MATH. SCAND. 79 (1996), 5–24

DESCENTE DE p-EXTENSIONS GALOISIENNES KUMMERIENNES

SYLVIE MONIER

0. Introduction.

Soit E/K une extension galoisienne de corps. Etant donné un sous-corps J de K, on peut se poser la question de savoir s'il existe un sous-corps D de E, galoisien sur J, tel que, d'une part $\mathrm{Gal}(D/J)$ soit isomorphe à $\mathrm{Gal}(E/K)$, d'autre part J soit l'intersection de D et K. Ceci traduit l'idée intuitive de "descendre sur J" l'extension galoisienne E/K (cf. Définition 2.1).

En 1989 Gudrun Brattström [Br] a obtenu le résultat de descente suivant. Soient p un nombre premier impair, μ_p le groupe des racines p-ièmes de l'unité, et K un corps de caractéristique différente de p contenant μ_p. Pour toute extension galoisienne non abélienne E/K de degré p^3, il existe une extension galoisienne D/J de translatée $(D(\mu_p) = E)/(J(\mu_p) = K)$.

Dans ce travail, on généralise les résultats de Brattström de la façon suivante. Après quelques rappels galoisiens (section 1), on définit précisément (section 2) la notion "d'extension descendue parallèlement à une extension K/J" d'une extension galoisienne finie quelconque E/K. Puis on obtient des conditions d'existence et d'unicité de descendues lorsque E/K est une p-extension. Soit $\Phi(\Gamma)$ le sous-groupe de Frattini du groupe de Galois Γ de E/K. Ces conditions d'existence s'expriment en termes d'une descendue de l'extension $E^{\Phi(\Gamma)}/K$ où $E^{\Phi(\Gamma)}$ désigne le corps des invariants dans E de $\Phi(\Gamma)$. Ceci permet de réduire le problème au cas d'une p-extension abélienne élémentaire. On montre ensuite (section 3), modulo une condition de compatibilité entre les degrés, qu'une descendue d'un compositum de p-extensions est le compositum de descendues de ces extensions; puis l'on construit explicitement, en termes de trace, un élément primitif de la descendue d'une extension cyclique de degré p parallèlement à une extension cyclotomique. La section 4 est le coeur de ce travail. On ajoute une classe de cohomologie au problème de descente. On résoud un problème de plongement non kummérien au moyen de la descente d'une solution du problème de plonge-

Received January 10, 1995.

ment kummérien translaté. Précisément, soit L/J une p-extension abélienne élémentaire. On obtient toutes les solutions d'un problème de plongement résoluble à noyau d'ordre p de L/J, en descendant sur J une solution du même problème pour l'extension translatée $(E := L(\mu_p))/(K := J(\mu_p))$, cette solution, disons N/K, étant telle que N/L soit abélienne. Enfin, la section 5 est consacrée aux exemples.

1. Rappels.

Pour tout nombre premier p, on note $\mathbf{F}_p$ le corps à p éléments, μ_p le groupe des racines p-ièmes de l'unité, et ζ_p un générateur de μ_p.

Soient K un corps de caractéristique différente de p, et E/K une extension galoisienne finie de degré quelconque de groupe $\Gamma := \mathrm{Gal}(E/K)$. On suppose que le corps E contient μ_p (sans nécessairement qu'il en soit ainsi pour K).

Les propriétés suivantes sont standard.

1.1. *Soient N/E une extension galoisienne de degré p, et x l'un quelconque des éléments de $E^\times$ tel que $N = E(x^{1/p})$.*

(1) *L'extension N/K est galoisienne si et seulement si pour tout $\gamma \in \Gamma$ il existe un entier $i(\gamma) \in \mathbf{F}_p^\times$, et un élément $x_\gamma \in E^\times$, tels que*

$$\gamma(x)/x^{i(\gamma)} = x_\gamma^p.$$

De plus, si m est l'exposant du groupe Γ, on a

$$i(\gamma)^m \equiv 1 \bmod p \quad (\gamma \in \Gamma).$$

Dans le cas particulier où E/K est une p-extension, on peut prendre $i(\gamma) = 1$ quel que soit $\gamma \in \Gamma$.

(2) *On suppose que N/K est galoisienne.*

– *Une condition nécessaire pour que N/K soit abélienne est que l'entier $i(\gamma)$ du (1) vérifie:*

$$\gamma(\zeta_p) = \zeta_p^{i(\gamma)} \quad (\gamma \in \Gamma).$$

– *Si de plus l'extension de base E/K est cyclique, cette condition nécessaire est aussi suffisante.*

DÉMONSTRATION. Conséquence directe de la théorie de Galois. Pour le (1) voir par exemple [B-J-Y, III], et pour le (2) [Wa, p.325].

Dans le cas particulier où $p = 3$, $\zeta_3 = j = e^{2i\pi/3}$, $K = \mathbf{Q}$, $E = \mathbf{Q}(j)$, on a la formulation explicite suivante.

1.2. *Pour tout élément $a + bj \in E^\times - E^{\times 3}$, l'extension $N = E((a + bj)^{1/3})$ est abélienne de degré 6 sur $\mathbf{Q}$ si et seulement si $N_{E/\mathbf{Q}}(a + bj) \in \mathbf{Q}^{\times 3}$. Il existe alors deux*

entiers m et n premiers entre eux, $m + nj \neq \pm(1 + 2j), m + nj \in \mathbf{Z}[j] - \mathbf{Z}[j]^3$, tels que

$$N = E(((m^2 - mn + n^2)(m + nj))^{1/3}).$$

DÉMONSTRATION. La condition $N_{E/\mathbf{Q}}(a + bj) \in \mathbf{Q}^{\times 3}$ est claire puisque d'après le 1.1 (2), l'extension $N/\mathbf{Q}$ est abélienne si et seulement si

$$(a + bj^2)/(a + bj)^2 \in E^{\times 3}.$$

Réduisons alors a et b au même dénominateur d: $a + bj = d^{-1}(m + nj)$ $(m, n \in \mathbf{Z})$. Il existe $z \in \mathbf{Z}$ tel que

$$d(m^2 - mn + n^2) = z^3.$$

On en déduit que le corps N a la forme annoncée. Inversement dans ce cas, il résulte des hypothèses sur m et n que le produit $(m^2 - mn + n^2)(m + nj)$ n'est pas un cube dans $\mathbf{Z}[j]$. D'où la conclusion puisque sa norme est dans $\mathbf{Q}^{\times 3}$.

Par ailleurs, étant donnés un groupe A d'ordre premier p, F/K une p-extension galoisienne de groupe $G := \mathrm{Gal}(F/K)$, et $(F' := F(\mu_p)/(K' := K(\mu_p))$ l'extension translatée de groupe $G' := \mathrm{Gal}(F'/K')$, on a l'équivalence suivante.

