Problèmes de descente galoisienne

Sylvie Monier-Derviaux

Un problème naturel de théorie de Galois classique est le suivant.
Problème de l'extension incomplète : Soit E/K une extension galoisienne. Si L/K est une sous-extension galoisienne de E/K, existe t-il une sous-extension galoisienne M/K de E/K telle que $L \cap M = K$ et $E = LM$?

On montre aisément que cette question n'est qu'un cas particulier du plus général problème de la descente galoisienne : Soit E/K une extension galoisienne. Etant donnée une extension algébrique K/J, existe-t-il un sous-corps $D \subseteq E$, galoisien sur J, tel que $D \cap K = J$ et $E = DK$?

Dans ce cas, on dira que l'extension D/J est "descendue" de E/K (en abrégé $(D/J) = \mathrm{desc}_J(E/K)$) ou que E/K est "descendable sur J" $((E/K)desc_J)$.

On résout positivement le problème de l'extension incomplète pour une sous-extension cyclique de degré p^n d'une p-extension homocyclique d'exposant p^n (c.f. Prop.1). Pour une généralisation, on se heurte au manque de critère d'existence d'un complément facteur direct à un sous-groupe donné. Lorsque l'on impose des conditions arithmétiques sur les degrés des extensions considérées, on dispose d'un théorème de Zassenhaus qui induit l'argument de théorie des groupes de l'objet principal de ce travail (autre cas particulier du problème de la descente galoisienne) :

Problème de la descente cyclotomique : Soit p un nombre premier impair. Soient K un corps de caractéristique différente de p contenant le groupe μ_p des racines p-ièmes de l'unité, et $J \subseteq K$ un sous-corps de K ne contenant pas μ_p : $J \cap \mu_p = \{1\}$. Si l'on se donne une p-extension galoisienne E/K, est-elle descendable sur J : $(E/K)desc_J$?

Dans [1], G. Brattström répond affirmativement pour tout p premier impair, $K = J(\mu_p)$ et E/K une p-extension galoisienne non abélienne de degré p^3. On généralise ici ce résultat au cas d'une p-extension galoisienne quelconque E/K de la faÃ§on suivante. On réduit d'abord la difficulté, en termes d'existence de descendues, en quotientant le groupe de Galois de E/K par son sous-groupe de Frattini, ce qui permet de se ramener au cas d'une p-extension homocyclique d'exposant p. 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 du problème translaté fournie par les théorèmes de Massy [6, 7].

Enfin, pour une extension de base E/J galoisienne finie de degré quelconque, on montre, modulo une hypothèse de descente, que l'obstruction à ce qu'un corps N, de degré p sur E, soit galoisien sur J, se concentre uniquement sur une p-sous-extension de E/J. On reformule ainsi un résultat récent de [4].

Nous nous limitons dans ce texte à des extensions finies.

Enoncé des résultats

Un critère général d'existence de descendues est le suivant.

Lemme 1 *Soient E/K et K/J deux extensions galoisiennes.*
Les conditions suivantes sont alors équivalentes :
(1) L'extension E/K est descendable sur J
(2) L'extension E/J est galoisienne, et le groupe $\Gamma := Gal(E/K)$ admet un complément facteur direct dans $Gal(E/K)$.

1. Problème de l'extension incomplète

Lemme 2 *Le problème de l'extension incomplète est équivalent à la question de l'existence d'un complément facteur direct de $Gal(E/L)$ dans $Gal(E/K)$. Il est aussi équivalent à la question de savoir si E/L est descendable sur K.*

Sans les conditions arithmétiques du théorème de Zassenhaus, on connaît peu de critères d'existence de complément facteur direct. Soit G un p-groupe homocyclique d'exposant p^n, c'est à dire produit direct de groupes cycliques du même ordre p^n. Tout sous-groupe H de G tel que le quotient G/H soit cyclique d'ordre p^n est facteur direct dans G.

