

Astérisque

WOLFGANG JENKNER

**Les corps p -adiques dont les groupes de Galois
absolus sont isomorphes**

Astérisque, tome 209 (1992), p. 221-226

<http://www.numdam.org/item?id=AST_1992__209__221_0>

© Société mathématique de France, 1992, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (<http://smf4.emath.fr/Publications/Asterisque/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

LES CORPS p -ADIQUES DONT LES GROUPES DE GALOIS ABSOLUS SONT ISOMORPHES

Wolfgang JENKNER

Soit p un nombre premier quelconque. Pour toute extension finie K/\mathbb{Q}_p , soit K^0/\mathbb{Q}_p la sous-extension abélienne maximale de K/\mathbb{Q}_p . De plus, on désignera par $\bar{\mathbb{Q}}_p$ une clôture algébrique de \mathbb{Q}_p , et par G_K le groupe de Galois $\text{Gal}(\bar{\mathbb{Q}}_p/K)$.

THÉORÈME.— Soient K/\mathbb{Q}_p et L/\mathbb{Q}_p deux extensions finies. Alors $G_K \simeq G_L$ entraîne $K^0 = L^0$.

Dans [3] M. Jarden et J. Ritter ont donné une démonstration de l'énoncé du théorème en faisant l'hypothèse supplémentaire que K et, par conséquent, L contiennent une racine de l'unité d'ordre $2p$. C'est là une restriction que J. Ritter a su enlever lorsque $p \neq 2$ ([6]).

D'un autre côté, tout en restant très proche des idées exposées dans [3], on peut montrer que le résultat reste encore vrai si l'extension de K engendrée par une racine de l'unité d'ordre $2p$ n'a pas de ramification sauvage (sur K), ce qui permet d'obtenir les résultats de [6] d'une manière quelque peu différente et, en même temps, d'aller un peu plus loin si $p = 2$.

D'ailleurs, c'est en supposant vérifiée cette condition-là que U. Jannsen, K. Wingberg ([2]) et V. Diekert ([1]) ont donné une description de G_K , à partir de laquelle on déduit les résultats susmentionnés d'une manière assez directe.

Or, pour ce qui concerne le but de cet article, les écueils de la ramification sauvage (dans le cas $p = 2$) seront tournés dans la proposition 2.

D'abord, fixons quelques notations: Pour toute extension finie K/\mathbb{Q}_p , soit n_K le degré, f_K le degré résiduel et e_K l'indice de ramification de cette extension. Si K'/K est une extension finie, on pose $f(K'/K) = f_{K'}/f_K$ et de même $e(K'/K) = e_{K'}/e_K$.

Pour tout $m \in \mathbb{N}$, on désigne par ζ_m une racine de l'unité d'ordre m (contenue dans $\bar{\mathbb{Q}}_p$).

De plus, soit $r_K = \max\{\nu \in \mathbb{N} \mid \zeta_{p^\nu} \in K(\zeta_{2p})\}$ et soit

$$d_K = \max\{\nu \in \mathbb{N} \mid K(\zeta_{p^{r_K+\nu}})/K(\zeta_{2p}) \text{ est non ramifiée } \}.$$

On voit facilement que $f_K = f_{K^0}$, $r_K = r_{K^0}$ et $d_K = d_{K^0}$ (cf. [3]).

PROPOSITION 1.- Soit K/\mathbb{Q}_p une extension finie telle que $\zeta_{2p} \in K$. Alors

$$\mathbb{Q}_p(\zeta_{(p^f-1)p^r}) \subset K^0 \subset \mathbb{Q}_p(\zeta_{(p^f p^d-1)p^{r+d}}) = K^0(\zeta_{p^{r+d}})$$

où f, d et r désignent respectivement f_K, d_K et r_K .

Preuve. - On utilisera des résultats de la théorie du corps de classes local ([7] XI, §4). Pour toute extension finie K'/\mathbb{Q}_p , soit $\mathcal{N}K'$ le groupe de normes (dans \mathbb{Q}_p^\times). Alors il est bien connu que $\mathcal{N}\mathbb{Q}_p(\zeta_{(p^f-1)p^r}) = \langle p^f \rangle \times U^{(r)}$, où $U^{(0)} = \mathbb{Z}_p^\times$ et $U^{(r)} = 1 + p^r \mathbb{Z}_p$ pour $r \geq 1$.

