

INSTITUTUL
DE
MATEMATICĂ

INSTITUTUL NAȚIONAL
PENTRU CREAȚIE
ȘTIINȚIFICĂ ȘI TEHNICĂ

ISSN 0250 3638

SUR LA THEORIE DE GALOIS ANALYTIQUE
POUR LES CORPS COMPLETS

by

Alexandru ZAHARESCU

PREPRINT SERIES IN MATHEMATICS

No. 18/1985

BUCUREȘTI

11.1.21.1985

SUR LA THEORIE DE GALOIS ANALYTIQUE
POUR LES CORPS COMPLETS

by

Alexandru ZAHARESCU *)

March 1985

*) Faculte de Mathematique Universite de Bucarest str. Academiei 14
70109 Bucarest Romania

SUR LA THÉORIE DE GALOIS ANALYTIQUE POUR LES CORPS COMPLETS

Alexandru ZAHARESCU

Soit K un corps de caractéristique zero, complet par rapport à une valuation discrète V de rang 1, telle que son corps résiduel soit perfect. Soit $\bar{K}$ la clôture algébrique de K et L le complété de $\bar{K}$ par rapport à la seule valuation qui prolonge V à $\bar{K}$ (notée aussi par V). Soit $\text{Gal}_c(L/K)$ le groupe des K -automorphismes de L qui sont continues par rapport à V . Le but de cette note est de montrer que les sousgroupes fermés de $\text{Gal}_c(L/K)$, topologisé avec la topologie de Krull, sont canoniquement en correspondance biunivoque avec les souscorps de l'extension L/K qui sont complets par rapport à V .

Let K be a field of characteristic 0, complete relative to a rank one discrete valuation V having a perfect residual field. Let $\bar{K}$ be the algebraic closure of K and L the completion of $\bar{K}$ relative to the unique valuation on $\bar{K}$ which extends V (also denoted by V). Let $\text{Gal}_c(L/K)$ be the group of all K -automorphisms of L which are continuous relative to V . The aim of this note is to show that the closed subgroups of $\text{Gal}_c(L/K)$ with the Krull topology are, in a natural manner, in a one-to-one correspondence with the subfields of the extension L/K which are complete relative to V .

1. Soit K un corps de caractéristique 0, complet par rapport à une valuation discrète V de rang 1, telle que son corps résiduel k soit perfect. Soit $\bar{K}$ la clôture algébrique de K et L le complété de $\bar{K}$ par rapport à la seule valuation qui prolonge V à $\bar{K}$. La valuation obtenue sur L sera notée aussi par V . Il est connu (voir

[1]) que L est algébriquement clos.

Soit $\text{Gal}_C(L/K)$ le groupe des K -automorphismes de L qui sont continues par rapport à V . Les automorphismes $\sigma \in \text{Gal}_C(L/K)$ sont analytiques: $V(\sigma(x)) = V(x)$, $\forall x \in L$. Nous munirons $\text{Gal}_C(L/K)$ de la topologie de Krull.

THÉORÈME. Avec les notations ci-dessus les sousgroupes fermés de $\text{Gal}_C(L/K)$ sont canoniquement en correspondance biunivoque avec les souscorps de l'extension L/K qui sont complets par rapport à V .

2. DÉMONSTRATION DU THÉORÈME

Soit d la distance sur L , définie par $d(a,b) = q^{V(a-b)}$ où $q \in (0, 1)$ est fixé d'avance. Si $\text{char } k = p \neq 0$, on suppose que V est normalisée, de sorte que $V(p) = 1$.

Notons

$$c_0 = \begin{cases} q^{p/(p-1)} & \text{si } \text{char } k = p \neq 0, \\ 1 & \text{si } \text{char } k = 0. \end{cases}$$

Nous avons besoin du lemme suivant:

LEMME. Soit $K \subset F \subset L$ et $a \in \bar{K}$. Alors il existe $\sigma \in \text{Gal}(\bar{F}/F)$ tel que $d(\sigma(a), a) \geq c_0 \inf \{d(a, x); x \in F\}$.

La démonstration de ce lemme sera donnée dans le paragraphe suivant.

