sait qu'il existe un élément β_0 de R vérifiant $\gamma - \beta_0 \in I^{\Delta_K(\gamma)}$.

Puisque K est contenu dans H, $\Delta_K(\alpha) \leq \Delta_H(\alpha)$ d'où

$$\alpha - \gamma \in I^{[\Delta_K(\alpha)/2]-r} \tag{1}$$

et comme en (b) on peut montrer que :

$$\Delta_K(\gamma) \geq [\Delta_K(\alpha)/2] - r.$$

d'où

$$\gamma - \beta_0 \in I^{[\Delta_K(\alpha)/2]-r}. \tag{2}$$

Les relations (1) et (2) donnent :

$$\alpha - \beta_0 \in I^{[\Delta_K[\alpha)/2]-r}$$

IV. — Éléments fixes sous l'action du groupe $G = \mathrm{Gal}(K_s/K)$

PROPRIÉTÉ 4. — *Si K un corps de caractéristique p, on a, avec les notations introduites au début de l'article :*

$$\hat{R}_s^G = \overline{\sqrt{R}},$$

où $\overline{\sqrt{R}}$ désigne l'adhérence de $\sqrt{R}$ pour la topologie I-adique.

Démonstration : si x est un élément de $\hat{R}_s^G$ pour tout entier N il existe un α qui est un élément de R_s avec $x - \alpha$ éleément de $I^N \hat{R}_s$. Si σ est un élément de G on a toujours $x - \sigma(\alpha)$ élément de $I^N \hat{R}_s$, et donc $\alpha - \sigma(\alpha)$ élément de $I^N \hat{R}_s$ d'où $\Delta_K(\alpha) \geq N$.

Donc on peut trouver, d'après la proposition 3, un élément β dans $\sqrt{R}$ où $\alpha - \beta$ est un élément soit de $I^{[N/2]-r}\hat{R}_s$. Donc $x - \beta$ est un élément de $I^{[N/2]-r}\hat{R}_s$. Il en résulte que x est un élément de l'adhérence de $\sqrt{R}$. La réciprocité étant immédiate on obtient la propriété annoncée.

BIBLIOGRAPHIE

[1] J. Ax. — Zeros of Polynomials over local fields, the Galois Action, *Journal of Algebra*, 15, 1970, 417-428.

[2] H. Matsumura. — Commutative Algebra, Second Edition, Mathematics Lecture Note Series, The Benjamin.cuminings publishing company.

PH. RAMBOUR
Université de Paris-Sud
Département de Mathématiques
URA D0752
Bâtiment 425
F-91405 ORSAY CEDEX