PHILIPPE ROBBA

Théorie de Galois p-adique

Groupe de travail d'analyse ultramétrique, tome 3, nº 1 (1975-1976), exp. nº 14, p. 1-8
<http://www.numdam.org/item?id=GAU_1975-1976__3_1_A8_0>

Groupe d'étude d'Analyse ultramétrique
(Y. AMICE, P. ROBBA)
3e année, 1975/76, n° 14, 8 p.
1er mars 1976

THÉORIE DE GALOIS p-ADIQUE

par Philippe ROBBA

(d'après un travail en commun avec B. DWORK [2])

Soit Ω un corps valué ultramétrique de caractéristique zéro, et soit K un sous-corps de Ω. Soit G le groupe des automorphismes continus de Ω sur K. La question se pose de savoir quels sont les éléments de Ω fixes pour tous les σ de G. Comme les σ sont continus, ils laissent fixes les éléments de l'adhérence de K (et donc dorénavant nous supposerons que K est complet). Y-a-t-il d'autres éléments fixes ?

Si Ω est une extension algébrique finie du corps complet K, on sait que la valuation de K s'étend de façon unique à Ω. Par ailleurs, si $\alpha \in \Omega$ et α' est un conjugué de α sur K, alors $|\alpha| = |\alpha'|$. Ceci montre que les automorphismes de Ω sur K sont automatiquement continus, et la théorie de Galois classique nous dit donc que les seuls éléments de Ω fixes pour tous les σ de G sont précisément ceux de K.

Un théorème de TATE [4] exprime que ce résultat subsiste si $G = \hat{K}$ est le complété de la clôture algébrique du corps complet K (rappelons que la valuation de K s'étend de façon unique à $\hat{K}$).

Nous allons montrer que ce résultat subsiste si G est une extension valuée maximalement complète et algébriquement close du corps complet K.

Nous utiliserons ce résultat pour montrer que les seuls éléments fixes pour certains automorphismes de fonctions méromorphes sont les éléments du complété de $K(x)$ pour la norme de Gauss. Ceci nous permettra de redémontrer certains résultats de factorisation d'opérateurs différentiels.

1. Théorie de Galois sur K.

Ici K désigne un corps valué ultramétrique complet de caractéristique zéro, $\hat{K}$ le complété de la clôture algébrique de K, Ω une extension algébriquement close maximalement complète, et G (resp. G_K) le groupe des automorphismes continus de Ω (resp. $\hat{K}$) sur K.

Remarquons qu'un automorphisme continu d'un corps valué préserve la valeur absolue (vérification laissée au lecteur).

1.1. THEOREME (TATE). - Les éléments de $\hat{K}$ fixes sous l'action des éléments de G_k sont précisément les éléments de K.

Nous indiquons le principe de la démonstration par AX [1] de ce théorème. L'étape essentielle est le lemme suivant qui est intéressant en lui-même. Si α est algébrique sur K, nous posons $\Delta(\alpha) = \max|\alpha - \alpha'|$ où α' parcourt l'ensemble dés conjugués de α sur K.

LEMME. - <u>Il existe une constante C, ne dépendant que de la caractéristique du corps résiduel $\overline{K}$, telle que l'on ait, pour tout α algébrique sur K,</u>

$$\Delta(\alpha) \geqslant Cd(\alpha , K) .$$

<u>Remarques.</u>

1° On a trivialement $\Delta(\alpha) \leqslant d(\alpha , K)$.

2° La valeur exacte de C est : $C = |p|^{-p/(p-1)^2}$, où $p = 1$ si $\operatorname{car} \overline{K} = 0$, et sinon $p = \operatorname{car} \overline{K}$.