PROPOSITION 1.3. (Comparer à [G, Thm. 5]). *Soit l'isomorphisme canonique*

$$H^2(G, A) \xrightarrow{\sim} H^2(G', A)$$
$$\bar{z} \mapsto \overline{z'}$$

où les 2-cocycles z et z' vérifient

$$z'(\sigma', \tau') = z(\sigma'|_F, \tau'|_F) \quad (\sigma', \tau' \in G').$$

Alors, pour toute classe non nulle $\bar{z} \in H^2(G, A) - \{0\}$, le problème de plongement $(F/K, \bar{z})$ est résoluble si et seulement si le problème translaté $(F'/K', \overline{z'})$ est résoluble.

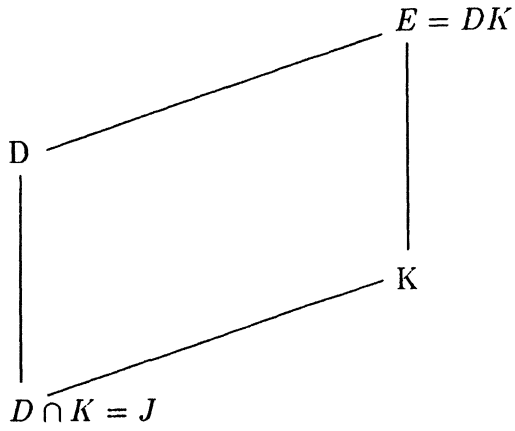
DÉMONSTRATION. Conséquence de l'équivalence bien connue d'Hoechsmann [Ho, 2.3].

2. Descendue d'une extension.

Dans cette section, on définit la notion "d'extension descendue" d'une extension galoisienne finie quelconque E/K. Puis l'on obtient des conditions nécessaires et suffisantes d'existence de descendues lorsque E/K est une p-extension.

DÉFINITION 2.1. Soient E/K une extension galoisienne finie et $\tilde{K}$ une clôture algébrique de K contenant E. On appelle "descendue de E/K sur un corps J", ou "descendue de E/K parallèlement à une extension K/J", une extension D/J vérifiant les trois conditions suivantes:

(D_0) D/J est galoisienne
(D_1) $D \cap K = J$
(D_2) Le compositum des corps D et K dans $\tilde{K}$ est égal à E: $DK = E$.



En abrégé, on dira alors simplement que D/J est "descendue" de E/K.

L'extension D/J étant galoisienne, la restriction à D induit l'isomorphisme $\mathrm{Gal}(E/K) \xrightarrow{\sim} \mathrm{Gal}(D/J)$. De même, si K/J est galoisienne, la restriction à K induit l'isomorphisme $\mathrm{Gal}(E/D) \xrightarrow{\sim} \mathrm{Gal}(K/J)$.

EXEMPLE 2.2. Soient $K = \mathbb{Q}(j), j = e^{2i\pi/3}$, et $E = K(\alpha)$ où α est une racine dans $\tilde{K}$ de $X^3 - j = 0$. Le corps

$$D = \mathbb{Q}(\alpha + \bar{\alpha})$$

où $\bar{\alpha}$ désigne le complexe conjugué de α, définit une descendue sur $\mathbb{Q}$ de l'extension kummérienne E/K.

LEMME 2.3. *Dans les notations de la définition* 2.1, *supposons l'extension* K/J *galoisienne. Les conditions suivantes sont alors équivalentes:*

(1) *L'extension* E/K *admet une descendue*

(2) *L'extension* E/J *est galoisienne et le groupe* $\Gamma := \mathrm{Gal}(E/K)$ *admet un complément facteur direct dans* $\mathrm{Gal}(E/J)$.

DÉMONSTRATION. Il résulte de la définition 2.1, par la théorie de Galois élémentaire, que

$$\mathrm{Gal}(E/J) \xrightarrow{\sim} \mathrm{Gal}(D/J) \times \mathrm{Gal}(K/J) \xrightarrow{\sim} \Gamma \times \mathrm{Gal}(E/D).$$

Inversement, il est clair par [L, p.307 (1.16)] que le corps $D := E^V$ des invariants

dans E d'un facteur direct V de Γ dans $\mathrm{Gal}(E/J)$ définit une descendue sur J de E/K.

Donnons maintenant une condition nécessaire et suffisante d'existence d'une descendue dans le cas abélien.

PROPOSITION 2.4. *Soient K/J et E/K deux extensions abéliennes de degré premiers entre eux. L'extension E/K admet une descendue parallèlement à K/J si et seulement si l'extension E/J est abélienne.*

DÉMONSTRATION. Toute descendue D/J de E/K est abélienne puisque $\mathrm{Gal}(D/J) \xrightarrow{\sim} \mathrm{Gal}(E/K)$, et il en est de même de E/J par composition. Réciproquement soit $U := \mathrm{Gal}(E/J)$. Comme $\mathrm{p.g.c.d}(|\Gamma|, |U/\Gamma|) = 1$, on déduit du théorème de Zassenhaus [Hu; p.126, Hauptsatz 18.1] qu'il existe un complément V de Γ dans U qui, à l'évidence, est facteur direct puisque U est abélien; d'où la conclusion par le lemme 2.3.

Nous utiliserons en fait la proposition 2.4 dans le cas particulier d'une p-extension abélienne descendue parallèlement à une extension cyclotomique.

COROLLAIRE 2.5. *Soient J un corps, n un entier tel que la caractéristique de J ne divise pas n, et $K := J(\mu_n)$ le n-ième corps cyclotomique au dessus de J, où μ_n désigne le groupe des racines n-ièmes de l'unité. Quel que soit le nombre premier p ne divisant pas le degré $[K : J]$, une p-extension abélienne E/K admet une descendue sur J si et seulement si l'extension E/J est abélienne.*

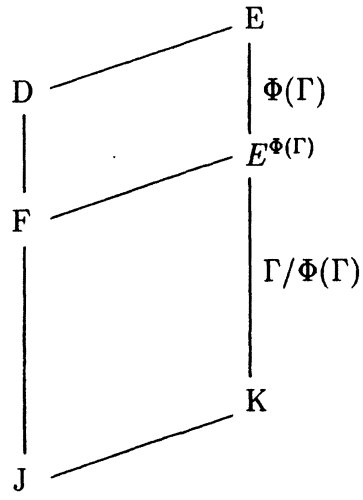
Dans le cas non nécessairement abélien, on a pour une p-extension galoisienne l'équivalence suivante.

THÉORÈME 2.6. *Soient p un nombre premier et K/J une extension galoisienne finie telle que p ne divise pas le degré $[K : J]$. Soit E/K une p-extension galoisienne de groupe $\Gamma = \mathrm{Gal}(E/K)$.*

(1) *Pour que E/K admette une descendue D/J, il faut et il suffit que les deux conditions suivantes soient vérifiées:*

(1.1) *L'extension E/J est galoisienne*

(1.2) *L'extension $E^{\Phi(\Gamma)}/K$ admet une descendue F/J, où $E^{\Phi(\Gamma)}$ désigne le corps des invariants dans E du sous-groupe de Frattini de Γ.*



(2) *Lorsqu'elle existe, la descendue est unique. Précisément, supposons que E/K admette une descendue D/J. Le sous-groupe Γ de $\mathrm{Gal}(E/J)$ admet un unique complément V. Ce complément V est facteur direct, et l'on a $D = E^V$.*

DÉMONSTRATION. (1) Le sens direct est vérifié indépendamment du fait que p ne divise pas le degré $[K:J]$. En effet, par la théorie de Galois, la restriction à D: $\Gamma \xrightarrow{\sim} \mathrm{Gal}(D/J)$ est un isomorphisme; et en écrivant $\Gamma|_D := \mathrm{Gal}(D/J)$, on

$$\gamma \mapsto \gamma|_D$$

a pour les sous-groupes de Frattini: $\Phi(\Gamma|_D) = \Phi(\Gamma)|_D$. On en déduit qu'il suffit de prendre pour F le corps des invariants $D^{\Phi(\Gamma|_D)}$.