Soit maintenant G l'ensemble des sousgroupes fermés de $\text{Gal}_C(L/K)$, E l'ensemble des souscorps complets de L/K , et soient $\alpha : G \rightarrow E, \beta : E \rightarrow G$ donnés par $\alpha(H) = \{x \in L \mid h(x) = x, \forall h \in H\}$ et $\beta(F) = \{\phi \in \text{Gal}_C(L/K) \mid \phi(x) = x, \forall x \in F\}$.

Soit $H \in G$. Alors $\alpha(H)$ est fermé dans L , parce que les automorphismes $h \in H$ sont continues. L est un espace métrique complet, donc $\alpha(H)$ est complet.

Soit $F \in E$. Si $\beta(F)$ n'était pas fermé dans $\text{Gal}_C(L/K)$, alors il existerait ϕ dans la fermeture de $\beta(F)$ dans $\text{Gal}_C(L/K)$ et $z \in F$, tels que $\phi(z) \neq z$. Soit $a \in \bar{K}$ tel que $d(a, z) = \epsilon < \epsilon_0 = d(\phi(z), z)$. Il existe $\psi \in \beta(F)$ tel que $\psi(a) = \phi(a)$; ϕ et ψ sont des isométries, donc $d(\phi(a), \phi(z)) = d(a, z) = \epsilon_0$ et $d(\phi(a), z) = d(\psi(a), \psi(z)) = d(a, z) = \epsilon_0$. On obtient ainsi $d(z, \phi(z)) \leq \max\{d(z, \phi(a)), d(\phi(a), \phi(z))\} = \epsilon_0 < \epsilon$, c'est-à-dire une contradiction. Cela montre que α et β sont bien définis.

THÉORÈME. Les applications α et β sont des correspondances biunivoques réciproques.

Démonstration. Montrons que $\beta \circ \alpha = \text{Id}_E$ et $\alpha \circ \beta = \text{Id}_G$. Soit $H \in G$. Évidemment $H \subset \beta(\alpha(H))$. Pour prouver l'inclusion contraire, H étant fermé, il suffit de montrer que H est dense dans $\beta(\alpha(H))$. Mais, pour toutes les extensions galoisiennes finies E de $\alpha(H)$, la restriction $\phi|_E$ coïncide avec la restriction d'un élément de H , parce que les restrictions des éléments de H donnent tous les $\alpha(H)$ -automorphismes de E . Donc $\beta(\alpha(H)) = H$. Soit $F \in E$. Il est clair que $F \subset \alpha(\beta(F))$. Pour prouver l'autre inclusion, il suffit de montrer que si $z \in L \setminus F$, alors il existe $\phi \in \text{Gal}_C(L/K)$ tel que $\phi|_F = \text{Id}_F$ et $\phi(z) \neq z$. Soit $d_0 = d(F, z) = \inf\{d(z, x); x \in F\}$. F est complet et $z \notin F$, donc $d_0 > 0$. Il existe $a \in \overline{K}$ tel que $d(a, z) = \varepsilon < c_0 d_0 \leq d_0$. Donc $d(F, a) = d_0$. Du lemme il résulte qu'il existe $\sigma \in \text{Gal}(\overline{F}/F)$ tel que $d(\sigma(a), a) \geq c_0 d(F, a) = c_0 d_0$. Mais F est complet par rapport à V (qui est de rang 1), donc σ est continu. Nous pouvons le prolonger à un élément $\phi \in \text{Gal}_C(L/K)$. Supposons que $\phi(z) = z$. Alors $d(z, \sigma(a)) = d(\phi(z), \phi(a)) = d(z, a) = \varepsilon$, donc $d(a, \sigma(a)) \leq \max\{d(a, z), d(z, \sigma(a))\} = \varepsilon < c_0 d_0$ et on obtient ainsi une contradiction. Il résulte que $\phi(z) \neq z$, donc $\alpha(\beta(F)) = F$, et le théorème est démontré.

