ACTA ARITHMETICA
103.1 (2002)

Une construction algorithmique des p-extensions cycliques de corps, de caractéristique différente de p, contenant les racines p-ièmes de l'unité

par

Richard Massy (Valenciennes)

Dans [7, p. 389], Karpilovsky pose le problème d'une description explicite de toutes les p-extensions cycliques. En 1999, T. Crespo [5] a donné une famille complète d'extensions cycliques de degré 8 d'un corps de caractéristique autre que 2. Par une méthode différente, initiée dans [8] ou [9], et quel que soit le nombre premier p, nous présentons ici une construction algorithmique de toutes les p-extensions cycliques des corps de caractéristique différente de p qui contiennent les racines p-ièmes de l'unité. Cette construction est effective via les méthodes de [4] (cf. Remarque (2)) qui permettent d'obtenir un élément y de norme une racine primitive p-ième de l'unité. Les éléments primitifs x que nous obtenons sont des produits, alors que l'on emploie généralement des résolvantes de Lagrange–Hilbert additives. Ils ne diffèrent de celles-ci, pour l'essentiel, que d'un élément du corps de base (cf. Remarque (1)), mais leur forme multiplicative permet de simplifier plus aisément par les puissances p-ièmes. L'intérêt majeur de ces éléments primitifs est qu'ils sont tous définis canoniquement, de manière algorithmique, par la seule donnée d'un y, ce qui n'est pas le cas des résolvantes dont la non nullité dépend à chaque fois d'un choix empirique.

Ultérieurement, grâce aux notions introduites dans [11], [12] et surtout [10], nous espérons pouvoir nous dispenser, au moins pour certains degrés, de la présence des racines p-ièmes de l'unité dans le corps de base.

Théorème. *Soient p un nombre premier, pair ou impair, et F_0 un corps de caractéristique différente de p contenant une racine primitive p-ième de l'unité ζ_p. Soit F_m/F_0 une p-extension cyclique de degré p^m ($m \in \mathbb{N} \setminus \{0\}$). Pour tout entier $n \in \{0, \dots, m\}$, notons F_n le sous-corps de F_m de degré p^n sur F_0 : $F_0 \subseteq F_n \subseteq F_m$, $[F_n : F_0] = p^n$. Soit x_0 un élément quelconque de $F_0^\times \setminus F_0^{\times p}$ tel que $F_1 = F_0(x_0^{1/p})$.*

2000 *Mathematics Subject Classification*: 12F10, 11R20, 11R32, 11S20.

1. *Il existe un corps* F_{m+1}, *contenant* F_m, *tel que l'extension* F_{m+1}/F_0 *soit cyclique de degré* p^{m+1} *si et seulement s'il existe un élément* $y \in F_m$ *de norme* $N_{F_m/F_0}(y) = \zeta_p$.

2. *Lorsqu'il en est ainsi, un élément primitif de* F_{m+1} *sur* F_m, $F_{m+1} = F_m(x_m^{1/p})$, *est donné par*

$$x_m = r_m x_{m-1}^{1/p} \prod_{i=1}^{p-1} \sigma_m^{ip^{m-1}}(y_m^i)$$

où successivement, pour tout $n \in \{1, \dots, m-1\}$, *un élément primitif de* F_{n+1} *sur* F_n, $F_{n+1} = F_n(x_n^{1/p})$, *est donné par*

$$x_n = r_n x_{n-1}^{1/p} \prod_{i=1}^{p-1} \sigma_n^{ip^{n-1}}(y_n^i).$$

Ceci avec les définitions suivantes :

- $r_1, \dots, r_m$ *des éléments fixés de* $F_0^\times$;
- σ_1 *le générateur de* $\mathrm{Gal}(F_1/F_0)$ *tel que* $\sigma_1(x_0^{1/p})/x_0^{1/p} = \zeta_p$, *et*

$$y_1 = N_{F_m/F_1}(y)\,;$$

- *pour tout* $n \in \{2, \dots, m\}$, σ_n *le générateur de* $\mathrm{Gal}(F_n/F_0)$ *prolongeant* σ_{n-1} *défini par*

$$\sigma_n(x_{n-1}^{1/p})/x_{n-1}^{1/p} = N_{F_m/F_{n-1}}(y), \qquad \sigma_{n|F_{n-1}} = \sigma_{n-1},$$

et

$$y_n = \prod_{j=0}^{p^{n-1}-1} \sigma_n^j(N_{F_m/F_n}(y)).$$

Démonstration. 1. Ce critère est bien connu : cf. par exemple [1, p. 207, Th. 11].