Réciproquement, notons $U := \mathrm{Gal}(E/J)$, et utilisons l'hypothèse $p \nmid [K:J]$. On a $\mathrm{p.g.c.d}(|\Gamma|, |U/\Gamma|) = 1$, donc, par le théorème de Zassenhaus [Hu; p.126, Hauptsatz 18.1], il existe dans U un complément V de Γ. D'après le lemme 2.3, il suffit de montrer que V et Γ commutent éléments par éléments. En tant que compositum des extensions F/J et K/J, l'extension $E^{\Phi(\Gamma)}/J$ est galoisienne. Soit G son groupe: $G := \mathrm{Gal}(E^{\Phi(\Gamma)}/J)$, et appliquons le lemme 2.3 à l'extension $E^{\Phi(\Gamma)}/K$. Le sous-groupe $\Gamma/\Phi(\Gamma)$ de G admet un complément V' facteur direct: $G = V' \times (\Gamma/\Phi(\Gamma))$. Par ailleurs, on vérifie que pour la restriction

$$r\colon U \to G$$

$$u \mapsto u|_{E^{\Phi(\Gamma)}}$$

l'image $r(V)$ est aussi un complément de $\Gamma/\Phi(\Gamma)$ dans G. Comme

$$\mathrm{p.g.c.d}(|\Gamma/\Phi(\Gamma)|, |G/(\Gamma/\Phi(\Gamma))|) = 1,$$

on sait, toujours d'après Zassenhaus ([Hu; p.127, Hauptsatz 18.2]), que tous les

compléments de $\Gamma/\Phi(\Gamma)$ dans G sont conjugués. Il en résulte que $r(V) = V'$, et que l'application

$$V \times (\Gamma/\Phi(\Gamma)) \to \Gamma/\Phi(\Gamma)$$
$$(v, \varphi) \mapsto r(v)\varphi r(v)^{-1}$$

est triviale. Pour tout $v \in V$, considérons alors l'automorphisme du p-groupe Γ

$$\alpha_v \colon \Gamma \to \Gamma \lhd U$$
$$\gamma \mapsto \alpha_v(\gamma) = v\gamma v^{-1}.$$

On a

$$\alpha_v(\gamma)\Phi(\Gamma) = \gamma\Phi(\Gamma) \quad (v \in V, \gamma \in \Gamma).$$

On déduit alors de [Hu; p.275, Satz 3.18] que l'ordre $o(\alpha_v)$ de chaque automorphisme α_v est une puissance de p. Mais par ailleurs $o(\alpha_v)$ divise $|V| = [K:J]$. Comme $p \nmid [K:J]$, on a nécessairement $\alpha_v = \mathrm{id}_\Gamma$, d'où la commutation voulue.

(2) Il existe un sous-groupe normal V de $\mathrm{Gal}(E/J)$ tel que $D = E^V$. Par l'hypothèse que p ne divise pas $[K:J]$, on vérifie que V est un complément de Γ dans $\mathrm{Gal}(E/J)$. Or d'après le Hauptsatz de [Hu; p.128, 18.3], tous les compléments de Γ dans $\mathrm{Gal}(E/J)$ sont conjugués; donc V est unique, et il en est de même du corps D.

Lorsque K/J est une extension cyclotomique, on a en particulier le

COROLLAIRE 2.7. *Dans les notations du corollaire* 2.5, *pour qu'une p-extension galoisienne* E/K *admette une descendue parallèlement à l'extension* $K = J(\mu_n)/J$, *il faut et il suffit que les deux conditions suivantes soient vérifiées:*

(i) *L'extension* E/J *est galoisienne*

(ii) *L'extension* $E^{\Phi(\Gamma)}/J$ *est abélienne.*

DÉMONSTRATION. Conjonction du corollaire 2.5 et du théorème 2.6.

COROLLAIRE 2.8. *On se place dans la situation du théorème* 2.6. *Soit* $\mathrm{Gal}_p(J)$ (*resp.* $\mathrm{Gal}_p(J, K)$) *l'ensemble des p-extensions galoisiennes de* J (*resp. de* K, *qui vérifient les conditions* (1.1) *et* (1.2) *du théorème* 2.6). *Alors l'application "translation"*

$$\mathrm{tran} \colon \mathrm{Gal}_p(J) \to \mathrm{Gal}_p(J, K)$$
$$D/J \mapsto DK/K$$

est bijective, et admet pour réciproque l'application "descendue"

$$\text{desc}: \text{Gal}_p(J,K) \to \text{Gal}_p(J)$$
$$E/K \mapsto \text{desc}(E/K)$$

où $\text{desc}(E/K)$ *désigne la descendue de* E/K *parallèlement à l'extension* K/J.

DÉMONSTRATION. Si $E/K = \text{tran}(D/J)$, on a $D/J = \text{desc}(E/K)$. On en déduit que les applications sont bien réciproques.

3. Constructions de descendues de p-extensions abéliennes.

Soient p un nombre premier et J un corps de caractéristique différente de p. Dans toute la suite K/J désigne une extension galoisienne de degré non divisible par p.

On a le résultat suivant de décomposition des descendues par rapport à une extension compositum.

PROPOSITION 3.1. *Dans une clôture algébrique* $\tilde{K}$ *de* K, *soient* E_i/K $(i = 1,\ldots,n)$ *des p-extensions galoisiennes telles que*

$$(E_1 \ldots E_i) \cap E_{i+1} = K \quad (i = 1,\ldots,n-1).$$

On suppose que le compositum $E := E_1 \ldots E_n$ *des* E_i *dans* $\tilde{K}$ *est galoisien sur* J. *Alors, étant donnés des extensions galoisiennes* D_i/J *où* $D_i \subseteq E_i$ $(i = 1,\ldots,n)$ *et leur compositum* $D := D_1 \ldots D_n$ *dans* $\tilde{K}$, *on a l'équivalence suivante: l'extension* D/J *est la descendue de* E/K *si et seulement si* D_i/J *est la descendue de* E_i/K *pour tout* $i = 1,\ldots,n$.

