Journal de Théorie des Nombres de Bordeaux **11** (1999), 161–172

Descente et parallélogramme galoisiens

par Richard MASSY et Sylvie MONIER-DERVIAUX

Résumé. Soit p un nombre premier impair. Soit D/J une p-extension galoisienne de corps ne contenant pas les racines p-ièmes de l'unité : $J \cap \mu_p = \{1\}$. Notons G le groupe de Galois de D/J et $\Phi(G)$ son sous-groupe de Frattini. Via une notion de descente galoisienne et les parallélogrammes galoisiens qu'elle induit, nous construisons ici toutes les extensions D/J telles que $\Phi(G)$ soit d'ordre p.

Abstract. Let p be a prime number. Lest D/J be a Galois p-extension which does not contain the p-th roots of unity: $J \cap \mu_p = \{1\}$. Denote by G the Galois group of D/J and by $\Phi(G)$ the Frattini subgroup of G. Via a Galois descent notion and the induced Galois parallelograms, we construct all the extensions D/J such that $\Phi(G)$ is of order p.

Connaissant une p-extension galoisienne qui contient le groupe μ_p des racines p-ièmes de l'unité, comment décrire une p-extension de même groupe de Galois mais ne contenant plus ces racines ? Pour répondre à cette question, nous introduisons une notion de "descente galoisienne" qui consiste intuitivement à translater sur un sous-corps une extension galoisienne donnée. Après avoir défini précisément un "problème de descente" induit par la donnée d'une extension galoisienne E/K et d'une extension algébrique K/J, nous obtenons d'abord un critère de résolubilité d'un tel problème lorsque E/K est une p-extension et K/J une extension galoisienne de degré non divisible par p comme lorsque $K = J(\mu_p)$ (théorème 1). Avec la contrainte supplémentaire d'une classe de cohomologie fixée, nous résolvons ensuite explicitement un problème de plongement à noyau d'ordre p d'une p-extension galoisienne non kummérienne via les solutions du problème kummérien translaté (théorème 2).

Lorsque l'on figure géométriquement par des segments parallèles de longueurs égales les extensions galoisiennes dont les groupes de Galois sont isomorphes, la descente galoisienne induit une notion de "parallélogramme galoisien" qui généralise celle d'extension galoisienne. Un parallélogramme galoisien est la donnée d'un problème de descente résoluble et de l'une de ses solutions. Toutes les propriétés usuelles de la théorie de Galois classique s'étendent aux parallélogrammes galoisiens (cf. [7]); nous en énonçons quelques unes dans la proposition 1. Puis nous prouvons l'existence arithmétique des parallélogrammes galoisiens et généralisons à ceux-ci le dévissage canonique d'une extension galoisienne de corps de nombres par les corps des invariants du groupe de décomposition et du groupe d'inertie d'un diviseur d'un idéal premier du corps de base (théorème 3). Nous montrons de plus que, comme une extension galoisienne, un parallélogramme galoisien de corps de nombres se localise (proposition 2). L'intérêt de la notion de parallélogramme galoisien étant ainsi établi, nous nous posons la question de son dépassement : comment prolonger un parallélogramme galoisien par un autre ? C'est l'objet du théorème 4 qui reprend, sans classe de cohomologie, la situation du théorème 2 avec un pas de descente cyclotomique. Ce théorème 4 constitue un premier résultat de prolongement de notre généralisation "en dimension 2" des extensions galoisiennes; en outre il fournit, comme cas particulier, une description, avec élément primitif explicite, de toutes les extensions cycliques non kummériennes de degré p ou p^2.

1. Problème de descente

Un problème naturel de théorie de Galois classique est le suivant.

"Problème de la descente galoisienne". *Soient E/K une extension galoisienne et K/J une extension algébrique. Nous appelons "problème de descente défini par E/K et K/J", et notons $[E/K, K/J]$, la question de savoir s'il existe un sous-corps $D \subseteq E$, galoisien sur J, tel que $D \cap K = J$ et $DK = E$.*

Si le problème $[E/K, K/J]$ est résoluble, on dira que E/K est "descendable sur J" (en abrégé $(E/K)\, desc_J$), et une solution D/J de $[E/K, K/J]$ sera appelée "une descendue de E/K sur J" (en abrégé $(D/J) = desc_J\,(E/K)$).

Un cas particulier de ce problème est le

"Problème de la p-descente cyclotomique" *où p est un nombre premier impair. C'est le problème de descente $[E/K, K/J]$ où :*

- K est un corps de caractéristique différente de p contenant le groupe μ_p des racines p-ièmes de l'unité;

- E/K une p-extension galoisienne;

- J un sous-corps de K ne contenant pas μ_p : $J \cap \mu_p = \{1\}$;

- K/J une extension galoisienne de degré non divisible par p.