Soient $k \in \mathbb{N}_0$ et $u \in \mathbb{N}$ tels que $p \nmid u$ et $p^k u = [K^0 : \mathbb{Q}_p(\zeta_{(p^f-1)p^r})]$. Alors on a aussi $p^k u = (\mathcal{N}\mathbb{Q}_p(\zeta_{(p^f-1)p^r}) : \mathcal{N}K^0)$. On en déduit que

$$\mathcal{N}K^0 \supset (\langle p^f \rangle \times U^{(r)})^{p^k u} = \langle p^f p^k u \rangle \times U^{(r+k)} = \mathcal{N}\mathbb{Q}_p(\zeta_{(p^f p^k u-1)p^{r+k}}).$$

Il s'ensuit que le corps K^0 est contenu dans $\mathbb{Q}_p(\zeta_{(p^f p^k u-1)p^{r+k}})$. Étant donné que

$$p^k = e(\mathbb{Q}_p(\zeta_{(p^f p^k u-1)p^{r+k}})/\mathbb{Q}_p(\zeta_{(p^f-1)p^r})) = p^k u e(\mathbb{Q}_p(\zeta_{(p^f p^k u-1)p^{r+k}})/K^0),$$

on obtient $u = 1$, donc $K^0 \subset \mathbb{Q}_p(\zeta_{(p^f p^k-1)p^{r+k}})$. De plus, il en résulte que $\mathbb{Q}_p(\zeta_{(p^f p^k-1)p^{r+k}})/K^0$ n'est pas ramifiée.

Puis on a

$$\begin{aligned} p^{2k} &= [\mathbb{Q}_p(\zeta_{(p^f p^k-1)p^{r+k}}) : \mathbb{Q}_p(\zeta_{(p^f-1)p^r})] \\ &= [\mathbb{Q}_p(\zeta_{(p^f p^k-1)p^{r+k}}) : K^0] [K^0 : \mathbb{Q}_p(\zeta_{(p^f-1)p^r})], \end{aligned}$$

ce qui donne $[\mathbb{Q}_p(\zeta_{(p^f p^k-1)p^{r+k}}) : K^0] = p^k$.

Évidemment, le corps $K^0(\zeta_{p^{r+k}})$ est contenu dans $\mathbb{Q}_p(\zeta_{(p^f p^k-1)p^{r+k}})$. Comme toutes les sous-extensions de $\mathbb{Q}_p(\zeta_{p^{r+k}})/\mathbb{Q}_p(\zeta_{p^r})$ sont de la forme $\mathbb{Q}_p(\zeta_{p^{r+\nu}})/\mathbb{Q}_p(\zeta_{p^r})$, il s'ensuit $[K^0(\zeta_{p^{r+k}}) : K^0] = p^k$, donc $K^0(\zeta_{p^{r+k}}) = \mathbb{Q}_p(\zeta_{(p^f p^k-1)p^{r+k}})$. Puisque $K^0(\zeta_{p^{r+k}})/K^0$ est non ramifiée, on a $k \leq d$. D'autre part, comme $K^0(\zeta_{p^{r+k+1}}) = \mathbb{Q}_p(\zeta_{(p^f p^k-1)p^{r+k+1}})$ est une extension ramifiée de $K^0(\zeta_{p^{r+k}}) = \mathbb{Q}_p(\zeta_{(p^f p^k-1)p^{r+k}})$, on a $k \geq d$. \square

Pour lier l'action de G_K sur des racines de l'unité à la structure même du groupe, on se servira du lemme suivant.

LEMME 1.— Soit k un corps et soit D le corps de décomposition du polynôme $x^n - a \in k[x]$, que l'on suppose irréductible sur $K = k(\zeta_n)$.

Soit le caractère $\chi : \text{Gal}(K/k) \rightarrow \mathbb{Z}/(n)^\times$ donné par $\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$. Alors pour tout $\sigma \in \text{Gal}(K/k)$ et pour tout $\tau \in \text{Gal}(D/K)$, on a $\tau^\sigma = \tau^{\chi(\sigma)}$.

Preuve. — Tous les caractères de $\text{Gal}(D/K)$ sont de la forme $\phi : \tau \mapsto \frac{\tau(\alpha)}{\alpha}$ pour tout $\tau \in \text{Gal}(D/K)$, où α est une racine de $x^n - a$. On voit aussitôt que $\phi(\tau^\sigma) = \sigma\phi(\tau)$. Il suffit de choisir l'automorphisme τ et le caractère ϕ tels que $\phi(\tau) = \zeta_n$. \square

Remarque. On peut prouver un résultat plus général : Soit D/k une extension galoisienne finie et K/k une sous-extension galoisienne telle que D/K soit abélienne. Soient $G = \text{Gal}(D/k)$ et $H = \text{Gal}(D/K)$. Alors

$$(D^\times/K^\times)^G \rightarrow \text{Hom}_G(H, K^\times)$$

$$\alpha K^\times \mapsto \left(\tau \mapsto \frac{\tau(\alpha)}{\alpha} \right)$$

est un isomorphisme.