DÉMONSTRATION. Prenons $n = 2$. Supposons que D/J soit la descendue de E/K. Il est immédiat que $D_i \cap K = J$ $(i = 1,2)$. D'autre part, comme $D_1K \cap D_2K = K$, on a

$$\begin{array}{ccc} \text{Gal}(D_1D_2K/K) & \xrightarrow{\sim} & \text{Gal}(D_1K/K) \times \text{Gal}(D_2K/K) \\ \| & & \\ \text{Gal}(E_1E_2/K) & \xrightarrow{\sim} & \text{Gal}(E_1/K) \times \text{Gal}(E_2/K) \end{array}$$

d'où $E_i = D_iK$ $(i = 1,2)$. Réciproquement, il est clair que $D_1 \cap D_2 = J$. On en déduit que D_1D_2/J est une p-extension car

$$\text{Gal}(D_1D_2/J) \xrightarrow{\sim} \text{Gal}(E_1/K) \times \text{Gal}(E_2/K).$$

Mais p ne divise pas $[K:J]$. Par conséquent, $D_1D_2 \cap K = J$. On généralise ensuite par récurrence sur n.

La proposition précédente ramène l'étude de la descendue d'une p-extension abélienne à celle d'une p-extension cyclique que l'on peut supposer de degré p via le théorème 2.6.

Le théorème suivant fournit explicitement en termes de trace, un générateur de la descendue d'une extension cyclique de degré premier parallèlement à une extension cyclotomique.

THÉORÈME 3.2. *Prenons* $K = J(\zeta_p)$ *où* ζ_p *désigne une racine primitive* p-ième *de l'unité. Soient* $E := K(\alpha)$, *où* $\alpha^p = a \in K^\times - K^{\times p}$, *une extension de degré* p *de* K, *de groupe* $\Gamma := \mathrm{Gal}(E/K)$. *Supposons l'extension* E/J *abélienne. Soit* $D := E^V/J$ *la descendue de* E/K *sur* J, *où* V *est l'unique complément de* Γ *dans* $\mathrm{Gal}(E/J)$ (cf. *Cor.* 2.5, *Th.* 2.6 (2)). *Alors:*

(1) *Pour la norme de* E *sur* D: $N_{E/D}(\alpha) \in J$

(2) *La trace* $t := \mathrm{Tr}_{E/D}(\alpha)$ *fournit un élément primitif de* D *sur* J: $D = J(t)$.

DÉMONSTRATION. (1) Soit σ le générateur de Γ tel que $\sigma(\alpha) = \zeta_p \alpha$. Comme l'extension E/J est abélienne,

$$\sigma(N_{E/D}(\alpha)) = N_{E/D}(\sigma(\alpha)).$$

Notons $d := [K : J] \leqq p - 1$ le degré de K sur J, h un générateur du groupe de Galois de K/J, et $i(h)$ l'entier de $\{2, \ldots, p-1\}$ tel que $h(\zeta_p) = \zeta_p^{i(h)}$. Soit v l'image de h par la réciproque $\mathrm{Gal}(K/J) \to \mathrm{Gal}(E/D) = V$ de la restriction à K. On a

$$\begin{aligned} N_{E/D}(\sigma(\alpha)) &= \sigma(\alpha) v(\sigma(\alpha)) \ldots v^{d-1}(\sigma(\alpha)) \\ &= \zeta_p^{1 + i(h) + \ldots + i(h)^{d-1}} N_{E/D}(\alpha) \\ &= \zeta_p^{\frac{i(h)^d - 1}{i(h) - 1}} N_{E/D}(\alpha). \end{aligned}$$

Or d'après le 1.1, il existe un entier n tel que

$$np = i(h)^d - 1 = (i(h) - 1)(1 + i(h) + \ldots + i(h)^{d-1}).$$

Clairement $i(h) - 1 \in \{1, \ldots, p-2\}$ divise n. Par suite

$$\sigma(N_{E/D}(\alpha)) = N_{E/D}(\alpha).$$

Comme D/J est la descendue de E/K, on obtient donc que

$$N_{E/D}(\alpha) \in D \cap K = J.$$

(2) Comme $[D : J] = p$, on a $D = J(t)$ dès que que $t \notin J$. L'extension E/J étant abélienne, on sait (cf. 1.1) qu'il existe un élément $x_h \in K^\times$ tel que $h(a)/a^{i(h)} = x_h^p$. Quitte à changer x_h en ζx_h, où ζ est une racine p-ième de l'unité, on peut écrire $v(\alpha) = x_h \alpha^{i(h)}$. Or

$$t = \sum_{n=0}^{d-1} k_n \alpha^{i(h)^n} = \sum_{n=0}^{d-1} k_n a^{q_n} \alpha^{r_n}$$

où par définition

$$k_0 := 1,\ k_n := \prod_{l=0}^{n-1} h^l(x_h)^{i(h)^{n-l-1}} \quad (n \geqq 1)$$

et par division euclidienne

$$i(h)^n = pq_n + r_n \quad (1 \leqq r_n \leqq p-1).$$

Si t appartenait à J, on aurait $\sigma(t) = t$, d'où

$$(\zeta_p - 1)\alpha + \sum_{n=1}^{d-1} k_n a^{q_n}(\zeta_p^{r_n} - 1)\alpha^{r_n} = 0.$$

Mais h étant un générateur de $\mathrm{Gal}(K/J)$, l'homomorphisme

$$\mathbf{Z}/d\mathbf{Z} \longrightarrow \mathbf{F}_p^\times$$

$$n \bmod d \longrightarrow r_n = i(h)^n \bmod p$$

est injectif. Comme $\{1, \alpha, \alpha^2, \ldots, \alpha^{p-1}\}$ est une K-base de E, on en déduit que $\zeta_p = 1$: contradiction. Par conséquent $t \in D - J$ ce que l'on voulait.

EXEMPLES 3.3. $p = 3$, $\zeta_3 = j$, $J = \mathbf{Q}$, et $K = \mathbf{Q}(j)$. On a $i(h) = 2$.

(1) Comme déjà vu dans l'exemple 2.2, la descendue parallèlement à $K/\mathbf{Q}$ de l'extension $E = K(\alpha)/K$ où $\alpha^3 = j$, est l'extension

$$D = \mathbf{Q}(\alpha + v(\alpha))/\mathbf{Q} \quad \text{où} \quad v(\alpha) = j^2\alpha^2 = \bar{\alpha}.$$

(2) *Descente d'une extension $E/\mathbf{Q}(j)$ lorsque $E/\mathbf{Q}$ est abélienne de degré* 6

D'après le 1.2, il existe m et n premiers entre eux avec $m + nj \in \mathbf{Z}[j] - \mathbf{Z}[j]^3$, $m + nj \neq \pm(1 + 2j)$, tels que

$$E = K(((m^2 - mn + n^2)(m + nj))^{1/3}).$$

Pour $\alpha^3 = (m^2 - mn + n^2)(m + nj)$, la descendue de E/K parallèlement à $K/\mathbf{Q}$ est l'extension

$$D = \mathbf{Q}\left(\alpha + \frac{\alpha^2}{m + nj}\right).$$

(3) *Exemple à la proposition* 3.1

D'après les exemples précédents, l'extension de degré 27

$$\mathbf{Q}\left(\alpha_1 + j^2\alpha_1^2, \alpha_7 + \frac{\alpha_7^2}{2 + 3j}, \alpha_{13} + \frac{\alpha_{13}^2}{3 + 4j}\right)\Big/\mathbf{Q}$$

où $\alpha_1^3 = j$, $\alpha_7^3 = 7(2 + 3j)$, $\alpha_{13}^3 = 13(3 + 4j)$, est la descendue de l'extension $K(\alpha_1, \alpha_7, \alpha_{13})/K$.