3. LA DÉMONSTRATION DU LEMME

Dans le cas où $[F:K]$ est fini, on notera $r_F = \inf\{V(F) \cap (0, \infty)\} > 0$ et $A_F = \{a \in \overline{F} \mid V(a) \notin r_F \mathbb{Z}\}$. Soit $f_F : \overline{F} \rightarrow \mathbb{Q} \cup \{\infty\}$, défini par

$$f_F(a) = \begin{cases} \min_{\sigma \in \text{Gal}(F/F)} \{V(\sigma(a)/a - 1)\} & \text{si } a \in \overline{F} \setminus \{0\} \\ \infty & \text{si } a = 0. \end{cases}$$

Alors $f_F(a) \geq 0$, $\forall a \in \overline{F}$, et $f_F(a) = \infty$ si et seulement si $a \in F$. Au cours de la démonstration, s'il n'y a confusion, nous omettrons l'indice F de r_F , A_F et f_F .

PROPOSITION 1. Si $[F:K]$ est fini et $0 \neq a \in \overline{F} \setminus A_F$ est tel que $f_F(a) > 0$, alors il existe $c \in F$ tel que $V(a - c) > V(a)$.

Démonstration. Il existe $b \in F$ tel que $V(b) = V(a)$. Soit $P(X) \in F[X]$ le polynôme minimal de $a_1 = a/b$. On a $f_F(a_1) = f_F(a) > 0$, donc toutes les racines de $P(X)$ ont la même image $\bar{a}_1$ dans le corps résiduel $k_{\bar{F}}$ de $\bar{F}$. Alors $(X - \bar{a}_1)^n = \bar{P}(X) \in k_{\bar{F}}[X]$. Le corps $k_{\bar{F}}$ étant parfait, il résulte que $\bar{a}_1 \in k_{\bar{F}}$, donc il existe $b_1 \in F$ tel que $V(a_1 - b_1) > 0$. La démonstration sera terminée si on prend $c = ab_1$.

PROPOSITION 2. Si $[F : K]$ est fini et $a \in A_F$, alors $f_F(a) \leq c_1$, où

$$c_1 = \begin{cases} p/(p-1) & \text{si char } k = p \neq 0, \\ 0 & \text{si char } k = 0. \end{cases}$$

Cette proposition représente la clé de cette note. Allons voir maintenant comment elle peut être utilisée dans la démonstration du lemme.

Démonstration du lemme. Supposons pour le moment que F est une extension finie de K . La propriété énoncée est évidente pour les éléments $a \in F$. Supposons qu'il existe $a \in \bar{K} \setminus F$ tel que $\forall \sigma \in \text{Gal}(\bar{F}/F)$, $d(\sigma(a), a) < c_0 d(F, a)$. Alors, $\forall \sigma \in \text{Gal}(\bar{F}/F)$ on a $V(\sigma(a) - a) > c_1 + \sup\{V(x - a); x \in F\}$. Si l'ensemble discret $\{V(a - x) \mid x \in F\}$ n'a pas de limite supérieure, soit a la limite d'une suite d'éléments de F ; parce que F est complet, nous avons $a \in F$, contradiction. Alors, il existe $b \in F$ tel que $V(a - b) = \sup\{V(a - x); x \in F\}$. À cause des relations $f_F(a - b) = \min_{\sigma \in \text{Gal}(\bar{F}/F)} \{V(\sigma(a) - a)/(a - b)\} = \min_{\sigma \in \text{Gal}(\bar{F}/F)} \{V(\sigma(a) - a) - V(a - b) > c_1 \geq 0$, la proposition 2 implique $a - b \notin A_F$, et la proposition 1 implique l'existence d'un élément $c \in F$ tel que $V(a - b - c) > V(a - b)$, ce qui contredit le choix de b .

Si $[F : K]$ n'est pas fini, soient $a_1 = a, a_2, \dots, a_n$ les conjugués de a sur K et $a_1, \dots, a_r$ ($2 \leq r \leq n$) les conjugués de a sur F . Alors les conjugués de a sur $F_1 = F \cap K(a_1, \dots, a_n)$ sont précisément $a_1, \dots, a_r$. Mais $[F_1 : K]$ est fini. Alors, il existe $i \in \{2, \dots, n\}$ tel que $d(a, a_i) \geq c_0 d(a, F_1) \geq c_0 d(a, F)$, et le lemme est démontré.