Esquissons brièvement une preuve de cette proposition : La suite exacte de Hochschild-Serre, appliquée au G -module K^\times donne un isomorphisme $H^1(G, K^\times) \xrightarrow{res} H^1(H, K^\times)^G = \text{Hom}_G(H, K^\times)$, tandis que

$$1 \rightarrow K^\times \rightarrow D^\times \rightarrow D^\times/K^\times \rightarrow 1$$

donne l'isomorphisme $(D^\times/K^\times)^G \xrightarrow{\delta} H^1(G, K^\times)$. \square

Donc, pour appliquer le lemme, il faudra construire des extensions appropriées.

PROPOSITION 2.— Soit K/\mathbb{Q}_p une extension finie et soit π un élément premier de K . Alors, pour tout $n \in \mathbb{N}$, on a

$$K(\pi^{p^{-n}}) \cap K(\zeta_{p^{r+d}}) = K.$$

(Ici $\pi^{p^{-n}}$ désigne une racine dans $\bar{\mathbb{Q}}_p$ du polynôme $X^{p^n} - \pi$, et $r = r_K$, $d = d_K$.)

Preuve. — Si $p \neq 2$, il suffit de comparer les indices de ramification : $e(K(\pi^{p^{-n}})/K) = p^n$, alors que $e(K(\zeta_{p^{r+d}})/K) \mid p - 1$.

Si $p = 2$, on s'appuie sur les deux propositions auxiliaires suivantes :

- (i) On a toujours $\sqrt{\pi} \notin K(\zeta_4)$.
 (ii) Si $d \geq 1$, on a $\sqrt{\pi} \notin K(\zeta_{2^{r+1}})$.

Preuve de (i). Supposons $\zeta_4 \notin K$ et soient $a, b \in K$ tels que $\zeta_4 = a + b\sqrt{\pi}$, alors $-1 = a^2 + b^2\pi + 2ab\sqrt{\pi}$ et, par conséquent, $a^2 = -1$ ou $b^2\pi = -1$, ce qui est une contradiction.

Preuve de (ii). Si $K(\sqrt{\pi}) \subset K(\zeta_{2^{r+1}})$, l'extension $K(\zeta_4)/K$ doit être ramifiée, puisque $K(\zeta_{2^{r+1}})/K(\zeta_4)$ ne l'est pas. Alors, il se trouve trois sous-extensions ramifiées de l'extension $K(\zeta_{2^{r+1}})/K$ de degré 4, que voici :

$$K(\zeta_4)/K, \quad K(\sqrt{\pi})/K, \quad K(\zeta_4\sqrt{\pi})/K.$$

Ces extensions de degré 2 sont différentes deux à deux grâce à l'assertion (i), pourtant il en existe une autre non ramifiée. Cela n'est pas possible.

Maintenant, pour prouver la proposition, on pourrait procéder par induction, mais il est plus facile d'utiliser un critère connu ([4], ch. VIII, 9). \square

Revenons aux données du théorème. Soient K/\mathbb{Q}_p et L/\mathbb{Q}_p deux extensions finies. Soit $\varphi : G_K \rightarrow G_L$ un isomorphisme de groupes topologiques.

Pour tout ce qui suit on fait la supposition que K'/K et L'/L sont des extensions finies telles que $G_{L'} = \varphi(G_{K'})$.

Les hypothèses entraînent que l'on a un isomorphisme $G_K^{ab} \simeq G_L^{ab}$ des groupes quotient abéliens maximaux. Du fait qu'un tel groupe est isomorphe au produit direct de \mathbb{Z} avec le groupe des unités du corps, on déduit facilement que $f_K = f_L$, $r_K = r_L$, $d_K = d_L$ et, de plus, si $K' = K(\zeta_n)$ on a $L' = L(\zeta_n)$ ([3]).

LEMME 2.- *S'il existe des extensions $K' = K(\alpha)$ et $L' = L(\beta)$ de degré n respectivement sur K et sur L telles que $\alpha^n \in K$, $\beta^n \in L$ et que $K(\alpha) \cap K(\zeta_n) = K$, alors, quel que soit $\sigma \in G_K$, on a $\varphi(\sigma)(\zeta_n) = \sigma(\zeta_n)$.*

Preuve. - C'est une conséquence du lemme 1 (compte tenu du fait que l'on a aussi $L(\beta) \cap L(\zeta_n) = L$). \square

PROPOSITION 3.- *Soit $n \in \mathbb{N}$ tel que $p \nmid n$. Alors, pour tout $\sigma \in G_K$, on a $\varphi(\sigma)(\zeta_n) = \sigma(\zeta_n)$.*

Preuve. - Soit π_K un élément premier de K et soit α une racine n -ième quelconque de π_K . Alors $K' = K(\alpha)$ est une extension modérément et totalement ramifiée de K et, par conséquent, L' l'est aussi de L . Comme une telle extension peut être engendrée par une racine n -ième d'un élément premier de L , toutes les conditions du lemme précédent sont satisfaites. \square

Rappelons que les éléments du groupe de Weil W_K^{ab} sont les automorphismes appartenant à G_K^{ab} dont les restrictions à l'extension non ramifiée maximale de K sont des puissances (à exposant entier) de l'automorphisme de Frobenius associé à K .