Dans [1], G. Brattström a résolu positivement le problème de la p-descente cyclotomique pour tout p premier impair, E/K une p-extension galoisienne non abélienne de degré p^3 et $K = J(\mu_p)$. Nous généralisons ici ce résultat au cas d'une p-extension galoisienne (finie) quelconque E/K de la façon suivante. On obtient d'abord un critère de résolubilité du problème de la p-descente cyclotomique en quotientant le groupe de Galois de E/K par son sous-groupe de Frattini. Ce critère permet de se ramener au cas d'une p-extension abélienne élémentaire. On ajoute ensuite une classe de cohomologie au problème de descente, et l'on résout un problème de plongement non kummérien au moyen de la descente d'une solution, fournie par les théorèmes de [6], du problème kummérien translaté.

Théorème 1. *Soient p un nombre premier impair et E/K une p-extension galoisienne de groupe $\Gamma := Gal(E/K)$. Soit K/J une extension galoisienne finie telle que p ne divise pas le degré $[K : J]$.*
(1) Pour que le problème de descente $[E/K, K/J]$ soit résoluble, il faut et il suffit que les deux conditions suivantes soient vérifiées :
(1.1) L'extension E/J est galoisienne
(1.2) Le problème de descente $[E^{\Phi(\Gamma)}/K, K/J]$ est résoluble, où $E^{\Phi(\Gamma)}$ désigne le corps des invariants dans E du sous-groupe de Frattini de Γ.
(2) Lorsqu'il est résoluble, le problème $[E/K, K/J]$ admet une unique solution. Précisément, supposons que E/K admette une descendue D/J. Le sous-groupe Γ de $Gal(E/J)$ admet un unique complément V. Ce complément V est facteur direct, et l'on a $D = E^V$.

Démonstration. Confer [8].

Ce théorème 1 permet de se ramener à une extension de base p-abélienne élémentaire. Notons :
- L/J une p-extension galoisienne de groupe $Gal(L/J)$ abélien d'exposant p;
- $K := J(\mu_p)$, $E := L(\mu_p)$, $\Gamma := Gal(E/K)$, $V := Gal(E/L)$;
- $i(v)$ l'un quelconque des entiers tels que $v(\zeta_p) = \zeta_p^{i(v)}$ $(v \in V)$ où $\zeta_p \in \mu_p$ est une racine primitive p-ième fixée;
- g_V l'homomorphisme défini par

$$\begin{aligned} g_V \,:\, E^\times &\longrightarrow E^\times/E^{\times p} \\ x &\longmapsto g_V(x) := \left(\prod_{v\in V} v^{-1}(x)^{i(v)}\right) \bmod E^{\times p}; \end{aligned}$$

- $\widehat{g_V} : E^\times \to E^\times$ un relèvement de g_V :

$$\widehat{g_V}(x) \bmod E^{\times p} = g_V(x) \quad (x \in E^\times);$$

- lg l'isomorphisme $\begin{aligned} \mu_p &\xrightarrow{\sim} \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}. \\ \zeta_p^n &\longmapsto n \end{aligned}$

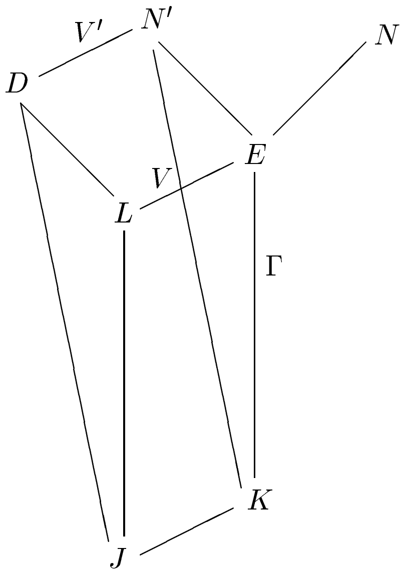
Identifions $Gal(L/J)$ à Γ par la restriction à L. On sait alors que pour toute classe de cohomologie $\varepsilon \in H^2(\Gamma, \mathbb{F}_p)$, un problème de plongement $[L/J, \varepsilon]$ est résoluble si et seulement si le problème translaté $[E/K, \varepsilon]$ est résoluble [3].

L'énoncé suivant est une version améliorée d'un théorème de [9].

Théorème 2. *Soit* $\varepsilon \in H^2(\Gamma, \mathbb{F}_p)$ *une classe de cohomologie induisant un problème de plongement* $[L/J, \varepsilon]$ *résoluble, et soit* $N := E(x^{1/p})/K$ $(x \in E^{\times})$ *une solution de* $[E/K, \varepsilon]$.