Pour obtenir la démonstration du Proposition 2, nous avons besoin de certains résultats (nous ne donnons pas tous les détails des démonstrations). Dans ce

qui suit F sera fixé.

1) Soient $0 \neq c \in F$ et $a \in \bar{F}$; alors $f(ca) = f(a)$.

2) Soient $a, b \in F$ tel que $V(a+b) = \min\{V(a), V(b)\}$. Alors $f(a+b) \geq \min\{f(a), f(b)\}$.

3) Soit $a \in \bar{F} \setminus \{0\}$, $f(a) > 0$ et soit $m \in \mathbb{N}^*$, $p \nmid m$. Alors, pour tout $\sigma \in \text{Gal}(\bar{F}/F)$, nous avons $V(\sigma(a^m)/a^m - 1) = V(\sigma(a)/a - 1)$. Par conséquent, $f(a^m) = f(a)$.

4) Soit $a \in \bar{F} \setminus \{0\}$ avec $f(a) > 1/(p-1)$; alors $\forall \sigma \in \text{Gal}(\bar{F}/F)$ nous avons $V(\sigma(a^p)/a^p - 1) = 1 + V(\sigma(a)/a - 1)$. Par conséquent $f(a^p) = 1 + f(a)$.

5) Soient $a, b \in \bar{F} \setminus F$ et $\sigma \in \text{Gal}(\bar{F}/F)$ tels que $V(b-a) > V(\sigma(a)-a)$; alors $f(a) = f(b)$. Il résulte que l'application f est localement constante sur $\bar{F} \setminus F$.

6) Soient $a, b \in \bar{F} \setminus F$ tels que $f(b) \neq f(a)$ et soit $P(X) \in F[X]$ le polynôme minimal de a (ayant le degré n). Alors $V(P(b)) \leq (n/(n-1))V(P'(a))$.

Démonstration. Soient $a_1 = a, a_2, \dots, a_n$ les racines de $P(X)$. L'inégalité annoncée est impliquée par l'inégalité $\max_{1 \leq j \leq n} V(b - a_j) \leq \min_{2 \leq i \leq n} V(a_1 - a_i)$ qui est une conséquence de 5) (on utilise ici le fait que $f(a_1) = f(a_2) = \dots = f(a_n)$).

7) Soit $a \in A$ tel que $[F(a) : F] = p$. Alors $f(a) \leq 1/(p-1)$.

Démonstration. Il est clair que l'extension $F(a)/F$ est totalement ramifiée et $V(a) = (h/p)r_F$, où $p \nmid h \in \mathbb{Z}$. Alors $V(P'(a)) = \min\{V(pa^{p-1}), V((p-1)c_1a^{p-2}), \dots, V(c_{p-1})\}$, où $P(X) = X^p + c_1X^{p-1} + \dots + c_p$ est le polynôme minimal de a . L'inégalité $V(P'(a)) \leq V(pa^{p-1})$ implique facilement l'inégalité $f(a) \leq 1/(p-1)$.

8) Soit $P(X) = X^p + c_1X^{p-1} + \dots + c_p$ un polynôme de $F[X]$, soit $m_0 = \min\{1 + r, V(c_1) + ((p-1)/p)r, \dots, V(c_{p-1}) + (1/p)r\}$, où $r = r_F$, et soit $a \in \bar{F}$ avec les deux propriétés $V(a) = r/p$ et $f(b) > 1/(p-1)$. Alors, $\forall \sigma \in \text{Gal}(\bar{F}/F)$, nous avons $V(\sigma(P(a)) - P(a)) \geq f(a) + m_0$.

Pour obtenir la démonstration on peut utiliser 3) et 4).

9) Avec les notations de 8), supposons que $P(X)$ est un polynôme d'Eisenstein et b un racine de $P(X)$. Alors $V(P'(b)) = m_0 - (r/p)$.

10) Soit $a \in \overline{F}$ tel que $V(a) = r/p$, $f(a) > 1/(p-1)$ et l'extension $F(a)/F$ est totalement ramifiée. Alors il existe un polynôme d'Eisenstein $P(X) \in F[X]$ ayant le degré p et tel que $(P(a))^p \in A = A_F$.