4. Descente et problème de plongement.

Soit G un groupe opérant sur un groupe abélien A. Supposons, d'une part que G se réalise comme groupe d'une extension galoisienne de corps F'/F, d'autre part qu'il existe un corps $F'' \supseteq F'$ pour lequel l'extension F''/F soit galoisienne et telle que $\mathrm{Gal}(F''/F')$ s'identifie à A. On appelle alors "classe de cohomologie de l'extension F''/F" (pour l'identification donnée de $\mathrm{Gal}(F''/F')$ à A) la classe dans $H^2(G, A)$ de l'extension de groupes

$$1 \to A \hookrightarrow \mathrm{Gal}(F''/F) \to G \to 1$$

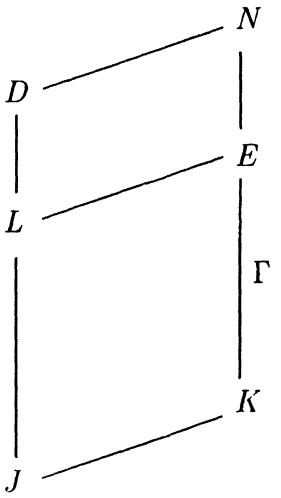
définie par les homomorphismes d'injection et surjection canoniques.

Soit p un nombre premier quelconque. Identifions le groupe μ_p des racines p-ièmes de l'unité à $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ par la donnée d'une racine primitive ζ_p fixée via l'isomorphisme

$$\begin{aligned} \lg\colon \mu_p &\xrightarrow{\sim} \mathbf{F}_p \\ \zeta_p^n &\mapsto n. \end{aligned}$$

Dans toute la suite, K désigne un corps de caractéristique différente de p contenant μ_p, et E/K une p-extension galoisienne de groupe $\Gamma := \mathrm{Gal}(E/K)$.

LEMME 4.1. *Soient K/J une extension galoisienne de degré non divisible par p, et $N = E(x^{1/p})/E$ $(x \in E^\times)$ une extension cyclique de degré p. Supposons qu'il existe une extension L/J (resp. D/L) descendue de E/K (resp. N/E).*



Identifions $\mathrm{Gal}(L/J)$ *(resp.* $\mathrm{Gal}(D/L)$*) à* Γ *(resp.* $\mathrm{Gal}(N/E)$*) par la restriction à* L *(resp. à* D*), et* $\mathrm{Gal}(N/E)$ *à* $\mathbf{F}_p$ *par l'isomorphisme*

$$\mathrm{Gal}(N/E) \xrightarrow{\sim} \mathbf{F}_p$$

$$v \mapsto \lg(v(x^{1/p})/x^{1/p}).$$

Alors, si D/J *est descendue de* N/K*, la classe de cohomologie dans* $H^2(\Gamma, \mathbf{F}_p)$ *de l'extension* D/J *est égale à celle de* N/K*.*

DÉMONSTRATION. Notons $z: \Gamma^2 \to \mathrm{Gal}(N/E)$ un 2-cocycle représentant la classe de l'extension N/K. Dans l'extension galoisienne N/L on a $z(\gamma, \eta)|_D \in \mathrm{Gal}(D/L)$ pour tout couple $(\gamma, \eta) \in \Gamma^2$, et un 2-cocycle représentant la classe de D/J est

$$z': \mathrm{Gal}(L/J) \times \mathrm{Gal}(L/J) \to \mathrm{Gal}(D/L)$$

$$(\varphi, \psi) \mapsto z'(\varphi, \psi) := z(\gamma, \eta)|_D$$

où γ et η sont les uniques éléments de Γ tels que $\gamma|_L = \varphi$, $\eta|_L = \psi$. En effectuant les identifications de l'énoncé, les 2-cocycles z' et z se confondent donc et sont à valeurs dans $\mathbf{F}_p$. D'où la conclusion.

Prenons maintenant $K = J(\mu_p)$, et supposons l'extension E/J galoisienne. Il existe un complément V de Γ dans $\mathrm{Gal}(E/J)$ [Hu; p.126, 18.1]. A ce complément V, associons l'endomorphisme du groupe multiplicatif $E^\times$ défini par

$$g_V(x) = \prod_{v \in V} v^{-1}(x)^{i(v)} \quad (x \in E^\times)$$

où $i(v) \in \mathbf{F}_p^\times$ est l'entier tel que $v(\zeta_p) = \zeta_p^{i(v)}$ $(v \in V)$ (cf. [Br]). Cet endomorphisme a la propriété d'induire au dessus de E des extensions galoisiennes, et même abéliennes, sur le corps L du lemme 4.1. Précisément:

PROPOSITION 4.2. *Soient* $K = J(\mu_p)$ *et* E/K *une p-extension galoisienne admettant une descendue sur* J*. Pour l'unique complément* V *de* Γ *dans* $\mathrm{Gal}(E/J)$ (cf. *Th.* 2.6 (2)), *et tout élément* $x \in E^\times$*, l'extension* $E((g_V(x))^{1/p})/E^V$ *est abélienne.*

DÉMONSTRATION. *Soit* $u \in V$. Quand v parcourt V, il en est de même du produit $w := vu^{-1}$. Donc

$$u(g_V(x)) = \prod_{w \in V} w^{-1}(x)^{i(v)}.$$

Mais il existe un entier, disons $n(w, u)$, tel que

$$i(v) = i(w)i(u) + pn(w, u) \quad (v \in V).$$

Par suite

$$u(g_V(x)) = \left(\prod_{w\in V} w^{-1}(x)^{i(w)}\right)^{i(u)} \left(\prod_{w\in V} w^{-1}(x)^{n(w,u)}\right)^{p}$$
$$\equiv g_V(x)^{i(u)} \bmod E^{\times p}$$

pour tout $u \in V$. D'où la conclusion par le 1.1 (2).

Reprenons les notations du début de la section. Pour la seule donnée de $G = \mathrm{Gal}(F'/F)$ et du G-module A, un problème de plongement de F'/F relativement à une classe $\varepsilon \in H^2(G, A)$, noté $(F'/F, \varepsilon)$, est la question de savoir s'il existe, au dessus de F', un corps F'' galoisien sur F, de groupe $\mathrm{Gal}(F''/F')$ s'identifiant à A, tel que la classe de cohomologie de l'extension F''/F soit précisément ε. Dans l'affirmative, on dit que F''/F est solution du problème résoluble $(F'/F, \varepsilon)$.

Dans [M1, 2] R. Massy a traité en général le problème du plongement à noyau d'ordre p d'une p-extension kummérienne E/K. Etant donnée une classe $\varepsilon \in H^2(\Gamma, \mathbf{F}_p)$, les solutions d'un problème résoluble $(E/K, \varepsilon)$ sont définies par un corps $N = E(x^{1/p})$ $(x \in E)$, galoisien sur K, tel que la classe de cohomologie de l'extension N/K soit précisément ε quand on identifie $\mathrm{Gal}(N/E)$ à $\mathbf{F}_p$ par l'isomorphisme du lemme 4.1.