(1) L'extension $N' := E(\widehat{g_V}(x)^{1/p})/K$ *est aussi une solution du problème* $[E/K, \varepsilon]$ *pour laquelle l'extension* N'/J *est galoisienne. De plus, dans* $Gal(N'/J)$, *le sous-groupe* $Gal(N'/K)$ *admet un unique complément* $V' \tilde{\to} Gal(K/J)$ *qui est facteur direct :* $Gal(N'/J) = V' \times Gal(N'/K)$.

(2) Soit X *une racine* p*-ième quelconque de* $\widehat{g_V}(x)$: $X^p = \widehat{g_V}(x)$. *Le corps* $D := L\left(\sum_{v' \in V'} v'(X)\right)$ *définit une descendue* D/L *de* N'/E, *et une descendue* D/J *de* N'/K.



(3) Identifions $Gal(D/L)$ *à* $Gal(N'/E)$ *par la restriction à* D, *puis* $Gal(N'/E)$ *à* $\mathbb{F}_p$ *par l'isomorphisme*

$$\begin{array}{rcl} Gal(N'/E) & \xrightarrow{\sim} & \mathbb{F}_p \\ \nu & \longmapsto & lg(\nu(X)/X), \end{array}$$

où X *est la racine du (2). Alors, la descendue* D/J *de* N'/K *est une solution du problème de plongement* $[L/J, \varepsilon]$.

Scholie. Par [6], on dispose de formules explicites qui fournissent les éléments $x \in E^\times$ induisant les solutions $N = E(x^{1/p})/K$ des problèmes kummériens $[E/K, \varepsilon]$ résolubles. Le (2) du théorème ci-dessus fournit donc, via l'homomorphisme g_V, un élément primitif explicite sur L du corps D d'une solution D/J de tout problème non kummérien résoluble $[L/J, \varepsilon]$.

Il suffit de reprendre la preuve du théorème 4.3 de [8] sans la puissance $[K : J]^{-1}$ pour l'élément primitif du corps N'. Cette puissance n'est en fait nécessaire que pour obtenir le bon 2-cocycle.

Exemple. Prenons $J = \mathbb{Q}$, $p = 3$, et $\zeta_3 = e^{2i\pi/3} = j$. Soit L le compositum des extensions cubiques galoisiennes L_1, L_2, L_3 de $\mathbb{Q}$ définies respectivement par les polynômes irréductibles

$$X^3 - 21X - 7, \quad X^3 - 39X - 26, \quad X^3 - 1533X - 2044.$$

La translatée sur $K = \mathbb{Q}(j)$ de l'extension $L = L_1L_2L_3/\mathbb{Q}$ est l'extension $E = K(\alpha_1, \alpha_2, \alpha_3)/K$ où

$$\alpha_1^3 = 7(2+3j), \quad \alpha_2^3 = 13(3+4j), \quad \alpha_3^3 = -7.73(11+26j).$$

Soient σ_1, σ_2 les K-automorphismes de $K(\alpha_1, \alpha_2)/K$ définis par

$$\sigma_i(\alpha_m)/\alpha_m = j^{\delta_{im}} \quad (1 \le i, m \le 2).$$

On a $x_1\sigma_1(x_1)\sigma_1^2(x_1) = j$ (resp. $x_2\sigma_2(x_2)\sigma_2^2(x_2) = -7.73(11+26j)$) pour

$$x_1 = \frac{(1+\alpha_1)(2-\alpha_1)^2}{(1-j)^3\alpha_2} \left(\textit{resp.}\ x_2 = \frac{7(-4+9j-3\alpha_2)(1-3j+\alpha_2)(2+3j+\alpha_2)}{2\alpha_1(1-3j-\alpha_2)} \right).$$

D'après ([6],Th.4(I)(1°)) pour $\omega = 1$, le problème de plongement $[E/K, \varepsilon]$ où

$$\varepsilon = ((7(2+3j)))_E + (13(3+4j), -7.73(11+26j))_E$$

est résoluble. Autrement dit, le corps $E = K(\alpha_1, \alpha_2, \alpha_3)$ se plonge dans un corps de degré 162 sur $\mathbb{Q}$, extension galoisienne de K de degré 81 de groupe de Galois le produit central du groupe cyclique d'ordre 9 et du groupe non abélien d'ordre 27 d'exposant 3 (cf.[6], Prop.2[ ]). Une solution $N = E(x^{1/3})/K$ est fournie par l'élément

$$x = k_1\, x_2\, \sigma_2(x_2^2)$$

où $k_1 \in K(\alpha_1)$ vérifie $\sigma_1(k_1) = k_1\, x_1\, \sigma_2(x_1)\, \sigma_2^2(x_1)$. On peut prendre

$$\begin{aligned} x \ = \ & (6 + 7j + \frac{1}{2107}(4450 + 1996j)\alpha_1 + \alpha_1^2)(-4 + 9j - 3\alpha_2)(1 - 3j + \alpha_2) \\ & \times \frac{(2 + 3j + \alpha_2)(-4 + 9j - 3j\alpha_2)^2(1 - 3j + j\alpha_2)^2(2 + 3j + j\alpha_2)^2}{(1 - 3j - \alpha_2)(1 - 3j - j\alpha_2)^2}. \end{aligned}$$