Démonstration. Supposons que $P(a) \notin A$, pour tous les polynômes d'Eisenstein $P(X) \in F[X]$ de degré p . Soit $t \in F$ tel que $V(t) = r$. Pour tous $u \in F(a)$ avec $V(u) \in (r/p)\mathbb{Z}$, il existe $h, m \in \mathbb{Z}$, $0 \leq m < p$, tels que $V(u/(t^h a^m)) = 0$. L'extension $F(a)/F$ est totalement ramifiée, donc il existe $c \in F$ tel que $V(u/(t^h a^m) - c) > 0$, d'où $V(u - ct^h a^m) > V(u)$. Pour $u = a^p$, il existe $b_1 \in F$ tel que $V(a^p - b_1) > V(a^p) = r$. Par hypothèse, $V(a^p - b_1) \in (r/p)\mathbb{Z}$, donc il existe $b_2 \in F$ et $m_2 \in \{0, \dots, p-1\}$ tels que $V(a^p - b_2 a^{m_2} - b_1) > V(a^p - b_1)$.

En continuant la construction, on obtient une suite de polynômes d'Eisenstein $P_1(X) = X^p - b_1$, $P_2(x) = X^p - b_2 X^{m_2} - b_1, \dots, P_m(X), \dots$ tels que la suite $V(P_m(a))$ est strictement croissante, donc convergente vers ∞ . F étant complet, il existe un polynôme limite $P(X)$ qui est aussi un polynôme d'Eisenstein et tel que $V(P(a)) = \lim_{m \rightarrow \infty} V(P_m(a)) = \infty$, donc $P(a) = 0$. Alors $[F(a) : F] = p$, ce qui contredit 7).

11) Soit F_1 une extension finie, totalement ramifiée de F . Alors l'ensemble $M = \{f_F(x) \mid x \in F_1 \cap A_F\}$ a un plus grand élément M_0 .

Démonstration. L'ensemble M est discret. Soit t une uniformisante de F_1 et $0 \in S \subset F$ un système de représentants pour le corps résiduel k_F . Supposons qu'il existe une suite (a_n) d'éléments de $F_1 \cap A_F$, avec $a_n = t^{h_0} + b_{1n} t^{h_0+1} + \dots$, où $b_{1n} \in S$, telle que $f(a_n) \rightarrow \infty$. De 5) on déduit l'existence d'un entier $h_1 > h_0$ maximal avec la propriété qu'il existe une suite (a'_n) , où $a'_n = t^{h_0} + b'_{h_1, n} t^{h_1} + b'_{h_1+1, n} t^{h_1+1} + \dots$, avec $b'_{in} \in S$, telle que $f(a'_n) \rightarrow \infty$. De 2) on déduit facilement qu'il n'existe pas de sous-suite $(b'_{h_1, n_k})_{k \in \mathbb{N}}$ d'éléments distincts, donc il existe une sous-suite $(a'_{n_k})_{k \in \mathbb{N}}$ de $(a'_n)_{n \in \mathbb{N}}$ telle que $b'_{h_1, n_1} = \dots = b'_{h_1, n_k} = \dots = c_{h_1}$. En répétant la construction on trouve un $h_2 > h_1$ et un c_{h_2} ayant la propriété qu'il existe une suite (a''_n) , où $a''_n = t^{h_0} + c_{h_1} t^{h_1} +$

$+ c_{h_2} t^{h_2} + b_{h_2+1,n}'' t^{h_2+1} + \dots$. En itérant la construction on obtient finalement un élément $a \in F_1 \cap A_F$, $a = t^{h_0} + c_{h_1} t^{h_1} + \dots + c_{h_n} t^{h_n} + \dots$ qui a la propriété: $\forall \epsilon > 0$ et $n \in \mathbb{N}$, il existe $a_{n,\epsilon} \in F_1$ tel que $d(a_{n,\epsilon}, a) < \epsilon$ et $f(a_{n,\epsilon}) > n$. Pour $\epsilon \rightarrow 0$ et $n \rightarrow \infty$, en utilisant de nouveau 5) nous obtenons une contradiction.