2. Le théorème est vrai pour $m = 1$ d'après [9, Th. 3(A)(1)] en modifiant légèrement la formule donnant x_1 comme dans l'énoncé. Supposons maintenant donné le corps $F_n = F_{n-1}(x_{n-1}^{1/p})$ et construisons F_{n+1}. Soit

$$x'_n := x_{n-1}^{1/p} \prod_{i=1}^{p-1} \sigma_n^{ip^{n-1}}(y_n^i).$$

On a

$$\sigma_n(x'_n)/x'_n = N_{F_m/F_{n-1}}(y)\sigma_n^{p^n}(N_{F_m/F_n}(y))^{p-1} \prod_{i=1}^{p-1} \sigma_n^{ip^{n-1}}(N_{F_m/F_n}(y))^{-1}.$$

Or σ_n est un générateur de $\mathrm{Gal}(F_n/F_0)$; donc $\sigma_n^{p^n} = \mathrm{id}_{F_n}$ et

$$\sigma_n(x'_n)/x'_n = N_{F_m/F_{n-1}}(y)N_{F_m/F_n}(y)^p \prod_{i=0}^{p-1} \sigma_n^{ip^{n-1}}(N_{F_m/F_n}(y))^{-1}.$$

Comme $\mathrm{Gal}(F_n/F_{n-1})$ est engendré par $\sigma_n^{p^{n-1}}$, on obtient que

$$\sigma_n(x'_n)/x'_n = N_{F_m/F_n}(y)^p.$$

Soit alors le corps $F'_{n+1} := F_n(x_n'^{1/p})$. Il est de degré p sur F_n car sinon, il existerait un $x \in F_n^\times$ et une racine p-ième de l'unité ζ tels que $\sigma_n(x)/x = \zeta N_{F_m/F_n}(y)$ d'où $1 = N_{F_m/F_0}(y) = \zeta_p$: absurde. Le fait que $\sigma_n(x'_n)/x'_n$ soit une puissance p-ième dans $F_n^\times$ assure par la théorie de Galois que l'extension F'_{n+1}/F_0 est galoisienne. Montrons qu'elle est cyclique. Soient $\widetilde{\sigma}_n \in \mathrm{Gal}(F'_{n+1}/F_0)$ de restriction à F_n égale à σ_n : $\widetilde{\sigma}_{n|F_n} = \sigma_n$, et $X'_n \in F'_{n+1}$ tel que $X_n'^p = x'_n$. On a

$$\widetilde{\sigma}_n(X'_n) = \zeta_p^i N_{F_m/F_n}(y) X'_n$$

pour un $i \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, et par suite

$$\widetilde{\sigma}_n^{p^n}(X'_n) = N_{F_n/F_0}(N_{F_m/F_n}(y))X'_n = \zeta_p X'_n.$$

Il en résulte que $\widetilde{\sigma}_n$ est d'ordre p^{n+1} ; donc $\widetilde{\sigma}_n$ engendre $\mathrm{Gal}(F'_{n+1}/F_0)$. Posons alors

$$\sigma'_{n+1} := \widetilde{\sigma}_n^{(p-i)p^n+1}.$$

On a toujours $\sigma'_{n+1|F_n} = \sigma_n$, et comme $\mathrm{pgcd}((p-i)p^n + 1, p^{n+1}) = 1$, on déduit de l'identité de Bézout que σ'_{n+1} est aussi un générateur de $\mathrm{Gal}(F'_{n+1}/F_0)$. La simplification est cette fois que

$$\sigma'_{n+1}(X'_n) = N_{F_m/F_n}(y)X'_n.$$

Considérons maintenant l'extension F_{n+1}/F_0. Par la théorie de Galois, on sait qu'il existe un $x''_n \in F_n^\times$ tel que $F_{n+1} = F_n(x_n''^{1/p})$ avec $\sigma_n(x''_n)/x''_n = z_n^p$ pour un élément $z_n \in F_n^\times$. Si l'on avait $N_{F_n/F_0}(z_n) = 1$, on déduirait du théorème 90 de Hilbert dans l'extension cyclique F_n/F_0 que $\mathrm{Gal}(F_{n+1}/F_0)$ est un groupe d'exposant p^n : contradiction puisque F_{n+1}/F_0 est cyclique de degré p^{n+1}. Donc nécessairement, il existe un entier $i \in \mathbb{F}_p^\times$ tel que

$$N_{F_n/F_0}(z_n)^i = \zeta_p = N_{F_m/F_0}(y) = N_{F_n/F_0}(N_{F_m/F_n}(y))$$
$$\Leftrightarrow \ (\exists f_n \in F_n^\times \ \ \sigma_n(f_n)z_n^i/f_n = N_{F_m/F_n}(y)).$$