Par ailleurs, soit $V = Gal(E/L) = \{id, v\}$. On a

$$v(\alpha_1) = \frac{\alpha_1^2}{2+3j}, \quad v(\alpha_2) = \frac{\alpha_2^2}{3+4j}$$

car $N_{E/L}(\alpha_i){=}N_{K(\alpha_i)/L_i}(\alpha_i)$ et $L_i \cap \mu_3{=}\{1\}$ $(i{=}1,2)$. Ainsi :

$$\begin{aligned} v(x) = &\left(\frac{1}{3+4j}\right)^6 \left(-1 - 7j - (1+3j)\ \alpha_1 - \frac{2}{2107}(603+811j)\ \alpha_1^2\right) \\ &\times \left(-3 - 43j - 3\alpha_2^2\right)(13j + \alpha_2^2)(9 - j + \alpha_2^2)(-3 - 43j - 3j^2\alpha_2^2)^2 \\ &\times (13j + j^2\alpha_2^2)^2(9 - j + j^2\alpha_2^2)^2 \ \ \frac{1}{(13j - \alpha_2^2)(13j - j^2\alpha_2^2)^2}. \end{aligned}$$

Soit maintenant X une racine cubique quelconque de $\widehat{g_V}(x) = xv(x)^2$. Clairement

$$\left(\frac{1}{v(x)}\right)^3 = \frac{v(\widehat{g_V}(x))}{\widehat{g_V}(x)^2} = \left(\frac{v'(X)}{X^2}\right)^3$$

où, dans les notations du (1) de l'énoncé, $V' = \{id, v'\}$. Or on doit avoir $Xv'(X) \in L$; par suite

$$v'(X) = X^2/v(x).$$

D'après le théorème 2, l'extension $D{=}L\left(X{+}(\frac{X^2}{v(x)})\right)/\mathbb{Q}$ est donc la descendue sur $\mathbb{Q}$ de $N' = E(\widehat{g_V}(x)^{1/3})/K$ et, pour les identifications de l'énoncé, c'est une solution du problème de plongement $[L/\mathbb{Q}, \varepsilon]$.

2. Parallélogramme galoisien

Définition. Nous appelons "parallélogramme galoisien" la donnée d'un problème de descente résoluble $[M/K, K/J]$, où K/J est une extension galoisienne, et de l'une de ses solutions L/J : $(L/J) = desc_J\,(M/K)$. Nous notons ce parallélogramme $[M/K, K/J, L/J]$, ou bien (J, K, M, L) en abrégé géométrique.

$$\begin{tikzcd}
 & M \arrow[dd, dash] \\
L \arrow[ur, dash] \arrow[dd, dash] & \\
 & K \\
J \arrow[ur, dash] &
\end{tikzcd}$$

Remarquons que :

- le problème de descente $[M/L, L/J]$ est résoluble de solution $(K/J) = desc_J\,(M/L)$, d'où le parallélogramme "transposé" (J, L, M, K);

- le parallélogramme (J, K, M, L), ainsi que son transposé, n'admettent qu'une seule diagonale, l'extension galoisienne M/J.

La notion de parallélogramme galoisien généralise celle d'extension galoisienne. En effet, la donnée d'une extension galoisienne E/F n'est que celle du parallélogramme "plat" (F, F, E, E) ou (F, E, E, F).

On peut voir un parallélogramme galoisien comme une première figure d'une théorie de Galois "en dimension 2" qui généralise, dans la catégorie produit $\mathbf{Gr^2}$ de la catégorie des groupes par elle-même, toutes les propriétés usuelles de la théorie de Galois classique [7].

Après avoir justifié arithmétiquement la notion de parallélogramme galoisien, notre objectif est ici le théorème 4 à suivre. Nous ne considérons que des extensions finies.

Proposition 1. *Soit (J, K, M, L) un parallélogramme galoisien.*
(1) Pour tout corps intermédiaire E, $K \subseteq E \subseteq M$, on a le parallélogramme galoisien $(L^{(A_{|L})}, E, M, L)$ où $L^{(A_{|L})}$ désigne le corps des invariants dans L de l'image par la restriction à L du groupe $A := Gal(M/E)$.
(2) Pour toute extension galoisienne intermédiaire E_1/E_0 de M/K, $K \subseteq E_0 \subseteq E_1 \subseteq M$, on a le parallélogramme galoisien $(L^{(A_{0|L})}, E_0, E_1, L^{(A_{1|L})})$ où $A_i := Gal(M/E_i)$ $(i = 0, 1)$.
(3) Soit F un corps intermédiaire, $J \subseteq F \subseteq L$, et toujours $K \subseteq E \subseteq M$. Si l'on a le parallélogramme galoisien (J, K, E, F), on a le parallélogramme galoisien (F, E, M, L).