COROLLAIRE 1.- $\varphi(W_K^{ab}) = W_L^{ab}$.

Preuve. - L'extension non ramifiée maximale est engendrée par toutes les racines de l'unité ζ_n telles que $p \nmid n$. \square

On désigne par $\varphi_{K',L'}$ la restriction $\varphi|_{W_{K'}}: W_{K'}^{ab} \rightarrow W_{L'}^{ab}$. De même, si $\psi = \varphi^{-1}$, on a un isomorphisme $\psi_{L',K'}$, de sorte que $\psi_{L',K'} = (\varphi_{K',L'})^{-1}$. En utilisant l'isomorphisme de réciprocité ([7] XIII, §4)

$$(\cdot, K^{ab}/K) : K^\times \rightarrow W_K^{ab},$$

et de même pour L , on obtient un isomorphisme $\bar{\varphi}_{K,L} : K^\times \rightarrow L^\times$ défini par $\bar{\varphi}_{K,L} = (\cdot, L^{ab}/L)^{-1} \circ \varphi_{K,L} \circ (\cdot, K^{ab}/K)$ (et de même pour K' et L').

PROPOSITION 4.- (i) $\bar{\varphi}_{K',L'}|_{K^\times} = \bar{\varphi}_{K,L}$.

(ii) $\bar{\psi}_{L',K'} = (\bar{\varphi}_{K',L'})^{-1}$.

(iii) Soit $M \subset \bar{\mathbb{Q}}_p^\times$ tel que $K' = K(M)$. Alors $L' = L(\bar{\varphi}_{K',L'}(M))$.

(iv) Soit π_K un élément premier de K . Alors $\bar{\varphi}_{K,L}(\pi_K)$ est un élément premier de L .

Preuve. - L'assertion (i) résulte de propriétés connues du transfert ([7] XI, §3 et XIV, §6 Ex 1.). La propriété (ii) est banale, alors que (iii) n'est qu'une conséquence de (i) et (ii). Pour ce qui concerne (iv), il suffit de remarquer que $(\pi_K, K^{ab}/K)$ est un prolongement de l'automorphisme de Frobenius ([7] XIII, Prop.13). \square

COROLLAIRE 2.- Si π_K est un élément premier de K tel que $K' = K(\sqrt[n]{\pi_K})$, alors il y a un élément premier π_L de L tel que $L' = L(\sqrt[n]{\pi_L})$, quel que soit $n \in \mathbb{N}$.

PROPOSITION 5.- Posons $r = r_K = r_L$, $d = d_K = d_L$. Alors, pour tout $\sigma \in G_K$ on a $\varphi(\sigma)(\zeta_{p^{r+d}}) = \sigma(\zeta_{p^{r+d}})$.

Preuve. - C'est là une conséquence immédiate des lemme 2, corollaire 2 et proposition 2. \square

Achevons la démonstration du théorème: Soit $F = \mathbb{Q}_p(\zeta_{(p^r p^d - 1)p^{r+d}})$. On obtient un isomorphisme $\text{Gal}(K(\zeta_{p^{r+d}})/K) \rightarrow \text{Gal}(L(\zeta_{p^{r+d}})/L)$ et, par conséquent, un isomorphisme $\text{Gal}(F/K^0) \rightarrow \text{Gal}(F/L^0)$ donné par $\sigma|_F \mapsto \varphi(\sigma)|_F$ pour tout $\sigma \in G_K$ (Prop. 1); mais ces restrictions sont identiques d'après la prop. 3 et la prop. 5. \square

Bibliographie

- [1] V. Diekert, *Über die absolute Galoisgruppe dyadischer Zahlkörper*, J. Reine Angew. Math. **350** (1984), 152 – 172.
- [2] U. Jannsen et K. Wingberg, *Die Struktur der absoluten Galoisgruppe p -adischer Zahlkörper*, Invent. Math. **70** (1982), 71 – 98.
- [3] M. Jarden et J. Ritter, *On the characterization of local fields by their absolute Galois groups*, J. Number Th., Vol 11, No 1 (1979).
- [4] S. Lang, *Algebra*, Addison-Wesley 1984.
- [5] J. Neukirch, *Class field theory*, Springer-Verlag, Berlin ... 1986.
- [6] J. Ritter, *p -adic fields having the same type of algebraic extensions*, Math. Ann. **238** (1978), 281 – 288.
- [7] J.-P. Serre, *Local fields*, Springer-Verlag, New York ... 1979.

Wolfgang Jenkner
Institut für Mathematik
Karl-Franzens-Universität
Heinrichstraße 36/IV
A-8010 Graz, Autriche