Proposition 1 *Soit E/K une p-extension galoisienne de groupe de Galois homocyclique d'exposant p^n. Pour toute sous-extension cyclique, de degré p^n, L/K de E/K, il existe une sous-extension galoisienne K de E/K telle que $L \cap M = K$ et $E = LM$.*

2. Problème de la descente cyclotomique

Ici, les degrés $[E : K]$ et $[K : J]$ sont premiers entre eux, et l'on dispose, pour les groupes, d'un résultat profond d'existence de complément par le théorème de Zassenhaus (c.f. [4]; p.126(127),18.1(18.2)). Il fournit directement une condition nécessaire et suffisante d'existence de descendues dans le cas abélien.

Proposition 2 *Soient K/J et E/K deux extensions abéliennes de degrés premiers entre eux. L'extension E/K admet une descendue parallèlement à K/J si et seulement si l'extension E/J est abélienne.*

Dans le cas non nécessairement abélien, on réduit la difficulté en quotientant le groupe donné par son sous-groupe de Frattini $\Phi()$. On en déduit le critère suivant.

Théorème 1 [8] *Soient p un nombre premier impair 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 $\Gamma := Gal(E/K)$.*
(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 F de $Gal(E/J)$ admet un unique complément V. Ce complément V est facteur direct, et l'on a $D = E^V$.

Le problème de l'obtention de formules pour la construction des p-extensions galoisiennes fut initié par Witt [10] en 1936. Répondant à une question de Serre [9], R. Massy [6, 7] a traité en général du problème de plongement à noyau d'ordre p des p-extensions kummériennes. On veut maintenant résoudre le même problème pour une p-extension L/J, encore abélienne, mais dont le corps de base ne contient plus cette fois les racines p-ièmes de l'unité : $J \cap \mu_p = \{1\}$. Une méthode consiste à décider si le problème translaté pour $(L(\mu_p)/J(\mu_p))$ admet ou non des solutions, puis à descendre l'une d'entre elles lorsqu'elle existe. Le théorème 1 s'appliquant à l'extension cyclotomique $(K = J(\mu_p))/J$, on se ramène au cas où le groupe $Gal(L/J)$ est d'exposant p. Le théorème suivant construit alors explicitement une solution d'un problème de plongement non kummérien en termes d'une solution du problème translaté.

Théorème 2 *Soit $E/(K = J(\mu_p))$ une p-extension homocyclique d'exposant p de groupe $\Gamma := Gal(E/K)$. Supposons l'extension E/J abélienne et soit $(L/J) = desc_j(E/K)$ (c.f. Prop.2). Notons :*

- *F_p le corps à p éléments,*
- *ζ_p une racine primitive p-ième de l'unité : $\mu_p =< \zeta_p >$,*
- *$d := [K : J]$,*
- *$Nor(K,E) := \left\{ x \in E^\times / \forall \gamma \in \Gamma \frac{\gamma(x)}{x} \in E^{\times p} \right\}$,*
- *$V := Gal(E/L)$ l'unique complément de F dans $Gal(E/J)$ (c.f.Th.1(2)),*
- *$i(v)$ l'entier de $\mathbb{F}_p^x$ tel que $v(\zeta_p) = \zeta_p^{i(v)} (v \in V)$,*
- *$g_{E/L}$ l'endomorphisme de $Nor(K,E)$ défini par $g_{E/L}(.) = \prod_{v \in V} v^{-1}(.)^{i(v)}$,*
- *$Nor(J,K,E,L) := \left\{ x \in \mathrm{Nor}(K,E) / g_{E/L}(x) \equiv x^d \bmod E^{\times p} \right\}$.*

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

(2) Supposons qu'il existe un corps D vérifiant les conditions du (1). Alors pour tout $x \in Nor(J,K,E,L) - E^{\times p}$ tel que $D \subseteq N := E\left(x^{1/p}\right)$, on a

$$(D/L) = desc_L(N/E), (D/J) = \mathrm{desc}_J(N/K).$$

De plus, pour l'unique complément V' de $Gal(N/K)$ dans $Gal(N/J)$, la trace d'une racine p-ième quelconque, mais fixée, $x^{1/p}$ de x fournit un élément primitif de D sur L :

$$D = L\left(\sum_{v' \in V'} v'\left(x^{1/p}\right). \right)$$

(3) $g_{E/L}(Nor(K,E)) \subseteq Nor(J,K,E,L)$.