Démonstration. Conséquences directes des définitions et de la théorie de Galois classique. □

Nous définissons le degré d'un parallélogramme (J, K, M, L) comme étant le couple $([M : K], [K : J])$.

Le théorème suivant montre que la notion de parallélogramme galoisien existe arithmétiquement. Pour un corps de nombres F, on désigne par O_F l'anneau des entiers de F et par $Spec\, O_F$ l'ensemble des idéaux premiers de O_F.

Théorème 3. *Soit (J, K, M, L) un parallélogramme galoisien de corps de nombres de degré (p^n, d) où p est un nombre premier ne divisant pas d. Soit $\mathcal{P} \in Spec\, O_K$ et $\mathcal{Q} \in Spec\, O_L$ deux idéaux premiers de même trace*

$$\mathcal{T} := \mathcal{P} \cap O_J = \mathcal{Q} \cap O_J$$

sur J. Pour l'unique idéal premier $\mathcal{R} \in Spec\, O_M$ tel que

$$\mathcal{R} \cap O_K = \mathcal{P}, \quad \mathcal{R} \cap O_L = \mathcal{Q},$$

on a les parallélogrammes galoisiens

$$(L^{D_\mathcal{Q}}, M^{D_\mathcal{R}}, M, L), \quad (L^{I_\mathcal{Q}}, M^{I_\mathcal{R}}, M, L), \quad (L^{D_\mathcal{Q}}, M^{D_\mathcal{R}}, M^{I_\mathcal{R}}, L^{I_\mathcal{Q}})$$

où $D_{\mathcal{Q}}$, $I_{\mathcal{Q}}$ (resp. $D_{\mathcal{R}}$, $I_{\mathcal{R}}$) désignent successivement les groupes de décomposition et d'inertie de $\mathcal{Q}$ (resp. $\mathcal{R}$) dans L/J (resp. M/K). Si de plus $D_{\mathcal{R}}$ (resp. $I_{\mathcal{R}}$) est normal dans $Gal(M/K)$, on a le parallélogramme galoisien

$$(J, K, M^{D_{\mathcal{R}}}, L^{D_{\mathcal{Q}}}) \quad (resp.\ \ (J, K, M^{I_{\mathcal{R}}}, L^{I_{\mathcal{Q}}})).$$

Démonstration. Soit $\mathfrak{P}$ un idéal premier de O_M divisant $\mathcal{P}$: $\mathfrak{P} \cap O_K = \mathcal{P}$. On a $(\mathfrak{P} \cap O_L) \cap O_J = \mathcal{Q} \cap O_J$. Dans le parallélogramme galoisien (J, K, M, L), il existe donc $\sigma \in Gal(M/K)$ tel que

$$\sigma(\mathfrak{P}) \cap O_L = \sigma_{|L}(\mathfrak{P} \cap O_L) = \mathcal{Q}, \quad \sigma(\mathfrak{P}) \cap O_K = \mathcal{P}.$$

Posons $\mathcal{R} := \sigma(\mathfrak{P})$, et soit $\mathcal{R}' \in Spec\, O_M$ tel que

$$\mathcal{R}' \cap O_K = \mathcal{P}, \quad \mathcal{R}' \cap O_L = \mathcal{Q}.$$

Soit $\sigma' \in Gal(M/K)$ tel que $\mathcal{R}' = \sigma'(\mathfrak{P})$. On a

$$(\sigma^{-1}\sigma')_{|L}(\mathfrak{P} \cap O_L) = \mathfrak{P} \cap O_L;$$

autrement dit, la restriction à L de $\sigma^{-1}\sigma'$ appartient au groupe de décomposition de $\mathfrak{P} \cap O_L$ dans L/J. Or dans le parallélogramme (J, K, M, L), de degré (p^n, d) où p ne divise pas d, il y a égalité des indices de ramification, des degrés résiduels, et du nombre de facteurs de la décomposition de $\mathcal{T}$ dans L et de celle de $\mathcal{P}$ dans M :

$$e_L(\mathcal{T}) = e_M(\mathcal{P}), \quad f_L(\mathcal{T}) = f_M(\mathcal{P}), \quad g_L(\mathcal{T}) = g_M(\mathcal{P}).$$

Il en résulte que la restriction à L induit, d'une part un isomorphisme du groupe de décomposition de $\mathfrak{P}$ dans M/K sur celui de $\mathfrak{P} \cap O_L$ dans L/J, d'où l'on déduit que $\mathcal{R}' = \mathcal{R}$, et d'autre part les isomorphismes

$$D_{\mathcal{R}} \xrightarrow[\;]{\overset{|L}{\sim}} D_{\mathcal{Q}}, \quad I_{\mathcal{R}} \xrightarrow[\;]{\overset{|L}{\sim}} I_{\mathcal{Q}}.$$

Les parallélogrammes galoisiens de l'énoncé s'obtiennent alors directement par la proposition 1. $\square$

Une extension galoisienne de corps de nombres se localise. Plus généralement, il en est de même pour les parallélogrammes.