12) Avec les notations de 11), si $M > 1/(p-1)$, alors il existe $a \in F_1 \cap A_F$ tel que $f(a) = M_0$ et $V(a) = r/p$.

Pour obtenir la démonstration on peut utiliser 1), 3) et 4).

Démonstration de la proposition 2. Soit $[F : K]$ fini et $a \in A_F$.

I) $\text{char } k = 0$. Nous devons montrer que $f(a) = 0$. Soit $P(X) = X^n + c_1 X^{n-1} + \dots + c_n$ le polynôme minimal de a et $a_1 = a, a_2, \dots, a_n$ ses racines. Si $f(a) > 0$, alors $V(c_1) = V(a_1 + \dots + a_n) = V(na_1 + (a_2 - a_1) + \dots + (a_n - a_1)) = V(a_1)$ (parce que $V(a_i - a_1) > V(a_1) = V(na_1)$), ce qui contredit l'hypothèse $a \in A_F$.

II) $\text{char } k = p$. Dans ce cas nous devons montrer que $f(a) \leq p/(p-1)$. Soit $F_1 = F(a)$. Nous pouvons admettre que F_1/F est totalement ramifiée. En effet, il suffit de remplacer F par F_2 , la sousexension nonramifiée maximale de F_1/F , et d'observer que $f_F(a) \leq f_{F_2}(a)$. Donc, nous pouvons supposer que F_1/F est totalement ramifiée et (avec les notations de 11)), que $M_0 > p/(p-1)$. De 11) et 12) on déduit qu'il existe $a_1 \in F_1 \cap A$, tel que $f(a_1) = M_0$ et $V(a_1) = r/p$. De 10) il résulte qu'il existe un polynôme d'Eisenstein $P(X) \in F[X]$ de degré p tel que $(P(a_1))^p \in A$. Soit $u = P(a_1)$. Si $f(u) > M_0 - 1 > 1/(p-1)$, alors de 4) on obtient $f(u^p) = 1 + f(u) > M_0$, c'est-à-dire une contradiction, parce que $u^p \in A$. Donc $f(u) \leq M_0 - 1$. Il existe alors $\sigma \in \text{Gal}(\bar{F}/F)$ tel que $V(\sigma(u)/u - 1) \leq M_0 - 1$; donc $V(u) \geq V(\sigma(u) - u) - M_0 + 1$. De 8) il résulte que $V(\sigma(u) - u) \geq f(a_1) + m_0 = M_0 + m_0$. Ainsi nous obtenons

$$(*) \quad V(u) \geq m_0 + 1.$$

Soit b une racine de $P(X)$. De 7) il résulte que $f(b) \leq 1/(p-1)$, donc

$f(a_1) > f(b)$. De 6) on déduit $V(u) = V(P(a_1)) \leq (p/(p-1))V(P'(b))$. Puis, de 9) il résulte que $V(P'(b)) = m_0 - r/p$. Nous obtenons donc:

$$(**) \quad V(u) \leq (p/(p-1))(m_0 - r/p) = (p/(p-1))m_0 - r/(p-1).$$

De (*) et (**) on déduit que $1 + m_0 \leq (p/(p-1))m_0 - r/(p-1)$, donc $1 + r/(p-1) \leq m_0/(p-1)$, d'où $p-1+r \leq m_0 = \min \{1+r, \dots\} \leq 1+r$, ce qui implique $p \leq 2$. Si $p \neq 2$, la démonstration est terminée. Pour $p = 2$, nous obtenons $m_0 = 1+r$ et $V(u) = m_0 + 1$. Mais $1 \in rZ$, donc $m_0 \in rZ$, d'où $V(u) \in rZ$, ce qui implique $V(u^p) \in rZ$. Nous obtenons donc une contradiction, parce que $u^p = (P(a_1))^p \in A$.

BIBLIOGRAPHIE

- [1] Ribenboim, P.: Théorie des Valuations, Les Presses de l'Université de Montréal, Montréal, Canada, 1964.
- [2] Schilling, O.F.G.: The Theory of Valuations, A.M.S. Math. Surveys, New York, 1950.

Zaharescu Alexandru
Faculté de Mathématiques
Université de Bucarest
Str. Academiei 14
70109 Bucarest
Romania