<u>Démonstration du théorème.</u> - Soit $a \in \hat{K}$, tel que, pour tout $\sigma \in G_k$, $\sigma(a) = a$. Étant donné $\varepsilon > 0$, soit α algébrique sur K tel que $|a - \alpha| < \varepsilon$. Si α' est conjugué de α sur K, il existe $\sigma \in G_k$ tel que $\sigma(\alpha) = \alpha'$, et alors

$$|a - \alpha'| = |\sigma(a) - \sigma(\alpha)| = |a - \alpha| < \varepsilon ,$$

et donc $|\alpha - \alpha'| < \varepsilon$, ce qui entraîne $\Delta(\alpha) < \varepsilon$, et donc d'après le lemme on a $d(\alpha , K) \leqslant \varepsilon/C$, ce qui implique $d(a , K) \leqslant \varepsilon/C$. Ceci étant vérifié pour tout $\varepsilon > 0$, on a $d(a , K) = 0$, et donc $a \in K$.

1.2. THÉORÈME. - <u>Les éléments de Ω fixes sous l'action des éléments de G sont précisément les éléments de</u> K.

<u>Remarques.</u>

1° Nous ne savons pas si ce résultat est encore vrai sans l'hypothèse que Ω est maximalement complet. Ce théorème n'implique donc pas le résultat de TATE.

2° Le résultat de TATE est utilisé dans la démonstration.

Le théorème est une conséquence immédiate des lemmes 1.3 et 1.4.

1.3. LEMME. - <u>Soit α un élément de Ω n'appartenant pas à K. Il existe un automorphisme continu σ de $\hat{K}(\alpha)$ qui laisse fixes les éléments de K, mais ne laisse pas α fixe.</u>

<u>Démonstration.</u> - Si $\alpha \in \hat{K}$, l'assertion équivaut au théorème de Tate. Nous supposons donc que $\alpha \notin \hat{K}$, et par conséquent

$$d(\alpha , \hat{K}) = \gamma > 0 .$$

Comme α est transcendant sur $\hat{K}$, pour chaque $b \in \hat{K}$, nous pouvons définir un automorphisme σ_b de $\hat{K}(\alpha)$ sur $\hat{K}$ en posant

$$\sigma_b(\alpha) = \alpha + b .$$

Nous allons montrer que si $|b| \leq \gamma$, alors σ_b est continu, c'est-à-dire une isométrie de $\hat{K}(\alpha)$. Il suffit de considérer l'action de σ_b sur $\hat{K}[\alpha]$, mais puisque $\hat{K}$ est algébriquement clos, il suffit de considérer l'action de σ_b sur $\alpha + a$ avec $a \in \hat{K}$. On a alors, si $|\alpha + a| > \gamma \geq |b|$,

$$|\alpha + a + b| = |\alpha + a| ,$$

et si $|\alpha + a| = \gamma = |b|$,

$$\gamma \leq |\alpha + a + b| \leq \gamma ,$$

et donc encore $|\alpha + a| = |\alpha + a + b|$.

1.4. LEMME. - <u>Soit</u> Ω <u>un corps maximalement complet, et soit</u> K <u>un sous-corps fermé. Alors, tout automorphisme continu de</u> K <u>peut être étendu en un automorphisme continu de</u> Ω.

Ce lemme est une conséquence du lemme suivant plus adapté à des arguments d'induction transfinie.

1.5. LEMME. - <u>Soient</u> Ω <u>et</u> K <u>comme ci-dessus. Soit</u> τ <u>un morphisme continu de</u> K <u>dans</u> Ω <u>tel que</u> $\overline{K} = \overline{K^\tau}$ <u>(c'est-à-dire que</u> K <u>et</u> K^τ <u>ont le même corps résiduel). Alors</u> τ <u>peut être étendu en un automorphisme continu de</u> Ω.

<u>Démonstration</u>. - Considérons l'ensemble des paires (L, σ), de corps L intermédiaires entre K et Ω et de morphismes continus σ de L dans Ω tels que $\overline{L} = \overline{L^\sigma}$. Ces paires sont ordonnées de façon évidente. Si l'on a une chaîne (L_i, σ_i) de telles paires, il est clair que (L, σ), où $L = \cup L_i$ et $\sigma|_{L_i} = \sigma_i$, domine les (L_i, σ_i). Il résulte alors du lemme de Zorn qu'il existe un élément maximal (L, σ) tel que $(K, \tau) < (L, \sigma)$.