On veut maintenant résoudre le même problème de plongement pour une p-extension encore abélienne, mais dont le corps de base ne contient plus, cette fois, le groupe μ_p des racines p-ièmes de l'unité. Soit L/J une telle extension. La méthode consiste à décider si le problème translaté $(I(\mu_p)/J(\mu_p), \varepsilon)$ admet ou non des solutions, puis dans l'affirmative, à descendre l'une d'entre elles en une solution du problème $(L/J, \varepsilon)$ via les identifications du lemme 4.1. Le théorème 2.6 s'appliquant à l'extension cyclotomique $(K = J(\mu_p))/J$, on se ramène au cas où le groupe $\mathrm{Gal}(L/J)$ est d'exposant p. Dans cette situation, le théorème suivant construit explicitement une solution d'un problème résoluble $(L/J, \varepsilon)$ $(\varepsilon \in H^2(\Gamma, \mathbf{F}_p))$ en termes d'une solution du problème translaté.

THÉORÈME 4.3. *Soient p un nombre premier, J un corps de caractéristique différente de p, et L/J une p-extension abélienne de groupe* $\mathrm{Gal}(L/J)$ *d'exposant p. Posons* $K := J(\mu_p)$, $E := L(\mu_p)$, $V := \mathrm{Gal}(E/L)$, *et identifions* $\mathrm{Gal}(L/J)$ *à* $\Gamma = \mathrm{Gal}(E/K)$ *par la restriction à L.*

(1) *Un problème de plongement $(L/J, \varepsilon)$ $(\varepsilon \in H^2(\Gamma, \mathbf{F}_p))$ est résoluble si et seulement si le problème translaté $(E/K, \varepsilon)$ est résoluble.*

(2) *Supposons $(L/J, \varepsilon)$ résoluble, et soit $N = E(x^{1/p})/K$ $(x \in E^{\times})$ une solution de $(E/K, \varepsilon)$.*

(2.1) *L'extension $N' := E((g_V(x)^{d^{-1}})^{1/p})/K$, où d^{-1} est l'inverse dans $\mathbf{F}_p$ du degré $[K : J]$ et $V \xrightarrow{\sim} \mathrm{Gal}(K/J)$, est aussi une solution du problème $(E/K, \varepsilon)$.*

$$v \mapsto v|_K$$

En outre, l'extension N'/J est galoisienne, et dans $\mathrm{Gal}(N'/J)$, *le sous-groupe* $\mathrm{Gal}(N'/K)$ *admet un unique complément* $V' \simeq \mathrm{Gal}(K/J)$ *qui est facteur direct*:

$$\mathrm{Gal}(N'/J) = V' \times \mathrm{Gal}(N'/K).$$

(2.2) *Soit X une racine p-ième quelconque de $g_V(x)^{d^{-1}}$: $X^p = g_V(x)^{d^{-1}}$. Le corps*

$$D := L\left(\sum_{v' \in V'} v'(X)\right)$$

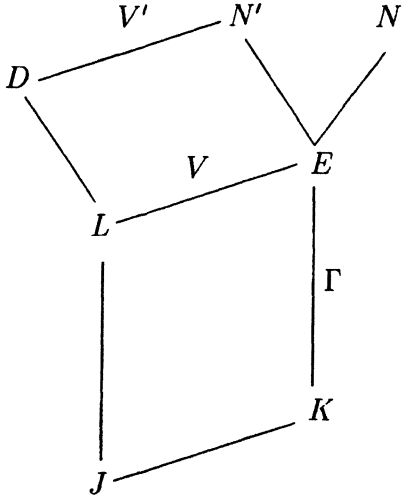
définit une descendue D/L de N'/E, et une descendue D/J de N'/K).

(2.3) *Identifions* $\mathrm{Gal}(D/L)$ *à* $\mathrm{Gal}(N'/E)$ *par la restriction à D, et* $\mathrm{Gal}(N'/E)$ *à* $\mathbf{F}_p$ *par l'isomorphisme*

$$\mathrm{Gal}(N'/E) \simeq \mathbf{F}_p$$

$$v \mapsto \lg[v((g_V(x)^{d^{-1}})^{1/p})/(g_V(x)^{d^{-1}})^{1/p}].$$

Alors la descendue D/J de N'/K est une solution du problème de plongement $(L/J, \varepsilon)$.



SCHOLIE. Par [M2] on dispose, d'une part d'un critère numérique permettant de décider mécaniquement de la résolubilité des problèmes $(E/K, \varepsilon)$ (loc. cit., théorème 2), d'autre part de formules explicites fournissant un élément $x \in E^\times$ pour leurs solutions $N = E(x^{1/p})/K$ lorsqu'elles existent. Via cet élément x, le (2.2) de l'énoncé précédent fournit donc un élément primitif explicite, sur L, des solutions D/J des problèmes non kummériens $(L/J, \varepsilon)$.

DÉMONSTRATION. (1) Confer proposition 1.3.

(2) (2.1) L'extension E/J est abélienne comme compositum de deux extensions abéliennes. Par suite

$$u(g_V(x)) = g_V(u(x)) \quad (u \in \mathrm{Gal}(E/J)). \tag{1}$$

Ainsi

$$\frac{\gamma(g_V(x))}{g_V(x)} = g_V\left(\frac{\gamma(x)}{x}\right) \quad (\gamma \in \Gamma).$$

Or dire que N/K est galoisienne signifie que pour tout $\gamma \in \Gamma$ il existe un élément $x_\gamma \in E^\times$ tel que $\gamma(x)/x = x_\gamma^p$. Donc

$$\gamma(g_V(x))/g_V(x) = (g_V(x_\gamma))^p \in E^{\times p} \quad (\gamma \in \Gamma)$$

et l'extension N'/K est galoisienne. Par ailleurs, on sait [M2,(3.2)] que la classe de cohomologie de cette extension est définie par un choix d'éléments $y_\gamma \in E^\times$ tels que

$$\gamma(g_V(x)^{d-1})/g_V(x)^{d-1} = y_\gamma^p \quad (\gamma \in \Gamma).$$

On vient de voir que l'on peut prendre

$$y_\gamma := g_V(x_\gamma)^{d-1} \quad (\gamma \in \Gamma).$$

Ainsi

$$\frac{y_\sigma \sigma(y_\tau)}{y_{\sigma\tau}} = g_V\left(\frac{x_\sigma \sigma(x_\tau)}{x_{\sigma\tau}}\right)^{d-1} \quad ((\sigma, \tau) \in \Gamma^2).$$

Or un 2-cocycle $z \in Z^2(\Gamma, \mathbf{F}_p)$ décrivant l'extension N/K est défini par

$$\frac{x_\sigma \sigma(x_\tau)}{x_{\sigma\tau}} = \zeta_p^{z(\sigma,\tau)} \quad ((\sigma, \tau) \in \Gamma^2)$$

et l'on a $g_V(\zeta_p) = \zeta_p^d$. Finalement donc

$$\frac{y_\sigma \sigma(y_\tau)}{y_{\sigma\tau}} = \zeta_p^{z(\sigma,\tau)} \quad ((\sigma, \tau) \in \Gamma^2)$$

ce qui exprime que $N' = E((g_V(x)^{d-1})^{1/p})/K$ est décrite par le même 2-cocycle que l'extension $N = E(x^{1/p})/K$.