Or on a montré que $\sigma_n(x'_n)/x'_n = N_{F_m/F_n}(y)^p$. Par conséquent

$$\frac{\sigma_n(f_n^p x_n''^i)}{f_n^p x_n''^i} = \frac{\sigma_n(x'_n)}{x'_n} \ \Leftrightarrow \ (\exists r_n \in F_0^\times \ \ f_n^p x_n''^i = r_n x'_n).$$

Il en résulte que

$$F_{n+1} = F_n(x_n''^{1/p}) = F_n(x_n''^{i/p}) = F_n((r_n x_n')^{1/p}) = F_n(x_n^{1/p})$$

où l'on a posé $x_n := r_n x_n'$. De plus

$$\sigma_n(x_n)/x_n = \sigma_n(x_n')/x_n' = N_{F_m/F_n}(y)^p.$$

En étendant σ_n à F_{n+1} comme on l'a fait pour F'_{n+1} avec σ'_{n+1}, on obtient finalement qu'il existe un générateur σ_{n+1} de $\mathrm{Gal}(F_{n+1}/F_0)$ tel que

$$\sigma_{n+1}(x_n^{1/p})/x_n^{1/p} = N_{F_m/F_n}(y), \quad \sigma_{n+1|F_n} = \sigma_n.$$

On se retrouve donc en situation de gravir une marche supplémentaire de la tour cyclique induite par F_m/F_0. ∎

Remarque. (1) *Résolvantes.* Dans les notations du théorème, on a

$$\sigma_m(x_m)/x_m = y^p, \quad N_{F_m/F_0}(y) = \zeta_p.$$

Par ailleurs, d'après le théorème de Dedekind sur l'indépendance des homomorphismes de corps, on sait qu'il existe un $\theta \in F_m^\times$ tel que la somme

$$z := \theta + \sum_{i=1}^{p^m-1} y^p \sigma_m(y^p) \dots \sigma_m^{i-1}(y^p)\sigma_m^i(\theta) \quad ([2, \text{p. } 172])$$

soit non-nulle : $z \neq 0$. Et l'on vérifie que $z/\sigma_m(z) = y^p$. On en déduit l'existence d'un élément $r \in F_0^\times$ tel que $x_m z = r$. Notre élément primitif multiplicatif x_m n'est donc que l'inverse d'une résolvante de Lagrange–Hilbert z, modulo la multiplication par un élément du corps de base. Mais le choix d'un $\theta \in F_m^\times$ tel que l'on ait $z \neq 0$ n'a rien de canonique, tandis que x_m est défini algorithmiquement par la seule donnée d'un élément y de norme ζ_p.

(2) *Équations normiques.* L'effectivité de notre méthode est subordonnée à l'obtention d'un élément y de norme ζ_p (l'existence de y étant équivalente à celle des extensions cycliques que nous voulons construire). Soient L/K une extension de corps de nombres et a un élément fixé de $K^\times$. Le problème du calcul d'une solution $x \in L^\times$ de l'équation normique $N_{L/K}(x) = a$ est résolu dans [4, Sect. 7.5]. Dans la terminologie de Cohen, un ensemble S_0 d'idéaux premiers de K est dit *convenable* si pour tout ensemble fini $S \supseteq S_0$, on a, dans les notations usuelles,

$$N_{L/K}(L^\times) \cap U_S(K) = N_{L/K}(U_S(L)).$$

On montre qu'une fois trouvé un ensemble convenable S_0, il suffit de résoudre l'équation donnée dans un groupe $U_S(L)$ de S-unités de L. Et Cohen fournit un algorithme [*op. cit.* p. 383, 7.5.15] qui permet effectivement d'exhiber, lorsqu'il existe, un $x \in U_S(L)$ tel que $N_{L/K}(x) = a$. De plus, dans notre cas, l'extension L/K est cyclique. Donc, d'après le théorème des normes de Hasse [6], la vérification de l'existence de x se ramène à un nombre fini

de conditions locales. Enfin, on dispose de la formule des classes ambiges de Chevalley ([3], [13, Th. 4.5]) qui donne explicitement, pour tout S, le quotient

$$N_{L/K}(L^\times) \cap U_S(K)/N_{L/K}(U_S(L)).$$

Exemples. (1) Soient, comme dans l'exemple 2 de [5] : $F_0 = \mathbb{Q}(\sqrt{17})$, $F_1 = F_0(\sqrt{5})$ et $F_2 = F_1(\sqrt{15+6\sqrt{5}})$. Pour

$$y = \frac{3+\sqrt{15+6\sqrt{5}}}{2(\sqrt{17}+2\sqrt{5})},$$

on a

$$y_1 = N_{F_2/F_1}(y) = -\frac{3(1+\sqrt{5})}{2(\sqrt{17}+2\sqrt{5})^2}, \quad N_{F_2/F_0}(y) = -1.$$