Nous allons montrer que $L = \Omega = L^\sigma$.

(i) L <u>est complet (à cause de la maximalité)</u>.

(ii) L <u>est algébriquement clos</u>.

En effet, si $z \notin L$ est algébrique sur L, alors σ peut être étendu en un morphisme de $L(z)$ dans Ω qui est une isométrie puisque la valuation de $L(z)$ qui étend celle de L est unique. Par une application du lemme de Zorn, σ peut être étendu en un morphisme $\hat{\sigma}$ de $\hat{L}$ dans Ω. Observons alors que $\hat{L}$ et $\hat{\sigma}\hat{L}$ ont le même corps résiduel que la clôture algébrique de $\hat{L}$. Ceci contredit donc la maximalité de (L, σ).

(iii) L <u>et</u> Ω <u>ont même groupe des valeurs</u>.

Sinon il existe $y \in \Omega$ tel que $|y| \notin |L| = |L^\sigma|$. Il en résulte que y est transcendant sur L et L^σ. Par conséquent, on peut étendre σ en un isomorphisme de $L(y)$ sur $L^\sigma(y)$ en posant $\sigma y = y$. Pour $\beta \in L$, on a

$$|y| \neq |\beta| = |\sigma(\beta)|$$

et donc

$$|y - \beta| = \max(|y| , |\beta|) = |y - \sigma(\beta)| ,$$

ce qui montre que cette extension de σ est continue. Par ailleurs, le corps de reste de $L(y)$ (resp. $L^\sigma(y)$) coïncide avec celui de L (resp. L^σ). Ceci contredit la maximalité de (L , σ).

(iv) L <u>et</u> Ω <u>ont même corps résiduel</u>.

Sinon il existe $y \in \Omega$, $|y| = 1$, tel que $\bar{y} \notin \bar{L} = \overline{L^\sigma}$, et donc y est transcendant sur L et L^σ. En posant $\sigma(y) = y$ on définit encore un isomorphisme continu de $L(y)$ dans $L^\sigma(y)$, et les corps residuels de $L(y)$ et $L^\sigma(y)$ coïncident avec $\bar{L}(\bar{y})$. Ceci contredit la maximalité de (L , σ).

(v) L <u>est maximalement complet</u>.

Sinon soit $\{D(a_i , \gamma_i)\}_{i\in N}$ une suite emboitée de disques avec leurs centres a_i dans L mais sans point commun dans L. Comme Ω est maximalement complet soit y un point commun dans Ω. Alors y est transcendant sur L.

Observons que $\{D(\sigma(a_i) , \gamma_i)\}_{i\in N}$ est également une suite de disques emboités qui ont donc un point commun z dans Ω. Ce point n'appartient pas à L^σ car autrement $\sigma^{-1}(z)$ appartiendrait à $L \cap D(a_i , \gamma_i)$ pour tous les i. Comme L^σ est algébriquement clos, z est transcendant sur L^σ, et on peut donc étendre σ en un isomorphisme de $L(y)$ dans $L^\sigma(z)$ en posant $\sigma y = z$. Pour vérifier la continuité, il suffit de montrer que $|y - \alpha| = |z - \sigma(\alpha)|$ pour tout $\alpha \in L$. Or

$$|y - \alpha| > d(y , L) = \inf \gamma_i ,$$

et donc il existe i tel que

$$|y - a_i| \leqslant \gamma_i < |y - \alpha| .$$

Par conséquent, $|y - \alpha| = |\alpha - a_i| > \gamma_i$. Comme $z \in D(\sigma(a_i) , \gamma_i)$, on a alors

$$|z - \sigma(\alpha)| = |(z - \sigma(a_i)) + \sigma(a_i - \alpha)| = |a_i - \alpha| = |y - \alpha| .$$

De plus, en vertu de (iv), la condition sur le corps de restes est trivialement vérifiée. Ceci contredit la maximalité de Ω.