(4) Un problème de plongement $(L/J, \varepsilon)$ $(\varepsilon \in H^2(\Gamma, \mathbf{F}_p))$ est résoluble si et seulement si le problème translaté $(E/K, e)$ est résoluble (cf.[2], [3]).

(5) Tout problème résoluble $(E/K, E)$ admet une solution N/K telle que l'extension N/J soit galoisienne. Précisément, toute solution $E\left(x^{1/p}\right)/K$ de $(E/K, \varepsilon)$ induit la solution $N := E(X)/K,\ X^p = g_{E/L}(x)^{d^{-1}}$, pour laquelle N/J est galoisienne.
(6) Supposons le problème $(L/J, \varepsilon)$ résoluble. Dans les notations du (5), soit $(D/J) := desc_J(N/K)$ (c.f.(2)). Identifions $Gal(D/L)$ à $Gal(N/E)$ par la restriction à D, et $Gal(N/E)$ à $\mathbb{F}_p$ par le choix d'un élément X. Alors la descendue D/J de N/K est une solution du problème de plongement $(L/J, \varepsilon)$.

Scholie. Grâce aux éléments $x \in Nor(K, E)$ des formules de [7], on obtient, par le (2) précédent, un élément primitif sur L, explicite, des solutions des problèmes non kummériens $(L/J, \varepsilon)$.

On peut maintenant aborder le problème de théorie de Galois suivant : comment étendre par une extension de degré premier une extension galoisienne finie de degré quelconque, disons E/J ? On montre, modulo une hypothèse de descente, que *tous* les corps N, de degré p sur E galoisiens sur J, admettent un élément primitif s'exprimant en termes d'un endomorphisme de E^X, que nous appelons "opérateur galoisien".

Théorème 3 *La situation est celle du théorème 1. Supposons que l'extension E/K soit descendable sur J, de descendue $desc_J(E/K) = (L/J)$, et que le corps E contienne le groupe μ_p. Notons $V := Gal(E/L)$ l'unique complément de Γ dans $Gal(E/J)$ (c.f.Th.1(2)). Alors, un corps N de degré p sur E est galoisien sur J si et seulement s'il existe un homomorphisme $f \in Hom\left(V, \mathbb{F}_p^\times\right)$ et un élément $x \in Nor(K, E)$ tels que*

$$N = E\left(\left(g_{E/L}^f(x)\right)^{1/p}\right);$$

où $g_{E/L}^f$ est l'opérateur galôisien défini par

$$\begin{aligned} g_{E/L}^f : E^\times &\longrightarrow E^\times \\ x &\longmapsto g_{E/L}^f(x) = \prod_{v \in V} v^{-1}(x)^{f(v)}. \end{aligned}$$

De plus, f est déterminé de manière unique par la condition

$$v(x) \equiv x^{f(v)} \bmod E^{\times p} (v \in V).$$

Ce résultat montre que l'obstruction à ce qu'un corps N soit galoisien sur J réside uniquement dans la p-sous-extension E/K de E/J. En effet, une fois obtenu un x dans $Nor(K, E)$, un générateur de N comme extension galoisienne de J est fourni mécaniquement par l'opérateur galoisien $g_{E/L}^f$.

Remerciements

Plusieurs résultats énoncés dans cette note ont été obtenus en collaboration avec le Pr. Richard Massy. Qu'il soit remercié de m'avoir permis de les mentionner.

Bibliographie

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

[2] *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.

[3] *K. Hoechsmann*, Zum Einbettungsproblem. J. reine angew. Math. **229** (1968), 81-106.

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

[5] *A. Ledet*, Subgroups of HolQ_8 as Galois Groups. J. of Algebra **181** (1996), 478-506.

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

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

[8] *S. Monier*, Descente de p-extensions galoisiennes kummériennes. Math. Scand. , 79 (1996), 5-24.

[9] *J.-P. Serre*, L'invariant de Witt de la forme $Tr\,(x^2)$. Comment. Math. Helv. **59** (1984), 651-676.

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

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