Proposition 2. *Dans les notations du théorème 3, on a le parallélogramme galoisien local $(J_{\mathcal{T}}, K_{\mathcal{P}}, M_{\mathcal{R}}, L_{\mathcal{Q}})$.*

Démonstration. D'après la démonstration du théorème 3

$$[L_{\mathcal{Q}} : J_{\mathcal{T}}] = |D_{\mathcal{Q}}| = |D_{\mathcal{R}}| = [M_{\mathcal{R}} : K_{\mathcal{P}}] \mid p^n,$$

et $[K_{\mathcal{P}} : J_{\mathcal{T}}] \mid d$. Comme $p \nmid d$, il en résulte que $K_{\mathcal{P}} \cap L_{\mathcal{Q}} = J_{\mathcal{T}}$. Alors

$$[K_{\mathcal{P}}\, L_{\mathcal{Q}} : J_{\mathcal{T}}] = [K_{\mathcal{P}} : J_{\mathcal{T}}]\,[L_{\mathcal{Q}} : J_{\mathcal{T}}] = [K_{\mathcal{P}} : J_{\mathcal{T}}]\,[M_{\mathcal{R}} : K_{\mathcal{P}}] = [M_{\mathcal{R}} : J_{\mathcal{T}}]$$

d'où $K_{\mathcal{P}}\, L_{\mathcal{Q}} = M_{\mathcal{R}}$, ce qui prouve que $(L_{\mathcal{Q}}/J_{\mathcal{T}}) = desc_{J_{\mathcal{T}}}(M_{\mathcal{R}}/K_{\mathcal{P}})$. $\square$

La notion de parallélogramme galoisien est donc pleinement justifiée. Comme pour une extension galoisienne, il est donc légitime de se poser la question de savoir comment prolonger un parallélogramme galoisien. On sait bien qu'il n'y a pas transitivité de la normalité. Par exemple, au dessus d'une p-extension galoisienne $E/K \supseteq \mu_p$, un corps cyclique de degré p sur E : $N = E(x^{1/p})\,(x \in E^\times)$ n'est normal, donc galoisien, sur K que si et seulement si x est un élément du groupe multiplicatif

$$Nor(K,E) := \{x \in E^\times / \forall\, \gamma \in Gal(E/K) \quad \gamma(x) \equiv x \mod E^{\times p}\}.$$

A fortiori, on n'a pas de propriété générale de prolongement des parallélogrammes galoisiens :

$$((J,K,E,L),\,(L,E,N,D)) \not\Rightarrow (J,K,N,D).$$

Sans classe de cohomologie (qu'il faudrait définir "en dimension 2"), le théorème 4 qui suit fait le lien avec le théorème 2. Il montre comment un parallélogramme galoisien $(J, K := J(\mu_p), E, L)$ de degré (p^n, d), où E/K est une p-extension abélienne élémentaire, peut être prolongé par un parallélogramme (L,E,N,D) de degré (p,d). Le critère s'exprime en terme du sous-groupe suivant de $Nor(K,E)$:

$$Nor(J,K,E,L) := \{x \in Nor(K,E)/\, g_V(x) = x^d \mod E^{\times p}\}$$

où g_V est l'homomorphisme de $E^\times$ dans $E^\times/E^{\times p}$ défini section 1.

Théorème 4. *Soit $(J, K := J(\mu_p), E, L)$ un parallélogramme galoisien de corps de caractéristique différente du premier p. On suppose que E/K est une p-extension galoisienne, ou bien triviale : $E = K$, ou bien de groupe $\Gamma := Gal(E/K)$ abélien d'exposant p.*

(1) Un corps D, de degré p sur L, est galoisien sur J si et seulement s'il existe un élément $x \in Nor(J,K,E,L) - E^{\times p}$ tel que $D \subseteq E(x^{1/p})$.

(2) Soit D un corps de degré p sur L pour lequel il existe un élément $x \in Nor(J,K,E,L)\ - E^{\times p}$ tel que $D \subseteq E(x^{1/p})$.

(2.1) Le corps $E(x^{1/p})$ est unique.

(2.2) Si $N := E(x^{1/p})$, on a les parallélogrammes galoisiens (L,E,N,D) et (J,K,N,D).