(vi) En vertu de (iii) et (iv), Ω <u>est une extension immédiate de</u> L, <u>mais puisque</u> L <u>est maximalement complet, on a</u> $L = \Omega$.

Montrons alors que $L^\sigma = \Omega$. Comme σ^{-1} est un morphisme continu de $M = L^\sigma$ dans (et même sur) Ω tel que $\bar{M} = \overline{\sigma^{-1}(M)}$, il résulte de ce que nous venons de démontrer que σ^{-1} peut être étendu en un morphisme θ de Ω dans (et même sur) Ω. Alors $\theta^{-1}\Omega$ coïncide avec Ω, ce qui montre que $M = \Omega$.

2. Théorie de Galois au-dessus de E.

2.1. Soient K et Ω comme précédemment. On suppose de plus qu'il existe

$$t \in \Omega , \quad |t| = 1 ,$$

tel que $\bar{t}$ soit transcendant sur le corps résiduel $\bar{K}$.

On note E le complété de $K(x)$ pour la norme de Gauss. On rappelle que E s'identifie (avec sa norme) à l'espace $H_K(D(t, 1^-))$ des éléments analytiques à coefficients dans K sur le disque générique $D(t, 1^-)$.

On notera $\mathfrak{A}_a^\rho$ l'espace vectoriel des fonctions analytiques dans le disque

$$D(a, \rho^-),$$

et $\mathfrak{M}_a^\rho$ son corps des fractions, espace des fonctions méromorphes dans $D(a, \rho^-)$.

2.2. Soit $\sigma \in G$ et $\rho \leq 1$. Alors on associe de façon canonique à σ une application encore notée σ, de $\mathfrak{A}_t^\rho$ dans $\mathfrak{A}_{\sigma(t)}^\rho$ par la formule

$$u = \sum_n a_n(x-t)^n \to \sigma u = \sum_n \sigma(a_n)(x-\sigma(t))^n .$$

Il est clair que σ est un isomorphisme d'anneau qui commute avec les dérivations. Enfin, si $|\sigma(t)-t| < \rho$, σ définit un endomorphisme de $\mathfrak{A}_t^\rho$. Cet endomorphisme se prolonge de façon unique au corps des fractions $\mathfrak{M}_t^\rho$.

2.3. LEMME. - <u>Les éléments de</u> E <u>sont laissés fixes par</u> σ.

<u>Démonstration</u>. - Il est évident que σ laisse invariant $K(x)$.

Par ailleurs, si u est une fonction analytique bornée dans $D(t, 1^-)$,

$$u = \sum a_n(x-t)^n ,$$

on a pour la norme de la convergence uniforme sur $D(t, 1^-)$,

$$\|\sigma u\| = \sup_n |\sigma(a_n)| = \sup_n |a_n| = \|u\| .$$

Donc, par continuité, on voit que σ laisse fixe les éléments de E qui est le complété de $K(x)$ pour la convergence uniforme sur $D(t, 1^-)$.

2.4. <u>Remarque</u>. - Soit σ un isomorphisme continu de l'anneau $\mathfrak{A}_a^\rho$ sur $\mathfrak{A}_b^\rho$ qui commute avec les dérivations.

Si $u = c$ est une constante, $u' = 0$, donc $(\sigma u)' = 0$, donc $\sigma u'$ est une constante. Il en résulte que σ définit un automorphisme continu de Ω.