Montrons que N'/J est galoisienne. Comme $E = LK$ et $L \cap K = J$, le groupe $\mathrm{Gal}(E/J)$ est le produit direct de ses sous-groupes V et Γ, en sorte que tout élément $u \in \mathrm{Gal}(E/J)$ se décompose d'une manière unique sous la forme

$$u = v_u \gamma \quad (v_u \in V, \gamma \in \Gamma).$$

On en déduit que

(2) $$g_V(u(x)) \equiv g_V(v_u(x)) \bmod E^{\times p}.$$

D'autre part, d'après la proposition 4.2 et le (1.1), il existe pour tout $v \in V$ un entier $i(v) \in \mathbf{F}_p^\times$ tel que

(3) $$v(g_V(x)) \equiv g_V(x)^{i(v)} \bmod E^{\times p}.$$

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

$$u(g_V(x)) \equiv g_V(x)^{i(v_u)} \bmod E^{\times p} \quad (u \in U)$$

ce qui prouve par le (1.1) que N'/J est galoisienne. Comme de plus E/J est abélienne, on obtient par le corollaire 2.7 que l'extension N'/K admet une descendue parallèlement à K/J.

Ceci étant, d'après le théorème 2.6 (2), le sous-groupe $\mathrm{Gal}(N'/K)$ de $\mathrm{Gal}(N'/J)$ admet un unique complément V' facteur direct:

$$\mathrm{Gal}(N'/J) = V' \times \mathrm{Gal}(N'/K).$$

(2.2) D'après la proposition 4.2, l'extension N'/L est abélienne et le théorème 3.2 s'applique. Pour le complément W de $\mathrm{Gal}(N'/E)$ dans $\mathrm{Gal}(N'/L)$, le corps

$$D := N'^W = L\left(\sum_{w \in W} w(X)\right) = L(\mathrm{Tr}_{N'/N'^W}(X))$$

où $X^p = g_V(x)^{d^{-1}}$, définit une descendue D/L de N'/E.

Montrons que pour ce même corps D, l'extension D/J est une descendue de N'/K. On a $D \cap K = J$ car $D \cap E = L$ et $L \cap K = J$. On a $N' = DK$ car $N' = DE$ et $E = LK$. La vérification de l'axiome (D_0) de la définition 2.1, à savoir que l'extension D/J est galoisienne, est moins immédiate. On va prouver que W est un complément de $\mathrm{Gal}(N'/K)$ dans $\mathrm{Gal}(N'/J)$; d'après le (2.1), il sera alors égal au facteur direct V', donc normal dans $\mathrm{Gal}(N'/J)$. Pour alléger l'écriture, posons $A := \mathrm{Gal}(N'/E)$ et $G := \mathrm{Gal}(N'/K)$.

La restriction à E de tout élément $w \in W \cap G$ est dans

$$\mathrm{Gal}(E/L) \cap \mathrm{Gal}(E/K) = V \cap \Gamma = \{1\};$$

donc $w \in W \cap A = \{1\}$, ce qui montre que $W \cap G = \{1\}$.

Clairement, dans l'extension galoisienne N'/L,

$$V \xrightarrow{\sim} \mathrm{Gal}(N'/L)/A = (W \times A)/A \xrightarrow{\sim} W.$$

Par conséquent

$$\mathrm{Gal}(N'/J)/G \xrightarrow{\sim} Gal(K/J) \xrightarrow{\sim} V \xrightarrow{\sim} W = W/W \cap G \xrightarrow{\sim} WG/G$$

d'où l'égalité $\mathrm{Gal}(N'/J) = WG$. Il est ainsi prouvé que W est un complément de G dans $\mathrm{Gal}(N'/J)$, et du même coup que l'extension D/J est galoisienne.

(2.3) Il suffit d'appliquer le lemme 4.1 à la descendue D/J de N'/K du (2.2).

Ceci achève la démonstration du théorème 4.3.

5. Exemples.

Les notations sont celles de la section 4. On exprime les classes de cohomologie au moyen des décompositions numériques de Massy. Rappelons brièvement leur définition (cf. [M2]). Soient $\cup$ le cup-produit $H^1(\Gamma, \mathsf{F}_p) \times H^1(\Gamma, \mathsf{F}_p) \to H^2(\Gamma, \mathsf{F}_p)$ défini via la multiplication dans F_p, et $\cdot$ le cup-produit

$$(\hat{H}^0(\Gamma, \mu_p) = \mu_p) \times H^2(\Gamma, \mathsf{Z}) \longrightarrow H^2(\Gamma, \mathsf{F}_p)$$
$$(\zeta, \bar{z}) \longrightarrow \zeta \cdot \bar{z} = \overline{\lg(\zeta^z)}$$

où lg est l'isomorphisme du début de la section 4. Si a est un élément du groupe de Kummer $(K^\times \cap E^{\times p})/K^{\times p}$ (ou de $K^\times \cap E^{\times p}$), soit $(a) \in H^1(\Gamma, \mathsf{F}_p)$ la forme linéaire définie par $\gamma(a^{1/p})/a^{1/p} = \zeta_p^{(a)(\gamma)}$ $(\gamma \in \Gamma)$. Quand $a, b \in (K^\times \cap E^{\times p})/K^{\times p}$ on pose

$$(a, b) := (a) \cup (b)$$
$$((a)) := \zeta_p \cdot \partial\left(\frac{1}{p}(a)\right)$$

où ∂ désigne le cobord $H^1(\Gamma, \mathsf{Q}/\mathsf{Z}) \to H^2(\Gamma, \mathsf{Z})$. On sait d'après [M2, Prop. 1] que pour toute classe $\varepsilon \in H^2(\Gamma, \mathsf{F}_p)$, il existe dans $(K^\times \cap E^{\times p})/K^{\times p}$ un élément a_0, unique si $p \neq 2$, et une famille $a_i, b_i, a_i \neq b_i$ $(i = 1, \ldots, n)$, tels que l'on ait

$$\varepsilon = ((a_0)) + \sum_{i=1}^{n} (a_i, b_i).$$

Une telle décomposition est dite "décomposition numérique de ε".

Dans les exemples qui suivent, la situation est celle du théorème 4.3. L'encombrement des solutions finales nous contraint ici à nous limiter aux deux groupes non abéliens d'ordre 27. Les exposants 1/3 désignent toujours une racine cubique arbitraire mais fixée.