(3) Dans les notations du (2), la trace de N sur D d'une racine p-ième quelconque, mais fixée, $x^{1/p}$ de x, fournit un élément primitif de D sur L : $D = L\left(Tr_{N/D}(x^{1/p})\right)$.

Scholie. Une justification supplémentaire de cet énoncé est la suivante. Il est dit dans ([5], p. 389) que la détermination explicite des p-extensions cycliques est un problème très difficile. Le théorème 4 précédent fournit en particulier une description de toutes les extensions cycliques de degré p ou p^2 non kummériennes, en en donnant un élément primitif explicite.

Démonstration. Elle se fait en plusieurs étapes. Notons $d := [K : J] = [E : L]$. Prouvons d'abord deux équivalences préparatoires.

(4.1) *Soit* $Nor(L, E, E, L) := \{x \in E^\times / \, g_V(x) = x^d \bmod E^{\times p}\}$. *Pour toute extension cyclique* M/E *de degré* p, *on a l'équivalence*

$$(M/E)\, desc_L \Leftrightarrow (\exists\, x \in Nor(L, E, E, L) - E^{\times p} \quad M = E(x^{1/p})).$$

Soit en effet $x \in E^\times$ tel que $M = E(x^{1/p})$. Supposons M/E descendable sur L. L'extension M/L est alors abélienne de sorte que

$$\forall\, v \in V, \quad \exists\, x_v \in E^\times, \quad \frac{v(x)}{x^{i(v)}} = x_v^p \qquad \text{(cf. [10])}$$

où $v(\zeta_p) = \zeta_p^{i(v)}$ $(v \in V)$. Donc

$$g_V(x) = \left(\prod_{v \in V} v^{-1}(x)^{i(v)}\right) \bmod E^{\times p} = \left(\prod_{v \in V} \left(x^{i(v^{-1})} x_{v^{-1}}^p\right)^{i(v)}\right) \bmod E^{\times p}$$

et par suite $g_V(x) = x^d \bmod E^{\times p}$. Réciproquement, comme $p \not| \, d$, on a $M = E(\widehat{g_V}(x)^{1/p})$. On en déduit que l'extension M/L est abélienne, ce qui suffit pour que M/E soit descendable sur L d'après le théorème de Zassenhaus de ([4]; p.126, Hauptsatz 18.1).

(4.2) *Pour tout corps* M *de degré* p *sur* E *tel que l'extension* M/K *soit galoisienne, on a l'équivalence*

$$(M/K)\, desc_J \Leftrightarrow (\exists\, x \in Nor(J, K, E, L) - E^{\times p} \quad M = E(x^{1/p})).$$

Comme l'extension M/K est galoisienne, il existe un élément

$$x \in Nor(K, E) - E^{\times p}$$

tel que $M = E(x^{1/p})$. Supposons M/K descendable sur J de descendue D/J, et plaçons-nous dans le parallélogramme galoisien (J, K, M, D). D'après le (2) de la proposition 1 pour $E_0 = K$, $E_1 = E$, et $A := Gal(M/E)$, on a le parallélogramme $(J, K, E, D^{(A_{|D})})$, de sorte que $D^{(A_{|D})}/J$ est descendue de E/K sur J. Or il en est de même de L/J dans (J, K, E, L), et par le (2) du théorème 1, E/K n'admet qu'une seule descendue sur J. Ceci prouve que $L = D^{(A_{|D})}$, d'où le parallélogramme (L, E, M, D) par le (3) de la proposition 1. En particulier M/E est descendable sur L. On déduit alors du (4.1) précédent que $x \in Nor(K, E) \cap Nor(L, E, E, L) = Nor(J, K, E, L)$. Réciproquement, supposons que $g_V(x) = x^d \bmod E^{\times p}$. Clairement, $M = E(\widehat{g_V}(x)^{1/p})$. Pour montrer que M/K est descendable sur J, il suffit, d'après le (1) du théorème 1, de prouver que M/J est galoisienne. Dans le parallélogramme (J, K, E, L), on a $Gal(E/J) = V \times \Gamma$.

Pour tout $u \in Gal(E/J)$, écrivons $u = v_u\gamma$ ($v_u \in V$, $\gamma \in \Gamma$). Comme $x \in Nor(K,E)$,

$$g_V(u(x)) = g_V(v_u(x)). \tag{1}$$

D'autre part, l'extension $E = LK/J$ étant abélienne, on a

$$u(\widehat{g_V}(x)) \equiv \widehat{g_V}(u(x)) \mod E^{\times p}. \tag{2}$$

Enfin, on vérifie que l'extension $E(\widehat{g_V}(x)^{1/p})/L$ est galoisienne; i.e que

$$\forall\, v \in V \quad v(\widehat{g_V}(x)) \equiv \widehat{g_V}(x)^{i(v)} \mod E^{\times p} \quad (v(\zeta_p) = \zeta_p^{i(v)}). \tag{3}$$

Il résulte alors de la conjonction de (1), (2) et (3) que

$$\forall\, u \in Gal(E/J) \quad u(\widehat{g_V}(x)) \equiv \widehat{g_V}(x)^{i(v_u)} \mod E^{\times p}$$

ce qui établit que M/J est galoisienne (cf.[2]).