Si maintenant $u = x - a$, $u' = 1$, donc $(\sigma u)' = 1$, et alors $\sigma u = x - c$. Comme $x - a$ n'est pas inversible dans $\mathfrak{A}_a^\rho$, $x - c$ n'est pas inversible dans $\mathfrak{A}_b^\rho$, donc $c \in D(b, \rho^-)$. Alors il est clair que si $u = \sum a_n(x-a)^n$,

$$\sigma u = \sum \sigma(a_n)(x-c)^n .$$

Si l'on désire que l'endomorphisme σ de $\mathfrak{A}_t^\rho$ associé à l'endomorphisme continu σ de Ω, et $s \in D(t, \rho^-)$ par

$$u = \sum a_n(x-t)^n \to \sigma u = \sum \sigma(a_n)(x-s)^n ,$$

laisse invariant $K(x)$, il faut que σ laisse K invariant et que

$$\sigma x = \sigma(t + (x - t)) = \sigma(t) + x - s = x$$

soit $s = \sigma(t)$.

On voit donc que les endomorphismes construits en 2.2 sont les seuls qui laissent invariants $K(x)$ (et donc E).

2.5. THÉORÈME. - <u>Les seuls éléments de</u> $\mathcal{M}_t^\rho$ $(\rho \leq 1)$ <u>fixes pour tous les automorphismes de</u> $\mathcal{M}_t^\rho$, <u>associés aux</u> $\sigma \in G$ <u>tels que</u> $|\sigma(t) - t| < \rho$, <u>sont les éléments de</u> E .

<u>Démonstration</u>. - Soit $u \in \mathcal{M}_t^\rho$ tel que $\sigma u = u$ pour tous les σ du théorème. On peut toujours supposer que t n'est pas un pôle de u (il est clair que la définition de σ ne dépend pas du centre choisi pour le disque $D(t , \rho^-)$).

(i) Supposons que $u(t) = 0$. Comme t est transcendant sur $\hat{K}$, on a vu dans la démonstration du théorème 1.2 (cf. lemme 1.3) que, pour tout $a \in \hat{K}$, $|a| < 1$, il existe $\sigma \in C$ tel que $\sigma(t) = t + a$. On aura alors

$$u(t + a) = (\sigma u)(\sigma(t)) = \sigma(u(t)) = 0 .$$

Ceci montre que u a une infinité de zéros dans tout voisinage de t , donc que u est identiquement nul.

(ii) Nous ne supposons plus que $u(t) = 0$.

Soit σ un automorphisme associé à un automorphisme continu de Ω sur $K(t)$, c'est-à-dire laissant invariant K et t . On a alors $\sigma(u(t)) = \sigma u(\sigma(t)) = u(t)$.

D'après le théorème 1.2, il en résulte que $u(t)$ appartient au complété de $K(t)$ pour la valeur absolue induite de Ω . Or si $f \in K(x)$, on a $|f(t)| = |f|_{Gauss}$. Donc l'adhérence de $K(t)$ dans Ω s'identifie à E . Il existe donc $v \in E$ tel que $u(t) = v(t)$.

Il résulte alors du lemme 2.3 et des hypothèses sur u que $u - v$ est invariant pour tous les automorphismes associés aux $\sigma \in G$ tels que $|a(t) - t| < \rho$ et de plus $u - v$ s'annule en t , ce qui d'après (i) implique que $u - v$ est identiquement nul, et donc $u \in E$.

3. Factorisation des opérateurs différentiels.

3.1. On note $W_t^{\rho,\alpha}$ l'espace vectoriels des fonctions analytiques ayant une croissance logarithmique d'ordre α dans le disque $D(t , \rho^-)$ [3], c'est-à-dire l'espace des $u = \sum a_n(x - t)^n$ tels que

$$\sup_n |a_n| \frac{\rho^n}{(n + 1)^\alpha} < +\infty .$$

On sait [3] que si $|s - t| < \rho$, et si l'on considère le développement de u autour de s , $u = \sum b_n(x - s)^n$, alors on a également $\sup_n |b_n| \dfrac{\rho^n}{(n + 1)^\alpha} < +\infty$.