EXEMPLE 5.1. Soit L_1 (resp. L_2) l'extension cubique galoisienne de Q définie par le polynôme irréductible $X^3 - 21X - 7$ (resp. $X^3 - 39X - 91$). On a

$$L_1 = \mathsf{Q}\left(\alpha_1 + \frac{\alpha_1^2}{2 + 3j}\right), \alpha_1^3 = 7(2 + 3j); \; L_2 = \mathsf{Q}\left(\alpha_2 + \frac{\alpha_2^2}{4 + j}\right), \alpha_2^3 = 13(4 + j).$$

Par adjonction des racines cubiques de l'unité, la translatée sur $K = \mathsf{Q}(j)$ du

compositum $L := L_1L_2/\mathbb{Q}$ est l'extension $E = K(\alpha_1, \alpha_2)$. Comme $N_{K(\alpha_1)/K}(y) = 13(4 + j)$ pour

$$y = \frac{(1 + \alpha_1)(2 - \alpha_1)^2}{(j - 1)^3},$$

on sait que E se plonge dans une extension galoisienne sur K de groupe non abélien d'ordre 27 d'exposant 3. D'après [M2, Th3.A(1)[ ]], le problème de plongement $(E/K, \varepsilon)$ où $\varepsilon = (7(2 + 3j), 13(4 + j))$ est résoluble, une solution $N = E(x^{1/3})$ étant fournie par l'élément

$$x = y\sigma(y^2)$$

avec $\sigma\alpha_1 = j\alpha_1$. On peut donc prendre

$$x = (1 + \alpha_1)(2 - \alpha_1)^2(1 + j\alpha_1)^2(2 - j\alpha_1)^4.$$

A partir de là, on suit le (2) du théorème 4.3. Comme $V = \mathrm{Gal}(E/L) = \{\mathrm{id}, v\}$, on a

$$g_V(x) = xv(x)^2.$$

Or d'après le théorème 3.2.(1),

$$v(\alpha_1) = \frac{\alpha_1^2}{2 + 3j}.$$

Donc

$$v(x) = \left(1 + \frac{\alpha_1^2}{2 + 3j}\right)\left(2 - \frac{\alpha_1^2}{2 + 3j}\right)^2\left(1 + \frac{j^2\alpha_1^2}{2 + 3j}\right)^2\left(2 - \frac{j^2\alpha_1^2}{2 + 3j}\right)^4.$$

Soit X une racine cubique quelconque de $g_V(x)^2$: $X^3 = g_V(x)^2$. Toujours dans les notations du (2) du théorème 4.3, on a

$$\left(\frac{1}{v(x)^2}\right)^3 = \frac{v(g_V(x)^2)}{g_V(x)^4} = \left(\frac{v'(X)}{X^2}\right)^3,$$

et l'on déduit de la condition $Xv'(X) \in L$ du théorème 3.2 (1) que

$$v'(X) = \left(\frac{X}{v(x)}\right)^2.$$

Par conséquent, l'extension $D := L\left(X + \left(\frac{X}{v(x)}\right)^2\right)\Big/\mathbb{Q}$ est la descendue de $N' = E((g_V(x))^{2/3})/K$ parallèlement à $K/\mathbb{Q}$. De plus, en vertu du 2.3 du théorème 4.3, $D/\mathbb{Q}$ est une solution du problème de plongement $(L/\mathbb{Q}, \varepsilon)$ quand on identifie $\mathrm{Gal}(L/\mathbb{Q})$ à Γ par la restriction à L.

EXEMPLE 5.2. Soit L_1 (resp. L_2) l'extension cubique galoisienne de $\mathbb{Q}$ définie par le polynôme irréductible $X^3 - 21X - 7$ (resp. $X^3 - 39X - 26$). On a

$$L_1 = \mathbb{Q}\left(\alpha_1 + \frac{\alpha_1^2}{2+3j}\right),\ \alpha_1^3 = 7(2+3j);\ L_2 = \mathbb{Q}\left(\alpha_2 + \frac{\alpha_2^2}{3+4j}\right),\ \alpha_2^3 = 13(3+4j).$$

Par adjonction des racines cubiques de l'unité, la translatée sur $K = \mathbb{Q}(j)$ du compositum $L := L_1L_2/\mathbb{Q}$ est l'extension $E = K(\alpha_1, \alpha_2)$. Comme $N_{K(\alpha_1)/K}(y) = 13j(3+4j)$ pour

$$y = \frac{(1+\alpha_1)(2-\alpha_1)^2}{(1-j)^3},$$

on sait que E se plonge dans une extension galoisienne sur K de groupe non abélien d'ordre 27 d'exposant 9. D'après [M2, Th3.A(2)], le problème de plongement $(E/K, \varepsilon)$ où $\varepsilon = ((7(2+3j))) + (7(2+3j), 13(3+4j))$ est résoluble, une solution $N = E(x^{1/3})$ étant fournie par l'élément

$$x = \alpha_1 y \sigma(y^2)$$

avec $\sigma\alpha_1 = j\alpha_1$. On peut donc prendre

$$x = \alpha_1(1+\alpha_1)(2-\alpha_1)^2(1+j\alpha_1)^2(2-j\alpha_1)^4.$$

Comme dans l'exemple 5.1,

$$v(\alpha_1) = \frac{\alpha_1^2}{2+3j}.$$

Donc

$$v(x) = \frac{\alpha_1^2}{2+3j}\left(1+\frac{\alpha_1^2}{2+3j}\right)\left(2-\frac{\alpha_1^2}{2+3j}\right)^2\left(1+\frac{j^2\alpha_1^2}{2+3j}\right)^2\left(2-\frac{j^2\alpha_1^2}{2+3j}\right)^4.$$

Pour X racine cubique quelconque de $g_V(x)^2 = (xv(x)^2)^2$, l'extension $D := L\left(X + \left(\frac{X}{v(x)}\right)^2\right)$ est la descendue de N'/K et l'extension galoisienne $D/\mathbb{Q}$ est solution du problème de plongement $(L/\mathbb{Q}, \varepsilon)$.

Signalons que le polynôme minimal sur $\mathbb{Q}$ de l'élément $X + \left(\frac{X}{v(x)}\right)^2$ a pour terme constant un entier de 77 chiffres.

REFERENCES

[Br] G. Brattström, *On p-groups as Galois groups*, Math. Scand. 65 (1989), 165–174.

[B-J-Y] 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.

[G] R. Gillard, *Plongement d'une extension d'ordre p ou p^2 dans une surextension non abélienne d'ordre p^3*, J. Reine Angew. Math. 268/269 (1974), 418–426.

[Ho] K. Hoechsmann, *Zum Einbettungsproblem*, J. Reine Angew. Math. 229 (1968), 81–106.

[Hu] B. Huppert, *Endliche Gruppen* I, Springer-Verlag, Berlin, 1967.

[L] S. Lang, *Algebra*, 2nd ed., Addison-Wesley Publishing Company, Inc., New York, 1984.

[M1] R. Massy, *Sur la construction à noyau d'ordre p des p-extensions galoisiennes*, Thèse d'État, Bordeaux, 1986.

[M2] R. Massy, *Construction de p-extensions galoisiennes d'un corps de caractéristique différente de p*, J. Algebra 109 (1987), 508–535.

[S] J-P. Serre, *Corps Locaux*, 3è éd., Hermann, Paris, 1980.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. 83, 1982.

[Wi] E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f*, J. Crelle 174 (1936), 237–245.

DEPARTEMENT DE MATHEMATIQUES
UNIVERSITE DE VALENCIENNES ET DU HAINAUT-CAMBRESIS
LE MONT HOUY B.P. 311
F 59304 VALENCIENNES
FRANCE