On peut maintenant prouver les trois assertions du théorème 4.

(1) Supposons l'extension D/J galoisienne, et posons $M := D(\mu_p) = DK$. Comme $D \cap K = J$, D/J est descendue de l'extension galoisienne M/K. Or dans le parallélogramme (J,K,E,L), on a $L(\mu_p) = LK = E \subseteq D(\mu_p) = M$ et

$$[D:L]\,[L:J]{=}[D:J]{=}[M:K]{=}[M:E]\,[E:K] \Leftrightarrow [D:L]{=}[M:E]{=}p,$$

d'où l'existence du x cherché par le (4.2) ci-dessus. Réciproquement, supposons qu'il existe $x \in Nor(J,K,E,L) - E^{\times p}$ tel que $D \subseteq N := E(x^{1/p})$. Comme $Nor(J,K,E,L) \subseteq Nor(L,E,E,L)$, on sait par le (4.1) que N/E est descendable sur L. C'est donc que N/L est abélienne. Ainsi D/L est galoisienne, et c'est la descendue sur L de N/E. Par ailleurs, l'extension galoisienne N/K est descendable sur J d'après le (4.2), donc N/J est galoisienne et le sous-groupe $Gal(N/K)$ de $Gal(N/J)$ admet un unique complément V' facteur direct (cf. Th.1(2)) : $Gal(N/J) = V' \times Gal(N/K)$. De même, le sous-groupe $Gal(N/E)$ de $Gal(N/L)$ admet un unique complément W facteur direct : $Gal(N/L) = W \times Gal(N/E)$, et l'on a $D = N^W$. Or on vérifie que $W \cap Gal(N/K) = \{1\}$ et $Gal(N/J) = W\,Gal(N/K)$. C'est donc que $W = V'$. En particulier, W est normal dans $Gal(N/J)$ et D/J est galoisienne.

(2) (2.2) On a vu dans la démonstration du (1) que D/L est la descendue sur L de N/E; d'où le parallélogramme (L,E,N,D). De plus $D \cap K = J$ car $p \nmid d$, et $N = DK$ car $N = DE$, $E = LK$. Comme D/J est galoisienne par l'équivalence du (1), on a bien le parallélogramme (J,K,N,D).

(2.1) L'unicité du corps $E(x^{1/p})$ résulte du (2.2) précédent puisque $DE = E(x^{1/p})$.

(3) Il suffit d'appliquer le (2) du théorème 2. $\square$

Bibliographie

[1] G. Brattström, *On p-groups as Galois groups.* Math. Scand. **65** (1989), 165–174.
[2] A.A. Bruen, C.U. Jensen and N. Yui, *Polynomials with Frobenius groups of prime degree as Galois groups II.* J. Number Theory **24** (1986), 305–359.
[3] K. Hoechsmann, *Zum Einbettungsproblem.* J. reine angew. Math. **229** (1968), 81–106.
[4] B. Huppert, *Endliche Gruppen I*, 2nd ed. Springer-Verlag, Berlin, 1983.
[5] G. Karpilovsky, *Topics in Field Theory.* North-Holland Mathematics Studies **155,** Amsterdam, 1989.
[6] R. Massy, *Construction de p-extensions galoisiennes d'un corps de caractéristique différente de p.* J. Algebra **109** (1987), 508–535.
[7] R. Massy et S. Monier-Derviaux, *Parallélogrammes galoisiens.* J. Algebra, à paraître.
[8] S. Monier, *Descente de p-extensions galoisiennes kummériennes.* Math. Scand. **79** (1996), 5–24.
[9] S. Monier-Derviaux, *Le Problème de la Descente Galoisienne Finie.* Thèse de Doctorat, Univ. Valenciennes, 1997.
[10] J. Wójcik, *Criterion for a field to be abelian.* Colloq. Math. **68** (1995), 187–191.

Richard Massy
Département de Mathématiques
Universi te de Valenciennes
Le Mont Houy, B.P.311
F-59304 Valenciennes
E-mail : `Richard.Massy@univ-valenciennes.fr`

Sylvie Monier-Derviaux
Département de Mathématiques
Université de Valenciennes
Le Mont Houy, B.P.311
F-59304 Valenciennes
E-mail : `Sylvie.Derviaux@univ-valenciennes.fr`