Pour $r_1 = 4$, on peut prendre

$$\sqrt{15+6\sqrt{5}} = \left(\frac{\sqrt{17}-2\sqrt{5}}{-3+\sqrt{5}}\right)\sqrt{x_1}.$$

On en déduit

$$y_2 = -\frac{20+6\sqrt{17}+(12+2\sqrt{17})\sqrt{5}+(3+3\sqrt{5})\sqrt{x_1}}{8\sqrt{17}+16\sqrt{5}}.$$

Ainsi, toutes les extensions cycliques $F_3 = F_2(\sqrt{x_2})/F_0$ de degré 8 sont données par

$$x_2 = r_2(40+4\sqrt{17}\sqrt{5}-(3+\sqrt{5})\sqrt{x_1}) \quad (r_2 \in F_0^\times).$$

(2) Soient $F_0 = \mathbb{Q}(j)$ où $j = e^{2i\pi/3}$ et $F_1 = F_0(X_0)$ avec $X_0^3 = 1-j$. Toutes les extensions cycliques $F_1(x_1^{1/3})/F_0$ de degré 9 sont données par

$$x_1 = r_1 X_0(1-jX_0)(1-j^2X_0)^2 \quad (r_1 \in F_0^\times).$$

Prenons $r_1 = 1$ et $F_2 = F_1(X_1)$ où

$$X_1^3 = 3+(3+j)X_0+(2+j)X_0^2.$$

Pour

$$y = 1-j^2X_0^2+(-1-j^2X_0+X_0^2)X_1+(2+j-jX_0-X_0^2)X_1^2,$$

on a

$$N_{F_2/F_1}(y) = 1-X_0, \quad N_{F_2/F_0}(y) = j.$$

On en déduit que toutes les extensions cycliques $F_3 = F_2(x_2^{1/3})/F_0$ de degré 27 sont données par

$$\begin{aligned} x_2 = r_2(&105+42j+(159-30j)X_0+(195+129j)X_0^2 \\ &+(-9+10j-(141+111j)X_0-99jX_0^2)X_1 \\ &+(63+6j+(6+105j)X_0-(73+38j)X_0^2)X_1^2) \end{aligned}$$

où r_2 parcourt $F_0^\times$.

Remerciements. Je remercie Arnaud Jehanne, de l'Université de Bordeaux I, pour la partie calculatoire des exemples numériques.

Références

[1] A. A. Albert, *Modern Higher Algebra*, Univ. of Chicago Press, Chicago, 1965.
[2] J. R. Bastida, *Field Extensions and Galois Theory*, Encyclopedia Math. Appl. 22, Addison-Wesley, Reading, 1984.
[3] C. Chevalley, *Sur la théorie du corps de classes dans les corps finis et les corps locaux*, J. Fac. Sci. Tokyo Univ. 2 (1933), 365–476.
[4] H. Cohen, *Advanced Topics in Computational Number Theory*, Grad. Texts in Math. 193, Springer, Berlin, 2000.
[5] T. Crespo, *Extensions cycliques de degré 8*, C. R. Acad. Sci. Paris 329 (1999), 753–756.
[6] H. Hasse, *Beweis eines Satzes und Widerlegung einer Vermutung über das allgemeine Normenrestsymbol*, Nachr. Ges. Wiss. Göttingen 1931, 64–69. (Mathematische Abhandlungen, Band 1, 155–160.)
[7] G. Karpilovsky, *Topics in Field Theory*, North-Holland Math. Stud. 155, Amsterdam, 1989.
[8] R. Massy, *Formules de construction de p-extensions galoisiennes*, C. R. Acad. Sci. Paris 303 (1986), 591–594.
[9] —, *Construction de p-extensions galoisiennes d'un corps de caractéristique différente de p*, J. Algebra 109 (1987), 508–535.
[10] —, *Galois averages*, en préparation.
[11] R. Massy et S. Monier-Derviaux, *Descente et parallélogramme galoisiens*, Actes des J. A. 97, J. Théor. Nombres Bordeaux 11 (1999), 161–172.
[12] —, —, *Parallélogrammes galoisiens*, J. Algebra 217 (1999), 229–248.
[13] D. Simon, *Solving norm equations in relative number fields using S-units*, Math. Comp., à paraître.

Département de Mathématiques
Université de Valenciennes
Le Mont Houy
F-59313 Valenciennes, France
E-mail: Richard.Massy@univ-valenciennes.fr

Reçu le 8.10.2000
et révisé le 12.7.2001 (3910)