Par ailleurs, $W_t^{\rho,\alpha}$ est contenu dans $\mathfrak{A}_t^\rho$.

Il en résulte que si σ est un automorphisme de $\mathfrak{A}_t^\rho$, associé à un $\sigma \in \mathbb{G}$, tel que $|\sigma(t) - t| < \rho$, alors σ laisse $W_t^{\rho,\alpha}$ globalement invariant.

Si $L \in E[D]$ est un opérateur différentiel linéaire à coefficients dans E, on notera $\mathrm{Ker}_t\, L$ l'espace des fonctions holomorphes dans un voisinage de t annihilées par L. C'est un espace vectoriel dont la dimension est égale à l'ordre de L.

3.2. Le résultat que nous allons énoncer est déjà connu [3]. La démonstration que nous proposons ici offre une nouvelle interprétation de ce théorème. C'est CHRISTOL qui nous avait suggéré que ce résultat de factorisation devait pouvoir s'interpréter en terme de théorie de Galois.

THÉORÈME. - Soit $L \in E[D]$. Etant donnés $\rho \leqslant 1$ et $\alpha \geqslant 0$, soit R l'unique opérateur différentiel unitaire tel que

$$\mathrm{Ker}_t\, R = \mathrm{Ker}_t\, L \cap W_t^{\rho,\alpha} \quad (\text{resp. } \mathrm{Ker}_t\, R = \mathrm{Ker}_t\, L \cap \mathfrak{A}_t^\rho) .$$

Alors les coefficients de R sont dans E.

Démonstration. - Comme les automorphismes σ de $\mathfrak{A}_t^\rho$, précédemment définis, laissent les éléments de E fixes et commutent avec les dérivations, on voit que, si $u \in \mathfrak{A}_t^\rho$ et $Lu = 0$, alors $\sigma(Lu) = L\sigma(u) = 0$. Il en résulte que σ définit un automorphisme de $\mathrm{Ker}_t\, L \cap W_t^{\rho,\alpha}$ (resp. $\mathrm{Ker}_t\, L \cap \mathfrak{A}_t^\rho$).

Par ailleurs, il existe un unique opérateur différentiel unitaire

$$R = C_0 + C_1 D + \dots + D^k$$

dont le noyau est $\mathrm{Ker}_t\, L \cap W_t^{\rho,\alpha}$ (resp. $\mathrm{Ker}_t\, L \cap \mathfrak{A}_t^\rho$), et les coefficients c_i de R sont méromorphes dans $D(t, \rho^-)$. Posons $\sigma R = \sum \sigma(c_i) D^i$. Il est alors clair que, pour tout $u \in \mathfrak{A}_t^\rho$, $\sigma(Ru) = \sigma R(\sigma u)$. Par conséquent,

$$\sigma(\mathrm{Ker}_t\, R) = \mathrm{Ker}_t\, \sigma R .$$

D'après ce que l'on vient de voir, R et σR ont donc le même noyau et sont unitaires, donc $R = \sigma R$, autrement dit $\sigma(c_i) = c_i$ pour tout i. Il résulte alors du théorème 2.5 que $c_i \in E$ pour tout i.

BIBLIOGRAPHIE

[1] AX (J.). - Zeros of polynomials over local fields, The Galois action, J. of Algebra, t. 15, 1970, p. 417-428.

[2] DWORK (B.) et ROBBA (P.). - On ordinary linear p-adic differential equations, Trans. Amer. math. Soc. (à paraître).

[3] ROBBA (P.). - On the index of p-adic differential operators, I, Annals of Math., t. 101, 1975, p. 280-316.

[4] TATE (J.). – p-divisible groups, "Proceedings of a conference on local fields, NUFFIC summer school held at Driebergen in 1966", p. 158-183. – Berlin, Springer-Verlag, 1967.

(Texte reçu le 12 juin 1976)

Philippe ROBBA
138 rue Nationale
75013 PARIS